paloalto NETWORKS® | ICT MEDIA

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

BENELUX

NAVIGATING THE DIGITAL AGE

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

BENELUX

Published by

ICT MEDIA

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers – Benelux

Printing and Binding: Damen Drukkers

Navigating the Digital Age:
The Definitive Cybersecurity Guide for Directors and Officers – Benelux

is published by:

ICT Media BV
Laan van Voorburg 1
5261 LS, Vught
The Netherlands
First published: 2017

Navigating the Digital Age:
The Definitive Cybersecurity Guide for Directors and Officers – Benelux

Cover illustration by Tim Heraldo

DISCLAIMER

Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers (the Guide) contains summary information about legal and regulatory aspects of cybersecurity governance and is current as of the date of its initial publication (April 2017). Although the Guide may be revised and updated at some time in the future, the publishers and authors do not have a duty to update the information contained in the Guide, and will not be liable for any failure to update such information. The publishers and authors make no representation as to the completeness or accuracy of any information contained in the Guide.

This guide is written as a general guide only. It should not be relied upon as a substitute for specific professional advice. Professional advice should always be sought before taking any action based on the information provided. Every effort has been made to ensure that the information in this guide is correct at the time of publication. The views expressed in this guide are those of the authors. The publishers and authors do not accept responsibility for any errors or omissions contained herein. It is your responsibility to verify any information contained in the Guide before relying upon it.

ISBN
978-90-819529-0-3

Preface: Institutions are Facing an era of Unprecedented Change – With Cyberattacks Provoking Disruption

Neelie Kroes – former European Commissioner for the Digital Agenda and Vice President to the European Commission – sets out why cybersecurity must be a top priority for boards and executives.

All our institutions—government, not-for-profit organisations and businesses—are facing an unprecedented era of change. We live in a turbulent world of volatility and uncertainty, both economic and political. The relentless rise of globalisation has delivered massive benefits for many, but not for all. This has contributed to widening inequality which, in turn, has made our world a more complex and dangerous place. It is the responsibility of our leaders to grapple with this backdrop and with the momentous speed of our digitally-connected world.

In an increasingly complex world, board members and corporate executives are responsible for processing information from a broader range of sources than ever to effectively lead their organisations. Additionally, to successfully compete, companies must constantly innovate, demanding agile leadership and organisation.

Without trust in the digital infrastructure that underpins this agility, however, organisations will find themselves increasingly unable to serve their stakeholders, including customers, employees and investors. The maintenance of this trust by effectively addressing cybersecurity risks, therefore, is of primary importance to board members and executives.

Cybersecurity is no longer a problem for IT staff alone. Indeed, according to the 2016 *Global Risks Report* from the World Economic Forum, one of the top risks facing the boards of directors is cybersecurity. The issue is on your desk, at the top of your in-tray. It requires your attention and focus.

The spectre of a cyberattack can provoke unease and concern. According to the World Economic Forum, "[cyberattacks] have been rising in both frequency and scale. They have so far been isolated, concerning mostly a single entity or country, but as the internet of things leads to more connections between people and machines, cyber dependency will increase, raising the odds of a cyberattack with potential cascading effects across the cyber ecosystem. As a result, an entity's risk is increasingly tied to that of other entities." It is our duty as leaders to remain calm and to work harder and smarter every day to protect our customers and citizens.

At the most basic level, the job of leadership is to assess and respond to the strategic risks facing their organisations. Cybersecurity is a paramount risk to virtually every business that has a digital connection to the outside world. How, then, does a board develop the necessary skills to effectively assess and respond to cybersecurity risk? New roles are emerging and boards must embrace a different mix of skills. Boards must work with people who can explain, in board-level language and tone, the most immediate risks, and design strategies to manage these risks. Increasingly, boards and companies have a new, technologically-astute colleague who understands the nature of cyber risk, the chief information security officer (CISO). It is, therefore, the mission of the CISO to help boards understand the strategic cyber risks to their organisations.

As a society, we bear a collective responsibility for cybersecurity. Business leaders must build solutions that prompt us in a simple way to live and work securely, adopting security by design and by default. Board members and corporate executives must ensure that their organisations are protecting more than the bottom line of profits and earnings—they must protect clients' and customers' data too.

Governments also are doing what they can. The NCSC is the central information hub and centre of expertise for cybersecurity in the Netherlands, a key figure in the operational coordination at a major ICT crisis and the computer emergency response team (CERT) for the Dutch central government. The Centre for Cybersecurity Belgium now manages the country's CERT under the authority of the Prime Minister. The CERT in Luxembourg is a community of public and private sector expertise working together to improve the security of the nation. Each of these organisations is playing a vital role in coordinating the response to a serious cyberattack and helping citizens and organisations raise their security defences.

EU-wide legislation is complementing country-specific efforts. The General Data Protection Regulation (GDPR), when it comes into effect in May 2018, will require organisations and businesses to do much more to protect and secure the personal information of European residents. The Network and Information Security (NIS) Directive, which member states must implement by May 2018, aims to raise the cyber resilience of all EU countries. It has security and incident notification obligations for covered companies as well as requirements for member states to adopt national NIS strategies. The GDPR and NIS Directive are important laws that can contribute to cybersecurity in the EU, complementing the ongoing activities in the Benelux countries.

Security is no longer a 'job on the side.' Given the importance of securing the digital assets upon which society relies, cybersecurity is, and will continue to be, a top priority for boards and corporate executives. What is admirable is that the best business leaders of the Netherlands, Belgium and Luxembourg have always shown themselves to be pragmatic, receptive and agile. To confront the challenge of cybersecurity, this agility matters now as never before.

Introduction

Palo Alto Networks – Greg Day, Vice President and Regional Chief Security Officer, EMEA

- The EU has adopted two far-reaching pieces of legislation on data and infrastructure protection from cyber threats
- Technology and cyber threats continue to evolve at a rapid pace
- It's important to validate where your business stands today re cyber risk
- Businesses need to find the right balance between risk and expense
- You should also balance your investment among human capital, technology, and insurance

New EU legislation provides an opportunity for business leaders to step back, possibly re-architect their cybersecurity, and achieve the right balance for their organisation.

Society has an addiction: we have become cyber dependents. The average person relies significantly on a smartphone, and it seems that even temporary separation from the device can be painful and provoke anxiety. Our incredibly interconnected world spans both business and personal lives, from shopping to tracking our health, to working on the move. This modern lifestyle has granted new freedoms and opportunities for the modern citizen, enabled through a cyber mesh of interconnected data, across applications and devices/systems—this is the so-called internet of things. What is apparent is that this mass of digital information will continue to increase exponentially, placing the issue of cybersecurity right at the forefront of the debate.

To help address this challenge, the European Union has introduced two of the most far-reaching legislative changes related to data protection and cybersecurity to date, both of which will come into effect in May 2018. The first is a revision of data privacy and protection requirements to ensure that all personal information belonging to EU residents is managed consistently and effectively. More significantly, personal data breaches require notification to authorities within an appropriate time frame and, in some cases, to the individuals affected. This is the General Data Protection Regulation (GDPR) and is explained more fully later in this book.

The second piece of legislation recognises that such essential services as energy, transportation, healthcare, and water, to name just a few, have significant technological dependencies that, if compromised by a cyberattacker, have the potential to impact society significantly. The EU's Network and Information Security (NIS) Directive recognises the importance of defending this infrastructure and requires each nation to identify such organisations, and that the organisations take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of networks and information systems that they use in their operations, having regard to the state of the art. The organisations are expected to work with their national authorities to ensure critical services are sustained and society can maintain confidence in these services in the event of a cyber incident.

The question you must ask yourself as a business leader is: *if our national governments have come to understand the significance of critical cybersecurity, what does this say about how important it is to your business?*

With both technology and cyberattacks continuing to evolve at pace, many find it tough to keep up, and this is little wonder: many feel ill-equipped to ask the right questions and ill-prepared to deal with cyberattacks that could impact their business. What makes this worse is that cyber and cybersecurity use what can seem to be a foreign language, with new terms and myriad abbreviations and acronyms that evolve as fast as the technology develops.

Unfortunately, as a business leader, this is a discussion you can ill-afford to ignore. I would suggest that the EU legislative changes are the most fundamental shift in cyber to date and, for many cybersecurity teams, will have significant impact. Yet this can be the catalyst to overhaul not only your own cybersecurity awareness but also your organisation's approach to cybersecurity. There is a genuine opportunity for your business to rearchitect your critical systems, to build state of the art cybersecurity for today that will be scalable for your future.

Constantly changing technology has become our Achilles' heel. For the cyberdefender, there's a need to continue to adapt

With both technology and cyberattacks continuing to evolve at pace, many find it tough to keep up, and this is little wonder: many feel ill-equipped to ask the right questions and ill-prepared to deal with cyberattacks that could impact their business.

Where do you start? There are three core elements:

THREE CORE ELEMENTS

1. Your business depends on cyber to function, with the technology systems installed on your premises and in the internet cloud. The data you hold in the form of customer records, business processes, and intellectual property are among your key assets. These differ depending on whether you are a service provider, retailer, or financial organisation, for example.

2. There are risks to your cyber dependencies, some easier than others to qualify. These range from the insider threat from human error or a disgruntled employee, to the constantly evolving external threat, for which there is an ever-perplexing array of techniques, attack actors, and motives. Too often we get caught up in the details of 'what' and 'how,' when we should focus on the impact and likelihood of the impact on our business. We can learn from both the military and the insurance industry's experience here, with each viewing cyber risk though a different lens.

3. The final part of the cybersecurity triangle is what you do to become more resilient. 'cyber resilience' is a continuing battle between 'good' and 'evil,' each looking to outflank the other. We need to plan for the best and prepare for the worst.

and respond to the changing threat. Often there is a complex collection of solutions to specific problems. Cybersecurity requires high levels of human intervention. Much like a high-performance sports car, cybersecurity is capable of pushing boundaries but at the same time can be extremely fragile.

For business leaders, your first action must be to validate where your business is today. There are numerous ways to achieve this. You could pull in an external third party to do a gap analysis, you could look at the existing metrics provided by your cybersecurity team, or you could simply test the effectiveness of your current capacities. We learn through experience. Running cyber drills and exercises is an obvious way to test capabilities across the business. This is not just about the technical capabilities, but also people skills, inter-team skills, right through to the board's effectiveness in presenting information to stakeholders and making critical decisions when a cyber incident occurs.

With cybersecurity, much as with life itself, there are no guarantees. Technology is made up of zeros and ones, and too many see cybersecurity as a binary requirement, meaning that nothing bad should happen. Yet the reality is that things can and will happen. The first step is living with this and deciding what is acceptable when a cyber incident does happen. This will bring you back to the business cyber risk equation, which is: understanding business IT dependencies, the cyber risks against them, and the business impact these would have. That is required to define the right balance between acceptable risk and investment to mitigate these for each business.

The next decision you must make is where to deploy your investment. For decades, security practitioners have focused on defending their businesses with the goal of preventing a cyber incident from ever happening. In recent years, there has been a shift towards accepting the inevitable—that some attacks will succeed—and therefore, your business must focus on how to respond to this to minimise the business impact.

Coupled with this has been the maturing of the cyber insurance industry. Cyber insurance seeks to transfer the risk, specifically the vast capital implications. Managing this risk can help smooth significant impact. Equally, leveraging the skills and knowledge of insurance experts can give you a broader insight on risk than if you were trying to do this on your own.

When considering best practice, you should determine if you are going to run your own internal 'fire brigade' or leverage an external service and its expertise. Just like the fire brigade, cyber incident response teams are professionals who typically require expensive tools and knowledge that ideally we call in only occasionally. Under the pending EU legislation, your organisation may need to notify relevant national authorities when defined incidents occur. You must decide what you can afford, and this again raises the question about the appropriate decision making between investment in cybersecurity—to prevent and detect business impact—and the potential costs of a breach.

Finding this balance requires managing the mix of state of the art capabilities with costs. To use a practical example, it's like mixing audio tape, CD, VHS, DVD, and HD digital media together and expecting a single player to deal with them all. A human is required to convert the different formats into a common medium that could be used on one player. Cybersecurity often can be no different, with lots of varying capabilities that require human intervention to function as a whole. This is an archaic solution for a digital age.

Human capital is typically the most expensive aspect of cybersecurity, in terms of both operational costs and holding up the implementation of a secure digital capability. Many businesses will have cybersecurity dashboards that aim to provide an assessment of cyber capabilities: these range from simple measurements to in-depth metrics. Many will focus on 'lagging indicators,' which manually examine the past and present status of differing security controls. What is often lacking is a proper frame of reference. Time is often the most important aspect. This is the effective differentiator between preventing and responding to an incident.

We should be looking to see how we leverage technology to make cybersecurity more efficient. This requires us to look at how we architect a common platform that allows the different capabilities required today to function together with minimal human input. But more important is building cybersecurity to be as future-proof as possible; i.e., as the next media format is developed, the existing player still needs to be able to accept and play the new format, without requiring a human to translate it into a compatible format.

Cybersecurity must function at the same digital speed as the technology it aims to protect. This technology will only continue to function at ever-increasing speed. You need to keep pace—or you will lose ground.

The EU legislative changes coming into effect in 2018 are a rare opportunity. They are moving the cybersecurity discussion into the heart of the boardroom. The changes will also allow different members of the business to become engaged with cyber risk and find a common language in which they can communicate. This will give your business the opportunity to step back from its myriad activities and look afresh at its security, enabling you to reassess and re-architect your approach to keep pace with future demands. This is about finding the right balance among detection, protection, and response, aligned to your business' risk appetite. Make the most of this opportunity—it may well define your business for the future.

TABLE OF CONTENTS

Navigating the Digital Age

EU Cybersecurity Legislation

Executive Responsibility

Leadership and Security Operations

Outsourcing and Moving to the Cloud

Enabling Innovation

Protecting Our National Organisations

Contributor Profiles

EU Cybersecurity Legislation

1

Pending EU Legislation on Data Protection and Cybersecurity has Strict Consequences for Your Board

Vondst Advocaten – Polo van der Putt and Puck Polter, Lawyers

- European citizens are getting better data protection
- The General Data Protection Regulation (GDPR) will impact your business
- There are hefty fines for serious data breaches
- In the event of a breach, you have 72 hours to make a public announcement
- Make everyone in your business aware of their obligations

Your board needs to pay much closer attention to pending EU legislation on data protection and cybersecurity—or face the consequences, say Polo van der Putt and Puck Polter, of Vondst Advocaten in Amsterdam.

A concerned client, who is a CEO, faced a sudden and rather nasty conundrum. His Dutch construction business tried to do the right thing after a personal data leak by following best practice. Yet, unwittingly, he and one of his employees faced the prospect of going to jail for breaking the law.

How can this be? You would normally expect your in-house lawyers or external legal advisers to decipher and shield you from much of the red tape that impacts your business. However, this particular construction firm was facing a critical moment and with imminent European Union legislation on its way, these moments could become even more critical. As a CEO, you need to understand the consequence of data protection legislation.

GDPR and NIS

For any organisation that holds personal details about its customers, employees or partners, the world is about to change. New EU legislation will impose stricter obligations on companies and will introduce huge penalties. The General Data Protection Regulation (GDPR) and the Network and Information Security Directive ('NIS Directive,' also known as the Cyber Directive) will apply from May 2018. The GDPR is designed to give the residents of Europe more protection for their personal digital data, while NIS is focused on ensuring greater confidence in key infrastructure services that have a digital dependency. As the CEO, you cannot ignore this. You must take full notice of the implications, as this new legislation requires companies to be able to show compliance. For the GDPR, failing to do so may result in penalties of up to €20 million or 4 percent of global turnover (this is for some types of infringements; infringements related to, for instance, personal data breaches are capped at up to €10 million or 2 percent, as described below). Penalties for the NIS Directive are yet to be determined as countries implement that law.

What was causing the CEO in our case such sleepless nights? Two IT employees from rival construction companies, Company A and Company B, were exchanging some coding information on how to perform a particular technical function. It is routine stuff. By accident, the employee from Company A sent all of its confidential log-in information and documentation for public procurement to Company B, run by our CEO client. One of Company B's team looked at the information, recoiled and realised this included personal data. Realising that this had serious ramifications, he went to his boss and reported it. Then Company B phoned Company A to alert them to the breach, which was stopped immediately. Company A thanked B for letting them know about this. It all sounds like a good-deed-for the day and the end of the story. But no. It appears that the poor guy from Company B had committed a criminal act in accessing this unauthorised environment. And that means Company B, who is his employer, and our CEO client who sits at the top, are responsible.

Under the new GDPR regulations, life could be even tougher on CEOs. For a start, in the above case, Company A might have to notify relevant authorities, and sometimes the individuals themselves, that data has been breached. They could potentially face a stiff fine unless they declare the breach to the relevant authorities within 72 hours. It is all going to get much tougher, unless you have strict procedures in place.

Of course, there will always be some who fail to follow the procedures and make a mistake that results in a data breach—and this is a challenge for you as a CEO. In essence, there will be a requirement for your business to:

- Plan
- Do
- Check
- Act with respect to the processing of personal data.

Your first step will be to identify the personal data being processed by your business. Here, the definition of personal data should be taken broadly. According to the EU data protection supervisors, the mere ability to identify someone from another could trigger data to become personal data. Supervisors do not even require the identity of the person concerned to be known, so even 'anonymous' data relating to someone's use of a service can be deemed personal data.

Implications of the General Data Protection Directive

The current EU regime for the protection of personal data—the 1995 Data Protection Directive (DPD)—is based on general concepts and does not impose many specific obligations on companies. The Directive is applied differently across various EU member states, resulting in different interpretations in France or in the Netherlands. At present, local regulators lack any real power to enforce this EU framework. From May 2018, GDPR will replace the 1995 Directive and address these shortcomings. For one, the GDPR introduces a level of harmonisation across the

EU countries that did not exist with DPD. In addition, the current general principles for treatment of personal data will not fundamentally change, but far more onerous obligations will be introduced. The biggest change is the introduction of a notification regime in the event of a data breach. Also, the scope of the personal data legislation broadens drastically. Whenever an organisation processes personal data on EU residents, the GDPR will apply. In short, it applies to organisations established in the EU and to non-EU-based organisations that sell to EU residents, and also to non-EU organisations that monitor the behaviour of EU residents (when that behaviour takes place in the EU).

> Executives should approach personal data protection and cybersecurity legislation as an opportunity, rather than as a threat.

Security requirements

The GDPR targets 'controllers' and 'processors.' These definitions are similar to the ones in the 1995 EU Directive. A controller is the party who is the owner of the data, who determines the purpose and means of processing personal data. For example, a Dutch company is in control of the human resources data of its own workforce, so every organisation is a 'controller' of its own data, while a processor, such as a service provider, processes personal data on behalf of a controller. To illustrate this, using the HR example, it could be an outsourced company that prints the salary slips for employees or stores data with a cloud service provider. Under GDPR, controllers and processors must have state of the art industry security measures in place, not only covering the confidentiality of data, but also its integrity and availability. GDPR requires your organisation to identify the various sets of data that are processed in your company and in some cases to perform a privacy impact analysis. The outcome of this analysis will provide insight into the risks represented by the processing and the nature of the data to be protected, thus determining the level of security required. Simple name and address data may require just password protection, whereas sensitive financial or health data may require the use of sophisticated encryption techniques. The ability to log access to, and use of, files and systems is generally believed to be standard security practice, and most businesses have established corporate security guidelines that describe required security levels and measures. Finally, you should test the effectiveness of your security measures periodically and if issues are found, you should evaluate the measures and improve them where necessary.

European data breach notification regime

The GDPR introduces a new mechanism for the notification of personal data breaches in Europe. Breaches of information security should be notified to the local supervisors within 72 hours. However, you do not need to notify if the breach is unlikely to result in any risks for individuals. To help with this you will need to have a system of internal escalation in place so the right managers can make an informed decision on whether to report or not. Some privacy regulations are longer than a Shakespeare play, and few people will read it all. You need to keep it simple so your company has transparent guidelines in a form that everyone understands.

Tough sanctions if you do not comply

The current EU data protection regime does not extend to penalties for personal data breaches, but GDPR does. A company that fails to comply with GDPR's personal data breach notification obligations may be fined, with the penalty being as high as €10 million or 2 percent of your organisation's total worldwide turnover, whichever is higher. Dutch, Belgian and Luxembourg regulators will look to see how prepared the company was and if it made the best efforts to prevent a breach. A regulator is likely to frown on repeat offenders who have been breached several times without seeking to resolve the issues.

The NIS Directive and its scope

Apart from the GDPR, the NIS Directive needs to be incorporated in the local law of EU member states. This directive combines with GDPR as part of the cybersecurity system to deal with breaches that the EU faces. The NIS Directive aims to achieve a high level of security of network and information systems which focus on national critical infrastructure.

The NIS Directive targets two types of organisations: operators of essential services and digital service providers. Industries where these organisations are doing business include, for example, energy, transport, banking, healthcare, financial market infrastructure, drinking water supply and distribution, online market places, online search engines and cloud computing services. Both operators of essential services and digital service providers are required to take 'appropriate and proportionate technical and organisational measures' to manage the risks posed to the security of network and information systems that they use in their operations. Such measures must take into account the following elements:

- The security of systems and facilities;
- Incident handling;
- Business continuity management;
- Monitoring, auditing and testing;
- Compliance with international standards.

The obligation to undertake stringent measures is likely to have a serious impact on different industries. Cybersecurity is increasingly important, so your business is obliged to take action. Such actions may make your business more risk averse. However, your business has the opportunity to improve its public image by highlighting the strength and security of its networks and customer data.

Meeting the cyber challenge

You should approach this personal data protection and cybersecurity legislation as an opportunity, rather than as a threat. You are advised to regularly back-up essential data on the premises, or at least at different external sites so that in the event of the bankruptcy of a third-party supplier, your business continuity is not impacted. From a strategic perspective, you need to consider the controlled probing, testing and exploration of weaknesses in your information security. For instance, ethical hackers may well expose your vulnerabilities and cause internal embarrassment but their deployment could also prevent serious exploitation by malicious adversaries and serious damage, both financially and reputationally. You may not want to sanction each intrusion of your internal procedures, but game-playing scenarios can often be highly revealing.

On top of this, you need to create a culture where notification of accidental violations and incidents is rewarded. Most importantly, you need to communicate the significance of this new legislation to all your employees. Share your business concerns with them and make them fully aware of the consequences. It will ensure they feel that they are being taken seriously as employees, which can only improve loyalty, creativity and productivity.

2

State of the Art – How and Why?

Palo Alto Networks – Greg Day, Vice President and Regional Chief Security Officer, EMEA

- Intelligence on cyber threats is key
- Be sure your cybersecurity is built on a solid foundation
- Multiple legacy technologies create inefficiencies —clear out the deadwood
- Cybersecurity should enable the business, not inhibit it
- Aim for more systemic success

'State of the art' is now a key term in new EU cybersecurity legislation—and outdated cyber capabilities could leave your business unnecessarily exposed to risk.

As our dependencies on technology grow, new EU legislation has introduced the term 'state of the art' into our vocabulary, as a part of the security by design and default concept in the General Data Protection Regulation. The term is also used in the Network and Information Security Directive, which is focused on the cybersecurity of essential services and digital services provision. Such a simple term will have significant impact on your business in the future, so it's worth considering now what it means to your business and others (such as auditors, customers, and partners).

On first glance, this may seem both easy and confusing, depending on your background. Those in financial services have been used to more prescriptive requirements from their own regulators, while others may look at this term as exactly what they, as security teams, do every single day: to continue to monitor the risk and adapt their cybersecurity capabilities to manage their risk. In many ways, the latter is why it is now the time to step back and consider what 'state of the art' really means.

You may consider this as detail, but here is why you should care and ask questions of your cybersecurity team: outdated cyber capabilities will leave your business unnecessarily exposed to risk, may cost you more to manage, and could lead to significant, unnecessary commercial impact.

In today's technology-driven world, the pace of change is relentless; as such, cybersecurity must continue to adapt to changing technology, new threats, and evolving business practices. In the 30 years I have spent working in the cybersecurity industry, the pace has never eased. Every year we have new problems to solve while we simultaneously try to consolidate existing capabilities. This creates a fundamental challenge: as we keep evolving, we never step back to look at the big picture. Are the cybersecurity fundamentals we started with so many years ago still sound today? For centuries we believed the world was flat, until science proved otherwise. Are our cybersecurity capabilities limited by similar, outdated beliefs?

So what are some of the principles that need to change?

1. Just as in every other aspect of business, intelligence is key. There is an ever-increasing number of cyber 'things' that could happen—the crucial questions are, 'Which are most likely?' and 'Which would have the most significant impact?' Validating this means not only leveraging commercial sources but also connecting to the right industry knowledge and sharing groups and effectively leveraging your own organic intelligence. The new legislation talks about 'having regard to' or 'taking into account' the state of the art, which could mean that you should be able to show you have current insight on what the threats are and how they could impact your business and your customers. You need to challenge your team to confirm not the problem but how they have qualified it and—more importantly—their confidence in its mitigation, whether that's the acceptance of the risk or prevention of it.

2. Cyberattacks have evolved from the equivalent of a single-celled organism into a complex life-form. Why is this important? It's important because cybersecurity has solved problem after problem, meaning that all too often we look for individual cells, to use the analogy, and in the modern world, this leaves us with lots of analysis (requiring expensive and slow human input) and often poor results. A house is built on solid foundations, yet in many ways, cybersecurity never had such foundations. Now is the time to step back and ask, 'What foundations will allow your cybersecurity to work cohesively and effectively, both today and in the future?' Remember that technology is here to automate human processes, not the other way round!

3. Just how much overlap has evolved through the natural evolution? In the physical world, we complain every week that someone else is digging up the road for a different purpose, yet in cybersecurity, the same also occurs. Multiple technologies are repeating core processes (such as decoding network traffic) just so they can do their piece of the security analysis. In an ever more digital world, technical inefficiency is inexcusable.

   A big part of this is clearing out the deadwood. When something has worked for years, we are always reluctant to let it go, but as the effectiveness decreases, that's exactly what we should do. Challenge the security team on their effectiveness and clear out the deadwood.

4. At the heart of technology are zeros and ones (binary switches that make decisions). However, people use technology, and they are definitely not binary! Too much of cybersecurity is based on how people should use technology, rather than how they do use it. It may be a hackneyed

expression, but cybersecurity should enable, rather than inhibit, the business. If it's not doing that, then it's likely to be based on the principles of how technology should be used, rather than how it is being used.

5. One of the biggest challenges in cybersecurity today is validating what success actually is. Historically, some may have suggested this would be that nothing bad is happening, but the reality is that online, just as in the physical world, bad stuff happens every day. The question then is, 'What is the goal of cybersecurity?' We can continue to respond to each instance, or we can aim for a more systemic solution. While new attacks take only minutes to produce, the underlying architecture they use typically remains constant. As such, rather than simply looking to stop the crime, we need to focus more on identifying the criminal methods being used, before they ever reach us. Compromised public systems and money flows all take time for the criminals to develop and should be considered part of the complex life-form we are looking to identify.

> In today's technology-driven world, the pace of change is relentless; as such, cybersecurity must continue to adapt to changing technology, new threats, and evolving business practices.

With the new legislation incoming, we have a rare chance to step back from being caught in the whirlwind of daily activities and evaluate just what 'good' looks like in cybersecurity. State of the art cybersecurity is a dynamic requirement that requires regular review of what is possible, balanced against the real and relevant risks. Mixing modern capabilities with legacy ones is the equivalent of Usain Bolt running a three-legged race with you: he can go only as fast as you can, much in the way that your cybersecurity is limited by its legacy.

If I could give you one piece of guidance as we move into this era of 'state of the art,' it would be to validate what success looks like in your business and what the state of the art should deliver to you in terms of protecting your business. Then test the reality, run what the industry calls 'red teaming' exercises (simulated attacks), including different functions of the business to see how well your state of the art stands up to scrutiny. Remember that the state of the art is dynamic, so this should be a regular exercise to ensure you remain current with the requirement and the best practices available. Lastly, discuss and compare with your industry peers to ensure you are getting a valid benchmark and drawing on the wisdom of crowds.

3

What is the Process for Achieving State of the Art?

PwC – Gregory Albertyn, Senior Director, and Avi Berliner, Manager

- 'State of the art' is about defending your 'crown jewels'
- Privacy architecture is evolving with new systems
- Cyber governance should be enshrined into company strategy
- Be clear about who is responsible for data sets
- If you're unfamiliar with something, ask the question

As a chief executive, you should fully understand who takes responsibility for guarding the most critical data inside your business.

Your board regularly makes enterprise decisions and choices based on the judgement of these guardians. However, the board simply can't be expected to examine everything in detail, and they need to deploy their time wisely. Yet cybersecurity increasingly requires more of your board's bandwidth because cyber risk continues to evolve in both regulatory and technical complexity: it is ongoing and iterative.

To meet forthcoming EU legislation you are expected to have relevant regard for 'state of the art' cybersecurity. While this might appear a fuzzy description, and it will likely not be defined by EU policymakers, a more solid definition for your own organisation is expected to become clearer as your organisation gains greater insight into the nature, scope and location of the cyber threats you face. However, fundamental to 'state of the art' is a sustained cybersecurity and privacy governance structure, accountable to senior leadership and mandated with continued monitoring of cyber and privacy risk and related enterprise response alignment.

Data privacy and security has traditionally been focused on implementing a set of governance models such as maturing data governance capabilities, performing assessments to create a baseline, and creating a target model to prioritise and manage risks. This has resulted in the introduction of monitoring and reporting tools that are reactive and responsive to threats. Yet, by its nature, 'state of the art' cybersecurity has to be dynamic, identifying and proactively responding in near real time to any new threat.

> By its nature, 'state of the art' cybersecurity has to be dynamic, identifying and proactively responding in near real time to any new threat.

Cyber resilient management is about keeping pace with the changing threat landscape, spotting and thwarting threats on the horizon to keep your critical assets and intelligence from falling into the wrong hands. What we are now seeing is the evolution of what is known as 'privacy architecture,' a set of guidelines and principles that are embedded into your business and technology processes from the ground upwards, rather than overlaid upon it. This bakes cyber resilience into your operating DNA, with reduced compliance overhead and resource requirements. You should be building cyber and privacy risk governance into your strategic plans as well as your day-to-day activities. 'State of the art' also leverages the exponential capabilities of big data. This includes not only the new storage and analytical techniques of constantly improving ecosystems of applications, but also the real-time, batch, and predictive analytical abilities. You will be able to deploy machine learning and other artificial intelligence tools to defend your critical business functions and data from yet unseen attack vectors.

Increasingly, you should adopt 'privacy by design' to ensure your security and enterprise architecture incorporates cyber resilience and privacy compliance requirements during initial scoping, and ensure review by all appropriate stakeholders.

To gain comfort on the adequacy of your cyber and privacy compliance programme, you should become familiar—although not necessarily an expert—with professional terms related to 'state of the art,' including:

- Encryption
- IAM (identity and access management)
- Anonymisation
- Data masking
- Risk-based activity monitoring controls with appropriate storage and report distribution channels.

If you are unfamiliar with these terms, then engage your chief information security officer (CISO) to explain their importance to operational and regulatory risk.

Furthermore, as a board leader, you should be aware of the risks in:

- The decentralisation of your data, particularly as it is used in the cloud;
- Streaming of data—and where the likely attack points might be;
- Unstructured data that is not held in safe and protected environments with appropriate controls;
- Global data transfer and access to your systems from staff, customers, and stakeholders.

Who should be handling your risk? Many organisations have disjointed threat analysis spread across several functions, physical locations, and systems. To close this gap, you should have a robust, centrally collated threat analysis capability—and an effective, centrally coordinated reactive capability. Based on our experience, the enterprise cyber and data governance capability should comprise a combination of three groups organised to carry out these task and responsibilities.

1. Cyber risk governance committee:

Key members of team: chief information security officer (CISO), chief operating officer (COO), chief risk officer (CRO), head of security, chief privacy officer (CPO), chief data officer (CDO), heads of businesses and functional areas, such as business continuity planning, legal, risk, and regulation.

Main responsibilities include:

- Working with senior leaders to develop cyber risk strategy.
- Classifiying and prioritising information assets—the 'crown jewels.'
- Setting the budget for cyber risk.
- Monitoring the organisation's cyber risk position and reporting on it to senior leaders and the board of directors.
- Reviewing reports from the cyber risk oversight and operations teams and helping prioritise emerging cyber threats.
- Revisiting strategy to adapt the program as the cyber risk landscape evolves.

2. Cyber risk oversight committee:

Key members of the team: information technology team, business support team, compliance/data governance team, and business teams.

Responsibilities include:

- Assessing the active risks the organisation faces, the people behind them, and the assets they threaten.
- Evaluating the effectiveness of the operations team.
- Identifying new threats and improving how information assets are protected.
- Determining how business changes affect the cyber perimeter—including new service offerings, suppliers, vendors, or business partners.
- Monitoring change control and ensuring privacy and security by design for changes to critical systems and data processing activities.
- Overseeing employee training programmes.
- Reviewing new regulatory and compliance requirements.

3. Cyber risk operations team:

Key members of the team: managers and SMEs for networks, information security, fraud, and corporate security. Security operations centre.

Responsibilities include:

- Acting as first line of defence for detecting and responding to cyber events.
- Compiling real-time information from all the groups that monitor cyber threats.
- Producing reports for the cyber risk oversight and governance committees, including number, type, and duration of cyberattacks.
- Maintaining a mature 'DevOps' framework to provide code and application quality as well as cyberthreat scanning and monitoring capabilities.

Adopting this structure can help you attain 'state of the art' cybersecurity, but you should also press your technical people about new, maturing, and expanding capabilities. The cyber and data risk programme should be able to identify your most valuable business assets, know where they are located at any given time, and who has access to them. Your 'crown jewels' are information and processes, which if stolen, compromised, or used inappropriately, could cause significant hardship and damage to your business—and harm your board's reputation for prudence and reliability. Such 'crown jewels' might be trade secrets, market-based strategies, trading algorithms, product designs, new market plans, market or customer data, or other vital business processes. Just as a crown and regalia worn by a sovereign have different values, so too do your own assets. Your executives will become accountable for protecting each of the crown jewels, in the same manner that you expect the finance director to be accountable for your company's financial results. You should be clear who in your organisation is personally responsible for each jewel.

Your governing team, with the right level of knowledge, expertise, and involvement at all levels of the organisation, is required to respond to cyber events. But waiting to prepare your response until after a cyber event is a recipe for disaster. The team should thoroughly understand the risks, the tools at their disposal, and their options in responding before a cyber event occurs.

The development of prepared and tested responses—'playbooks'—is a necessary step in adequately planning and preparing responses to cyber events.

Using the intelligence gathered throughout the playbook development process, each playbook details who should take action, what their responsibilities are, and exactly what they should do. 'State of the art' also means continually revisiting each playbook at appropriate periods, according to classification and risk prioritisation, to ensure updated cyber intelligence gathering techniques, cyber technology, and insurance options. Cyber threats and regulatory mandates remain fluid and dynamic.

If in any doubt, seek advice and consider a 'state of the art' assessment to develop an appropriate road map to help ensure you have the highest level of hardened resilience.

About PwC:
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 223,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

4

Organisations Must Put In Place the Right Policies and Procedures for Cyber Insurance

First Lawyers – Judith Vieberink, Lawyer

- Cyber insurance is becoming mainstream quickly
- You need to do everything in your power to mitigate risk
- Someone at C-level has to be responsible for data protection
- Organisations need to evaluate all their data processes and make sure they are robust
- Working hard on General Data Protection Regulation (GDPR) compliance can lower your deductible

Judith Vieberink, an advocate with First Lawyers in The Hague, says organisations must put in place the right policies and procedures to ensure that insurance can enable you to recover after a cyber breach where data has been lost or stolen.

Insurers have seen a significant uptick in cybersecurity policies over the last year, notably in the Netherlands. Whereas insurance used to be something that the company secretary, the head of legal or the finance controller have been able to take care of without taking up precious boardroom time, now you—as a board member—should be asking how you make your organisation more insurable so that you are not paying over the odds for cyber insurance.

As Benelux organisations begin to appreciate the implications of impending data protection regulation, they are looking at how to best prepare for new requirements and the role that insurance may be able to play. In the legal courts, you are innocent until proven guilty. It works the opposite way with cybersecurity insurance: you really need to prove that you've done everything reasonable in your power to stay secure in order to have any claims honoured. It is a fact that businesses need to recognise that insurers will always look to manage the amounts paid out in order to stay profitable. Insuring confidential business data or personal data against cybersecurity breaches with an 'open door' is extremely expensive. To get an affordable premium, organisations need to 'close their door' by evaluating all their data processes, making sure they are robust and implementing technical and organisational measures.

The cyber insurance market is becoming more relevant

The market for cybersecurity insurance is maturing and evolving. There is a growing volume of claims related to cyber coverage, especially in the United States where the market is better established. In my experience, a client seldom phones up and says: 'Hey, I want to get cyber insurance.' The client is generally asking about the EU's General Data Protection Regulation (GDPR) legislation, which will come into force in May 2018, and they want to know how to prepare for this. Mandatory disclosure of a personal data breach within 72 hours, or face the prospect of significant fines, is focusing the minds of many CEOs.

The questions are about the tips and tricks needed for a client to implement best practices for data and privacy protection and, within this context, the subject of cyber insurance is increasingly relevant. First, many clients are asking: 'OK, I don't want to be over-insured, so what is already covered with my existing policies?' They also want to know what is needed to ensure specific cover for the data protection officer (DPO) within their organisations—just as individual board members are usually covered by a liability insurance.

You need to measure your data processes

Before you start signing up for cyber insurance, you need to be fully prepared. You must view your compliance with the GDPR requirements through your duty of accountability. Experiencing a personal data breach is not the problem, rather, it is how you resolve that breach that matters. Your time spent post-breach, where the full extent and damage must be assessed, is costly both in financial and reputational terms and the longer it takes to fix, the higher the costs. The quicker you handle a breach and reach a satisfactory conclusion, the more likely you are to keep a reputable insurer on your side. The longer and messier it gets, the more you should expect to pay.

What kind of measurements should you undertake?

Essentially, to ensure satisfactory insurance cover you should have proper measurements and procedures in place, so that in the event of a breach you can assert to your insurer that your organisation has done everything within its power to mitigate the risk.

An insurance company always sets the terms and conditions about its willingness to pay out in the event of an incident. In general terms, the onus is on your organisation to meet certain levels of common sense, compliance and security. You need to focus on three steps:

- What is the organisational structure of the company?
- Who is responsible for the company's cybersecurity and data protection?
- Do you have robust company data protection and security processes in place?

1. What structure does your organisation have?

The size and reach of your organisation matters. It stands to reason that the risks for larger companies with more entities are greater. As the CEO, you need to know the reach of your organisation by asking: 'What is the extent of my corporate family?' Are you an entity only in the Netherlands, Belgium or Luxembourg, or does this extend to the rest of the European Union and beyond? While GDPR covers European Union member states, it also extends to any international business that holds personal data of European Union residents.

Once you've determined your corporate family, you must identify your company data protection processes, how these processes are being implemented, and how individual rights relating to personal data are being guaranteed. You must find out what kind of data processes are flowing through your business, and what personal data is exchanged with other external organisations—such as processors who may have access to your data—and those in your supply chain. Even so, it's not just about personal data here. Confidential company data is equally important, although it's not subject to data protection regulation. You and your board will now be held responsible for this.

2. Who is responsible for the company's cybersecurity and data protection?

As the board, you cannot be expected to know everything about this, so you must delegate to someone who takes on this role and responsibility. Within the Netherlands, the *feitelijk leidinggever* is the person within the organisation that can be held liable for shortcomings. This individual is often a data protection officer (DPO), chief executive officer (CEO), chief information security officer (CISO) or chief technology officer (CTO) and he or she is directly responsible to the board for the privacy protection policies within the company and the agreement about processes. Under Dutch legislation, the *feitelijk leidinggever* also has a personal responsibility, so make sure your insurance covers any slips, mishaps or damage they may inadvertently cause.

3. Do you have robust company data protection and security processes in place?

The third step is about formulating a baseline. Here you must implement this within your own corporate family and ensure all or any of your external processors are governed by a contract.

Focus needs to be on mapping what kind of personal data you are processing. If you are a traditional Brussels retailer you need to know where all your customer information is being held, even if you are using a third-party to process your online transactions. You need to have sight of the places where this data is being stored and processed. This becomes valuable information for your insurance provider also. It is well understood that you cannot secure everything, so you need to focus on the areas and locations that present the highest risk and perhaps where the most valuable information is located. You should be able to assess your own vulnerabilities rather than allow a malicious outsider to expose them for you.

You will also need to articulate what kind of processes are being used to protect the data. Some questions to ask include:

- What types of encryption, security, firewalls and password protection does the data processor have in place?
- Who is responsible for implementation and maintenance of these controls?
- Do we only monitor incoming traffic?
- Do we meet or exceed the industry standard?

> Good business behaviour goes a long way with reputable insurers. But beware, they might be promising more than they can deliver.

For example, if you are working in the Dutch healthcare sector, you must meet the national standards of MEM7510, MEM7712 and MEM7513. If this requires extra staff training and examination, then you need to set aside time and resources for this. You need to ask if you have implemented these standards and are continuously monitoring implementation. The more relevant information you can give, the more accountable you will be in the eyes of your insurer. As the CEO, you need to make sure this is all reviewed frequently and that you are testing and scenario-planning in the event of attack.

Building your own insight

Many business will have developed an application checklist for the insurer. At First Lawyers, we have developed our own system, which extends way beyond a checking procedure. It is about assessing your risks on a dynamic and ongoing basis. This application process concentrates on various focal points.

For example, if you know the kind of data that might be visible or valuable to an attacker, then you can calculate how much value might be lost in the event of an attack. There are additional tools available, including benchmarking, used by insurance underwriters to gather large amounts of independent data on firms. These are used to establish a firm's attractiveness to hackers and their vulnerability to attack. If you know the true scope of a breach and its impacts, this will help your insurer too. If you have no idea or indication, you enter this dangerous territory at your peril.

How do you assess the cost of reputational damage?

Your organisation's reputation is essential for sustainable business. So, what if a breach undermines public confidence in your brand? This is the hardest part for which to determine financial loss. It is not just an insurance problem, as most companies find it hard to put brand value and reputation on their balance sheets.

It remains difficult to insure against reputational damage simply because it is hard to define the financial impact of a personal data breach on your business. We've seen instances in the last 12 months where some organisations have been able to assess, for example, customer loss in the aftermath of a breach. This was quantifiable, but it was challenging to quantify the opportunity cost incurred by those who decided not to become customers. If you cannot make this clear to your insurer, nine out of ten times they will not cover it. It is often based on an assumption, rather than pure logical assessment.

How can you be sure of lower premiums?

When preparing an application for cyber insurance, it is imperative to have answers to the following key questions that insurers are sure to ask:

- What entities would you like to insure?
- Your organisation may have implemented measurements, but your data processor may not have, so they become a weak link within the chain of data processing. Are your data processors involved and have you made sure they facilitate you in becoming compliant and secure?

- Is there someone at C-level who is responsible for cybersecurity, data and privacy protection?

- Did you appoint a DPO?

- Do you have an emergency response team available? If so, who is in this team and what are their roles in the event of a breach?

- What are the channels of communication?

- Do you have a robust action plan to improve your defences?

- Who will be the public face of your organisation in the event of a breach, and how well briefed are they to handle what can often become a short-term storm of media and customer interest?

- How quickly do you anticipate getting back online in the event of a cyberattack?

Good business behaviour goes a long way with reputable insurers. Insurance companies are not keen to reduce premiums over a longer spell, and having five years without a breach does not necessarily lower the risk of a serious cyberattack. With cyberattacks increasing exponentially, the cyber insurance industry is still calibrating its cost structures. However, insurance companies are willing to negotiate the deductible, the excess sum that must be paid by the insured in the event of a breach.

The longer your company goes without a breach, the larger the sum that may be paid out in event of a cyberattack that damages your business. Your deductible is more negotiable than your premium and in the Netherlands, you can only cover your own damages and damages caused to others. Cover for damages caused to customers or clients is more complex. Most insurance companies will cover the damages up to the sum to be paid out in an event. But beware, because insurers might be promising more than they can deliver.

In essence, the more work you do to protect your business from cyberattacks, the better your prospects for finding suitable levels of insurance.

Executive Responsibility

5

Cyber Risk as an Enabler for Cybersecurity

Palo Alto Networks – Fred Streefland, Senior Product Marketing Manager, EMEA (formerly LeaseWeb, CISO)

- Make sure your chief information security officer (CISO) and board talk the same language
- Understand your risk appetite and define your security end state
- Align your cybersecurity strategy with your business strategy
- Security awareness training is a good way to build resilience
- You are responsible, but your CISO is the chief architect of your digital home

Just like with any other aspect of running your business, you and your board have to know what risks you are willing to take on when it comes to cybersecurity. Only then can you define a cybersecurity strategy that is in line with your overall business strategy.

If you are a soccer league referee, as I am, you regularly make split-second decisions about players who deliberately or unintentionally break the rules and spoil the spirit of the game. It is much like this with cybersecurity as well, except that the consequences of allowing the rules to be breached can be infinitely more severe than a penalty kick or a lost match. Foul play can pull down the critical functions of your organisation.

If you are a CEO or a senior board member of any organisation, you must face this interesting paradox. Traditionally, you and your colleagues might have come from senior backgrounds in finance, legal, marketing or engineering. During my time as a CISO within LeaseWeb (July 2015 - February 2017), a Dutch-based technology infrastructure-as-a-service (IaaS) provider with a global footprint, managing 80,000 servers in several global data centres and more than 20,000 worldwide clients, the board's background was in the aviation industry and they had safety in their DNA. The LeaseWeb board members were also very aware of security and they provided me with great support as a CISO, even though they couldn't also be specialists themselves within the cybersecurity domain.

Yet, it is the board's responsibility to define the multiple risks that can damage or bring down its business. Corporate annual reports now dedicate several dense pages to discussing the geographical, financial and market risks facing the company, and companies are required and expected to assess each of these risks. Nevertheless, a board is unlikely to be equipped to make this kind of judgement on cybersecurity without some help. The development of the security strategy is one of the main tasks of the CISO or a similar appointment, and it should comprise a vision, a mission and an 'end-state' for your business. Your CISO has to be the developer, consultant, manager and chief architect of your information security. But it is unfair to think your CISO can conjure this up on their own.

> Information security must be a 'business enabler,' never a 'business obstruction.'

This cybersecurity strategy must be aligned to your business strategy, so it is essential that the CISO develops this in consultation with you and your fellow board members. And the CISO must understand and talk your business' language. During my time as a CISO, I was asked by my manager to visit a client who he felt was 'not in control' when it came to cybersecurity. I visited this company and spoke to their management and asked what they saw as the problem. One of the board members of that company shared that 'our technical guy is extremely good but we get lost with what he is telling us after two sentences. He only talks IT language.'

The starting point is to speak in easy-to-understand business language. In terms of corporate governance, 'information security governance' is all about 'the security of the essential information that you need to conduct your business.' In simple terms, it must always be aligned with your business objectives, rather than obstructing them. Information security must be a 'business enabler,' never a 'business obstruction.'

The security end state means the desired security maturity of an organisation at a given point in time, perhaps in a year's time or even three to five years down the line. Based on that end state, the CISO can then reverse-engineer their security strategy. It is important to note that the development and design of this end state must start in the boardroom and must be based on the risk appetite of the board of directors of a company.

Building a risk model

Creating the risk model for your company is similar to designing a house. You discuss with the architect whether you want a flat or pitched roof, open-plan space or intimate rooms, air conditioning or open fires, brick or stone. But before all of this, you need to look at the foundations, how services enter your premises and even the flood plain. It's the same with cyber risk: you start very simply with the basics. You really don't need to know the technical details of plumbing or electrical systems; that's why you employ an architect. Yet you must know the risks. And to mitigate the risks you must ask informed questions. If you don't know the risks, you set yourself up for some unpleasant surprises further down the line.

How much risk are you and your fellow executives willing to take? This depends on factors such as the character of the business, the current threat environment and your budget. A commercial web-based business, which depends primarily on uninterrupted internet access for its customers, must focus on the risks of losing that connection and the consequential impact on its reputation, while a governmental organisation must focus on the confidentiality of citizens' information. They need to prioritise the risks that come with storing sensitive data. There is a simple way to evaluate the risk appetite so that a security strategy can be developed with the desired end state in mind.

So, how to assess risk?

Risk assessments can be executed in many ways and there is no standard method that fits all organisations. There are, however, some best practices. One of the easiest methods is to set up departmental or cross-departmental risk workshops. This means involving as many employees as possible from different departments and getting them to score different levels of risk. From this, overall organisational risk can be defined.

It does not have to be too technical and can all be recorded on an Excel spreadsheet. At the workshops, the employees of a particular department or team will be invited to brainstorm on information security risks and categorise each risk by impact (1-5) and probability (1-5). The impact number is multiplied by the probability figure. The outcome of this brainstorm session is a matrix of risk, categorised by a number between 1-25. (1 = low impact/low probability, 25 = high impact/high probability). Within LeaseWeb, these risk workshops were executed in 2016 and during these brainstorming sessions, 225 business risks were identified and they were all scored on this rating. While it is often subjective, most people roughly agreed on the risk scores. It means looking at the highest number and working to see the residual risk.

There is another element to consider: risk is fluid. It is changing every day. This means that risk assessments must be held regularly, just to keep the overall risk position as accurate as possible. Within LeaseWeb, we reviewed the list of risks on a monthly basis and held a risk assessment workshop with the departments once every year. This process is a constantly changing journey, never a destination. The road map of risk is always taking you on new and often unexpected paths. If a new risk gains a high score, then it must go to the top of the to-do-list, and your board needs to be aware of this.

Cybersecurity awareness is an easy win

Coupled with this is the importance of cybersecurity awareness training. While it is an easy win, many businesses neglect this. With training, you will see greater awareness among your personnel and it remains one of the best ways to build resilience. It's low-hanging fruit, easy to set up and will improve your organisation's collective knowledge. Within LeaseWeb, all new employees have to complete one hour of security awareness training during their on-boarding days and are obliged to follow e-learning modules that are provided by a specialised cybersecurity education organisation. By doing all of this, all employees, ranging from front-desk receptionists to the board executives, start to build a comprehensive understanding of information security risks, which forms the basis for the defence of the company.

Align security measures with your business

As we have seen, the outcome of a comprehensive risk assessment forms the starting point for the information security roadmap, which consists of several security measures or projects, prioritised in time. Once the CISO develops this roadmap, the board needs to approve it.

During this approval phase, the board should check the feasibility of the security measures against the corporate strategy, to make sure that they align with the business. For example, mandatory 2-factor authentication for accessing a company's network must be implemented in such a way that all employees are able to execute this login process with minimal effort. Once this 2-factor login is too difficult, or not even possible for employees at remote locations, it can greatly hamper the business. When implementing security measures such as these, there must always be a balance between security and usability. Your board needs to make these decisions, aligned to the risk priorities identified earlier. Then, the progress of the security projects must be taken to the board regularly in order to update them about the security strategy and the roadmap.

On a quarterly basis, you should expect your CISO to present the results of security projects compared to the risks so that you and the other board members can provide additional guidance and direction to the CISO. Once the security strategy has been approved by the board, the corporate security programme that pertains to this strategy must be further developed by the CISO. This security programme consists of a roadmap, supported by clear objectives in a timeline. Development of this roadmap is another important task of the CISO and starts with a comprehensive risk assessment.

Conclusion

Information security remains the responsibility of the board of directors, although it is delegated to a CISO or the head of IT. The information security strategy must be derived from the corporate strategy, aligned with the business and based on the risk appetite of the board and the desired end state. The security strategy must then be translated into a security roadmap, consisting of security measures or projects with clear objectives. During this process you can expect your CISO to keep you informed about progress, so you maintain your focus on business strategy. A CISO doesn’t have to be an IT nerd—although it might help—but they need to be the chief architect working with your executives and directors to decide the style and security of your digital home.

6

Prevention: Can it be Done?

Palo Alto Networks Inc. – Mark McLaughlin, CEO

Frequent headlines announcing the latest cyber breach of a major company, government agency, or organisation are the norm today, begging the questions of why and will it ever end?

The reason cybersecurity is ingrained in news cycles, and receives extraordinary investment and focus from businesses and governments around the world, is the growing realisation that these breaches are putting our very digital lifestyle at risk. This is not hyperbole. More and more, we live in the digital age, in which things that used to be real and tangible are now machine-generated or only exist as bits and bytes. Consider your bank account and the total absence of tangible money or legal tender that underlies it; you trust that the assets exist because you can ‘see’ them when you log in to your account on the financial institution’s website. Or the expectation you have that light, water, electricity, and other utility services will work on command, despite you having little to no idea of how the command actually results in the outcome. Or the comfort in assuming that of the 100,000 planes traversing the globe on an average day, all will fly past each other at safe distances and take-off and land at proper intervals. Now, imagine that this trust, reliance and comfort could not be taken for granted any longer and the total chaos that would ensue. This is the digital age; and with all the efficiencies and productivity that has come with it, more and more we trust that it will just ‘work.’

This reliance on digital systems is why the tempo of concern due to cyberattacks is rising so rapidly. Business leaders, government leaders, education leaders and military leaders know that there is a very fine line separating the smoothly functioning digital society built on trust and the chaotic breakdown in society resulting from the erosion of that trust. And it is eroding quickly. Why is that, and do we have any analogies? And, more importantly, can it be fixed?

Machine vs. human

At the heart of the cybersecurity battle is a maths problem. It is relatively simple to understand, but hard to correct. One of the negative offshoots of the ever-decreasing cost of computing power is the ability for cybercriminals and adversaries to launch increasingly numerous and sophisticated attacks at lower and lower costs. Today, bad actors without the capability to develop their own tools can use existing malware and exploits that are often free or inexpensive to obtain online. Similarly, advanced hackers, criminal organisations and nation states are able to use these widely available tools to launch successful intrusions and obscure their identity. These sophisticated adversaries are also developing and selectively using unique tools that could cause even greater harm. This all adds up to tremendous leverage for the attackers. (See Figure 1.)

In the face of this increasing onslaught in the sheer number of attacks and levels of sophistication, the defender is generally relying on decades-old core security technology, often cobbled together in multiple layers of point products; there is no true visibility of the situation, nor are the point products designed to communicate with each other. As a result, to the extent attacks are detected or lessons are learned from an attack, responses are highly manual in nature. Unfortunately, humans facing-off against machines have little to no leverage, and cyber expertise is increasingly hard to come by in the battle for talent. Flipping the cost curve on its head with automation, a next-generation, natively integrated security platform is required if there is any hope of reducing the 'breach du jour' headlines. (See Figure 2.)

It is unlikely that the number of attacks will abate over time. On the contrary, there is every reason to expect that their number will continue to grow. In fact, we can also expect that the 'attack surface' and potential targets will also continue to grow as we constantly increase the connections of various things to the internet.

An understandable but untenable response to this daunting threat environment is to assume that prevention is impossible, so we must simply detect and respond to all intrusions. The fundamental problem with this approach is that without significant prevention, no combination of people, process and technology can prioritise and respond to every intrusion that could significantly impact a network and those who rely on it. The maths problem is simply insurmountable. Quite simply, detection and response should be supplements to, instead of substitutes for, prevention.

FIGURE 1

As computing power becomes less expensive, the cost for launching automated attacks decreases. This allows the number of attacks to increase at a given cost.

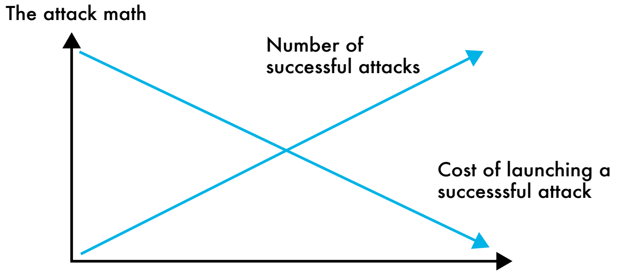
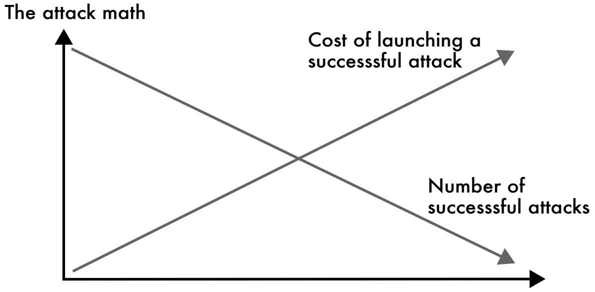


FIGURE 2

Harnessing automation and integrated intelligence can continually raise the cost of making an attack successful, eventually decreasing the number of successful attacks.



So, the strategy must be to significantly decrease the likelihood of, and increase the cost required for, an attacker to perform a successful attack. To be more specific, we should not assume that attacks are going away or that all attacks can be stopped. However, we should assume, and be very diligent in ensuring, that the cost of a successful attack can be dramatically increased to the point where the incidence of a successful attack will sharply decline.

When this point is reached, and it will not come overnight, then we will be able to quantify and compartmentalise the risk to something acceptable and understood. It's at that point that cyber risks will be real and persistent but that they will leave the headlines and fade into the background of everyday life, commerce, communications and interaction. This should be our goal—not to eliminate all risk, but to reduce it to something that can be compartmentalised. There is a historical analogy to this problem and an approach to solve it.

Sputnik analogy

The analogy, which is imperfect but helpful, is the space race. In 1957 the Soviet Union launched Sputnik. The result was panic at the prospect that this technology provided the Soviets with an overwhelming advantage to deliver a nuclear attack across the U.S. Suddenly, the very way of life in the Western world was deemed, appropriately so, at risk. The comfort and confidence of living in a well-protected and prosperous environment was shattered as citizens lost trust in their ability to follow their daily routines and way of life. It appeared as though there was an insurmountable technological lead, and everywhere people turned there was anxiety and cascading bad news.

In the years immediately following Sputnik, the main focus was on how to survive a post-nuclear-war world. Items like backyard bomb shelters and nonperishable food items were in great demand, and schools were teaching duck-and-cover drills. In other words, people were assuming attacks could not be prevented and were preparing for remediation of their society post-attack.

However, this fatalistic view was temporary. America relied on diplomacy and traditional forms of deterrence while devoting technological innovation and ingenuity to breakthroughs such as NASA's Mercury programme. While it took a decade of resources, collaboration, trial and effort, eventually the Mercury programme and succeeding efforts changed the leverage in the equation. The space-based attack risk was not eliminated, but it was compartmentalised to the point of fading into the background as a possible, but not probable, event. It was at this stage that the panic and confusion receded from the headlines and daily reporting. We will know we are in good shape in the cyber battle when we have reached this point. So, how do we get there?

As with all things in life, ideas and philosophy matter. This is true because if you do not know what you are trying to get done, it's unlikely that you will get it done. In the space race analogy, the philosophy shifted over time from one that primarily assumed an attack was imminent and unstoppable, with the majority of planning and resources geared toward life in the post-attack world, to one of prevention where the majority of resources and planning were geared to reducing the probability and effectiveness of an attack.

Importantly, the risk of an attack was not eliminated, but the probability of occurrence and success was reduced by vastly increasing the cost of a successful attack. It was previously noted that no analogy is perfect, so the analogy of 'cost' here for space-based attacks and cyberattacks is, of course, measured in different ways. Most notably, cyber threats are not the sole purview of superpower nations, and the technological innovation most likely to reverse the cost of successful attacks is most likely to come from industry, not governments. However, the principle is the same in that a prevention philosophy is much more likely to result in prevention capabilities being developed, utilised and continually refined over time.

Is prevention possible?

The obvious question then is whether prevention is possible. I think that most security professionals and practitioners would agree that total prevention is not possible. This is disheartening but also no different from any other major risk factor that we have ever dealt with over time. So, the real question is whether prevention is possible to the point where the incidence of successful attacks is reduced to something manageable from a risk perspective. I believe that this is possible over time. In order to achieve this outcome, it is an imperative that cost leverage is gained in the cyber battle. This leverage can be attained by managing the cyber risk to an organisation through the continual improvement and coordination of several key elements: technology, process and people, and intelligence sharing.

Technology

It is very apparent that traditional or legacy security technology is failing at an alarming rate. There are three primary reasons for this:

- The first is that networks have been built up over a long period of time and often are very complicated in nature, consisting of security technology that has been developed and deployed in a point product, siloed approach. In other words, a security 'solution' in traditional network architecture of any size consists of multiple point products from many different vendors all designed to do one specific task, having no ability to inform or collaborate with other products. This means that the security posture of the network is only as 'smart' overall as the least smart device or offering. Also, to the extent that any of the thousands of daily threats are successfully detected, protection is highly manual in nature because there is no capability to automatically coordinate or communicate with other capabilities in the network, let alone with other networks not in your organisation. That's a real problem because defenders are relying more and more on the least leverageable resource they have—people—to fight machine-generated attacks.

- Second, these multiple point solutions are often based on decades-old technology, like stateful inspection, which was useful in the late 1990s but is totally incapable of providing security capabilities for today's attack landscape.
- And third, the concept of a 'network' has morphed, and continues to do so at a rapid pace, into something amorphous in nature: the advent of software as a service

(SaaS) providers, cloud computing, mobility, the internet of things, and other macro technology trends, have the impact of security professionals having less and less control over data.

In the face of these challenges, it is critical that a few things are true in the security architecture of the future:

- First is that advanced security systems, designed on definitive knowledge of what and who is using the network, be deployed. In other words, no guessing.
- Second is that these capabilities be as natively integrated as possible into a platform, such that any action by any capability results in an automatic reprogramming of the other capabilities.
- Third is that this platform must also be part of a larger, global ecosystem that enables a constant and near-real-time sharing of attack information, this can then be used to immediately apply protections preventing other organisations in the ecosystem from falling victim to the same or similar attacks.
- Last is that the security posture is consistent regardless of where data resides or the deployment model of the 'network.' For example, the advanced integrated security and automated outcomes must be the same whether the network is on premise, in the cloud, or has data stored off the network in third-party applications. Any inconsistency in the security is a vulnerability point as a general matter. And, as a matter of productivity, security should not be holding back high-productivity deployment scenarios based on the cloud, virtualisation, SDN, NFV and other models of the future.

Process and people

Technology alone is not going to solve the problem. It is incumbent upon an executive team to ensure their technical experts are managing cybersecurity risk to the organisation. Most of today's top executives did not attain their position due to technological and cybersecurity proficiency. However, all successful leaders understand the need to assess organisational risk and to allocate resources and effort based on prioritised competing needs. Given the current threat environment and the maths behind successful attacks, leaders need to understand both the value and vulnerabilities residing on their networks and prioritise prevention and response efforts accordingly.

Under executive leadership, it is also very important that there is continued improvement in processes used to manage the security of organisations. People must be continually trained on how to identify cyberattacks and on the appropriate steps to take in the event of an attack. Many of the attacks that are being reported today start or end with poor processes or human error. For example, with so much personal information being readily shared on social networking, it is simple for hackers to assemble very accurate profiles of individuals and their positions in companies and launch socially engineered attacks or campaigns. These attacks can be hard to spot in the absence of proper training for individuals, and difficult to control in the absence of good processes and procedures regardless of how good the technology is that is deployed to protect an organisation.

> It is very apparent that traditional or legacy security technology is failing at an alarming rate.

A common attack on organisations to defraud large amounts of money via wire transfers relies on busy people being poorly trained and implementing patchy processes. In such an attack, the attacker uses publicly available personal information gleaned off social networking sites to identify an individual who has the authority to issue a wire transfer in a company. Then the attacker uses a phishing attack, a carefully constructed improper email address that looks accurate on a cursory glance, seemingly from this person's manager at the company, telling the person to send a wire transfer right away to the following coordinates. If the employee is not trained to look for proper email address configuration, or the company does not have a good process in place to validate wire transfer requests, like requiring two approvals, then this attack often succeeds. It is important that technology, process and people are coordinated and that training is done on a regular basis.

Intelligence sharing

Given the increasing number and sophistication of cyberattacks, it is difficult to imagine that any one company or organisation will have enough threat intelligence at any one time to be able to defeat the vast majority of attacks. However, it is not hard to imagine that if multiple organisations were sharing what they are seeing from an attack perspective with each other in near-real-time, that the combined intelligence would limit successful attacks to a small number of the attempted attacks. This is the outcome we should strive for. Getting to this point would mean that the attackers need to design and develop unique attacks every single time they want to attack an organisation, as opposed to today where they can use variants of an attack again and again against multiple targets. Having to design unique attacks every time would significantly drive up the cost of a successful attack and force attackers to aggregate resources in terms of people and money. This would make them more prone to being visible to defenders, law enforcement and governments.

The network effect of defense is why there is such focus and attention on threat intelligence information sharing. It is early days on this front, but all progress is good progress and, importantly, organisations are now using automated systems to share threat intelligence. At the same time, analytical capabilities are being developed rapidly to make use and sense of all the intelligence. This will result in advanced platforms being able to reprogramme prevention capabilities in rapid fashion, such that connected networks will be constantly updating threat capabilities in an ever-increasing ecosystem. This provides immense leverage in the cybersecurity battle.

Conclusion

There is understandable concern and attention on the ever-increasing incidence of cyberattacks. However, if we take a longer view of the threat and adopt a prevention-first mindset, the combination of next-generation technology, improvements in processes and training, and real-time sharing of threat information with platforms that can automatically reconfigure the security posture, can vastly reduce the number of successful attacks and restore the digital trust we all require for our global economy.

7

Understanding how Your IT Department Thinks

Institute for Software Quality (IfSQ) – Graham Bolton, Chairman

- Software does not keep itself clean
- Reward your developers for doing their work well
- Being able to fix software quickly is essential for security
- Playing catch-up stops you from concentrating on things that matter
- If you can't test your software, your clients will have their patience tested

Today's C-suite leader must be agile in delivering new products and services but how can they take responsibility for the development of digital systems to make this change happen? Graham Bolton, chairman of the Institute for Software Quality, offers his solution.

A hundred years ago, a Rhine barge captain would send an instruction to the engine room to raise more steam to increase speed. The captain didn't need to understand the intricacies of the boiler and transmission systems; he had faith that his engineers would deliver what he requested. It used to be the same for chairmen and chief executive officers when it came to the technology in their businesses. They would define their business strategy and leave it to the IT department to deliver the systems needed to drive business growth. The boardroom's interest seldom extended further than two questions: 'Why are our IT projects always over budget?' and 'Why do they take so long to implement?'

Today, if you are on the board of an organisation, this is no longer acceptable. There is tremendous value in deploying relevant technology to benefit your business. The more we connect information, the greater its worth. There is no doubt that this will apply to your business, sooner or later. Yet the more we interconnect systems, the greater we multiply the risks. For this reason alone, you need to sit up and take note, not least because assessing cyber risk in your company is part of your fiduciary duty. Yet how can you visualise what you need to know?

Understanding how to mitigate cyber risk: *The Lord of the Rings* story

It is often difficult to explain cyber risk to a non-technical board director with a financial, marketing or sales background. We all understand that the application of digital technology has made business more efficient, allowing our people to undertake new forms of working and develop new products and delivery mechanisms. It is clear that the more we connect data, the greater its value.

Yet it is essential that you have some conceptual understanding of how to assess the risks, and an ability to ask the right questions. This will help board-level leaders understand the vulnerabilities within their own systems and how they are susceptible to attack.

Let's try this explanation: the trilogy of *The Lord of the Rings* by J.R.R. Tolkien is well-loved and luckily you don't need to have read the whole thing to understand this analogy, which relates to the text of three large volumes with a total of over 450,000 words.

Let's say that we don't like the name Frodo, the central character, and we decide to change it every time it is mentioned. We search for the text 'Frodo' and make all the changes. That's a simple enough task. But what if we want to change the sex of Frodo, changing him from a 'him' to a 'her'? Then we have to read more deeply, changing various words from the male to the female form. We are changing 'he' into 'she,' and 'his' into 'her,' which means that we must understand the text, carefully reading every sentence. This is about 'analysing' the context. Here we start to understand a programmer's mind-set because computer programmes are just like text, and you have to make consistent changes in multiple places if you want to make something work properly.

Replacing the word Frodo is fairly easy: changing the gender of a character without missing a reference or making a mistake is much harder. Making changes like this involves two concepts: 'analysability' (how easy it is to understand what has been written) and 'modifiability' (how easy it is to alter the text without making mistakes). And why is that important to you? When malicious attackers get inside your systems, your people need to alter programmes, and you need them to be able to do it quickly without making mistakes along the way.

Your board is expected to make a decision about whether to add new products to your sales funnel. This will require changes to existing programmes, and perhaps the development of some new ones. Do you know and appreciate the risks? And how are you able to assess this?

Updating a system to make it more secure

You press ahead with developing new products or the introduction of another service. Perhaps you want your business to be more transactional, so sales can be made directly through a cloud application. This a strategic board decision. Using our *Lord of the Rings* example, this is not just adding an extra chapter, but introducing an entirely new imaginary world. We are inventing a new country and introducing fresh characters to the existing story. We have to hook this addition into the existing narrative so it makes sense. Your team has to get all the hooks right, all the characters in place, all the proper references to impending and previous battles. This really starts to get complex, when all you want to achieve is simplicity and increasing usability for your customers. In a digital context, this becomes a difficult piece of work for even the smartest technical people.

How to prevent a malicious attack

The sophisticated cybercriminal only needs a tiny entry point into your complex system. With simple access, the attacker can do a great deal of harm. Every day, Benelux businesses face constant probing from a nefarious army of those seeking to break through their perimeters. Increasingly professional and well-organised, such determined criminals can quickly find new vulnerabilities in older infrastructures and hide in a dormant state. They can find the spots where Frodo's gender has not been changed, and they can exploit this. The altruism of 'open' source code (non-proprietary software that can be modified by any developer) was to make it universally available: security was not the driving force. Your business can be left with a hole in a system that you do not even know exists. Discovery is often too late and the application of a patch to some corrupted software is never a complete answer. Increasingly, the malicious intruder is able to reverse engineer patches to find a gap.

It is a constant cat and mouse game: as soon as your IT teams manage to secure the system, there will be a temporary lull as the attackers reel from the change in tactics. But, within a short cycle of IT upgrading, they will adapt. They will find fresh ways of attacking. It will be an ebb and flow of defence and attack. You must never be lulled into a sense that everything is secure.

It can get worse. Perhaps, as a board member, you make the strategic decision to engage multiple suppliers. This is like having a sequel to The Lord of the Rings written by a completely new author in another language. And so your supply chain becomes another potential weak spot to be targeted by attackers.

■ How can you defend your business?

What do you need to do? As a board leader, you must insist on certain procedures. The starting point is the maintainability of your system, which breaks down into three abilities:

- Your ability to analyse
- Your ability to modify
- Over-arching this, your ability to test.

If you fail to maintain your ability to analyse and to modify software, and you fret about the costs of implementation and protection, your software will become less maintainable and your development processes will become less efficient. This is the danger zone, where cyberattacks can seriously disrupt your business. Maintainability is about your ability to rapidly and effectively respond to a problem.

The big board question: do you keep modifying or start again?

Your board must accept that your organisation will face serious cyber threats. At one time, the number of people using your computer system was restricted to the people you employed. Now, the number of people using your systems has the potential to be the world's connected population. This brings more demand for safety features and new layers of software. This, as we have seen, means more changes and modification. The cybercriminal knows that you need to change and update. Here you must insist on vigilance in your coding teams to prevent the introduction of 'sloppy' code. This is how your business can become vulnerable. Sloppy code is hard to analyse, difficult to change and can actually be impossible to test. You need assurance that your code is structured properly, and free of sloppiness. This gives you more resilience and makes you a harder nut to crack: if you are able to crack down on attackers quickly and consistently, they may choose to move on to an easier target.

> Sloppy code is hard to analyse, difficult to change and can actually be impossible to test.

Your key board question for your technology leader

As a board-level leader you must be clear about what your digital strategy is aiming to achieve. You need to ask two questions:

- How can we make sure the programme does what it should do?
- How do we ensure that it does not do things that it should not do?

A programme must deliver what you requested in your strategic goals, and it should not do anything you did not expect. That sounds a simple concept but it is of paramount importance. This is where testing comes into its own.

You must ask:

- How often are your test programmes being run?
- How well are key processes tested, especially those involving critical customer information?
- How do you manage snow blindness? This is when your team is so close to the problem, that they see the same positive results every time.

You must also consult your chief information security officer (CISO) about the frequency of testing and set in place a policy that deals with liabilities arising from mistakes in coding introduced by third parties.

Your IT leadership should inform you that an effective and efficient test framework (a suite of automated processes that can demonstrate the correctness and completeness of individual units of code, and stress-test them when integrated into a system) has been created, is performing and is being extended and maintained. It is essential that such tests be fully automatic. This is a major part of the maintainability of your systems.

Testing is critically important so you don't lose your customers when a system goes live. If you fail to detect mistakes in the testing phase and your customer feels the impact, then your business has serious problems.

Is it better to start from scratch?

What about beginning with a blank sheet of paper, on which to write another great trilogy? This is not recommended. There is one thing worse than software maintenance, and that's building a new system from scratch. If you have a bunch of old systems and decide to throw them out and make a new integrated system, this is like writing a brand new book. That's a phenomenal undertaking. If you're writing from scratch and there's nothing, then people have to work together to find out what the narrative is all about and how it should be told. You have to do maintenance on the new story. It's actually just like maintenance, but likely to be a hundred times more risky and expensive.

Your call to action

With coding at the heart of most evolving businesses, it is clear that your business should aim to meet—and exceed—industry standards. Here there are softer issues about how you reward your staff to ensure that their work is of high quality. Delays caused by sloppy coding can allow malicious hackers to gain a foothold. You should be thinking about how you balance agility, and the need to get moving on a project, with code quality levels. This is about setting benchmarks for maintainability assurance. You must make the right decisions between using existing and extending open source systems versus your own new code, written by your own people or by third parties.

If you're the business leader, it's your responsibility

Your strategic decision-making as a board has a serious impact on your business when it comes to creating new products. From now on, you need to ask these important questions about maintaining, analysing, changing and testing. All of this can be daunting as a board member with little technical knowledge. You need to find, hire and keep people with the knowledge and ability to respond rapidly when there is a problem, and you have to stop them from producing sloppy code. Otherwise you might find yourself in deep trouble, like a character from *Lord of the Rings.*

8

The CEO is a Serious Source of Cyber Risk. How to Adopt a Zero Trust Security.

ON2IT – Marcel van Eemeren, CEO

- The CEO is increasingly the top target for cyber crooks
- Be digitally aware and protect your business
- Adopt a 'never trust, always verify' approach
- Segmented gateways build a stronger defence

The chief executive officer is a serious source of cyber risk. To defend yourself more effectively, your business must adopt a top-down approach with a 'zero trust' strategy at its heart. Marcel van Eemeren explains.

Why you are a major risk

If you are a CEO in the Benelux, you are in the frontline of selling your services and products. That's your job. And because it's an international task, you are likely to have a big travel budget and need to be connected at all times. Increasingly, your business has accumulated a wealth of data about customers and how they use your products and services. This is precious information that allows you to provide new offerings to meet customer needs. But how do you ensure that those who have access to your data are acting in the best interest of your business? This includes you! While media attention is given to high-profile cyberattacks from nation states or organised criminal gangs, it is your employees and you, the company leader, who can make your business most vulnerable.

Your own people are a danger…

Your employees can unwittingly do damage to your business. Often human curiosity wins over alertness, although a disgruntled employee inside your business might also have malicious intentions. Whether someone is unconsciously reckless or deliberately out to do harm, a data breach has the potential to cause reputational damage to your business and your brand. Furthermore, if it involves your customers' private data, your breach may need to be reported.

… but you are a more serious threat!

Never presume the weakest spot is your employees. Unwittingly, you are now a target for malicious attackers, and their tactics are increasingly sophisticated. Let us assume you are the CEO of a successful worldwide company that has just been launched onto the public market. Satisfied with the IPO, you plan a long trip with your adventure-loving family. You decided on a safari in Africa. The whole family starts Googling, visiting websites in countries that are not so advanced in IT security. Even without entering sensitive data, a simple website visit could mean your family's account is being hacked before their journey starts. When you finally set off on your trip, danger is lurking at Schiphol Airport by way of the free Wi-Fi offered to travellers. Or if you register for a popular newsletter, such as NU.nl, you are also at risk. Many email servers and clients are not set up to handle encrypted messages, and you have not enforced this as a company. Before the flight, you download your email and attachments onto your notebook so you can work on it. After a 12-hour flight, you and your family arrive at their destination where they check if there's an open Wi-Fi hotspot. Your wonderful hotel has a free and open wireless network, which is a digital lifeline.

After a sensational holiday, you arrive home and suddenly start to receive foreign emails. This could be an innocuous hotel bill or a note saying the wildlife photos you took have not come out well and would you prefer a souvenir album with some publicly available pictures. Inadvertently, your son who wants that elusive picture of a lion or a rhino, downloads infected files to the rest of the family. This gives hackers a wide opportunity to infect your notebook and your mobile devices. Your happy holiday thus leads to business danger.

It's a simple point: how do you know if a Wi-Fi connection that you sign on to is legitimate? You don't. It might be free, so it is unlikely to have high levels of security. If your email is not encrypted, then everyone can read it. In the Netherlands, sites such as NU.nl have been shown to harbour malicious viruses that can attack your system.

There is more to consider: your username and password is only required when you are working online. Yet that same username and password is out in the ether, 24 hours a day, 365 days a year. This gives the malicious hacker a lot more time to find and use your email. This can lead to the creation of shadow websites using information gleaned from LinkedIn and Facebook profiles to build shadow profiles. These create bogus email addresses and send out plausible requests for financial information and secret technical know-how. You then receive LinkedIn invites perhaps from unknown but seemingly trustworthy people, or someone impersonating a friend. They send an email with an attachment, which you open. You did not know it contained malware. It is happening now and an increasing number of CEOs have fallen foul of this kind of scam.

So, what should you do? Introducing the principle of zero trust

You must ask whether the adoption of a zero trust strategy will suit your organisation. Zero trust allows only what is needed for any given application to function effectively, and it restricts access to only those who need it for a legitimate business purpose. This can be a difficult concept to introduce when you have previously encouraged a culture of openness and collaboration across systems and processes. As such, it requires careful communication of why this is necessary. It is not simply a matter of imposing zero trust on your organisation. You need to ensure that this does not lead to increased levels of annoyance for your workforce. It is your job as their leader to explain why security of one is security for all—and for their jobs and livelihoods.

The basic premise of zero trust is: 'never trust, always verify.' With zero trust, all network traffic is untrusted. Access is on a need-to-know basis. Zero trust is a key vendor-neutral design philosophy for modern IT security, as identified by Forrester.[1]

One of the features is the creation of an architecture system of segmented gateways as the nucleus of the network. You must insist that individuals—and this includes your board—apply zero trust to their personal data, only sharing data if it is absolutely necessary and using encryption in doing so.

Defending like Dutch dikes

Without becoming too technical, segmenting gateways is similar to the 22,000km network of dikes that act as flood defences for the Netherlands. Each part of the dike network is segmented and categorised in terms of how much can be done to protect the segment. Each segment has a different value, depending on its position. It is about protecting the higher value areas and being willing to surrender less valuable segments in the event of a breach in the infrastructure. Dikes defend against natural forces, while segmented gateways defend against cyberattacks. According to Forrester, there are only two types of data that exist in your organisation: data that someone wants to steal, and everything else.

Your data that is under risk can be logged and categorised as follows:

- Intellectual property
- Personal data
- Financial data
- Process data (from IoT sensors and remote controlled industry systems, also known as SCADA).

Nuclear and toxic data

Within these categories you will have your ‘crown jewels.’ You must decide what these jewels look like. Here there are two levels: so-called nuclear data and toxic data. For example, the hidden recipe for Coca-Cola’s syrup is known only to a tiny group of perhaps five key executives in the Coca-Cola Corporation. These five people don’t tolerate anyone around them—and you don’t want to be around because of the massive litigation potential with hundreds of lawyers guarding that recipe. This formula would be defined as ‘nuclear,’ whereas the financial data might be ‘toxic.’ If financial data is leaked before the announcement to the market, that is a serious breach that will need to be investigated. So, the company will want to safeguard this too, but not as much as the formula. Nuclear is what you cannot afford to lose. Toxic data remains highly significant and it would still be very damaging if it is stolen or released into the public domain, but it is unlikely to destroy the business.

In the pre-digital era, we classified everything as secret, confidential and public. Now, data classification needs to be more granular, starting with exactly what you want to protect. One of the crown jewels might be to say that everything that is a classified as personal and identifiable information will be known as toxic. Then you need to set out your stall accordingly, and you need to find this information and know where it is held.

Network segmentation gateway

In this gateway, a piece of hardware sits at the centre of your network running special software—and it should be part of one platform. This takes all the features and functionality of individual, standalone security products and embeds them into the very fabric of the gateways. This device knows where your crown jewels are stored. It can properly segment the crown jewels in an ultra-secure manner and build state of the art security into your business DNA. It flags whether an unusual request for a substantial money transfer has come from a bogus email account purporting to be the finance director or restrict a dodgy download from your animal-loving son.

Data is not the issue because it is purely a collective of ones and zeros. Data comes to life through an application which makes it viable. You might never know how a data centre with massive inflows and outflows of data operates but your IT team should know how an application works and performs. You should be able to work with all metrics of this application so you can work with a strict policy on each application.

Networks have evolved in an ad hoc, bolt-on way, relying on numerous security devices and controls to protect the network and data. These include firewalls, intrusion prevention systems, web application firewalls, content-filtering gateways, network access control, VPN gateways and other encryption products, all of which has become messy and complex.

A single zero trust platform, where intelligence is automatically consolidated, means more time can be spent focusing on safeguarding your organisation in-depth. This is about only allowing data to pass through the system that is entitled to do so. This can stop up to 98 percent of data entering, allowing you to scrutinise the remaining 2 percent more effectively. This is likely to have definite benefits for your bottom line and profitability while satisfying stricter criterion for the provision of cyber insurance. Zero trust means organisations and society will be a lot more secure from malware infections, data breaches, attacks by hackers with only those who are authorised getting access to the data.

Organisations that are most open and agile to change will be the ones that survive. You need to consider the adoption by your business of zero trust protection. While this is a discussion for your chief information security officer (CISO) and security teams, you need to understand the outcomes. This must be about freeing up your company's time by automating what can be automated, choosing the correct platform and letting your security team focus on security in-depth.

As a CEO, your responsibility increasingly includes an obligation to protect your own data, the data of your business partners, and of your customers alike. Zero trust should be applied to your own technology, whether it is used for business or for pleasure. It means developing an acute awareness of the vulnerabilities that you bring as a CEO. Finally, make your employees aware of the fact that business continuity is their professional responsibility too. Above all, it keeps everyone, including you, in a job.

Works Cited

[1] https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682

Leadership and Security Operations

9

Ensure the Right Blend of Cyber Talent in Your Security Leadership

SecureLink – Peter Mesker, CTO

- Build the best security team you can afford
- Understand there is a skills gap
- Know your appetite for risk
- Find a chief information security officer (CISO) who is business-focused
- Develop a strong team that is a blend of skills

The continuing battle for cybersecurity talent has serious implications for your business. Peter Mesker, CTO, security consultant and co-founder of SecureLink, offers his advice on how to attract—and retain—the best people to help defend your organisation.

If you own or run a business in the Netherlands, Belgium or Luxembourg, you should accept one inescapable fact: cyberattackers are constantly probing your digital defences. But you are not alone, because all organisations around the globe face the same kinds of threats.

I had been the co-founder of SecureLink in Sliedrecht, the Netherlands, working with many significant business customers for more than 20 years, when I had my Eureka moment about cybersecurity. I was witnessing great companies doing all the right things. They were investing in the best available technologies, deployed according to advanced techniques. They were segmenting their infrastructure and reducing their attack surfaces. Yet the number of security incidents was still increasing. How was this happening? This made me look at cybersecurity from a different perspective: my conclusion was we were trying to help businesses that were being continuously compromised.

This constant attack is often difficult for a CEO or their non-technical C-suite colleagues to fully appreciate, but we are operating in the global world, with the internet of things (IoT), where customers want easier access to your goods and services. It means your 'always-on systems' are potentially open to perpetual and malicious attack.

This might be fine if there was a balance between defenders and attackers, but there isn't. So, another issue is that your organisation is likely to have a serious skills gap with an inability to keep pace with evolving methods of cyberattack. A growing number of incidents may well overwhelm your understaffed security teams.

Why you must adopt a platform approach

So, what internal capacity should you be building? The starting point is to ensure you appoint a chief information security officer (CISO) who understands your business, who knows your appetite for risk and how you would like to guard and defend your key customer and business data. This is a board-level appointment so you need to ensure that the CISO has the right credentials and mandates.

Your CISO needs to understand integrated solutions and has the knowledge and skills to work with the board members. And he or she will need a flexible mindset that puts the aims of the organisation first. You should ensure your CISO is familiar with security architectures, such as Gartner's Adaptive Security Architecture[1] model, which is often used when designing solutions and services.

The Gartner model describes four critical competencies of an adaptive protection architecture:

- 'Preventive' describes the set of policies, products and processes that is put in place to prevent a successful attack. The key goal of this category is to raise the bar for attackers by reducing their surface area for attack, and by blocking them and their attack methods before they impact the enterprise.

- 'Detective' capabilities are designed to find attacks that have evaded the preventive category. The key goal of this category is to reduce the dwell time of threats and, thus, the potential damage they can cause. Detection capabilities are critical because the enterprise must assume that it is already compromised.

- 'Retrospective' proficiencies are required to investigate and remediate issues discovered by detective activities (or by outside services), to provide forensic analysis and root cause analysis, and to recommend new preventive measure to avoid future incidents.

- 'Predictive' capabilities enable the security organisation to learn from external events via external monitoring of the hacker underground to proactively anticipate new attack types against the current state of systems and information that it is protecting, and to proactively prioritise and address exposures. This intelligence is then used to feed back into the preventive and detective capabilities, thus closing the loop on the entire process.

This is a very useful framework for your CISO to help classify existing and potential security investments to ensure that there is a balanced approach. As the Chairman or CEO, you need to insist on a regular board-level report from your security teams to determine if security measures are properly deployed and where they might be deficient. I always advise CEOs to think of a 'platform approach' instead of a 'point-solution approach.' Solutions that provide multiple capabilities, natively engineered to work together, are likely to be more strategic than the ones that only fit a single category.

How to attract and retain the right talent

Unless you strike it lucky, you and your board will face a serious challenge in finding the right talent to build and operate your security architecture. The knowledge you need to make an appointment goes beyond a good-looking CV and great interviewing skills. You need to appoint a CISO who can build a proactive team that understands the business imperatives.

Your CISO must build a dynamic blend of

skilled professionals, such as architects, security consultants, project/product engineers, service engineers, security operators, developers, security analysts and forensic specialists. These are all appointments beyond the experience of a mainstream human resources department. And, be aware, there is a serious skills shortage in the Netherlands, Belgium and Luxembourg so you may need to pay a premium to encourage the best people to come to your company and live in your community.

> Successful cybersecurity specialists must be agile, multi-functional, dynamic, flexible, customer focused and informal.

There are four factors when building a team:

1. Attracting talent: This is about creating the right culture to make people want to work for your company. The technically competent millennials have a very different view of the workplace to those who have been in professional employment for much longer. The tone is often set by the CEO or entrepreneurial leadership at the top, but it must pay attention to the needs of the team.

2. Talent development: Once they start work, they will need assistance to get up to speed with your systems, processes and way of working. Again, your CISO must work to create the right cultural environment to keep everyone well informed.

3. Talent integrity: This is about ensuring that your team does the right things for the right reasons. It is about ensuring you don't built a climate of fear and that you deal fairly and truthfully with matters when things go wrong. You need to encourage, reward and acknowledge best practice.

4. Talent blend: This is about team building and allowing talent to flourish and grow. Building a great security team requires collaborative working, often with people who are 'lone wolves.' Good leadership is required to build the right blend.

Frost & Sullivan predicts a global gap of 1.5 million cybersecurity specialists by 2020. The world needs to come up with new ways of schooling and attracting these professionals. So, you need to nurture an environment where these professionals can develop themselves and stay with your business. It becomes a costly exercise trying to fill regular vacancies. You must aim to employ the A-players, who have the mindset, cultural fit and learning capabilities, by offering an appealing work environment and allowing the empowerment of your people.

■ What skills should you look for in your CISO?

First and foremost, the CISO must understand the purpose of the business and how it operates. While your CISO will be comfortable speaking the language of the board, they must have other qualities and softer inter-personal skills. Successful cybersecurity specialists must be agile, multi-functional, dynamic, flexible, customer focused and informal. You should be challenging or validating these characteristics for your CISO:

- Agility—offering security services requires agility. Professionals act like chameleons, shifting quickly and decisively as threat warrants a change in course. And as a unit, they should be alert to new circumstances.
- Multi-functional—security operations is a team sport. A strong cyber practice is built of teams with diverse knowledge sets who can execute a variety of activities at once. Employees do not have to be good multi-taskers, but the overall team must be.
- Inquisitive—cyber professionals embrace learning and should be curious; they want

to solve problems, regardless of how hard it is to find the solution.

- Flexible—the threat landscape changes fast. With constantly changing work requirements, the team must be enabled to adapt to new areas of focus. Security team members embrace a strategy that allows employees to expand or change their roles to increase the capability's flexibility.

- Customer first—your customers' interests are paramount, and increasingly so with new legislation coming down the track. 'Customer first' is about adopting a customer-centric mindset that always asks: 'What would I expect as a customer?'

- Informal—cybersecurity professionals thrive in a non-traditional environment. Team members will likely look for unconventional working hours and shifting duties. Security operations professionals work from diverse locations, have matrixed reporting lines, around-the-clock shifts and a more relaxed dress code than much of the workforce. If you are a formal business leader, you need to get used to this.

According to the Ponemon Institute, breaches go undetected between 98 days (financial organisations) and 197 days (other organisations), and it is most often an external party that notifies you of the breach. Often it comes after your customers' information has been damaged or compromised. It is clear we don't spend enough money and effort on prevention, detection and response.

Conclusion

There is no such thing as perfect security, which means that breaches will happen.

You must work to build the best security team you can afford—or decide to outsource this.

You need integrity and a proper blend of people to create a great team that will do the right things and do them well.

You need a CISO who understands your business and how best to protect it. Your organisation should always retain control of essential services and stay in the lead when it comes to defining and calibrating your security strategy.

Works Cited

1 Gartner, *Designing an Adaptive Security Architecture for Protection From Advanced Attacks*, February 2014, refreshed January 2016

10

Hiring the Next-Generation CISO

Heidrick & Struggles – Chris Bray, Gavin Colman, and Gilles Orringe, Partners

- The chief information security officer (CISO) is an increasingly important board-level role
- The CISO must speak the language of the board
- Reporting structures vary—depending on the type and sector of business
- The CISO needs to fully understand the wider company culture
- Great all-round CISOs remain in short supply

A key figure in your top leadership team is the CISO. How do you find the right CISO for your business?

You are the chairman or chief executive officer, and you're about to conduct an interview to find the best person to protect your business. You've been persuaded that you must add a CISO to your leadership matrix. Yet how do you evaluate the position and the best person for the post?

As corporate businesses have evolved to embrace digital transformation, we've witnessed the C-suite integration of the chief technology officer (CTO), the chief information officer (CIO), the chief operational risk officer (CORO). Now you're told you need a CISO.

What kind of CISO do you need?

- You are looking for someone capable of handling a wider commission across your organisation. A vigilant CISO wields a great deal of power and can close down strategic business processes that have been compromised, without recourse to the chief executive. So you need to be able to trust their judgement implicitly.

- Your CISO must operate in different spheres, depending on the structure of your business. In whatever way the structures are set up, the CISO needs to have an authoritative voice, with his views and recommendations heard and discussed at board level.

- Your CISO will be an individual who understands the conceptual, practical, and actual challenges of cyber risk, and can switch seamlessly from a deeply technical discussion to a more business orientated one.

- Your CISO must be sensitive to your organisation's unique culture. Many institutions believe that resolving security issues is about building the highest walls of a cyber citadel, yet the threats often come from underneath and within. Here your CISO must be diplomatic and create the culture and processes within an organisation that fundamentally address the security issues. Stolen log-ins, user accounts hacked, credit card fraud, internal emails about contracts, have all shown that security can be easily breached. If staff are behaving in a contradictory and inappropriate way, then increasingly technological barriers will flag up such patterns. Internal processes need to be sensitively and delicately handled to ensure that employees don't feel they are being spied upon.

- Your CISO's job is to communicate regularly and determinedly with the board. His role—and there are still far too few women candidates—is about ensuring the board is asking the right questions and then helping them process the answers. While it is the board's job to set the business strategy, they will need the CISO's guidance when it comes to cyber risk.

- Your CISO needs to make strong friends outside the business. The job extends beyond the board by contributing to a broader, non-competitive community, which will involve government, trade bodies, regulatory authorities, intelligence agencies, and might well involve working alongside commercial competitors. Your CISO should become part of this collaborative defensive community, including Interpol, Scotland Yard, the Ministry of Defence, GCHQ, and specialist industry bodies that can share information and protect business and other entities against sophisticated attacks.

- Your CISO needs the emotional intelligence to be a skilled influencer and a persuader. It is unlikely to be a position for an introvert technology geek, no matter how smart he might be.

- The CISO needs to know what management is thinking. A board's fiduciary duty is to do everything it can to protect itself from attack. Anything that is going to jeopardise the business is going to harm shareholder value and stakeholder interest. Every major FTSE board is regularly examining its position on cybersecurity and physical security, with the CISO expected to define and report on the principal challenges.

- Your CISO needs to show that he has raised the risks with you and that you have understood them. The recurring questions to ask your CISO are: 'Are we secure? And how do we know we are secure?'

Where is the talent?

This exponential rise in security challenges has taken many boards by surprise. The pace of this change means that leadership talent is struggling to keep up. In the CISO space, candidates will have grown their careers with one component part of a wider picture. So finding talent with the requisite five or six component parts is extremely difficult.

While the new breed is emerging from the intelligence, security, and law enforcement service community, including high-level candidates in the Ministry of Defence, MI5, MI6, or GCHQ, it should be understood that there is also a cohort from the global mobile and telecom infrastructure sector and network security in hardware and software firms.

However, many potential CISOs fall short on strategic commercial business experience, and have a lack of knowledge in working collaboratively with external bodies. As a specialist, your preferred CISO will have moved across sectors gaining different business experiences.

> Typically, what drives your CISO is the challenge, and the ability to make a significant mark, perhaps by setting standards in a new industry.

Your CISO is likely to be unassuming, highly attuned to people's behaviour patterns and values, and well connected. The ideal, well-rounded CISO has been emerging from the United States, particularly from Silicon Valley. They are highly educated, discreet and capable of influencing, and commercially astute. Here the difficulty for European organisations is prising these prime Americans to move to London, Paris, Amsterdam, or Berlin. There is a tiny pool of qualified people, and they are in big demand.

If you can't find one who fits, specialist consultants are increasingly being deployed to undertake strategic projects, which involve putting the right metrics and processes in place, so that, when completed, they can be handed over to an operational, in-house team. You need to decide if this is the board's preferred option.

Pay scales are reflecting the scarcity in California, where a CISO in a top Silicon Valley outfit can command up to $2 million a year, plus benefits and bonuses. While remuneration for the CISO is high on the agenda, it is not necessarily the main reason. Typically, what drives your CISO is the challenge, and the ability to make a significant mark, perhaps by setting standards in a new industry. They need to be resilient, so they are not deterred by being rebuffed. What differentiates the best CISOs is the motivation and passion for their work.

The CISO must have business interests at heart

The CISO position is now widely recognised—but they must understand the objectives of making a return for investors. An effective CISO is not expected to apply more controls and barriers across an organisation. They need to be acutely commercially focused and able to assess where security spending on controls is unnecessary. Many companies have shied away from publicly commenting or reporting about security breaches. Stupid things do happen: a manager walking out with a laptop with sensitive files and leaving it in a taxi shouldn't happen, but it does. Legislation is changing too. For example, when it comes to critical national infrastructure, there is a pool of organisations, such as the government, utilities, mobile phone companies, airports, and air traffic control, that would prefer not to talk openly about risks. They don't want to put off stakeholders or scare the wider community, but increasingly they will be legally expected to disclose cyberattacks. It requires a CISO who is calm and measured in the heat of demands for a response. It requires proper procedures that the board have noted and approved.

In conclusion

This is not a technology discussion, it is a business one. The effective CISO needs to be business-centric—he or she is a polished and sophisticated communicator able to influence both internal and external stakeholders. But there should be no illusions about this new breed. A robust and fully fledged CISO is still difficult to find.

11

The Value of Your CISO: Responsibilities and Metrics

IBM Security – Alan Jenkins, Associate Partner, and Palo Alto Networks – Greg Day, Vice President and Regional Chief Security Officer, EMEA

- Technology leaders can be deal-makers or deal-breakers
- Companies are at different stages of cyber maturity
- It can be daunting to find the right chief information security officer (CISO) for your business
- Leading indicators are a better measure than lagging ones
- Cyber drills and testing help build leading indicators

How do you measure cybersecurity effectively and ensure your CISO is up to the job?

Your chairman is in advanced negotiations about making a significant acquisition. The target is a high-growth social media darling with what appears to be smart new technology. It's a massive step up. Your finance director and the head of legal have done their due diligence. They like the numbers and the intellectual assets. The director of marketing is certain it will help sales rocket. Then the CISO comes out of the deal data room and says: 'Hold it, folks! Don't touch this company with a bargepole, it's a cybersecurity nightmare!'

This is a litmus test for today's companies. How much store do you place on your technology chief's assessment of a strategic commercial decision? Furthermore, is a (probably not technically savvy) board able to measure the success of the cybersecurity your CISO has put in place? In the above case, the CISO has found that the ownership of the customer data is dubious; the software system is riddled with flaws, and the cost of fixing the target's legacy infrastructure might be more than the cost of purchasing the firm.

Do you take his/her advice—or press on? And then expect the CIO/CISO and their teams to fix it after the purchase? In today's reality, your CISO is right to flag the issues. But having been in a similar situation working with a FTSE 100 board, the solution was to flag the underlying risks without stopping the acquisition, thus allowing the board to make the purchase. And then insisting on operating the new business at arm's length until the technology team could move in and clean up the new business unit's IT infrastructure. Only then would we consider making any kind of integration. This increased the acquisition price substantially, but the board accepted it as a necessary cost. This is highly unusual. Does your own board have this kind of discussion?

When considering your metrics, decide on the level of cyber leadership you require

Companies are all at different stages on their journey. Some are more mature in their cyber understanding than others—and requirements vary dramatically. This leads you to ask two fundamental questions:

- What level of CISO will be acceptable and good enough for our business and to our stakeholders?
- Do we require someone who can help with M&As and other strategic business issues—or do you simply want a technical expert?

Your board must decide on the level of security that it needs. This will depend on the technology you use and the regulatory environment you are operating in. This will determine the level of the CISO you engage. When you appoint your first board-level CISO, expect him or her to unearth cyber risks within the business of which your board was previously unaware. At this stage, doing nothing is not an option. Your board must act.

How can you be sure that your CISO is good enough to sit on your board? One measure of success has been how effectively they have been able to respond to a crisis. Yet your board will need comfort about this vital appointment long before the firestorm of a crisis—and you don't want to find them wanting during the first critical stages of the crisis.

Key indicators to measure your cybersecurity

There are a series of key indicators to measure your cybersecurity, but they don't all sit comfortably with the cycle of the business. Commonly, these are 'lagging indicators,' showing events after the fact through the rear-view mirror. Typically, such indicators are captured on a security dashboard with a red, amber, green traffic-light display on how many systems are antivirus protected, numbers of patches deployed, and malware disrupted. Most of these volume-based statistics are in the past tense, with indicators measuring the 'what happened' rather than the 'how it/they affected the business.' For example, your systems have all been patched within an agreed timescale: this might be a positive. However, you must also ask how this is aligned with the risks to the business. Too many report on the number of antivirus systems in place or secure passwords checked rather than the likelihood and impact of an attack on the business.

It is more helpful to have 'leading indicators.' Here, this may be a struggle for your board, which strives to see life in a predictable manner based on past performance; it will need to embrace the unpredictability of cybersecurity and (often) the pure randomness of whether you were hit by a 'bad' attack or managed to avoid it. Leading indicators are infuriatingly difficult for the board to quantify. This has much to do with the cyberthreat timescale being remarkably short. With traditional business activity, devising a new product, ramping up production, and taking it to market is normally a 12-month cycle at least. Yet it does not take six months for a malicious attacker to find your weaknesses and try to get into your system. This is a different dynamic for the board to appreciate because they are not used to this rapid timescale of change.

The business-orientated CISO will appreciate that they do not seek to make major changes on a financial system at the end of the month, and they don't ask for more funding for technology projects in the third and/or final quarter. However, this is the time to be requesting budget for the following fiscal year. Correspondingly, the IT security team need to understand when they can undertake routine change windows within the business dynamic and when the business risk justifies an exceptional change request.

An effective, modern CISO will articulate to the board why he is regularly requesting investment to manage risk and to keep pace with the changing threat-scape, to build and maintain resilience in your system—but no one can ever give a 100 percent cast-iron guarantee of security. Here, the leading indicators will focus on how the cyber team responds to events and minimises the disruption to the business by getting systems up and running after a reasonable outage period. It will also be about how your defences have been modelled and the gaming that has gone on across the business.

The mantra *'when the going gets tough, the tough get going'* applies, meaning that the responders are not going away from the problem but heading right into it. If a fire breaks out, most people run away. With a cybersecurity attack, you need the team running towards the 'fire' and sticking with it until the danger is contained, controlled, and eventually closed down. Here, leadership plays its part because you see who comes into their own: and they are not always the people you might expect!

One of the leading indicators here is the time it takes to resolve a crisis or an attack. You might have a breach into a critical system, but if you stop it in a timely manner, then the damage to the business is limited and manageable. Alternately, there might be a low-risk attack in the business that has gone undetected for years: then the long-term commercial impact can be very high. After such incidents, a lagging indicator is about validating whether detection and clean-up was done within the timescales and risk agreed within the business. However, to make it a leading indicator, you can now use this to run proactive drills and exercises, whether internally or, as in the UK, using a third party to run a CBEST test, as set up by the Bank of England to test cyberthreat vulnerability to known attack vectors.

> Undertaking actual cyber drills is more visceral and helps people at all levels of the business understand that they all have a part to play.

Here the importance of 'fire drills'—whether company-wide or restricted to certain key domains—can be a critical part of measuring your cybersecurity readiness. This kind of cyber drill or gaming should include the board-level public spokesperson in the event of a breach, supported by your legal and HR teams. Such mock exercises can do much to ensure the business is capable of responding to a full-scale crisis. It helps remove the jargon and replace it with language that the business understands. It is the equivalent of actually using a fire extinguisher to put out a fire, rather than ticking the box that it is on a wall bracket. Undertaking actual cyber drills is more visceral and helps people at all levels of the business understand that they all have a part to play. This gives a leading indicator to the board about how effective the cybersecurity measures are. This can then be used to assess the commercial value of doing it better next time.

With this information, the board can then ask: 'Are we getting better? Is the time from breach to detection getting shorter? Are we getting better at rolling out patches? Are we more secure?'

You are also able to measure your crisis management capability more clearly through gaming it. Has everyone involved rehearsed their public response and shown they understand the broader issues? And have you exercised your crisis management plan within your business continuity strategy, or is it still gathering dust on the shelf? You need to ensure the details, such as contact information, are up to date in case of a cyber breach.

There is no guarantee of success

You can throw money at the best technology and be undone by someone inside your firm clicking on a Trojan link within an email. This is not an excuse for failure, merely a statement of reality: there is no guarantee of success with security. Your board is looking for surety from its security leadership. Yet often, the first head to roll in the event of a breach is that of the CISO or head of IT security because there was an (unrealistic) expectation that they would stop ***all*** breaches. This is counter-intuitive. A board that has been through one breach and come out the other side is often better placed because it realises it did not do enough as a board. There is never a 'bad' example of a response to a cyberattack because we are all learning lessons from this. From a governance perspective, cybersecurity should be not the sole responsibility of the CISO but that of the whole of your organisation; that is what underpins the concept of 'Three Lines of Defence.' He or she is the executive leader and project owner, spanning the whole of the business. We learn from our mistakes—and it is almost sacrilegious to kick out your CISO, unless they have been shown to be truly negligent or criminal. Use that experience to improve your defences for the next time—because there surely will be a 'next time'!

12

Ensuring Security Operations are More Accountable in Your Organisation

Rabobank – Kelvin Rorive, Delivery Manager Security IT Threat Management

- Ensure you know what the 'normal' state of operations is
- In event of alarm, do your first triage internally
- Automate as much of your incident response as possible
- Present all security events in a simple visual way to the board

As a CEO, how can you make sure your security operations are working effectively to protect your organisation? Kelvin Rorive, who heads the IT security threat management team at Rabobank, offers some pointers for board leaders to follow.

A doctor monitoring a sick patient in hospital knows what normal health should look like. Checking the vital signs of heartbeat, blood pressure and oxygen levels gives a picture of a patient's condition. Any deviation from the norm indicates stress on the patient.

It is a similar position running the cyber defence centre (CDC) of Rabobank in the Netherlands, which is more widely known as a security operations centre (SOC). Like any other business, protecting our IT systems is an integral part of supporting and serving our customers. Our Security operations centre is constantly monitoring the health of our business, looking for any signs of deviations, then quickly moving to deal with any threats and challenges. The well-being of the business and our customers is central to everything we do. A SOC team must try and prevent or lower the impact of any operational security risks.

But how can a CEO be assured that their SOC is effective and doing the right job? The board leadership cannot simply leave this to chance, or to the 'geeks and boffins' in the

IT department. They must have channels and procedures in place to appreciate and evaluate what is going on.

Why do you need a SOC?

The SOC is the last line of defence of all your preventive security measures such as firewalls, virus scanners and so on. A typical SOC is the eyes and ears and should see everything that is happening across the IT systems. Firstly, your organisation needs to decide what is 'normal' and what behavioural patterns you expect to see. From this you can deduce what is abnormal. In the past, monitoring was based on detecting malicious patterns. Now the variety is too high, so monitoring has switched to anomaly detection. The main goal is to minimise or prevent the impact of a cyberattack on your organisation. This means protecting financial information and transactional or customer data.

> Don't expect your SOC to catch all the missed attacks at last line of defence. This is not an excuse, it's a reality your board needs to accept.

What does the CEO need to know?

Every hour of the day we see a host of things that are abnormal and so we need to prioritise. We cannot mitigate against all the cyber issues that we come across. We also require colleagues from across the bank to work together on cybersecurity. From this, the CEO and the boardroom colleagues need to know the consequences of the most serious cyberattacks. We do this by understanding our operational environment well. This starts with our network systems but also goes down to application level. This is not simply about understanding technology because we also need to understand the bank's core business. Your SOC needs to know what type and variety of applications are being used and the risks when those systems are compromised by hackers. You need to have in place a red light system to inform your board when there is a heightened risk. A red light is raised, for example, when a data theft is discovered which includes the personal information of customers. The threat is then escalated upwards so that the CEO is aware of the most serious threats.

As an international bank operating around the clock in every time zone and in many countries, we need to be vigilant 365 days of the year and this means we operate security operations 24 hours a day, seven days a week. The SOC is staffed during office hours. Outside office hours we run standby in cooperation with the control room. Our control room in the Netherlands is active 24 hours a day, seven days a week overseeing the critical business applications for the bank worldwide. The control room monitors critical security processes outside office hours, performs the triage and informs the SOC in case of a security incident. Together we can guarantee 24/7 monitoring of our systems.

The importance of triage

Triage emerged from battlefield medics as a way of identifying life-threatening cases and dealing with them more quickly. It involves making an assessment of a situation and then quickly escalating a response depending on the scale and potential damage of an attack. Within Rabobank, we are capable of doing our first triage internally within our SOC. By applying triage, we are capable of rapidly prioritising an event, enabling us to focus on the highest risk for the bank. Our SOC is deeply embedded into the bank's business and this helps in doing the triage more accurately.

However, a separate discussion for your board is whether to run the SOC internally or whether it can be outsourced. We undertook thorough research which showed that outsourcing this critical function was more expensive than undertaking it on our own. It also gives us more flexibility when acting on new threats because adjusting threat monitors can be done very quickly. With a security-as-a-service, there are far more formal agreements on what to deliver and not, and any additions or changes to the agreed service requires negotiations, additional costs and time to process. However, it should be recognised that not all organisations have the ability to build their own SOC. Again, this is a decision for the CEO to understand.

Using your early warning spotters

Ensure you have a well-motivated team of early warning spotters. Our threat intel team, called the cyber security incident response team (CSIRT), which works independently of the SOC, is continually searching all kinds of sources in the 'wild' for signals, up-coming trends and types of malicious code. Their role is to be predictive about what threats we are likely to face. We also need to follow what is happening externally in other spheres, so when we hear of an Eastern European or North American bank under attack, we need to understand the mitigating issues to our institution. If there is a new hacker campaign emerging, the CSIRT then provides the SOC with prompt and reliable information about how this might impact the business. This allows us to prepare our defences.

Based on your own triage experience, you can work out whether this is a new attack or something that you have not seen and dealt with before. If this is the case, you can escalate this to your A-team of fire-fighters.

As a CEO, you need to be aware of the number and the status of critical 'security incidents' in your organisation. You also need to have a classification of all systems. At Rabobank, this is registered in our asset management system and this allows us to act faster, giving us the ability to give events higher priorities. At the highest level, this is about promoting the attack to the level of a 'security incident' which means an immediate follow up to mitigate the risk and prevent any impact as much as possible. We cherish our team's expertise and knowledge. This is where they earn their pay, keeping our organisation safe. If we see something and don't know what it is, we need to figure it out from all kinds of sources through thorough investigation. Once resolved, we can then retune our security monitoring sensors to prevent this type of event next time.

You must automate as much as possible

Automation is the key for our organisation. If there are any repeating actions, then these can be automated by our security engineers. This give us a lot of head-room and space for security analysts to do the interesting work that really matters. Typically, our organisation will see 2,500 suspicious aggregated 'events' per month out of the billions of logged entries that attract attention on our IT infrastructure. And 85 percent of our security responses to these events are automated in a follow-up. Here, this is purely on an infrastructural level and not financial transactions where another department in the bank has the task of verification of financial accounts. Other organisations may opt to integrate these two functions, which again is something for the CEO to discuss with the board.

How to keep the board up to speed

How do we ensure that the board understands what is being done to keep our business in good cyber health? As a CEO, you should expect an integrated report of all the IT threats. In our case, it is a never too technical but involves two to three colour-coded slides to inform the board about our status and performance levels. This is on an abstract level indicating whether there is an increase, for instance, in malware levels or distributed denial of service (DDoS) attacks. Every incident that is picked up is scored on a 1-5 grading (with 5 the greatest threat). We calculate the number based on what would happen if we were unable to pick up this threat, and then we score its threat level now that it has been spotted and dealt with by the centre. We call this the security indicator. This shows the effectiveness and added value of the SOC.

This should give the board a sense of comfort that there is an active structure in place. Every quarter the security statistics are included in board reports and every month the management report shows how many viruses have been cleaned and how many DDoS have gone on, along with the aggregated impact on the organisation. By showing this in a more visualised overview, the board, who are seldom IT experts, can gain a broad picture of developments.

What the CEO needs to consider when setting up a SOC:

- Start small. Too many SOCs are scaled up too quickly and given too much responsibility.

- Do things well or not at all. When building security operations, get your CISO to focus the team on doing one thing exceptionally well. If it is a small team, it should be able to demonstrate the added value to your board very quickly.

- No-one sees everything. Don't expect your SOC to catch all the missed attacks at last line of defence. This is not an excuse, it's a reality your board needs to accept.

- As your SOC matures it will move to a higher level of security. Encourage maturity so your team can automate as much as possible to keep your engineers working on real security problems and enhancing security.

- In a scarce job market, maintaining the best technical staff is important as you build your top-level SOC. So keep the team motivated. You have a highly skilled group of people working in a complex environment. You need to ensure they have a level of challenge commensurate to their experience. This helps them stay longer, enjoy their work and keep your business as secure from attack as possible.

Outsourcing and Moving to the Cloud

13

To Outsource, or not To Outsource? That is the Question.

Proximus – Christophe Crous, Head of Cyber Security Solutions

- For most organisations, outsourcing security is an option worth considering
- You must ensure that a managed security service provider has state of the art systems
- Don’t outsource all your security: keep a chief information security (CISO) on board

To outsource, or not to outsource? That is the question. Christophe Crous, head of cyber security solutions at Proximus, sets out the pros and cons of asking a managed security partner to help your organisation.

Your board regularly sanctions significant sums to be spent on securing your business data and IT systems. But have your board members debated the issue of whether this should all be done in-house or whether to hire a specialist security provider to look after your business? It’s a crucial question to ensure the well-being of your organisation. This need not be a long and drawn-out discussion but it is well worth having and recording your decision-making.

Start your discussion by setting out an inventory of your risks and defining the best way to mitigate those risks. The key question is, can this mitigation be done by your existing in-house teams or is it more efficient to outsource to a third party?

If you choose the in-house option, you must maintain the high levels of skill and competencies of your IT staff and, with an acute dearth of talent, it is difficult to ensure you will hold on to the key people that you require. Even average IT operatives are being poached these days. Outsourcing security operations to a managed security service provider (MSSP) might well be a feasible option, especially for small and medium businesses, although it is increasingly a preferred route for large enterprises too.

What are the advantages? Unless you can afford a top-level, well-staffed cybersecurity operation, it is practically impossible to keep up with the cyber threats your business is facing these days. Outsourcing your security operations can add value and it may also be more economical. One Dutch SME worked out the capital expenditure for an in-house state of the art system was running at €250,000 per annum, whereas the subscription fees for outsourcing were around €125,000. Moreover, there were different price points depending on levels of security. The probability is that your business could save money by engaging a reputable MSSP. The reason it may be cheaper is the costs are spread out and shared across the MSSP's clients rather than you employing a full-time team.

So how do MSSPs work? Some providers route all your traffic through their data centres to assure its safety. Others place hardware in your network for monitoring and analysis, while others combine a bit of both in a hybrid approach. Considering the maturity of the cybersecurity business, it is likely that an MSSP can add value to your business in more than one field. For instance, you might not get the same results out of 24/7 network monitoring as an MSSP does, because these companies gather a wealth of threat intelligence and have the expertise to analyse anomalies in your traffic. When it comes to forensics, it is generally much cheaper to have a professional from an MSSP come over than to keep one on the payroll. This might well apply to other labour-intensive IT tasks such as patching breaches and firewall management.

What are the drawbacks of outsourcing?

It is a big step to outsource your crown jewels, particularly if your organisation has taken care of its own security since its inception. Letting a third-party step in and manage your network and applications carries a risk of losing control over your data. Also, it might be harder to keep track of regulation and compliance in the different jurisdictions where your company operates. More than this, there is an emotional aspect: outsourcing cybersecurity might well leave your IT people with a deep sense of insecurity and vulnerability. Even if this unwarranted, it does not bode well if your organisation is trying to build a high level of trust and cooperation with this new service provider partnership.

Outsourcing organisations, especially those with departments overseas, can struggle to have the local business knowledge, so beware of added costs or a reduction in levels of security if the collaboration is not right. Your IT team and the outsourced partner must communicate regularly and act together as one team, working to protect your business.

Be cautious when shopping for providers

While there are obvious risks involved in outsourcing security management, the benefits generally outweigh the possible advantages of maintaining an in-house team. You can mitigate risks by conducting rigorous research and checks when selecting your service providers. Be thorough.

- Let your CISO and legal department check the service level agreement. A service level agreement should be a commitment to service, not something to hide behind.

- Ensure your confidentiality agreement covers who will have access to your data.

- Be clear about where your data is being stored and who is handling it. This is increasingly important as EU regulations over GDPR come into effect.

- You need to be satisfied with the kind of encryption that the MSSP would use to protect your data.

- What are the clear processes in the event of an outage?

- When can you reasonably expect to be back online? It is worth asking how the

MSSP has handled any previous data breaches, if they have occurred, and what lessons they have learned.

- Check out the MSSP's reputation by asking qualified peers and reading reviews from reputable sources.

The cybersecurity industry is still evolving and there is a host of established providers that are highly experienced in keeping networks, applications and data flows safe. The range and complexity of the services you choose to deploy depends on your industry. For example, a finance house, which is heavily regulated, may require higher levels of security and therefore use an MSSP with specialist levels of compliance. The MSSP you select will be expected to know your industry well and how it operates—although they should be able to bring the benefit of diverse knowledge from a range of industries. A good MSSP employs well-motivated security professionals from different backgrounds and industries to keep up with the ever-evolving cyber threats. They will be sharing threat intelligence and information with other like-minded professionals in the industry and governments, to the benefit of society.

The technology of an MSSP is only part of the service. While artificial intelligence (AI) and machine learning makes significant inroads in cybersecurity operations, notably in the detection of anomalies in data traffic, there is still an important human factor. Security personnel must prevent, detect and report attacks, as well as repair possible damage. Given the increasing volume and sophistication of attacks, these four major tasks can be hard to run in-house. An MSSP can provides 24/7 support with short response times. You are buying professional know-how and intellectual insight.

A reputable MSSP should have extensive knowledge of compliance with data and privacy regulation in the territories where you operate. As a board director, your main concern must be about accountability and who is ultimately responsible for the data and information. Remember, in the event of an incident, you are still responsible for the integrity of your company and customers' data.

You will require a senior person in your business, usually a CISO, to oversee the MSSP's performance and report directly to your board of directors. Even if you outsource most of your security, it is impossible to outsource accountability. Your company needs an executive to design and oversee cybersecurity strategy, help select the MSSP that best suits your specific needs, and take care of governance once the contract is signed. The CISO regularly liaises with the service provider, giving your board peace of mind while, at the same time, acting as a conduit between your internal IT function and the MSSP.

Conclusion

Cybersecurity is a specialised field in the IT industry. Maintaining your own fully-staffed security operations centre can be expensive and carries the risk of overlooking threats and breaches. Increasingly, we live in a hybrid world with often multiple partners engaged in different parts of IT and cybersecurity management. Because of their scale, a dedicated service provider can play a strategic part in your organisation's safety. By outsourcing selected parts of your cybersecurity, your IT organisation can focus on running daily IT operations and accommodate new demands from the business. So, unless your organisation is very large and specialised—the financial industry comes to mind—and you can afford to keep a large, dedicated cybersecurity team on your payroll and run a dedicated service centre, it may make sense to consider outsourcing your security operations.

14

How to Become a Cloud-First Champion. The Stepping Stone to Success.

Cloud Security Alliance – J.R. Santos, Executive Vice President Research, Ryan Bergsma, Research Analyst

- You need to be a cloud champion in your executive team
- Decide on your cloud model
- Build the best team to deal with cloud
- Remember, you are still responsible for your data
- Make sure your legal team reviews cloud contracts

How do you become an informed cloud champion for your business? J.R. Santos and Ryan Bergsma of the Cloud Security Alliance offer some guidance for CEOs.

Your executive team has made the strategic decision to move to the cloud. Now comes the tricky part. Your journey to the cloud introduces many unknown factors and a multitude of new decisions, including which applications, data—and precious customer information—belong in the cloud. Yet your knowledge is limited and you have little spare time to immerse yourself in this vast topic.

So how do you become the most effective cloud champion for your own business? For many organisations, the adoption of a 'cloud-first' strategy begins with an elaborate and sometimes complex series of business and technology decisions. There is a lot to understand and it is not a minor decision that can be taken lightly or simply delegated to someone further down the chain of command. Yet few people on the executive team have time to understand and weigh-up the various software-as-a-service (SaaS), platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offerings. Even for the most technologically literate, it can be a monumental task. It can be hard to know where to begin but your business requires a 'cloud champion' at board level.

Why do it then?

The benefits of cloud computing are now generally understood at a high level. What is not necessarily clear are the details of the potential security, legal, financial and compliance impacts that cloud adoption will produce. As the CEO, you and the executive team are responsible for these areas but are unlikely to be sufficiently familiar with how a cloud-first strategy affects your roles and functions. While your organisation is still responsible for ensuring that all its obligations are met, the cloud changes the nature of risks, roles and responsibilities and how everyone within the organisation manages them. You must encourage everyone to see cloud computing as a shared responsibility between the organisation and the provider. Whether your board decides to move most or all of its infrastructure to the cloud, or starts with just a few SaaS applications, cloud-first is the beginning of a process of assessments and decisions that you will need to understand at a higher level.

You need to identify the business drivers

Your first step is to identify the specific business challenges that need to be addressed. As the cloud champion, you are mandating or authorising a cloud-first strategy. So you will play a significant role in specifying the motivations and expectations behind the cloud-first directive. You must then look at specific requests from individual business groups through the cloud-first lens. Your business needs to appreciate the difference between a deployment and a service model. For example, any of these service models (IaaS, PaaS and SaaS) can reside on any of these deployment models (public, private, hybrid, community). It is not correct to refer only to PaaS and IaaS as public cloud.

Be warned: the further you go into the process, the more you are likely to become distracted and dazzled by the sheer quantity and versatility of all the cloud service models and deployment models that are available. Business best practices dictate that you start with a small project that offers a quick return, so you can build on early success. It is also suggested that the process you follow be documented in a manner that makes it repeatable and consistent as your cloud-first initiative takes hold.

Who do you need on your team?

As the cloud champion, you are not expected to know it all. Gathering the right people to embark on this collaborative journey is perhaps your most important role in creating and implementing a successful strategy. Remember, even when responsibilities and data have been shifted to the cloud service provider—which will vary according to the SaaS, PaaS or IaaS model that you choose—it is you, as the CEO or senior executive, who will ultimately bear the consequences of any failures that damage your organisation. Pick people who are competent and who you can trust.

As cloud champion, you and your team need to identify and establish the business drivers for implementing a cloud strategy. Your team should include the:

- Cloud lead, who is tasked with managing the cloud decision-making process.
- Cloud strategist, if your organisation does not already have experience in cloud adoption, it will be important to consult or hire a person with the necessary expertise.

Your team needs to include legal, governance, risk and compliance (GRC), finance, vendor management, information security and information technology.

What cloud model do you adopt?

One of the key decisions you will need to make is ‘buy (find it as an already existing service from a provider) versus build (develop the required service in house).’ The buy versus build decision-making process is well known but when it comes to cloud services, you’ll need to expand your research to understand how the respective vendors will treat your data, what steps are taken to provide security, how many security certifications do they hold and what recourse do you have if a security incident occurs. Ultimately, over time, most organisations may find themselves utilising a mix of service models and deployment models.

> As the cloud champion, you are not expected to know it all. Gathering the right people to embark on this collaborative journey is perhaps your most important role in creating and implementing a successful strategy.

Keep your key business objectives

You need to ensure key business objectives are kept in focus. Your cloud lead must organise the stakeholders to document a complete set of the security, compliance, legal, contractual, financial and other business requirements that are relevant to the specific initiative. Providing effective guidance may require the cloud lead to educate your teams on their changing roles and ensure they understand and meet their responsibilities.

Your governance model needs to describe:

- Who makes the decisions?
- How are the decisions being made?
- How does the business evaluate the results of decisions over time?
- Has your board sufficient oversight?

Assessing the cloud service providers' controls

During this phase, your team must take full responsibility for verifying all controls required by the business. You must protect your client and customer information at all times. Your security team will work with the cloud service providers to validate that all security controls are appropriate and correctly implemented.

It is very important that there is clear identification of your responsibility and your cloud service providers' responsibility when it comes to security controls (this is discussed in more detail in Attila Narin's chapter). In all cases, your organisation is responsible for the security of the data, an important fact that should never be minimised.

Launch

Once you have made a decision about which models to use, the cloud-first effort does not stop there. With due diligence and planning complete and designed architecture in place, it is now time to go live and make the cloud accessible to all the approved business units initiated in the process.

Monitor

Moving to a cloud-first strategy is just the beginning. Each member of your team will be responsible for contributing to the optimisation of your cloud-first strategy through continued measurement and feedback. As part of managing the cloud service provider relationship, vendor management should conduct regular/quarterly meetings with the provider to review the quality of service and adherence to the contract. There should also be periodic auditing to assess if the cloud service provider is still the best fit for your needs.

Make sure your legal team is reviewing the contract to assess if the cloud service provider continues to meet its contractual obligations or if any penalties or service credits should be invoked.

Protection against cyber threats

Never lose sight of the fact that, unless a contract is in place that specifies otherwise, the responsibility for protecting your data is solely yours, regardless of whether you are relying on a service provider or your own development effort built on your deployment model of choice. Your provider will profess that 'their data centre infrastructures are more secure,' which is very likely to be true. But a shared security model could mean they protect the underlying infrastructure, you protect the data. Be certain that it is well known and well documented where, and with whom, responsibilities lie.

Malicious attackers do not care where their target is located. Their goal is to gain access to your network, navigate to a target, be it personal data or intellectual property, then execute their end goal—regardless of the location. From this perspective, any way your business relies on cloud service can be considered an extension of the company and the steps to protect cloud based assets should be no different than those you take to protect any other company assets. Your team must take the time to fully understand what native security features are available.

Responding to any incidents

Whenever anomalous behaviour is detected, your response plan must be initiated. For many incidents that arise, a response plan may already be in place and it will be critical to initiate execution as soon as the incident is fully understood. For any unforeseen incidents, it is important to document the response to facilitate a more rapid response to that type of incident in the future.

Conclusion

Moving to a cloud-first strategy is not a single event. It is a permanent shift in how your organisation implements its business processes. While most enterprises already have some presence in the cloud, many have made these moves without a clear process to ensure that critical business interests are protected.

The decisions you make today will have lasting consequences for how the organisation meets its legal and compliance requirements, SLAs, financial targets and other business imperatives. In fact, as your cloud adoption increases, the outcomes of a cloud-first strategy will have an even larger impact on the business in terms of efficiency and agility. Ultimately, most organisations will find their unique business will require unique mixes that balance SaaS, PaaS and IaaS solutions over specific public, private, community or hybrid deployments.

Introducing a clear process early in your cloud maturity provides the opportunity to ensure positive outcomes for your business. By engaging the right stakeholders at the right time, you will be able to create secure, efficient and productive cloud initiatives that will support growth and success long into the future.

15

How to Stay Safe on the Public Cloud

Palo Alto Networks – Attila Narin, CTO, EMEA

- Security in the cloud is now proven
- Companies of all sizes are using cloud services
- Your organisation must embrace the shared security model
- You need to understand which additional security solutions your business requires
- Many mission—critical and regulated/compliant workloads run in the cloud

Your organisation can make the most of public cloud security by ensuring you adopt an approach of 'shared responsibility.' Attila Narin, the VP of systems engineering, the CTO of Palo Alto Networks for EMEA, and the former head of solutions architecture and business development at Amazon Web Services, explains.

As a business leader, you will be acutely aware that the cloud is the most significant technological shift in the last 20 years. The adoption of the public cloud across organisations of every size has transformational benefits on dozens of industries and on our wider society. But how well do you understand the underlying impact and, more significantly, your own board-level responsibilities?

In almost every case, your organisation is already using the cloud. Consider that your marketing team might well be running a next-generation sales campaign from the cloud, using the likes of Salesforce.com and other cloud-based applications; or your on-the-move staff are sharing documents with Box, bypassing your IT leaders who were once the gatekeepers of all things technology; or your development team is using agile methodologies of developing, testing and deploying a growing number of systems in the public cloud while embracing DevOps. These initiatives have a common goal of improving the business but introduce 'tension' between the business groups and IT.

Today, your IT department is increasingly challenged by the need to maintain traditional oversight of systems and data, while simultaneously evaluating new and disruptive technologies and proactively recommending technology strategies to differentiate and improve the business.

Why have companies shifted to the public cloud?

In the technological landscape, cloud is the most significant disruptor of our time. While this is a bold statement, it remains true. The benefits of the cloud for your business are numerous. Public cloud services, regardless of whether they fall into the category of software-as-a-service (SaaS), platform-as-a-service (PaaS), or infrastructure-as-a-service (IaaS), have become a fundamental part of business strategy. The public cloud enables you to:

- Be more agile, giving your business the ability to innovate;
- Reduce the time it takes to bring new services to market;
- Make your organisation more mobile, supporting employees on the move;
- Extend your global reach more easily;
- Increase efficiencies while, in most cases, reducing costs;
- Enable your teams to get going more quickly with certain technologies, for example, in the sphere of mobile applications, data analytics and the internet of things (IoT).

On top of all this, the leading cloud providers' public cloud infrastructure is also more stable and more secure than just about any on-premise data centre—again, a bold but true statement. Those are the positives, and you should be embracing them right now. Pause for a moment though, because you are also the business leader who must assess risk and ensure that cloud fits with your business strategy.

Why is security stronger in the public cloud?

It may seem counter-intuitive at first, but the public cloud infrastructure offered by reputable providers is generally considered more secure, with higher security measures than most enterprises have with their own data centres. There has been a perception that public cloud is less secure due to its shared nature, but that's not the case. Don't confuse the public cloud with the public library, where anyone can walk in and read any book or article that is there. Of course, some of the fundamentals of security still depend on the end user following cloud security best practices, so you must understand what is expected of you. In fact, with proven security in the cloud, some organisations are also now shifting to the cloud specifically to improve their security stance. How can this be?

Over the last 10 years, cloud services have come a long way. Cloud providers have been focusing on security as their top priority, as they understood their customers were running critical systems on top of their cloud infrastructure. With their size and scale, leading public cloud providers spend more on security than just about any other company individually. By running in the cloud, customers of any size and in any vertical are taking advantage of this security at every level, including security-related processes and security teams that operate around the clock. For example, an increasing number of financial institutions are running workloads—often regulated workloads—in the public cloud. Regulators in many countries have vetted the public cloud and endorsed its use for regulated workloads and industries. For example, the Dutch National Bank (DNB) has endorsed the use of cloud for financial

> Make sure you understand and embrace the shared responsibility model: security of the cloud—the responsibility of the cloud provider—and security in the cloud—your responsibility.

services institutions in the Netherlands. Of course, you need to be certain you are using a reputable cloud provider. Such a provider should be able to show a number of certifications, control reports and industry standards, including SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70), SOC2, SOC3, PCI DSS Level 1, and ISO 27001, a premium level of security.

Even if you are a smaller cloud user with just a few workloads running in the cloud, you have access to the same high level of infrastructure security as any large corporation. The important word is infrastructure because this is central to the shared responsibility model, with the cloud provider protecting the infrastructure, while your business, as the user or consumer, protects the applications and the data on top of this infrastructure.

■ Shared responsibility: What is expected of you?

You can't simply push everything into the cloud and step back. Your organisation needs to share responsibility for the information you are putting in the cloud. Think of it as a mutual partnership between yourself and your cloud provider. There are two aspects to cloud security: the security of the cloud and security in the cloud. Security of the cloud is what the cloud service provider does in terms of its physical and logical security of its data centres and the security of the services offered, including compute, storage, databases, networking and the higher-level and differentiated services. Security in the cloud is what the customer must do on top of this. This is about using all the various features and options that the cloud provider offers, including encryption features, key management, access policies, audit trails, multi-factor authentication, firewalls and many other service-specific settings. This, by definition, is the shared responsibility model and, as the CEO, it is something that you should be aware of. This is about your board ensuring you have the correct cloud security model in place.

Your part of this 'contract' is that your business is expected to do certain things and behave in a security conscious way. Here you must also consider which workloads require additional security technologies beyond those offered by the cloud provider.

■ What kind of extra security do you require?

Certain workloads may require additional technologies that perform deeper and more sophisticated inspection of the traffic flowing in and out of your systems, and increase your ability to protect your customers and digital estate. Specialist security companies can augment the levels of security that already exist in the cloud by offering technologies that increase the control and visibility of how data is being used, giving you the ability to assess cybersecurity risks and help prevent successful attacks.

You must define security and protection levels and categorise your data and systems

While all your systems and digital assets need to be protected, some are more important than others. Companies typically come up with data classification models which dictate the level of security and protection required, ranging from negligible or low to medium or high/confidential, and to very high, critical, or highly sensitive. All this is part of a broader business risk and continuity discussion by your board.

■ How about risk, compliance, data privacy and protection?

Cloud providers offer a number of resources to help you understand the controls in place to maintain security and data protection. While a full discussion of this topic would be out of scope here, large numbers of enterprises have successfully built and deployed highly secure and compliant applications and have worked with external auditors to get the appropriate validations.

In terms of data privacy and data protection, often there is a misunderstanding of where data needs to reside and how it needs to be protected. For example, the EU Data Protection Directive and the forthcoming General Data Protection Regulation (GDPR), contain numerous data protection requirements when processing personal data of EU residents. To comply with data protection laws, people sometimes mistakenly think that data needs to stay within a certain jurisdiction. In most cases, that is not the case—there are ways to process data in other jurisdictions and maintain compliance.

For example, some cloud providers are certified under the EU-US Privacy Shield (which enables compliant transfer of personal data from the European Union to the United States of America) or have executed data processing agreements that include EU Model Clauses (enabling personal data to be transferred in a compliant way outside the European Economic Area). Many of the leading cloud providers are also members of the Association of Cloud Infrastructure Services Providers in Europe (CISPE), which has the goal of helping customers prepare for the EU's new GDPR.

Consult the guidance provided by cloud providers to learn more, and seek legal advice if it is needed. Also, remember that this is a quickly evolving space and cloud security and compliance keeps getting stronger, covering an increasing number of jurisdictions. Be suspicious about pushback from those who remain unconvinced and challenge any objections to truly understand if a real hurdle exists or not. Even then, a conversation with your cloud provider can help unlock things.

How about securing SaaS applications your organisation is using?

Your company is likely using various SaaS applications running in the cloud already. Such applications include customer relationship management (CRM) systems such as Salesforce.com; file sharing and storage applications like Box, Dropbox or Google Drive; your office productivity in the cloud such as Microsoft Office 365; or GitHub used by your developers. This 'shadow IT' often began without IT oversight and approval and you now lack the visibility and ability to control the secure usage of these applications. This is not to say such SaaS applications are not secure. They generally are, especially those provided by reputable companies, and similar shared responsibility models as discussed above apply. In many cases, such SaaS applications are implemented on top of public cloud infrastructure.

So, what's the problem? One of the top challenges is the administrative manageability and the integration into the business' identity and access management and information control systems. This has led to the increasing adoption of cloud access security brokers (CASB) solutions and the continuing focus on data loss prevention (DLP) solutions. SaaS applications can also introduce new threats that need to be understood and controlled. For example, one of the risks of SaaS applications is that many synchronise files with users automatically.

On top of that, SaaS applications are often used to collect data from, or share data with, third parties that are out of the control of your company. The combination of these two issues presents a risk of malware, which can not only get in from external shares, but can also sync malicious files across your organisation, automatically and without any user intervention required. You may well consider the benefit of additional security measures to safely enable SaaS applications in your business.

Lastly, there are a large number of cloud-based applications out there and the space is quickly growing with new companies and startups providing their services. Not all of them have the same level of security. Before making production use of a SaaS application, ensure that due diligence has been done.

What are the key points to consider?

The public cloud is a major opportunity for your organisation. If you are not using it, your board needs to ask why. Leading enterprises around the world have come to understand that public cloud offers:

- Top-level security of leading infrastructure providers, available as a basis for even security-sensitive workloads (of course, with the need to correctly fulfill their responsibility in the shared security model);
- Differentiated services, enabling them to be more agile and innovate more quickly;

- The ability to go global, reaching new markets faster;
- The prospect of saving money and creating extra value.

Make sure your organisation understands and embraces the shared responsibility model: security of the cloud (the responsibility of the cloud provider) and security in the cloud (your responsibility). Also understand what cloud providers offer in terms of security, and which additional advanced cybersecurity solutions might be required on top of this to satisfy the security requirements of your business.

Enabling Innovation

16

How Should Businesses Put a Price On Digital Risk?

BT – Mark Hughes, President, BT Security, BT Global Services

- Companies must consider how to 'cost' cyber risk
- Understand what you need to protect
- Gather all of your factual information
- There will be trade-offs on security
- Be clear about your priorities

Cybersecurity comes at an increasing cost to your business. So how do you balance cost versus reward?

Right now, chief information officers (CIOs) have a lot on their plate. The board wants to press ahead with digital transformation, and customers want to do business through multiple digital channels. Every company must consider the risks associated with cybersecurity when developing its business strategy. But this is a significant challenge for many chief executives and finance directors because of how difficult it is to put a price on digital protection.

We know that cybersecurity will make or break the digital business. It is the number one enabler, allowing a business to run at speed and to build customer trust and investor confidence. Conversely, poor security is a disabler and will undermine all efforts at digital transformation.

BT is in a fortunate position. As the oldest telecommunications company in the world, protecting customer data has been an ingrained part of our business from the outset. For BT, security is a competitive advantage. Security is behind our service and our brand, and it's a massive differentiator for us. We can promote services such as BT Sport with confidence because we have assessed the risks and designed appropriate controls. But too many organisations are still working with a fragile, insecure IT environment, which cannot support their digital ambition.

So how exactly do you attribute a value to digital risk? How do you set about finding out how much cybersecurity should cost your business?

It's certainly difficult to quantify using traditional methods, and we found that cyber risk was practically impossible to build into business cases. We took a step back and looked at risk evaluation methods more common in the insurance industry—in particular focussing on downside risk. BT has its own insurance company and also has one of the largest pension funds in Europe—so we could draw on our existing experience at assessing unknown and unpredictable risk.

> In order to determine how to build and invest in your security architecture, you first need to ensure that you have complete understanding of what needs protecting.

In costing risk you've got to look at your assets holistically. With over 6,500 properties and 100,000 people worldwide, as well as a large global network and confidential personal data, we needed to consider and attribute a 'risk' value to a significant number of areas.

Once you have evaluated each element of risk, you can then make the decisions about how and where you are going to invest. We followed some general rules:

Rule 1: Understand what you need to protect and why

In order to determine how to build and invest in your security architecture, you first need to ensure that you have complete understanding of what needs protecting. This is often easier said than done, as many corporate networks have been built over time and often through acquisition. This is not just about creating a list of assets—corporations need to also understand which aspects of their network will, if attacked, cause the most damage—either reputational or economic. For example, BT has a major task because we underpin the UK's telecoms infrastructure. Our customers expect that classic 99.999 percent reliability when it comes to communication. They also have a reasonable expectation that any data they give us so that we can manage their bills and accounts is secure. Furthermore, BT's network is a core economic asset upon which all of our business customers rely. Any compromise to our network can have a massive economic impact and therefore attracts the lion's share of our security investment.

Another way to do this is try to think about how embarrassed your company would be to see its name associated with a cyberattack on the front page of a national newspaper. What would this headline look like? Quite often it is not about technology or systems but about the impact on your customers when their data is exploited. Start from impact and keeping on asking 'why.'

Rule 2: Do not underestimate reputational risk

While the justification for security investment largely revolves around protecting tangible equipment (servers, networks, buildings) and the data that resides on or in them, one of the most powerful motivations needs to be an understanding of the impact a cyberattack can have on one's brand and reputation. This is especially critical for BT because of the central role we play in protecting the UK's critical national infrastructure. But all companies could also risk the loss of trust of their customers if they are found to have been negligent in protecting their critical assets.

Up until now, most companies could take comfort in knowing that most cyberattacks were not made public except in very high profile cases. Many countries do not force companies to report breaches. However, this is changing. For example, the upcoming EU General Data Protection Regulation will require most companies to report any loss of customer data to government authorities, and they will potentially face major fines (up to 4 percent of global turnover) if they are found not to have had adequate protections in place. As more of these regulations come into place, the potential for a cyberattack to damage a company's brand becomes almost a certainty.

Do not think only of the potential harm to your customers, but think what impact this could have on your suppliers. It they lose trust in you, your costs will go up, options and leverage go down. Reputational risk is a genuine end-to-end issue.

Rule 3: Establish there are going to be trade-offs

A good security architecture must strike a balance between providing robust protection for critical assets whilst not being a barrier to productivity. In fact, a state of the art architecture can be viewed as a key enabler for doing business, as it gives the employees the confidence of knowing that their day-to-day activities will be secured without worrying that they may take an action that could put the company at risk. Therefore, companies need to make sure that they are putting in the most appropriate security controls and process for the asset or activity. Making security too tight can have its own negative side effect in preventing your employees from getting their work done efficiently.

Taking advantage of the cloud is forcing companies to take a new look at these trade-offs. There are massive economic and productivity advantages for businesses and organisations that adopt cloud services, especially those with large mobile workforces. Often innovation has been held back by cautious security chiefs who are nervous about the inability to control the security of these third-party cloud services. However, new security capabilities are being developed to enable CISOs to get more comfortable with the balance between potentially massive increases in productivity and a need to ensure the integrity of any corporate data being sent to and stored on third-party clouds.

In fact, these third-party cloud services can often be more secure than your own data centres. For these services, providing reliable cloud capability is core to their business. Therefore, it is in their own self-interest to invest heavily in security in order to earn your trust and loyalty and defend their reputation.

Rule 4: It's about people and process, as well as technology

Most conversation about investing in security revolves around purchasing of appliances and technology. However, almost as important is to invest in your people and processes I'm not talking about your security operations—managed service providers such as BT can do that work for you, so that your business can focus on what it is really good at. However, it is conventional wisdom that the biggest vulnerability in any company's business comes from the 'insider threat.' This is often not (in fact, usually isn't) malicious. The insider threat comes from people who make simple mistakes such as using overly simple passwords, or clicking on links in emails that they shouldn't be trusting. To complete your security architecture, you must invest in a programme to develop a robust set of security policies and processes and ensure that your employees are trained to understand that following these policies and processes are an essential part of their day-to-day job.

In addition, companies should ensure that they have plans in place in the event to deal with the potential fallout of that inevitable breach caused by their people or processes. Too many companies have been caught flat-footed and mishandled the aftermath of a cyberattack, particularly when it comes to managing public relations.

Rule 5: Boil it down to the essentials

It all comes down to one thing: it is about looking after information. Bill Clinton's famous election aphorism was: 'It's the economy, stupid.' For us, 'It's all about the information, stupid.' When it comes down to it, some of the most valuable assets companies hold is either intellectual property or customer data. A good analogy is to think of your data as gold bars. If you had gold bars, you'd want to keep them secure and make some money from them. But you wouldn't just choose the closest person or organisation who offered you a huge return, and you wouldn't just throw them in a box and forget about them. You'd want to research the organisation and ask what they would do to look after your gold bars as well as make you money. You'd ask who would have access to them and how you would be able to access them. And you'd want to make sure that the bars got to the organisation safely in the first place. This is why we normally use banks to store gold bars. These are the types of questions people should be asking about their data.

Infrastructure can be 'fixed,' laptops and phones can be easily replaced—it's the data that resides on those devices that are the real assets cybercriminals are looking for. The growth of mobile workers and cloud services means that this valuable data is often kept 'offsite.' However, too often endpoint security and network security are managed completely separately, leaving open potential gaps that cybercriminals will be quick to find. So make sure that your security architecture takes a holistic approach and not only covers the infrastructure in your HQ and branch offices, but also all of the end-user devices and cloud services that your employees use and how that data gets from A to B.

The price is right

Too few companies are talking about the real cost of cybersecurity. They are not even able to calculate how much it costs their firm—and how a breach will damage their reputation. Yet without pricing in the cost of their security, they face an unknown—and potentially catastrophic—bill in the event of a major incursion by sophisticated and malicious invaders.

17

Building a Holistic Security Function in a Global Organisation

Barclays – Troels Oerting, Group Chief Security Officer, and Elena Kvochko, CIO, Group Security Function

- Security models that are currently prevalent in global companies haven't been adapted to the current realities
- Global companies should consider a whole new approach to security that relies on bringing together different security-related units and sharing of intelligence
- Most global institutions don't have an ability to connect crime, trends, patterns, or suspects across business units
- Cybersecurity should be integrated with physical security and, in case of financial institutions, work much closer together with financial crime divisions, anti-money laundering investigations, and intelligence divisions
- Coordinated 24/7 intelligence, investigation, and rapid reaction security teams should work side by side

By integrating duplicative functions, building security operations centres, and taking a holistic approach, companies can optimise their resource allocation, drive down costs, maximise results, and create increased security.

As more and more services, assets, and operations become digital and delivered online, cyberattacks have become the way to access institutions' 'crown jewels.' Cybercrime is a fast-growing business that is continuously evolving and has become high profit and low risk; in addition, it does not have geographical boundaries. Losses of assets from cyber heists are clearly a current danger financial institutions face. Despite institutions' efforts and investments to fight cybercrime, the rate at which threats evolve exceeds the organisational capabilities in most institutions. Security models that are currently prevalent in global companies have grown organically over many years and haven't been adapted to the current realities. The increasing sophistication of the threat, prioritisation of openness and functionality over security, and a lack of relevant tools on premises are many of the reasons institutions can be exposed to cyber heists. There are a variety of adversaries who are a threat to financial institutions, such as organised criminal groups, nation states, hacktivists, or terrorists. Insider threats are a growing challenge. The ability to prevent, detect, protect, respond, and recover fast becomes a priority, as attacks have no borders. For this reason it is important for global companies to consider a whole new approach to security that relies on bringing together different security-related units and sharing of intelligence. A holistic management of security will provide better understanding of threats and a coordinated response that will protect all business channels and products.

> Currently, most global institutions don't have an ability to connect crime, trends, patterns, or suspects across business units.

In the hyperconnected world, all the roads to a successful digital future rely on security. Trust is at the core of the business for a growing number of industries. The biggest risk to an institution's competitive future is to lose trust from customers, investors, stakeholders, shareholders, or regulators by being a victim of large-scale breaches, large monetary losses, wiping of digital assets, manipulation of data, or disruption of services.

The environment surrounding an institution is composed, among other elements, of employees and all stakeholders, physical locations, on-premise and cloud infrastructure, and third-party providers. All of these components work in parallel towards a common goal, but are rather independent from one another. In addition, many business units are also structurally isolated from one another. Security models of institutions should account for the often disjointed nature of the technology infrastructure and business units, and have a holistic approach to better detect, react, and recover from sophisticated security threats. These models should be able to coordinate with reporting lines, enable real-time sharing of information, and deploy 'corporate memory' with the ability to recognise patterns and anomalies across channels, products, entities, and lines of business.

Currently, most global institutions don't have an ability to connect crime, trends, patterns, or suspects across business units. Technology and physical crime teams have limited strategies that do not take into consideration the capabilities of other teams. Institutions don't have true group-wide strategies for how collectively they can minimise crime, increase detection risk, or improve trust with customers and regulators. Intelligence is limited and segregated—it is not used to predict and prevent incidents. There isn't intelligence to debrief on important know-how, what to do and what not to do next time. In addition, there is scarce contact with local, regional, national, and international law enforcement, except for case-to-case incidents.

In order to prepare, prevent, protect, predict, detect, and recover from cybercrime, organisations should consider refining their security models. Cybersecurity should be integrated with physical security and, in case of financial institutions, work much closer together with financial crime divisions, anti-money laundering investigations, and intelligence divisions, in order to have a holistic visibility into security. The strategy is to establish an intelligence-led defence resting on adequate cyber hygiene, physical security and cybersecurity controls, with the ability to detect and react to the right 'signals'. The objective is to eliminate the mentioned inefficiencies through clearly identifying security goals aligned with the business goals, and organising various functions towards these goals, which will result in removing duplication, delivering savings, improved performance, increased visibility and coordination through better management, and unified/integrated security platforms for the bank. We also believe that companies should focus not on notions—such as 'information,' 'cyber,' or 'physical'—describing security, but simply focus on the core: to deliver 'security.'

In order to deliver security, there is a need for group-wide minimum security standards accepted by business lines. Cybersecurity programmes should be run on common data sets and work together with law enforcement entities. Security methods and procedures should be based on global acceptable standards with respect for data protection and privacy. Given that products will be delivered online, security, safety, privacy, and trust should be enhanced, ensuring that all available information/intelligence is analysed. Security teams should support prevention and mitigation of attacks and breaches regardless of their nature—cyber, physical, information leaks, and internal threats—or their detection methods. This one-stop-shop could gather intelligence and forensic evidence, as well as help investigate and recover financial losses. It should also make sure that any new modus operandi—any new tools and techniques—are exchanged with the appropriate partners to enhance cyber hygiene and resilience. Internal policies to face the new threats and risks should be updated accordingly.

In addition, coordinated 24/7 intelligence, investigation, and rapid reaction security teams should work side by side. This would lead to reduction in losses and costs and improve security. Initial steps should be oriented towards:

- Enabling holistic pattern recognition to distinguish between 'normal behaviour' and 'abnormal behaviour' to accurately detect suspicious behaviour;
- Allowing cross-channel visibility to detect complex patterns of behaviour that may involve multiple layers across channels, products, and accounts;
- Establishing an alert management system to automate decisions and score risk before the investigation process and establishment of a central case management is initiated;
- Creating the ability to link complex cases, in which threats are detected locally within a business line but are part of a global threat that targets several business lines.

To reiterate, when developing innovative security models, global organisations, in our view, should:

1. Consider a global security strategy on how to minimise risk, improve trust, and align with business goals by removing duplication, delivering savings, and improving performance;
2. Focus on the core mission—to deliver 'security';
3. Define security based on business needs and acceptable standards with respect for privacy;
4. Enable the ability to connect various security incidents regardless of their nature;
5. Analyse past events and perform analysis not only of what has hit organisations already, but of what is likely to hit in the future;
6. Enable a coordinated 24/7 rapid reaction team.

By integrating the duplicative functions, building security operations centres, and focusing on all aspects of 'security,' companies can direct, monitor, and control the implementation of security and trust as a whole. This way they can uphold maximum security for fewer investments. Institutions need to optimise their resource allocation, drive down costs, maximise results, and create increased security.

Protecting Our National Organisations

18

Legacy Industrial Control Systems are Increasingly Vulnerable as we Embrace the Internet of Things

XiaK (center of eXcellence in industrial automation Kortrijk) Ghent University – Johannes Cottyn and Tijl Deneut

- Industrial control systems (ICS) are poorly protected and largely open to exploits
- A prevalent non-security attitude in many industries using ICS must change
- Businesses in the digital domain can have backup systems in place, while industries that produce tangible goods usually don’t have that luxury
- The internet of things (IoT) is connecting more ICS to the outside world
- ICS-dependent industries need to take action urgently

CEOs in industrial organisations need to understand their legacy control systems are now increasingly vulnerable to attack as we embrace the internet of things, say Professor Johannes Cottyn and Tijl Deneut of Ghent University.

If you are the chief executive officer or a board-level leader in a reputable industrial or manufacturing business in Benelux, then you need to get serious about the vulnerabilities in your systems. In our view, many senior executives have been oblivious to the dangers, passively observing from the sidelines as cyber breaches damage firms in sectors such as financial services, retail and telecommunications. Leaders managing industrial organisations have been living under the false belief that somehow their company’s industrial control systems (ICS) are secure and safer from cyberattacks.

‘Industrial control systems’ is the collective term for the computer systems that run thousands of factories and plants in Benelux, and indeed elsewhere, ranging from automobile manufacturing facilities to power plants to transport systems, including railways and airports. Such systems are directed by specialist 'operational technology' (OT) dealing with manufacturing, assembly and production lines. Operational technology is the vital computer hardware and/or software used to monitor and manage your physical systems, whether that's pumps, valves, robots or other industrial systems.

'It can't happen to us, we're secure,' is the head-in-the-sand thinking that must be confronted and senior leaders, whose organisations depend on ICS, need to recognise the threat that cybersecurity risks pose—without delay.

The inherent dangers of ICS

Of course, ICS have been in use for many years and have had a transformative effect on the efficiency and profitability of countless businesses and their operations. Historically, ICS ran on segregated internal networks and communicated using their own proprietary languages, most being unique. This environment was secure, in a passive manner.

In recent years, however, the security risks to these systems have changed dramatically and exponentially. In continued efforts to increase flexibility and reduce costs, firms introduced standard methods of communication used by IT systems to ICS. Likewise, for varying reasons, a lot of operational technology has become connected at one level to the broader IT network—and by extension, in some instances, to the internet. Furthermore, many ICS environments have been built separately and have never been connected to the IT security systems. Not only does this make industrial systems vulnerable to cyberattacks, exploitation of these systems by someone with malicious intent requires less expertise given the convergence of IT and OT.

The vulnerable systems that run your business

Increasingly, the smartest industrial and manufacturing companies use operational technology to design, make and shape their products and services. Here in Benelux, this has helped create our region's economic prosperity. However, these systems are increasingly vulnerable to cyberattack and are being targeted by a range of adversaries including rival foreign businesses attempting to steal the 'crown jewels' or criminals seeking to obtain sensitive information for financial gain.

Meanwhile, the internet of things (IoT), and in particular the industrial internet of things (IIoT), has become a recent buzz phrase and an organisational fact of life. Yet, the IIoT is about convenience and speed, not hardened security. For all our beautifully connected industrial control systems, security is an afterthought. Whole industry sectors now rely on industrial control systems that are vulnerable. By their very nature, IIoT devices are designed with connectivity and ease of use in mind. The result is that connected devices in industrial environments can function and be controlled virtually through an open door. If a systems engineer sitting on a train on the way to work can control the speed and flow of your production line, think what a cybercriminal might do.

Nevertheless, an insecure future is not inevitable, but only if we embrace change. This change begins with recognising the fundamental importance of securing ICS.

Key questions to ask your ICS leaders

As a CEO, how well equipped are you to deal with such a cultural shift? As with every other business, you must develop your strategic responses. You must start by asking your head of engineering or process managers about the future state of your own operational systems.

Start by asking: 'How are we assessing this risk?' While financial, retail and cyber technology companies are fully aware of the dangers, in our experience, the levels of awareness in industrial and manufacturing organisations is still not high enough.

If your team is already assessing the danger, your follow-up questions should be:

- How closely are IT and OT teams collaborating on a security strategy for OT?
- What is currently in place to prevent cyber breaches?

- Who is monitoring our system?
- Where are our weakest points?
- How can we verify that our system is safe and secure?
- How are we assessing our system?
- What are our legal and regulatory responsibilities?

The truth might be hard for your board to accept. You must determine how long you can maintain your existing legacy industrial system. Your board will need to understand why a system that you sanctioned, spending hundreds of thousands of euros to implement and was guaranteed for 20 years of service, now needs a significant upgrade—or else it becomes obsolete.

Your operational technology was designed to last decades because of the high capital expenditure cost of setting up bespoke processing systems for your distinct needs. Originally, there was little need to upgrade the IT infrastructure. Now this may mean there is either limited or no support available by the machine tool manufacturer who sold the original equipment or security vendors to protect these systems. Understanding what support is available is critical in determining how long legacy systems can continue to function within acceptable risk levels for the business.

Accept a basic premise: You will be a target

Your board must start to change its mindset. In every industrial and manufacturing company, it is not a matter of 'will there be an attack?,' but rather 'when will it happen?'

Like all other businesses, you need to be prepared and understand your vulnerabilities. You must have a plan if every document on your internal environment becomes unreadable, or a hacker crashes your main servers and has remote access to your sites and regional sales offices.

What kinds of impact can cyberattacks have?

We have witnessed entire companies grind to a halt because of cyberattacks. In one instance, an assistant opened an email with a link to reset a password, only the link opened a piece of malware that encrypted all documents that this assistant had access to. In addition, all the documents on the central server, used by many engineers and managers, were impacted. The backups were a week old, which meant many orders had to be reset by hand.

In another case, a supplier delivered a new forklift truck for the factory system with a preconfigured network address. Due to a misunderstanding and a badly configured internal network, this single device meant the entire network became dysfunctional.

Elsewhere, a machine was broken and a supplier's engineer called to fix it. An infected USB key entered the network during the maintenance. The engineer decided to also perform an upgrade of the operating system which worked, but this introduced malicious code that leaked valuable business critical information.

> In recent years, the security risks have changed dramatically and exponentially, because standard methods of communication used by IT systems were introduced to ICS.

All of this is happening in industrial organisations across Benelux, and this will only increase unless companies start to look again at how they protect their operational systems. Our industrial systems were not originally built with security in mind and must be properly shielded from harmful exploitation. Addressing this challenge requires a cultural shift that must be led from the top. Securing the IIoT begins with recognising the seriousness of the challenge, making security a strategic priority, and holding IT, OT and business unit leaders accountable for this priority.

A salutary case study

One Antwerp industrial manufacturer uses a transport system with a small picking robot on the production line. The core technology comprises a controller (PLC), a device with touchscreen visualisation (HMI), an industrial switch (a device that connects several devices on the network), and a controlling server (OPC). The data it gathers and several small configuration options are shown on the touchscreen via a web interface running on the controller.

This configuration is connected to the company network which is, in turn, connected to the internet and secured by standard hardware/software safety measures. However, the operating system (OS) on the server was very outdated, as the vendor of the controlling software did not support recent versions. Despite limited security measures, this server is very vulnerable.

The configuration of the switch brought higher flexibility, but also greater visibility of the setup on the company network. A cyber breach occurred when an intruder used the same protocol as the hardware vendor. This protocol sent out one packet to the entire network and every device from the same vendor responded with its name, device type, IP address et cetera. This made it easier for intruders.

There was no authentication because the HMI is nothing more than a simple touchscreen interface that displays the website running on the controller. There was no support for a keyboard, hence no possibility for proper authentication, so anyone on the network could browse the controller interface and take it over. The configuration and programming of the controller was done on a Windows system, which may have been outdated. Software with support for older PLCs rarely gets updated. Some vendors even withdraw support for patched Windows systems, making them extremely vulnerable. To make matters worse, the software used to programme the controller is freely available on the vendor's website. Since there is no authentication, anyone with access to the network can reprogramme any controller. This is a major breach waiting to happen.

19

Secure Collaboration in the Academic World: Tackle Cyber Risk Without Harming Legitimate Users

Wageningen University and Research (WUR) – Raoul Vernède, Information Security Officer

- Passwords are no longer enough
- An identity access management system determines who gets in and under which authentication conditions
- Proper classification of data ensures the appropriate trust levels
- A central identity provider (CIDP) is essential to remain in control and to have oversight

Educational and research institutions exist to encourage engagement and learning but this opens the door to cybersecurity risk. Raoul Vernède, information security officer at Wageningen University and Research, says all organisations can learn from the adoption of a robust, but at the same time flexible, identity access management (IAM) system, which keeps the users and data secure.

Our great seats of learning have been able to thrive and prosper thanks to the openness of thought and their ability to challenge norms. But, increasingly, large institutions such as universities, research organisations, technical institutions and other public sector bodies are open to loss of vital data and intellectual assets. With a single password no longer strong enough for secure access, institutions are learning how to live more effectively with two-factor authentication (2FA).

Our chancellors, principals and deans of school in our educational, research and knowledge institutions face the dilemma of how to protect intellectual property on the one hand, while allowing collaboration with other parties on the other. In the world of education and research, academics and researchers want the freedom to choose the systems that work best for their professional work. When undertaking research that involves massive computing power and new levels of digital innovation, the academic often purchases their own systems to suit their specialist area of research. Moreover, these systems are frequently purchased in the cloud without seeking the approval of—or even consulting—the IT and cybersecurity professionals within the organisation. Smartphones and tablets have multiplied this challenge as both students and teachers bring their own devices to their place of learning.

For new employees and students, it may be easier, and preferable, to use their current digital identities rather than a university-approved account to gain access to institutional information. However, the danger is that multiple accounts, with easy-to-hack passwords, are frequently used, while corporate passwords are regularly shared among colleagues, which increases the level of risk.

Furthermore, students study at universities in their own country and abroad, while satellite campuses in other countries and massive open online courses (MOOCs) are gaining popularity and will qualify for credits. Yet, a physical check on identity is required when giving out that the initial identity. Here, too, the challenge is using a digital identity that allows easy participation without compromising an institution's vital systems.

The key to protection is authentication

An institution's assets will have multiple layers of protection, so how should state of the art, multi-factor authentication and protection take place? The question we ask is: 'Do I need an additional lock on my bike?' It's a simple question when considering security in any organisation. Of course, the answer depends on the value of your bike and, therefore, the importance of keeping it safe. If you've just spent €1,000 on a Gazelle Cityzen, you are more likely to use a hardened security lock than if you had an old second-hand bike that you picked up at a stall.

In terms of authentication, the traditional password, with its upper and lower case and random numbers, has had its day and is no longer fit for purpose on its own. Attacks by phishing emails have become effective in compromising accounts, about 10 percent of users divulge their password on the basis of even a mediocre phishing email. Many organisations are now using more comprehensive information classification to get a grip on minimum security requirements, or security baselines, and are adopting terms and conditions of use for specific classes of information.

For access to confidential or sensitive information, a second factor is required above the traditional password. This is 2FA—also called MFA (multi-factor authentication).[1] However, administrators in an academic institution may face resistance for laying down rules and insisting on 2FA. Researchers, and the academic world in general, do not like rules and always want to break out and do things in their own way. The enforcement of regulations is weak with people placing more importance on the value of their open research and educational work than in working securely. These cyber risks are underestimated by institutional leaders.

Building levels of assurance

From a traditional perspective, most institutions are generally well-organised in identity management, yet are less focused on access management. A next step is required, combining control and access to ensure identity access management (IAM).[2]

Besides additional authentication or secure cooperation, it is advisable for institutions to put in place easier means of cooperating with external parties. To this end, there must be clearer differentiation of the identities within your organisation, with different levels of access based on levels of assurance. It stands to reason that an organisation's own employee, who has gone through a formal human resources procedure, with the additional step of presenting their passport or identity card in person, will be given a much higher trust level than somebody who is only known from an email address, without further validation. Consequently, assurance levels will differ from person to person.

Our experience of a trust-level framework

For open and secure access and cooperation to be properly realised, a vision is required. This means a clear understanding and approval at leadership level. In our own case, Wageningen University and Research is in the process of implementing a trust-level framework. For this, the following trust levels are distinguished:

- Information
- Device
- Identity
- Network
- Authentication.

1. Trust level information

Many organisations put corporate information into four classifications or more. The classification determines whether authentication with a password or with 2FA is required:

- Public
- Internal
- Confidential (including all personal identifiable information details)
- Secret.

2. Trust level device

Your organisation must decide its levels of confidence in any device. The device categories are:

- Unknown machine (e.g. access from internet café computers);
- Recognised and seen earlier, determined by profiling and the 'fingerprint' of the browser;
- Known machine on the basis of user certificate placed by the user to indicate the machine can be trusted. The certificate can only be downloaded after 2FA;
- Machine registered via a formal MDM (mobile device management) process, where the MDM agent is placed on a BYOD (bring your own device), via MDM tooling;
- Fully managed machine, so that extensive security requirements can be enforced (exclusively for users and machines that are linked to the enterprise directory).

3. Trust level identity

This concerns a valid user identity and a level of certainty about who this person says they are:

- Anonymous; such as a visitor to a website;
- Socially federated; a user's identity has only been established via e-mail verification;
- Partner-federated and/or sector-federated; users for whom it is assumed that for partners or communities a robust registration process is in place;
- Own identity (mostly in enterprise directory); employee's identity confirmed on the basis of robust registration process with physical check for identity.

4. Trust level network

This relates to the network or zone where information is being accessed. It is about secure internal institutional networks against external networks outside the firewall (that are unknown and untrusted until proven as secure).

5. Trust level authentication

This is about the levels of trust you have in each individual user. These are:

- No authentication required;
- Password of a federated social or e-mail account;
- Password of a partner-federated and/or sector-federated user;
- Password of own identities (employee accounts);
- Password and 2FA of a partner-federated and/or sector-federated user. The 2FA setup of the other organisation is trusted, and the federated user can be authenticated with his own 2FA method. SAML[3] protocol arrangements to be made between the federative organisations;
- Password and 2FA of own identities.[4]

Large institutions must remain open. But there are often dozens of people each day who require access at various levels, making these institutional networks vulnerable to those with malicious intent. Our vision is to allow access to all who genuinely require admittance. In reality, there are more and more gradations, and access depends on the integral level of these factors and is based on decision rules in the central identity provider (CIDP). One size does not fit all.

> People in the academic world place more importance on the value of their open research and educational work than in working securely. Cyber risks are underestimated by institutional leaders.

While this has led to a more complex setup, it ensures that access can be set at a more intricate, even individual, level. As a consequence, the level of acceptance of 2FA in academic organisations increases. On the basis of the trust levels above, rules can be set for every combination. For our institution, context-based authentication via a CIDP is a major step forward. However, it does not solve the problem of provisioning the accounts or identities to the various cloud service providers. Many cloud providers demand that identities are provisioned, particularly when it comes to authorisation of users for assigning rights or licences. This is another matter that will require your attention.

Conclusion

Technological developments in our institutions are a fact of life and are occurring rapidly. With such technologies not yet crystallised and with complexity increasing, IAM is emerging as a highly dynamic solution. As a C-suite executive or director of an academic or research organisation, and indeed any other kind of institution where both open access and high-level security are required, you need to be aware of the challenges and possibilities. Don't re-invent the wheel, but start the discussion with organisations that have already gained experience in this subject, such as the University of Wageningen. Start now to make your organisation as secure and open as possible. Think big, act small.

Works Cited

1. *User Authentication Technologies Beyond the Password*, Anne Elizabeth Robins & Trent Henry, Gartner 2015
2. http://www.surf.nl/binaries/content/assets/surf/en/knowledgebase/2014/reportidmaas-jan2014-def.pdf
3. https://www.forumstandaardisatie.nl/standaard/saml
4. Magic Quadrant for User Authentication. Ant Allan, Anmol Singh & Eric Ahlm, Gartner, 2014

20

Cybersecurity in the Netherlands: The Dutch Perspective[1]

National Cyber Security Centre (NCSC-NL) – Hans de Vries, Head NCSC

- The Netherlands has become an international internet hub
- Both government and private sector should increase investment in cybersecurity
- The Dutch cybersecurity approach is an example of successful public-private cooperation
- Investment in innovation and education initiatives, to improve cybersecurity knowledge and skills, has increased significantly

The digital domain has been an integral element of Dutch society for more than 20 years and has made a spectacular contribution to the growth in national productivity and innovation, says the head of the Dutch national cyber security centre, Hans de Vries.

Due, in part, to the substantial investments in the way it responds to technological trends and the effective use of ICT tools and skills, the Netherlands has become an international internet hub, with one of the world's most competitive internet markets and one of the highest penetration of internet users. In this respect, the digital domain is intertwined with our daily lives. Citizens, government bodies and businesses are using digital applications for online interactions, transactions, more efficient collaboration, communication and entertainment.

Opportunities and security

The Netherlands is a digital gateway to Europe and, as a result of our first-class digital infrastructure, one of the most IT-intensive economies in the region with the Amsterdam Internet Exchange (AMS-IX)—the largest internet exchange in the world—and our high-speed broadband telecom networks.

This increasingly digital world is not only for ease, efficiency and pleasure, but also an important driver of innovation and economic growth. Increasing the Netherlands' digital resilience cannot be achieved by the government alone, as the ICT infrastructure itself, and knowledge about it, is largely in the hands of national and international private parties. Therefore, cybersecurity is the sum of joint efforts of government bodies, the business community, organisations and citizens, on a national and international level. Just like in the physical world, 100 percent security in the digital domain can never be achieved. This reality, however, should not prevent us from striving for as much security as possible.

The importance of cybersecurity, and the need for public-private cooperation, has been underlined in a report published in 2016 by Herna Verhagen, CEO of Post NL, entitled, *The economic and social need for more cybersecurity: keeping dry feet in the digital era*. She points out that digitisation presents huge opportunities for our society and economy in the 21st century. This does, however, make it all the more important to ensure that the digital world remains safe and secure. Just as we protect our nation from flooding, we must take effective defensive measures to protect the Netherlands in cyberspace. Only then will we be able to protect ourselves from outside threats and make the most of the opportunities for the Netherlands.

■ Worrying increase in cyber threats

Given the scale of cyberthreat, keeping our nation safe is not a trivial task. Professional criminals are increasingly better organised and are using advanced digital attack methods. In the past year, several large-scale attacks have taken place with a high degree of organisation, focusing on the theft of money and valuable information. In addition to the government, the victims were, increasingly, companies and private citizens. Professional criminals are therefore a growing threat to our national digital security. That is confirmed by the *Cyber Security Assessment Netherlands 2016 (CSAN 2016)* annual report, issued in September 2016 by the National Cyber Security Centre (NCSC). It paints a worrying picture of digital security. The *CSAN* is drawn up in close collaboration with many private and public sector partners. It offers a concise and complete picture of core/vital interests, threats and resilience in the field of cybersecurity and is an excellent example of successful public-private cooperation.

> Cybersecurity is the sum of joint efforts of government bodies, the business community, organisations and citizens, on a national and international level.

■ Digital 'safe place'

This public-private cooperation is unique and perfectly fits the Netherlands. The public sector is used to 'poldering' and closely working together with the private sector and academia to achieve collective results. A good example is the Cyber Security Council, where leading representatives of academia and the public and private sector develop a strategic vision of new technological developments and provide advice to the government. The NCSC also collaborates with private organisations in 16 information sharing and analysis centres (ISACs), organised per sector, where participants exchange information, analyses and experiences about cybersecurity. This digital collaboration between the NCSC and other public and private parties is enhanced because of the appointment of liaison officers representing those public and private parties within the NCSC.

In this regard, we believe the approach in the Netherlands is world-leading and our nation is one of the forerunners in the international digital domain. However, this does not mean we can sit back. If the Netherlands really wants to stay a digitally safe place to do business, both the government and the private sector should increase investment in the coming years.

Strengthening cybersecurity—steps forward

In accordance with the Dutch National Cyber Security Strategy 2, many steps have been taken in recent years to strengthen cybersecurity in the Netherlands. Public and private parties are increasingly required to bring forward new measures. Public and private efforts cannot stand alone, and must be mutually reinforcing. The starting point is looking for common interests and setting common goals in cooperation with public and private partners. This includes:

- Several legislative proposals have been submitted to parliament inter alia a legislative proposal in which the Dutch police will be given more powers and resources to be able to tackle cybercrime effectively; and the proposal for the Dutch Data Processing and Cybersecurity Notification Obligation Act including an obligation for public and private organisations in vital sectors to notify the NCSC of serious cybersecurity incidents. The Netherlands is also currently preparing the implementation of the Directive on Security of Network and Information Systems (the NIS Directive).

- Cybersecurity is top of the agenda for an increasing number of organisations. Cooperation is key. Large companies depend on smaller organisations for their digital security because of chain dependencies. Fortunately, big companies in the two major trade nexuses, Amsterdam Schiphol Airport and the Port of Rotterdam, recognise the importance of a secure and effectively functioning cybersecurity ecosystem. As a result, they have launched two pilot projects, in cooperation with the Dutch NCSC, to strengthen the entire digital security chain, consisting of affiliated companies and organisations. These are excellent examples of public-private cooperation in the Netherlands.

- The Netherlands will continue to strengthen and further develop the National Detection Network (NDN). Within NDN, the NCSC and the national intelligence services work together to perform activities (such as the sharing of indicators of compromise) to strengthen detection of attacks on systems of government agencies and private organisations in vital sectors.

- Investment in innovation and education initiatives, to improve cybersecurity knowledge and skills, has increased significantly partly due to the launch of the Dutch cybersecurity platform for higher education and research (Dcypher). Dcypher's main tasks are agenda setting and coordination (scientific and practical) of cybersecurity research and higher education. The aim of Dcypher is to increase the number of cybersecurity specialists and encourage more students to participate and successfully complete relevant courses and training.

- As cybersecurity also requires an international approach, the Netherlands took the lead in placing cybersecurity on the agenda during the Global Conference on Cyberspace 2015 (GCCS) and during the Dutch EU Presidency in 2016.

- During the GCCS 2015, the Global Forum on Cyber Expertise (GFCE) was launched to enhance international knowledge and capacity in the field of cybersecurity and to encourage and facilitate the fight against cybercrime. The GFCE has since facilitated the process of awareness and capacity building in countries all over the world.

2017 and beyond

Digital attacks in the information age are a given. While the path ahead may appear arduous, the Netherlands is well-positioned to continue its journey of protecting its digital infrastructure, which underpins our national economic vitality for today and the future. All actions will strengthen the cybersecurity of the Netherlands as a whole.

Public and private parties should take responsibility and work together. Only then will all parties be able to protect themselves from outside threats and fully benefit from the opportunities the digital future presents us. The pursuit of this will continue based on a pragmatic Dutch approach, where partnerships are fully enhanced and strengthened. When it comes to encouraging partnerships, the NCSC will help make partnerships sustainable by acting as a facilitator of regular meetings and as an initiator of dialogues between organisations—on all levels, from strategic to operational—in search of common interests.

Note

[1] Reproduction and further publication of this article is permitted, if the user clearly states the name and function of the author and mentions whether this article has been modified.

21

Let's get off the Dreaded Security Roller Coaster: Adopting a More Measured Approach

KPN Telecom – Jaya Baloo, CISO

- Move towards financial evaluation of cyber risk
- Rapid response to any attack is imperative
- Sharing information makes us all more secure
- A key indicator is the average time to resolve an issue

There's no need to 'ride the security roller coaster' if you adopt a more measured approach to keeping your organisation on track, says Jaya Baloo, the CISO of KPN.

At some stage in their career, most chief information security officers (CISOs) end up 'riding the security roller coaster.' Before a major hack or security incident happens, they are in the deepest dip of the ride, down in the shadows. Suddenly, there is the full beam of a glaring spotlight. The board is alarmed and paying full attention after a cybersecurity breach. Very rapidly, the CISO starts soaring upwards to the top. The board is anxiously throwing money at the problem to solve it. They want immediate results. The CISO can hire top people, get the best equipment and pull in external advisors. Everything is open for them. This reaches a crescendo at the top of the ride. Then, as the imminent danger subsides, the board's focus and attention shifts to some other pressing issue in the business. No longer able to demonstrate their value, the CISO faces a white-knuckle ride hurtling on the way back down. Resources and money begin to dwindle from the security department. They face the same budget targets as everyone else, figuring out how to do things more cheaply. They ride the rollercoaster down the mountain, awaiting the next incident when they ride skywards again.

It's a futile way to create a strategy. Often a CEO or a board member will ask: 'When are we done with this whole security thing,' as if it is a project with a well-defined endpoint. It is hard for your board to realise that security is a never-ending journey with temporary stops but no final destination. As the actors and targets change, your organisation is in the situation of constantly re-evaluating your security policy in line with the potential threats to the business. It is the board's duty to ensure that the CISO and the security department do not live in this permanent roller coaster state, but have a much smoother journey with the ability to handle the bumps in the road.

While the board is now liable for the state of information security in an organisation, it cannot be blamed for the roller coaster experience. In the past, IT and technical people have not made a compelling and understandable enough case about security to their C-suite colleagues. They have talked in technical jargon rather than look at the potential exposure, the financial implications and the quantifiable impact on the business.

In order to inform the board regularly, KPN introduced a weekly risk intelligence report in October 2012. This weekly risk intel is an uncensored factual statement of the security situation, with five internal and external risk items that are only for the board to see. These are the top five risks we follow-up on. We also have a live dashboard, on which everyone in operations, and from board to middle-management, can see the current vulnerabilities. Here, the most important statistic is the average time it takes to resolve an issue. You can't really prevent vulnerabilities and incidents from occurring but you can make the window of opportunity available to a hacker to take advantage of them as small as possible.

How to ensure the value of your IT team

There is now a different and more rational approach for cyber risk. Dealing with a threat can still be as challenging and intense but you don't want to create a sense of panic. However, as a CEO, you need to ensure that your IT team is creating value, able to prove its worth to your business and also helping, where possible, to improve security across society.

KPN is part of the vital infrastructure of the Netherlands. As a telecommunications and ICT provider, secure networks and systems are the absolute prerequisite for our customers, to safeguard their privacy and prevent misuse of their digital identity. Our customers depend on us for their wireless telephony, internet and TV, while businesses depend on the ICT service and network critical infrastructure. But we know that the weakest part of any chain is where we can expect to be hacked. It happened at KPN in 2012 and I was hired to rebuild our IT Security team from the ground up.

Today my chief information security office follows the security life cycle of prevent, detect, respond and verify. We are able to proactively detect vulnerabilities in our systems and conduct rapid responses when incidents occur. The office consists of five teams:

- Prevention: this is our strategy and policy team who are on top of current events and are like battlefield generals. They need a plan of attack and they study and understand the evolving enemy, such as sophisticated cybercriminals, state-backed espionage, and hacktivism as well as traditional threats of theft, fraud and vandalism.

- Detection: these are the REDteam—our 'Ninjas' —who are proactively testing and probing, using ethical hackers, and the BLUEteam, who are reactively defending our systems and the security operations centre (SOC) who provide our first and second line of defense.

- Response: KPN-CERT (computer emergency response team) is the bombsquad, who have to decide to defuse or detonate a particular situation. They work closely with the SOC for serious level three incidents and above.

- Verification: this consists of our senior security officers, who are the ambassadors throughout the wider organisation of 20,000 employees and not only talk the talk, but walk the walk too. They ensure we are all dedicated to scaling-up, to best practice and serving our customers' needs.

In all, about 100 professionals across the five teams cover the whole business. So, with all this at the organisation's disposal, we feel compelled to make a wider contribution through collaboration. We want to get our partners and our customers to the same place when it comes to physical and information security and business continuity. It has become enshrined in my mission as a CISO: *'To protect and defend KPN, to make us secure, reliable and trusted by customers, partners and society as a whole.'*

> In the past, IT and technical people have not made a compelling and understandable enough case about security to their C-suite colleagues. They have talked in technical jargon rather than look at the potential exposure, the financial implications and the quantifiable impact on the business.

■ The creation of PHOSI

Just over a year ago, we decided to produce the KPN security policy (KSP) application, where we published our security approach, policies and tools in a downloadable app. It sets out how we operate and the purpose of an unambiguous set of measures and requirements that we must fulfil on a daily basis. It was my belief, backed by our CEO and our board, that publishing and promoting our KSP would contribute to higher levels of security, continuity and privacy not only for our organisation but for society as a whole.

Central to our KSP, is a digital tool we have developed: PHOSI (potential harm of security incident) Calculator, which can quantify in moments the potential harm of a security incident, and helps other IT security organisations speak to their board of management in financial terms. This helps all people working in security explain the value they add in financial terms from this easy to use app. It looks at:

- Likelihood (scale: negligible, very low, low, medium, high, very high, extreme);
- Publicity impact (scale: insignificant, minor, significant, damaging, serious, grave);
- Service impact (scale: insignificant, minor, significant, damaging, serious, grave);
- Privacy impact (scale: insignificant, minor, significant, damaging, serious, grave);
- Direct cost impact (scale: insignificant, minor, significant, damaging, serious, grave).

In the 'grave' category for privacy, it could mean that the data of ten thousand customers is at risk, or it may cause a system to be permanently closed and may result in the complete compromise of services. This is all costed on a scale the business can easily understand and instantly quantify. This PHOSI scale is based on our known costs and the anticipated damages. We are encouraging other boards or security departments to fill in their own values and costs when they use this app. The calculation of the cost of an incident will depend on your business objectives and cultural values.

■ Why make it available to the public?

We feel it is our civic responsibility to improve security and to empower our customers in coping, with and responding proactively to, online security and privacy issues. KPN is a technology company and our board of management and supervisory board have extensive technology knowledge and our CEO, Eelco Blok, sits as co-chairman of the national Cyber Security Board in the Netherlands. We drive innovation embedded with privacy and security.

Our KPN security policy looks at 11 aspects, which are:

- Top-level policy;
- Security and continuity management;
- Human resource security;
- Information handling;
- Physical security;
- System and network security;
- Innovation and development;
- Supplier relationships;
- Incident management;
- Business continuity;
- Regulatory requirements.

The policy compliance cycle

From a board-level point of view, our top-level policy sets out what needs to be in place in terms of the requirements, and why it needs to be in place. Mandatory rules describe the practical manner of how certain measures must be implemented. These rules are aimed at software developers and architects, administrators, asset owners, security professional, corporate departments and shared service centres across the business. This needs to be continuously evaluated, so there is one major and three minor releases per year. This continuous improvement is mandatory in order to just keep up with the evolving threats from the outside world. It is one thing to have legacy components in your network you know you need to fix, but the goal here is to stop building new legacy. All mandatory documents in the framework are reviewed at least once a year by the owner of the document. Any major changes or new documents must be approved by the management board. We have created what is called the policy compliance cycle.

The necessity of external collaboration

No company, however large, can do everything themselves. It is just not possible or even preferable. I am very fortunate to have the security team that I have in KPN. Very few companies can afford the level and depth of expertise that we have at our disposal. When we do good things, or have intel information, we need to share it and we are grateful for reciprocity. As a part of the vital infrastructure of the Netherlands, we maintain contacts with regulatory authorities, law enforcement organisations and special interest groups. One of our closest partners is the National Cyber Security Centre (NCSC) with whom we have near-daily contact. But the partnership that maybe the most unexpected is the one we share with colleagues in the telecoms sector, the Telecom ISAC (information sharing and analysis centres). Together we not only work on large incidents but also on structural improvement for national security.

We are trying to make our company, and our country, more secure. Every person, team or company that we work with to improve their security helps to improve the resilience of our interconnected fabric. Every small step matters, because it is all about the cumulative effect of marginal gains. Above all, it is a step closer to ending the dreaded security roller coaster.

22

View From the Front Line

NATO Communications and Information Agency – Ian West, Chief of Cyber Security

- NATO collaborates with private industry on cybersecurity—part of our collective defence
- Identify the crown jewels of your business
- Your network needs more than a crunchy exterior: it must detect attacks from within
- Address the skills shortage
- Collaboration is key

Something will happen this year that we never predicted —and your business has to expect the 'known unknown.'

We are in the frontline trenches in the battle against cyberattacks. Every minute of every hour of every day, we are seeing various levels of threat, and we have to be vigilant and nimble to resist attacks that are increasing in sophistication and intensity. At NATO, cyber defence is a core capability because of the alliance's dependence on its ICT infrastructure, and also because the cyber dimension is part of current conflicts and will inevitably be an increasing component in future conflicts.

The positive news is that cybersecurity is at the front of mind for almost every business in operation today. We all depend on our networks, use similar technology and face similar threats, so NATO has been very forward-leaning in collaborating, particularly with industry, to defend from those who seek to undermine and destroy our way of life. NATO, as a transatlantic alliance of 28 (soon to be 29) nations, shares the values of strong collective defence and the protection of its members' territories and populations against attack. This includes cybersecurity. In our core treaty, the alliance stands ready to act together and decisively to defend freedom, and the shared values of individual liberty, human rights, democracy, and the rule of law.

Increasingly, the 'dark' web is where the bad folks collaborate, hone their skills, and organise themselves. This is where they congregate to commit cybercrime.

In terms of threats, we have to categorise the types and levels of attack. There are *non-specific* threats such as malware that can infect our systems and *specific* threats, which are attacks targeted specifically against NATO, where we focus most of our attention. Here an adversary might be a hostile nation or organised criminals who are crafting attacks to entice users to click on a link and open a corrupted document to gain access to our systems and sensitive information.

In recent years, these *specific* attacks have grown in frequency and sophistication. With a laptop and a modicum of knowledge, a malicious attacker can get right into your organisation and do significant damage. There are also 'hacktivists,' often with an extreme political or social agenda, who hack into an organisation's website and post illegal messages, deny service to your website, or steal sensitive information. Increasingly, they are attacking commercial companies, non-governmental organisations, or governments, seeking to embarrass, ridicule, or destroy reputations. Then there is the insider threat—from us, the users, who can cause serious security incidents, either deliberately or accidentally.

All of these diverse threats mean that you can't just have a crunchy exterior to your network. You need the ability to detect attacks from inside your own networks as well.

Within NATO, our job is to try to prevent these incidents, of course, but we will never be 100 percent successful, so we need the capability to detect, respond, and recover from incidents. It is also important for us to try to find out who is behind these targeted attacks, and their motivation. We investigate, looking at each piece of the jigsaw, to find out who is behind the attack and what they want to gain. Following are some common strategies that are proven and necessary to mitigate the risks from cyberattacks.

Identify the crown jewels of your business

It is impossible to protect yourself 100 percent from cyberattack. Our NATO commanders understand this very well. Cybersecurity tends to be expensive and, like commercial organisations, we cannot afford to protect everything to the same level. Nevertheless, we need to deploy scarce and expensive cyber resources based upon our assessment of the risks to the entire enterprise.

In order to identify our crown jewels, our military commanders ask:

- What is the most important information we hold?
- What are the most significant services we offer to customers—and what are the inherent cyber risks?
- Where do we hold secure information about our processes and our business? How safe is it?
- How can we continue to assess and monitor the risks?
- Do we have a cyber risk register?
- How do we respond to each type of risk?

It requires a sense of clarity about the depth of risk that the business is willing to take. Once we are clear about our commanders' appetite for risk, we need to put in place the planning, implementation, and an assessment of the security controls and procedures.

How good is your protection?

Strong cyber defence is not about perfection. We expect our cyber perimeter to be breached from time to time. Rather it is about how quickly we identify the intruders and any potential damage they caused, and how quickly we sort it out. There are also ways to mitigate the risk by working with conscientious partners to prevent threats by looking at potential flaws, exploits or 'zero-days' that have come to light. This is why it's necessary to have strong connections and undertake research to keep up to speed with these professional challenges.

Within NATO, we place a lot of emphasis and effort into preventative security. As the saying goes, this is frequently better than a pound of cure. We work towards system and security 'hardening,' reducing the attack surface of many of the threats. The aim of Attack Surface Reduction (ASR) is to close all the non-essential doors to your technical infrastructure and limit access to the open doors through monitoring, assessment of risk, and access control.

Our methodology is: *prevent*, *detect*, *respond*, and *recover*. It's a loop.

However, 'zero-day' attacks—which exploit a previously unknown vulnerability in a piece of software, and there are a lot of them—can and will occur. So there is an element of risk regardless of how strong your defences are.

What you need to do to mitigate 'zero-days' is:

- Undertake as much research into current threats as you feel necessary. There is plenty of information about 'system hardening' that is out there and does not cost anything to implement.
- You need to verify your coding and technology as much as you can. Here, many companies don't have the skill sets to fully undertake this on their own.
- If you don't have the capacity or resources, to do deep-dive analysis on all the software you are loading, you need to undertake an audit or sample of key stress points.
- Do as much standard verification, vulnerability assessment, and penetration testing when the software is running as you can.
- Set in training protocols for how employees use their technology and personal mobile devices in the workplace.
- Create a plan for the eventuality that something might go wrong. You need to have in place measures to detect when something has gone wrong and is exploited.

The ability to respond

If you have been the victim of a successful breach or attack, then stay calm and focus clearly. What matters most is how you respond to an incident. Your business requires strong resilience and good backup. At NATO, we have our incident teams, who have the ability to respond immediately and across our systems to mitigate the effects of an attack. These teams can be sent out to frontline sites or work online to recover the services that have been attacked.

The ability to recover

You also need the ability to recover your services quickly. This is supremely important. You need to swiftly reassure your customers you are both secure and open for business. Sharing attack information aids recovery, as there is commonality between organisations and businesses around the globe that use similar systems and software and are being subjected to the same types of attack. Divulging and sharing your experience with reputable third parties and with law enforcement agencies is also good business practice. Let's share this knowledge so we can know more than the attackers.

Addressing the skills shortage

Globally, there is a shortage of qualified people who can defend our freedoms and civic society from cyberattacks. Company executives need to appreciate and value that it is a highly specialised skill, and those experts who understand vulnerabilities are highly in demand. This demand reaches across the commercial, military, public, and governmental sectors.

In my 30 years in the security business, I have seen the position of the security manager move from the uncooperative techie who said, 'The answer is no, now what's the question?' to a new breed of committed individuals who are far more attuned to business needs. In truth, the old-guard security people weren't particularly helpful to the rest of the business and were referred to as 'the sleeping

The increasingly strategic importance of digital infrastructure has led to a seismic change that has placed the information security experts right into the heart of the decision-making process.

policeman on the information superhighway.' Some of the stereotypes were true, and some of this attitude does still persist.

Many of our most skilled cyber defenders are younger people who have been brought up on computer gaming, legal hacking, and code creation. What is important is to build a team from a variety of different experiences and backgrounds to provide strength and depth of experience. This includes the grey-haired veterans alongside the millennial generation raised with IT connectivity.

The increasingly strategic importance of digital infrastructure has led to a seismic change that has placed the information security experts right into the heart of the decision-making process. This, in turn, requires the security guys to talk in a language that other C-level executives understand.

The need to collaborate with good business

For many years, NATO has understood that no matter how good you think or believe you are, you never have the whole picture. Collaboration is the absolute key. We work across the alliance with our 28 national allies and member states, and since the Wales Summit Declaration in September 2014, a Defence Planning Package was agreed, which placed cyber defence as one of a number of priorities to enhance the alliance's capabilities. It recognised that cyberattacks can reach a threshold that threatens national prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. Cyber defence then became NATO's core task of collective defence.

At NATO, we are committed to developing national cyber defence capabilities and enhancing the cybersecurity of national networks upon which NATO depends for its core tasks. Close bilateral and multinational cooperation plays a key role in enhancing the cyber defence capabilities of the alliance. Strong partnerships play a key role, and NATO continues to engage actively on cyber issues with relevant partner nations.

Technological innovations and expertise from the private sector are crucial to enabling NATO and allies to achieve the Enhanced Cyber Defence Policy's objectives. Industry, quite often, understands the technology better than we do, and understands where these threats come from. That is why we have established and strengthened our relations with business over the last few years, including information-sharing agreements. We are actively talking and working together to share threat information about vulnerabilities. It is a force multiplier and what we call 'smart defence.'

NATO has signed a memorandum of understanding with a number of private-sector companies, and this experience has proved invaluable as we develop the partnership. Coupled with this, NATO has increased its cyber defence education, training, and exercise activities, at our own NATO CIS School and working with other training and education bodies.

If one thing is for sure in this digital age, something will happen this year that we never predicted. And your business has to expect what is the 'known unknown.' Defending your business from cyberattack is a 'top-down' issue that includes everyone. Let's work together on this.

Contributor Profiles

Contributor Profiles

NEELIE KROES

Former Vice President to the European Commission

Neelie Kroes, former European Commissioner and Vice President to the European Commission, joined both Salesforce's Board of Directors and Uber's Public Policy Advisory Board in 2016. She is also a Special Advisor to Bank of America Merrill Lynch.

From 2014 until 2016 she led StartupDelta, a public-private initiative to help promote her native country, the Netherlands, as a destination for startup companies. In 2015, she also became a non-executive member of the Open Data Institute's Board of Directors.

Ms. Kroes worked for the European Commission between 2004 and 2014. She started as Competition Commissioner responsible for ensuring a level playing field for business in Europe, fair prices and a wide choice for consumers, and in 2010 became Vice President of the European Commission responsible for the Digital Agenda. Her portfolio included the information and communications technology (ICT) and telecommunications industries.

Before her work at the European Commission, Ms. Kroes was President of Nyenrode University in the Netherlands (from 1991-2000) and served on various company boards, including Lucent Technologies, Volvo and P&O Nedlloyd.

paloalto NETWORKS®

Palo Alto Networks

GREG DAY

**Vice President and Regional Chief Security Officer,
Europe, Middle East and Africa**

Greg Day is vice president and regional chief security officer, EMEA, at Palo Alto Networks. In this role he oversees Palo Alto Networks' regional security operations and is responsible for regional cybersecurity strategy and the development of threat intelligence, security best practices, and thought leadership for Palo Alto Networks in EMEA.

With 25 years' experience in the area of digital security, Greg has helped organisations, large and small and across the public and private sectors, to understand risk posture and put in place strategies to manage it. He is widely acknowledged as an industry thought leader and experienced practitioner, capable of translating technology challenges into actionable business solutions.

Greg began his career with Dr Solomon's, later part of McAfee (now Intel Security) as a technical support analyst, and in a career that spanned 20 years he held a number of positions including information security consultant, global best practices team leader, security analyst, and director of security strategy. During this time, he led a range of initiatives to support customers, partners, and sales teams, authored a number of papers on topics across the security landscape, directed key cybersecurity initiatives, and provided guidance to governments and malware forensics training to law enforcement authorities. At Symantec he held the post of Security CTO for EMEA, managing a team of security strategists and driving Symantec's regional cybersecurity strategy. Most recently, as VP and CTO EMEA at FireEye, he was responsible for technology strategy and thought leadership.

Greg currently sits on the UK National Crime Agency steering committee, the UK-CERT/CISP advisory team, and the VFORUM research community, having formerly held the position of vice chair of the tech UK cyber security group. He has been part of the Council of Europe Convention on Cybercrime and has participated in a number of industry and advisory groups. He is widely acknowledged as an industry thought leader and is a familiar face at many cybersecurity events, as a regular on the speaker circuit, and has also been an active media spokesperson across much of the EMEA region.

Greg holds a BSc (Hons) in Business Information Systems from the University of Portsmouth.

vondst
advocaten

Vondst Advocaten

POLO VAN DER PUTT

Lawyer

Polo van der Putt heads the information technology practice at Vondst Advocaten. He has been practicing law for over 20 years, both in a national and and international setting. Amongst others, Mr. Van der Putt advises on sourcing and cloud projects, data analytics and processing, bot technologies, license and support deals, the structuring and termination of co-operation agreements and IT, and (public) procurement projects. He has a broad experience in drafting and negotiating commercial contracts and litigates on a regular basis. Mr. Van der Putt is arbitrator for the Foundation for the Settlement of Automation Disputes and board member of the Netherlands Association for Information Technology and Law. He is also a member of the editorial board of the magazine Internet and Law and is chief editor of the online Dutch IT and Law magazine www.ITenRecht.nl. He is the former chairman of the Dutch Outsourcing Association (Platform Outsourcing Nederland) and is the former chairman of the Dutch Association of IT Lawyers (VIRA). He is author of a legal text book on software distribution, publishes regularly and is often asked as a speaker.

PUCK POLTER

Lawyer

Puck Polter gained experience at full-service as well as niche law firms during her time studying Dutch law, information law and computer science in Amsterdam and in Edinburgh. Additionally, she worked at a fintech start-up in Berlin. Mrs. Polter's practice includes intellectual property law as well as IT law, with a focus on IT law and privacy. Mrs. Polter is a board member of the youth division of the Dutch Association for Information Technology and Law (NVvIR Jong) and publishes regularly, recently, for example, about exhaustion of copyright on software.

PwC

GREGORY ALBERTYN

Senior Director

Gregory is part of PwC's Data Governance and Security practice, advising complex organisations on all aspects of global data security, privacy and governance. Prior to joining PwC, Greg served as Global Privacy Officer for a Fortune 500 biotechnology company, where he built a multi-functional privacy organisation, based on leading risk and compliance frameworks such as NIST and ISO programmes.

AVI BERLINER

Manager, Financial Services Technology Consulting

Avi Berliner is a Manager within PwC's Financial Services Technology Consulting practice, with a focus on architecture, information management and data privacy, and cybersecurity issues.

First Lawyers

JUDITH VIEBERINK

Lawyer

Judith Vieberink is a senior associate at First Lawyers. She focuses on smart contracting, regulatory investigations and civil litigations. She represents corporations on a broad range of IT matters, such as data protection and privacy matters. Her clients are either public entities (or related) or private partners involved, for instance, within health care, retail or software sectors. First Lawyers specialises in IT law, resolving privacy issues, contract negotiations and proceedings.

Palo Alto Networks

FRED STREEFLAND

Senior Product Marketing Manager, EMEA; former CISO, LeaseWeb

Fred Streefland, EMSD, Bc. is Senior Product Marketing Manager for Palo Alto Networks, EMEA. Prior to Palo Alto Networks, Fred was the Corporate Information Security Manager (CISO) of LeaseWeb. Within this organisation, he was managing a small team of security engineers and was globally responsible for the corporate security of the LeaseWeb Group and its entities. LeaseWeb is a Dutch hosting provider with the largest network in Europe and operating worldwide with several data centres in the US, Singapore, Germany and the Netherlands.

After graduating from the Military Academy, Fred served more than 20 years as an Intelligence & Security officer (LtCol) in the Royal Netherlands Air Force (RNLAF) before he was offered a role as security consultant at IBM. After several years with IBM, Fred moved to Accenture as a senior manager where he led a team of 20 security consultants and delivered a risk assessment project on Industrial Control Systems (ICS) within the energy domain. After this he became Director Education & Training at the European Network for Cyber Security (ENCS), a start-up company in The Hague and developed the Red Team/ Blue Team course for ICS/SCADA systems.

Since 2008, Fred has been involved in the development of the Netherlands Cyber Security Strategy and the set-up of the National Cyber Security Centre (NCSC). Besides this, Fred is also a cybersecurity advisor for several Members of Parliament.

Fred holds an Executive Master of Security & Defense (EMSD) from the Air Defense College and a bachelor’s degree (Bc.) from the University of Applied Sciences of Amsterdam. He has certificates of several security courses (Black Hat, SABSA, Idaho National Lab, IBM Big Data Analytics).

Palo Alto Networks

MARK D. MCLAUGHLIN

Chairman and CEO

Mark D. McLaughlin joined as President and CEO of Palo Alto Networks in August of 2011 and became Chairman of the Board in 2012.

Before coming to Palo Alto Networks, Mark served as President and CEO of Verisign. Prior to that, he held a number of key positions at Verisign including serving as Chief Operating Officer, Executive Vice President of Products and Marketing, and head of the company's Naming Services business. Prior to Verisign, he was the Vice President of Sales and Business Development for Signio, a leading internet payment company. Before joining Signio, he was the Vice President of Business Development for Gemplus, the world's leading smart-card company. Previous to Gemplus, he also served as General Counsel of Caere Corporation and practiced law as an attorney with Cooley Godward Kronish LLP.

Mark also has the honor of providing the President of the United States with national security advice and expertise as a member of the National Security Telecommunications Advisory Committee (NSTAC), a body that, for three decades, has brought industry chief executives together to provide counsel on national security policy and technical issues to U.S. government leadership. Mark has served two-year terms as Chairman and Vice Chairman of the NSTAC. He received his J.D., magna cum laude, from Seattle University School of Law and his B.S. degree from the United States Military Academy at West Point. He served as an attack helicopter pilot in the U.S. Army and earned his Airborne Wings. Mark currently serves on the board of directors for Qualcomm Inc. (NASDAQ: QCOM).

Institute for Software Quality (IfSQ)

GRAHAM BOLTON

Chairman

Graham Bolton is a renowned software quality expert, experienced big data practitioner and performance specialist—in the media he has been labelled as a ‘Software Detective’.

Since choosing to specialise in database systems in 1982, he has designed and programmed large and complex systems around the globe, including those at the United Nations Food and Agriculture Agency, NATO, the Abu Dhabi Investment Authority and the South African Ports Authority. His 21-year involvement with the Postcode Lotteries of the Netherlands, UK and Sweden is a source of particular professional pleasure—the lotteries have raised more than €7 billion for more than 300 charities.

His passion for well-written, highly-maintainable software led Graham to establish the Cambridge-based Institute for Software Quality (IfSQ) in 2005 (where he is currently chairman) as well as its commercial counterpart, The OSQR Group, in 2010. He represents IfSQ on the ISO/IEC JTC 1/SC7 (Software and Systems Engineering) as chair of the Dutch mirror committee NEN 381007.

Graham is committed to furthering and promoting best practice in the software development industry, and their clients around the world.

.ON 2 IT.
SMARTER IT SECURITY

ON2IT

MARCEL VAN EEMEREN

Chief Executive Officer

Marcel van Eemeren started his career in 1990 with Acal as Plc Divisional Manager and was responsible for the divisional IT Products (a.o. Networking & Security) and new innovations and introductions to the market. Under his responsibility, Acal became Cisco distributor of the year and four years in checkpoint executive council. Marcel was with Acal for 14 years.

In 2005 Marcel established his own company, ON2IT. Under his supervision as CEO, ON2IT is still growing and is very successful within the IT security business in terms of new winning technologies, building a vision, broad network and experience. A strong co-operation with Palo Alto Networks was created in 2009. Palo Alto Networks is a specialised partner & managed service provider.

Secure Link
Infrastructure Security Solutions

SecureLink

PETER MESKER

CTO, Security Consultant, Co-founder

Peter Mesker is one of the founders of SecureLink in the Netherlands. He is an experienced architect/designer with a focus on presales and a visionary for (complex) security and infrastructure architectures. With a skill for converting a concept into a real design, he uses the best technical solution for each customer environment, taking care of the manageability and integration of a complex infrastructure. Managed security services and next generation security solutions are a special focus area besides supporting the customer on cloud (security) strategies and with the road to SDN. Involvement in hunting for and developing the right talent for SecureLink is a key activity on Peter’s agenda.

HEIDRICK & STRUGGLES

Heidrick & Struggles

CHRIS BRAY

Partner

Chris joined Heidrick & Struggles in 2010 and is a Partner in London. He leads the firm's Software & Systems Practices for EMEA. Chris's practice focuses on recruiting leaders for leading NASDAQ-listed technology companies, high-growth venture-backed and private companies in the technology sector, including enterprise software, cloud services, security, storage, embedded technology, and hardware companies. Chris specialises in CEOs, EMEA and UK regional presidents, sales directors, CTOs, heads of engineering, and CMOs. Chris holds a BA Hons degree from the University of Reading. He also leads the H&S Mobility Practice in EMEA and is a member of the firm's Sales Officer Practice.

GAVIN COLMAN

Partner

Gavin Colman is a Partner in Heidrick & Struggles' London office and is a member of the global Technology & Services Practice. With over ten years' experience in executive search, Gavin works with companies across various sectors to fill their senior IT roles (e.g., CIO, CTO) and with technology companies to fill executive roles. Prior to joining Heidrick & Struggles, Gavin was a partner at a boutique executive search firm as the head of their technology and CIO division. He began his career at Accenture, working on systems integration, business process reengineering, programme management, and change management projects. He has an MA in economics and accountancy from Aberdeen University.

GILES ORRINGE

Partner

Giles Orringe is a Partner in Heidrick & Struggles' global Financial Services Practice. He is head of the Fin Tech Practice for EMEA. He joined Heidrick & Struggles after having served as a Partner and head of the global infrastructure practice at a boutique international executive search firm. He previously spent eight years at another leading executive search firm, where he was a Partner and head of the global technology practice. During this time, he moved to New York in 2005, where he set up and ran the office. He has a Business History degree from the University of Manchester. He is based in the London office.

IBM Security

ALAN JENKINS

Associate Partner

Alan Jenkins is an Associate Partner with IBM Security in the UK. He has worked for the biggest system integrators. He runs his own consultancy and been a Chief Information Security Officer (CISO) for a number of different entities. He was CISO at Babcock International, a FTSE 100 company, and worked at Cheltenham. He works in the financial services division of IBM. He was a squadron leader in the RAF, and worked in security for the UK MoD.

Rabobank

KELVIN F. RORIVE

Delivery Manager Security IT Threat Management

Kelvin F. Rorive heads the IT Security Threat Management team within the Cyber Defense Centre of Rabobank, based in Utrecht, the Netherlands. The team is responsible for global threat management, security monitoring and incident response. Mr. Rorive has over 15 years experience in the field of information security in different sectors in several positions, including Manager Security Operations, Head of Security Management, Security Architect, Product Manager Security and Compliancy Officer.

Mr. Rorive contributes to the Dutch Platform voor Informatie Beveiliging (PvIB) as chairman of the activities committee. This platform is the knowledge centre in the field of information security in the Netherlands. He is also active in various national initiatives in the field of information security, including contributions to publications of the Cyber Security Raad and Expert Letters of the PvIB. He also sits on the jury of the prestigious Joop Bautz Information Security Award. In this way, Mr. Rorive strives to share his knowledge and experience with a broad audience and helps to develop the field of information security accordingly.

proximus

Proximus

CHRISTOPHE CROUS

Head of Cyber Security Solutions

Christophe Crous is Head of Cyber Security Solutions at the Belgian telecommunications operator Proximus and is responsible for the company's enterprise security practice. Mr. Crous was also an Executive Advisor to the Executive Vice President for the Enterprise Business Unit. He has been working for the Proximus Group—formerly Belgacom—for over two decades. With a background in networking (CCIE), Mr. Crous has been working in security for more than 10 years. He is responsible for the development, sales and delivery of security solutions to business customers. His clients include small businesses with more than five employees up to large banks, government institutions and multinationals. Mr. Crous has a degree in Industrial Engineering Electronics from the Katholieke Hogeschool Brugge-Oostende.

CSA cloud security alliance®

Cloud Security Alliance

J.R. SANTOS

Executive Vice President Research

J.R. Santos is the Executive Vice President of Research for the Cloud Security Alliance. He oversees the Cloud Security Alliance's research portfolio that covers a diverse range of cloud security topics such as IoT, quantum security, big data, artificial intelligence and application containers and microservices. He is responsible for the execution of the research strategy worldwide. In addition, he advises over 30+ working groups that develop industry-leading security practices, education and tools. J.R. has over 19 years of experience working in information security in a variety of industry sectors including finance, healthcare, aerospace, retail and technology. J.R. is an active professional in the security industry and has served on various boards and committees throughout his career. J.R. holds various professional certifications and a bachelor's degree from the University of Washington.

RYAN BERGSMA

Research Analyst

Ryan Bergsma is a Research Analyst for Cloud Security Alliance. He works with CSA's Enterprise Architecture, Big Data, Quantum Safe Security and Cloud CISC working groups to research and promote best practices in cloud computing security and has assisted with the development of CSA's STAR-Watch, a SaaS tool for security assessments. Ryan has more than 15 years of experience in various aspects of information technology including system support and administration, networking and development. Ryan has an associate's degrees in Computer Information Systems and Computer Information System Security from Whatcom Community College, and will complete his bachelor of science degree in Computer Information System Security at Western Washington University in 2017.

paloalto
NETWORKS®

Palo Alto Networks

ATTILA NARIN

VP of Systems Engineering and CTO, EMEA

Attila Narin joined Palo Alto Networks in November 2016. Before joining Palo Alto Networks, Attila was at Amazon for 12 years, and the last 10 years of this at Amazon Web Services (AWS). His most recent role at AWS was Head of Technology and Solutions Architecture for EMEA, an executive manager in the AWS team with a strong focus on leadership, building and guiding elite teams, business and technology transformation, and innovation through latest technologies.

Prior to joining Amazon, Attila held several software development and leadership roles at Microsoft and served on Bill Gates' Executive Strategy Team building innovative prototypes.

Attila holds a Computer Science degree from the University of Florida.

BT

BT

MARK HUGHES

President, BT Security, BT Global Services

Mark Hughes is President of BT Security, BT Global Services. He was appointed in January 2013 and reports to the Global Services Chief Executive Officer. BT Security brings together expertise from several areas of BT. As its President, Mark is responsible for all of BT's security activity around the world. Mark also leads on our security market offer, the BT Assure portfolio. When he joined BT in 2002, Mark managed various projects, including a partnership with the UK Government for the Criminal Records Bureau in Scotland. Before joining BT, Mark was commercial director of MWB Business Exchange.

Barclays

TROELS OERTING

Group Chief Security Officer

Troels Oerting is Group Chief Security Officer at Barclays Bank, in London. He started in the Danish Police in 1980 and went through the ranks, serving as Director of the Danish NCIS, Director of National Crime Squad, and later as Director of the Danish Serious Organised Crime Agency (SOCA). He held positions as head of NCB Copenhagen, head of Europol National Unit group (HENU), member of DK Europol management board delegation, and head of DK Schengen / Sirene. Later he became director of operations in the Danish Security Intelligence Service and was promoted to Assistant Director in Europol in 2009. He has had various responsibilities in Europol's Operational Department and serves as head of the European Cybercrime Centre (EC3).

ELENA KVOCHKO

CIO, Group Security Function

Elena Kvochko is CIO for the Group Security Function at Barclays. Previously, she was Head of Global Information Security Strategy and Implementation at Barclays. Prior to that, she was Manager in Information Technology Industry at World Economic Forum and ICT Specialist at the World Bank headquarters in Washington, DC. Elena has co-authored industry books on cybersecurity and contributed to *Forbes*, *The New York Times*, *Harvard Business Review*, and other media outlets.

XiaK (center of eXcellence in industrial automation Kortrijk) Ghent University

JOHANNES COTTYN

Assistant Professor in Automation, Automation Coordinator

Johannes Cottyn received his master's degree in industrial automation at Howest in 2003. In 2012, he obtained his doctoral degree in engineering sciences for industrial management and operations research at Ghent University. Since then he has been assistant professor and coordinator of the automation division at XiaK-UGent. He is an active member of the education committee of ISA Belgium, promoting a national/international network of automation professionals. His main research interests lie in material handling and logistics, industrial automation software, continuous improvement and manufacturing operations management.

TIJL DENEUT

Security Researcher, Collaborator

Tijl Deneut is a researcher at Ghent University and lecturer at Howest University College. He has several years of experience as an IT pentester and teaches, amongst others, Certified Ethical Hacking in Bruges in the Computer & Cyber Crime Professional programme. Since January 2015, Tijl has taken part in a research project concerning applied industrial security, the lock on your automation network. Applied research is targeted towards industrial (factory) floors where an Ethernet network is being used to control machines, robots and engines.

WAGENINGEN
UNIVERSITY & RESEARCH

Wageningen University and Research (WUR)

RAOUL VERNEDE

Information Security Officer

Raoul Vernède knows the Wageningen University well, not only working there but having studied there too. In the past he was IT-project leader, service manager and team manager operations and is now, and has been for some years, the corporate security officer of the WUR.

He is responsible for the CERT-incident response team and internal security policies with regard to information security. He advises the board and the privacy officer on current incidents and updates them on threats and risks envisaged. Some of his recent special interests are context aware identity and access management, security network segmentation and integrated vulnerability scanning of networks and web applications. He is an active part of the Dutch SURF (Collaborative organisation for ICT in Dutch education and research) security community in which national education and research organisations work together on secure and open information exchange.

National Cyber Security Centre
Ministry of Security and Justice

National Cyber Security Centre (NCSC-NL)

HANS DE VRIES

Head NCSC

Hans de Vries has been the Head of the National Cyber Security Centre (NCSC-NL) since November 2014. The NCSC falls under the Cyber Security Department of the Office of the National Coordinator for Security and Counterterrorism. Hans came to this position from the Ministry of the Interior and Kingdom Relations, where he served as head of the ICT Management Division and head of Operational Management Coordination. In recent year's he has worked in ICT security at interministerial and international level within the Ministry. Hans studied law at Leiden University and began his career in the private sector, working for Dutch department store chain Vroom & Dreesmann. He has worked for central government since 2002. Hans will also deputise for the Director of Cyber Security, Patricia Zorko.

KPN Telecom

JAYA BALOO

CISO

Jaya Baloo is the CISO of KPN Telecom in the Netherlands and in 2017 was recognised as one of the top 100 CISOs globally. Jaya works with an amazing information security team of highly driven specialists. Working in the information security arena for the past 18 years, she has worked mostly for global telecommunications companies such as Verizon and France Telecom. Jaya is also a frequent speaker at security conferences on subjects around lawful interception, mass surveillance and cryptography.

NATO Communications and Information Agency

IAN WEST

Chief of Cyber Security

Ian West is the Chief of Cyber Security within the NATO Communications and Information Agency—the primary provider of ICT solutions and services for the Alliance. From 2004 until his current appointment in January 2014, he was the Director of the NATO Computer Incident Response Capability (NCIRC) Technical Centre. He was formerly a law enforcement and security officer in the Royal Air Force and later responsible for INFOSEC policy, inspections, and security accreditation for NATO's Allied Command Operations.

In the *SC Magazine* awards for 2016, the NCI Agency cyber security team was awarded a Highly Commended in the Best Security Team of the Year category. Ian was named Chief Information Security Officer of the Year, the cyber security industry's highest award.

NOTES

CONTRIBUTORS

- **Alan Jenkins,** Associate Partner, IBM Security, UK
- **Attila Narin,** CTO, EMEA, Palo Alto Networks, Luxembourg
- **Avi Berliner,** Manager, PwC, USA
- **Chris Bray,** Partner, Heidrick & Struggles, UK
- **Christophe Crous,** Head of Security, Proximus, Belgium
- **Elena Kvochko,** CIO, Group Security Function, Barclays, USA
- **Fred Streefland,** Senior Product Marketing Manager, EMEA, Palo Alto Networks, the Netherlands; former CISO, LeaseWeb
- **Gavin Colman,** Partner, Heidrick & Struggles, UK
- **Gilles Orringe,** Partner, Heidrick & Struggles, UK
- **Graham Bolton,** Chairman, Institute for Software Quality (IfSQ), UK
- **Greg Day,** Vice President and Regional Chief Security Officer, EMEA, Palo Alto Networks, UK
- **Gregory Albertyn,** Senior Director, PwC, USA
- **Hans de Vries,** Head of the National Cyber Security Centre, (NCSC-NL), the Netherlands
- **Ian West,** Chief of Cyber Security, NATO Communications and Information Agency, Belgium
- **Jaya Baloo,** CISO, KPN Telecom, the Netherlands
- **Johannes Cottyn,** Assistant Professor in Automation, XiaK, center of eXcellence in industrial automation Kortrijk, Ghent University, Belgium
- **J.R. Santos,** Executive Vice President Research, Cloud Security Alliance, USA
- **Judith Vieberink,** Lawyer, First Lawyers, the Netherlands
- **Kelvin Rorive,** Delivery Manager Security IT Threat Management, Rabobank, the Netherlands
- **Marcel Van Eemeren,** CEO, ON2IT, the Netherlands
- **Mark Hughes,** President, BT Security, BT Global Services, UK
- **Mark McLaughlin,** CEO, Palo Alto Networks, USA
- **Neelie Kroes,** former Vice President to the European Commission, the Netherlands
- **Peter Mesker,** CTO, SecureLink, the Netherlands
- **Polo van der Putt,** Lawyer, Vondst Advocaten, the Netherlands
- **Puck Polter,** Lawyer, Vondst Advocaten, the Netherlands
- **Raoul Vernède,** Information Security Officer, Wageningen University and Research, the Netherlands
- **Ryan Bergsma,** Research Analyst, Cloud Security Alliance, USA
- **Tijl Deneut,** Security Researcher, XiaK, center of eXcellence in industrial automation Kortrijk, Ghent University, Belgium
- **Troels Oerting,** Group Chief Security Officer, Barclays, UK

SecurityRoundtable.org