BDO SCOPE

EXPERT UPDATES FOR INTERNATIONAL BUSINESS

‘We can only solve the problem with **coordinated action’**

Lokke Moerel Member Dutch Cyber Security Council

CYBERSECURITY: HOW TO MAKE YOURS BETTER

CREATING A RELIABLE **CHAIN**

BDO

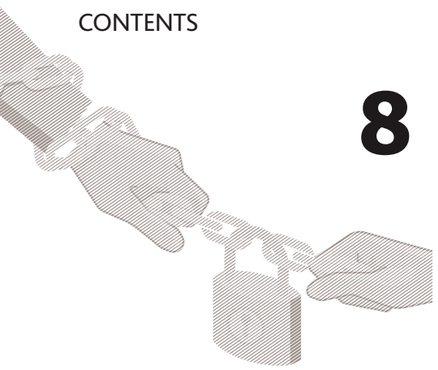
‘If you spend more on coffee than on IT security, **you will be hacked. What's more, you deserve to be hacked’**

Richard Clarke,
White House Cybersecurity Advisor

CYBERSECURITY ~ [saɪbəˌsɪˈkjʊərɪtɪ]

Cybersecurity means freedom from danger or damage caused by the disruption, failure or abuse of ICT systems. This danger or damage may consist of a limitation in the availability or reliability of ICT systems, a breach of the confidentiality of information stored in them, or damage to the integrity of that information.

Safeguarding digital security and freedom and maintaining an open and innovative digital domain are among the essential preconditions for the proper functioning of a society.



‘You should focus on **recovering quickly** after a cyber-attack’

Marcel Verbruggen,
Security and Privacy Officer,
Vanderlande Industries

COLOPHON

BDO SCOPE is published by BDO • **Concept and production** Monte Media • **Texts and interviews** Leonard van den Berg, Paul Groothengel
Photography Sander Nagel, BDO, Monte Media • **Illustrations** Ivo van IJzendoorn • **Art direction and layout** Veronique Gielissen
More information BDO, Van Deventerlaan 101,3528 AG Utrecht, PO Box 4053, NL-3502 HB Utrecht, +31 (0)30 284 98 00, www.bdo.nl/corporateclients

Cybersecurity

THE **DOMINO** EFFECT

Are you familiar with the domino effect? One falls, knocking over another, and another. In the right hands, it's mesemerising – millions of colourful domino blocks tumbling artfully against each other in ingenious patterns. Yet one accidental tap while setting it up and it’s a disaster.

I was reminded of it when compiling this cybersecurity-themed issue of BDO Scope. Our discussions and interviews highlighted the need to look beyond your own doorstep when protecting your organisation from digital threats in today’s interconnected world. Individual organisations are part of a greater, interdependent whole. Suppliers, partners, your staff and external hires, logistics, distributors, buyers and end users – the entire spectrum of the chain must be addressed.

In addition to discipline, good cybersecurity requires reliable controls throughout that chain. You’ll only really be safe when all relevant players are 100% serious about cybersecurity, all the links in the chain are strong and you’ve built good security zones between them. Only then can you ensure a single cyber weakness won’t bring down the entire chain. And you’ll also comply with new, more stringent international legislation in the process.

I hope this magazine gives you useful insights and the inspiration to create a strong, reliable business chain – to protect your organisation and safeguard the ecosystem around it against a potentially devastating domino effect.

If you’ve any questions or comments, feel free to contact me at john.hijmans@bdo.nl. And please don’t hesitate to ask me for help. Together, we can find a secure solution.

Sincerely,

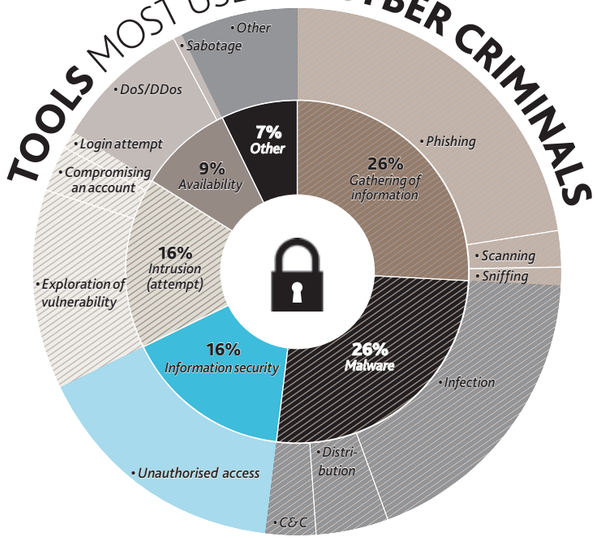
John Hijmans,
Partner, BDO Corporate Clients
Utrecht

WEAPONS OF MASS DECEPTION

Source: NCSC, Cybersecurity matrix for the Netherlands (CSBN) 2016, Cyber Security Advice 2016.

1

TOOLS MOST USED BY CYBER CRIMINALS



Inner ring: main categories
Outer ring: sub-categories

2

4 DUTCH CYBER FACTS

1. 36% of all economic growth in the Netherlands is generated online (1990-2013).
2. The Amsterdam Internet Exchange (AMS-IX) is the world's largest online trading platform.
3. The digital infrastructure is the fourth main port of the Netherlands after Schiphol Airport, the Port of Rotterdam and the Eindhoven Brainport Top Technology Region.
4. Together with the UK, the Netherlands has the most ICT-intensive economy in Europe, with ICT accounting for more than 5% of national income in 2015.

3

TOP 5 CYBER RISKS

1. Human action and (inadvertent) behaviour; lack of knowledge.
2. Chain-based interdependencies.
3. Mixing of private and professional dealings in the use of mobile devices.
4. Vulnerable ICT systems that are not up-to-date.
5. Software that has not been securely developed.

4

CYBER-THREAT MATRIX

Cybercriminals do not all behave in the same way. So where do the biggest threats lie? And which 'bad guys' target which victims?

SOURCE OF THE THREAT	TARGETS: GOVERNMENTS	PRIVATE ORGANISATIONS	CITIZENS
PROFESSIONAL CRIMINALS	THEFT AND PUBLICATION OR SELLING OF INFORMATION	THEFT AND PUBLICATION OR SELLING OF INFORMATION	THEFT AND PUBLICATION OR SELLING OF INFORMATION
	MANIPULATION OF INFORMATION	MANIPULATION OF INFORMATION	MANIPULATION OF INFORMATION
	DISRUPTION OF IT	DISRUPTION OF IT	DISRUPTION OF IT
	IT TAKEOVER	IT TAKEOVER	IT TAKEOVER
STATE ACTORS	DIGITAL ESPIONAGE	DIGITAL ESPIONAGE	DIGITAL ESPIONAGE
	OFFENSIVE CYBER CAPABILITIES	OFFENSIVE CYBER CAPABILITIES	
TERRORISTS	DISRUPTION/TAKEOVER OF IT	DISRUPTION/TAKEOVER OF IT	
CYBER VANDALS AND SCRIPT KIDDIES	THEFT OF INFORMATION	THEFT OF INFORMATION	THEFT OF INFORMATION ↘
	DISRUPTION OF IT ↗	DISRUPTION OF IT ↗	
HACKTIVISTS	THEFT AND PUBLICATION OF ↗ OBTAINED INFORMATION	THEFT AND PUBLICATION OF ↗ OBTAINED INFORMATION	
	DEFACEMENT	DEFACEMENT	
	DISRUPTION OF IT	DISRUPTION OF IT	
	IT TAKEOVER	IT TAKEOVER	

KEY: WHAT THE COLOURS MEAN

↗ THREATS HAVE INCREASED SINCE 2015	LIGHT RISK: No new trends or phenomena are recognised that pose a threat. OR (Sufficient) measures are available to remove the threat. OR No appreciable manifestations of the threat occurred during the reporting period.	MEDIUM RISK: No trends or phenomena are observed that pose a threat. OR (Limited) measures are available to remove the threat. OR Incidents have occurred outside NL and there have been several minor incidents in NL.	HIGH RISK: There are clear developments that make the threat expedient. OR Measures have a limited effect so the threat remains substantial. OR Incidents have occurred in NL.
↘ THREATS HAVE DECREASED SINCE 2015			

BUILDING A RELIABLE CHAIN

BEAT **CYBERCRIME** TOGETHER

Malware, phishing, ransomware, DDoS attacks… cybercrime is the plague of the 21st century. Chain-based cooperation is a good way to foster cyber resilience.

We all know we should never open attachments to unfamiliar emails, but cybercriminals go much further and work in increasingly clever ways. That's why it can be difficult to quantify the damage caused by cybercrime, not just the direct losses suffered, such as theft of confidential information, personal data and money, but also the indirect losses, which are often underestimated. Specialist knowledge is needed to properly clean and (where necessary) reconfigure ICT systems after a cyber-attack.

Then there's the damage to your corporate image, which shouldn't be underestimated, either. You can't simply win back the confidence of your clients once their private data has been stolen, say BDO cybersecurity advisers Sandra Konings, Robert van Vianen and Jeffrey de Bruijn. What's more, the fine for privacy violations is hefty, in some cases €820,000 or 10% of your revenue. At the end of May 2018, these fines will increase under the EU Data Protection Directive to a maximum of €20 million or 4% of a company's total global revenue. ›

'People still aren't always fully aware of the risks of cybercrime'

7 TIPS **FOR MORE CYBERCRIME RESILIENCE**

1. Make sure your employees recognise the signs of hacking and make them aware of the risks.
2. Create a culture in which employees are confident enough to report warning signs and incidents.
3. Define your companies' core data and protect these with proper measures (in ICT and business processes).
4. Monitor your ICT systems to detect incidents at an early stage.
5. Have a response ready. Know how to react when an incident occurs. This response should at least include technical (ICT) actions and internal and external communications plans.
6. Collaborate with your supply chain in the fight against cybercrime.
7. Cybersecurity is a form of risk management that should be on the management agenda.

TOP 4 **ARGUMENTS FOR CROSS-CHAIN COLLABORATION**

1. The chain as a whole will become more resilient and hence stronger.
2. Together, you will spot hackers' new attack patterns faster.
3. Together, you will identify interdependencies more easily and see which shared links need to be strong.
4. Together, you will have a better understanding of your clients' requirements for continuity, quality and data protection – elements that come under pressure during a cyber incident.

Sandra Konings is Cybersecurity Partner at BDO. She previously served as Chief Information Security Officer at ASML and Rabobank Group.

Robert van Vianen is Cybersecurity Partner at BDO. Before this, he worked at PricewaterhouseCoopers and Nuon.

Jeffrey de Bruijn is Senior Advisor Cybersecurity at BDO. He was previously a consultant at Power of 4, an information security and data protection consultancy.

› Are companies sufficiently aware of the need for cybersecurity?

Konings: 'This differs widely from sector to sector, with the financial sector in the lead. Hackers have always been motivated chiefly by financial gain, so the financial sector has been dealing with cyber-attacks for far longer than other sectors. Client confidentiality is also of paramount importance to financial institutions. Chemical companies, which traditionally focus on safety and security, also lead the field in combating cyber-attacks. Other sectors show a varying degree of cyber resilience. People still aren't always fully aware of the risks of cybercrime.'

De Bruijn: 'Sometimes I hear that businesses aren't giving priority to cybersecurity mainly because they're worried about what it will cost them in terms of time and money. They don't realise the enormous cost of not doing so, or the damage to their image if things go wrong.'

Companies are now required to report data leaks. How strictly is this enforced?

Van Vianen: 'Since January 2016, the Dutch Personal Data Protection Act has required companies to report leaks of personal data to the Dutch Data Protection Authority. If a data leak is due to serious culpable negligence or a deliberate infringement, the Dutch Data Protection Authority can impose a fine. And if a data leak results in a company failure, this may be regarded as mismanagement and the liquidators could even hold the managing director personally liable.'

'Businesses forget the immense cost of a major cyber-attack in terms of monetary loss and damage to credibility'

Employees must handle their clients' personal data in confidence. How difficult is this in practice?

Van Vianen: 'The same applies here as anywhere else. A minor infringement can precipitate a major incident. At the end of November 2016, 700 pages of confidential information belonging to Europol fell into the hands of Zembla, a television programme. A Europol employee had taken sensitive information home, in contravention of the rules, and copied it onto a back-up disk, which was linked to an insecure internet connection. Europol called the data leak a "very serious incident". In another example, a local authority representative emailed a file containing the medical details of a large number of private citizens to the wrong address, a case of human error that had major implications.'

Businesses increasingly operate in a network-based economy and chain-dependency is growing. Can we work together to minimise cyber risks across the chain?

Konings: 'Certainly. In fact, it's essential for every chain. Cyber-attacks are now so sophisticated that companies rarely realise they've been hacked. It generally takes them around 200 days to realise what has happened. So it's often a very long time before companies fully appreciate the losses they've sustained. The same applies to their partners in the chain. If a supplier has to suspend production due to a cyber-attack, this could cause problems for companies further down the line. Organisations are increasingly having to acknowledge that their chain is only as strong as its weakest link. Resilience to cyber-attacks demands a fully chain-based approach.'

De Bruijn: 'For example, it's very risky for all partners in a chain to use the same IT supplier, because if these IT systems are compromised by a cyber incident, this can affect the entire chain. What's more, you'll only find out what has happened when you come to exchange relevant information with other partners in the chain. So it's wise to work across the chain to put together scenarios for a possible cyber-attack and to conclude clear agreements about what each partner should do to increase their cyber resilience.' ›

'MAIN PORTS LEARN FROM EACH OTHER'

Schiphol Airport and the Port of Rotterdam are working closely to improve their 'digital resilience'. They each provide supply chain partners with a platform for exchanging ways to secure their IT systems.

Sjoerd Blüm (Schiphol): 'Risk awareness is in our DNA. We work closely with our two main partners, KLM and Dutch air traffic control, since digitisation is making us increasingly interdependent. If a system in one organisation fails, this can affect the continuity of another. However, our ecosystem is much bigger, which is why we've launched the CYSSEC platform for all our supply chain partners so we can help each other by sharing information.'

Marijn van Schoote (Port of Rotterdam): 'The same applies to us. We use our digital platform FERM to encourage employees and hundreds of supply chain partners to exchange information on cybersecurity. We want them to adopt identical standards and learn lessons from incidents and near-incidents. Only then will they make the chain as a whole more resilient to cybercrime. We're working closely with Schiphol Airport to learn from each other how best to structure an ecosystem of this kind. It's proving highly instructive and inspiring for us all.'

Sjoerd Blüm is Head of Business Technology at Schiphol Airport. **Marijn van Schoote** is Senior Risk Officer at the Port of Rotterdam.

'SMART DATA ENCRYPTION IS A MUST'

'At our university, cybersecurity is as much about the conduct of students and staff as about technology. Because we're sharing more information externally and can store it in the cloud, the human factor is increasingly critical.

'Each year, the ICT innovation partner for higher education, SURFnet, publishes key cyber trends. I endorse its findings: the biggest high-impact threats are manipulation of digitally stored data and identity fraud. In the sphere of research, they are access to and publication of data and espionage. Last year, around 200 computers at VU University Amsterdam were attacked by cryptoware. Fortunately, that's not something we've experienced so far.

'We classify all the information within our university into three levels, with appropriate security measures for each. We also maintain a high level of information exchange with our partners, chiefly in the hi-tech and manufacturing industries. This exchange covers intellectual property rights, since we need to know who owns what rights and is responsible for securing what information. We work closely with many partners, for whom we must operate a secure digital environment. That's why smart data encryption based on secure algorithms is a must.'

Martin Romijn is Chief Information Security Officer at Eindhoven University of Technology.

› **Which chains have made the most progress on a joint cybersecurity approach?**

Konings: 'As early as the 1990s, Dutch banks teamed up to ward off cyber-attacks against their cash-point machines. The big problem at the time was "skimming", where criminal gangs copied bank cards to withdraw money from cash machines. Early on, bankers decided to take combined action to counter these attacks. They've since used the same strategy in their fight against cybercrime.'

De Bruijn: 'As an adviser to the Dutch National Cyber Security Centre, I oversaw a project in which energy supply companies – Shell, TenneT, Alliander (see the case study on p18), Nuon and Gasunie – worked together to identify the existing cyber risks in their chain. They found that consultation and information exchange could highlight many cyber risks that might not be visible to individual organisations. The relevant players also recognised that they were growing increasingly interdependent, and that this brought with it other, newer risks. The project yielded a methodology that BDO plans to roll out to other sectors.'

Can you give an example of specific aspects that companies can tackle?

De Bruijn: 'With your partners in the chain, identify the privacy-sensitive data you are exchanging, how you are going to secure it and, if there is a data leak, who will report it to the authorities. You must also always draw up a detailed processing agreement if you're going to have personal data processed by an external player such as a cloud provider. This will clarify who is responsible for what. You should also check whether the companies you're working with have the correct ISO certifications.'

Van Vianen: 'I also often advise companies to appoint an Information Security Officer, to carry out annual risk assessments and to implement additional protection measures when developing their products and services.'

'Proper security requires a fully chain-based approach'

What is the EU doing about cybersecurity?

Konings: 'The European Commission regards cybersecurity as vital and has adopted the directive on security of network and information systems (the NIS Directive). The NIS Directive is designed to secure network and information systems that are crucial for maintaining a wide range of vital infrastructures throughout Europe - energy, transport, water, banking, financial market infrastructures, healthcare, digital infrastructure, and digital service providers. Over the next few years, EU member states must enshrine the new regulations in their own national legislation. The idea is that a cyber-attack or data leak in vital sectors should always be reported to the relevant local government so that it's aware of what's happening and can share information about the appropriate response with other EU countries.'

'Decide with your chain-based partners how to regulate the security of your privacy-sensitive data'

Can you insure against the risk of a cyber-attack?

Van Vianen: 'Not entirely. Reputational harm, for instance, can't be insured, as a result of which many companies live in fear of the possibility of cybercrime. But that really isn't necessary since you can quite easily assess all the potential cyber risks, after which you should decide what data you really want to protect so that you can take appropriate action, such as encrypting sensitive data files. However, there are some risks you can't or don't want to avoid, and you can insure yourself against them. But it would be unworkable to try to insure yourself against everything.'

Konings: 'That's why you've got to start at the source: identify the main cyber risks for your organisation and apply the best measures to manage them. Be aware that 100% prevention is impossible and focus instead on detection so that you can intervene swiftly if, despite all precautions, something has still gone wrong. Then you can minimise the impact.' ‹

AIVD
Sector national security
Services counter-terrorism, strengthening national security, gathering civil defence information abroad
Staff complement approx 1,700

‘YOU CAN **NEVER** BE SECURE **ENOUGH**’

Robert Spronk (61, left) has been Director of Operations for the Dutch government’s General Intelligence and Security Service (AIVD) since 2015.
Marcel Tuinder (53, right) is Deputy CIO of AIVD and has served as Head of the National Signals Security Bureau since 2008.

CASE | **1**

AIVD has its work cut out with our cybersecurity. The agency focuses mainly on state-sponsored cyber espionage, primarily by countries such as China, Russia and Iran, where the aims are political but also include theft of vital corporate data. What can a company director do to prevent this?

Unrest on the EU's outer borders, the threat of radical Islam, cyber hacking – the risks continue to mount. The Dutch government's General Intelligence and Security Service (AIVD) is hard at work dealing with these many challenges. The agency does most of its work away from the spotlight, but for this interview, Robert Spronk and Marcel Tuinder, both of whom work for the Netherlands' 'least visible public service', have agreed to step briefly out of the shadows.

How important is cybersecurity in AIVD's activities?

Robert Spronk: 'Our main brief is national security. Terrorism is a very important part, but w're increasingly focusing our investigative work on cyber threats. The incidence of cyber-attacks is growing, in its extent, complexity and professionalism. We ourselves don't deal with cybercriminals. That's more a job for our colleagues in the police force. The focus of our work is more on state-sponsored cyber espionage. Hostile states use cyber-attacks for political and economic gain, influencing populations and social destabilisation. They're also increasingly using cyber to sabotage critical social infrastructures. This constitutes a direct threat to national security, which makes it a focus for the AIVD, increasingly in partnership with the security services of other countries. Thanks to its unique mandate, the AIVD can make a vital contribution to countering this threat.'

Which states currently pose the biggest threat to our national security?

Marcel Tuinder: 'China, Russia and Iran. Cyberspying on Dutch government agencies by Russia is chiefly politically motivated. Their aim is to gather information about our political decision-making processes and standpoints and the development and content of our political and economic plans. We may be a small country but we're still members of NATO, the EU and many other alliances, which makes us influential and an attractive target for cyberspies. China has more of an economic interest in the companies that form part of the Dutch top technology infrastructure, such as those in the hi-tech, chemicals, energy and life sciences and health sectors. These cyber-attackers are primarily on the lookout for highly specialist, sometimes even experimental technologies that haven't come to market yet – blueprints, investment plans, research results, tenders for large-scale projects, anything of that kind. This trend is undermining our knowledge economy and is especially disastrous for the companies affected.'

How concerning is the threat at present?

Spronk: 'Extremely concerning and I'm not optimistic about the future. The Netherlands has always been a very open economy and, with the advent of the Amsterdam Internet Exchange, the world's largest internet exchange point, now has a highly developed online infrastructure. We have more and more online traffic running on a growing number of servers. This makes our network highly attractive to those who want to do us harm. What is more, cybercriminals often use servers in the Netherlands to attack entities in other countries. A cyberattack on the US Democratic party, for example, was carried out on the server of someone working for the self-styled digital rights organisation Bits of Freedom in Amsterdam. Another worrying factor is that it's becoming progressively easy to mount a cyber-attack. The dark internet, for example, is advertising more and more facilities for carrying out cyber-attacks.'

'Many organisations in both the public and private sectors are still incredibly naive'

How can companies adequately secure themselves against these attacks?

Spronk: 'Many organisations in both the public and private sector are still incredibly naive. They often think they've done enough to secure themselves, but we know the threat is growing and becoming ever more complex. In this business, you can never do enough. Hackers have a permanent and detailed eye open for innovative initiatives. And technical developments are making it easier for them to conceal and shield off their cyber activities. That's why you've got to remain constantly alert to new forms of attack and devise specific countermeasures to ward them off. Our advice to large corporates is never to leave cybersecurity to the ICT department alone. The severity, nature and extent of the threat is so great that it can only really be addressed at Executive Board level.'

'The severity, nature and extent of the threat is so great that it can only really be addressed at Executive Board level'

So it's not a question of if you're going to be hacked but when?

Tuinder: 'Absolutely. But there's nowhere near enough awareness of that. In the old days, you caught your spy, extradited him and that was that. Cyber-attacks, by contrast, are effective, efficient and relatively low-cost. They're also difficult to tribute, so the perpetrators can often carry them out as often as they like and in complete anonymity. The likelihood of a successful investigation and prosecution is minimal.'

Presumably once a hacker has got into the system, many companies either don't realise it or do so too late?

Spronk: 'Unfortunately, yes. Once a hacker has gained access to a computer system, it can be very difficult to remove him permanently. Very little attention is being given to dynamic security measures aimed at detecting activity by hackers who have already got into your system. After a successful cyber break-in, hackers can often remain active in a network undetected for quite some time. So we tell companies to regularly train their staff to spot anomalies and unusual or unexplained developments in their business processes and infrastructure. Try to think like a spy and focus your primary attention on your crown jewels.'

Such as?

Tuinder: 'Unusual data transactions in the middle of the night. Detecting the presence of an intruder as soon as possible is absolutely crucial for every company since it then takes you less time to intervene. And securing the gateway to your system remains essential. This is relatively easy to achieve since you have to concentrate on only one point in your infrastructure. It's much easier, after all, to detect an unauthorised person at a border crossing than in a big city, although use of the cloud is making it more difficult to secure gateways.'

If AIVD detects a state-sponsored cyber-attack on a company in a critical sector, would it notify that company?

Spronk: 'Yes, although we don't see this as our primary task. We'll either notify the affected company directly or through the National Cyber Security Centre.'

How do companies react to the news that they've been hacked?

Spronk: 'It varies. They're pleased to be told and to know they can do something about it. But the news also frightens them. They want to know what has been stolen. And it's always bad news since it will cost them time, money and effort to repair the damage and close the leak.' ‹

CYBERSECURITY: HOW DO YOU RATE YOURS?

What score does **Aad Dekker** give Alliander's cybersecurity? 'A 7 out of 10: 100% cybersecurity is a utopian dream, but there's certainly still room for improvement.'

'CONTROL THE FIRE'

Alliander has decided to work with key partners to ensure optimum cybersecurity across the chain. This is crucial because technological developments are making these companies progressively interdependent.

So far, grid operator Alliander hasn't had much trouble from cybercriminals (touch wood) apart from the usual 'knocking on the front door', as Privacy and Security Officer Aad Dekker puts it. By this, he chiefly means the standard spam that's targeted at all companies these days.

Is it difficult for such a large organisation to become and remain alert to the risks of cybercrime?

Dekker: 'Not in principle, although we do have to keep on working to maintain our cyber awareness. The threat of hacking is growing and cybercriminals are becoming increasingly professional.'

How many of your 7,000 employees are working on cybersecurity?

'We currently have 15 dedicated staff, but we'll be recruiting more. At the same time, we need to make managers in our business more security aware. We're constantly working to raise internal awareness.'

How?

'Through internal communication campaigns and testing – for instance, by sending out phishing emails or a contaminated USB stick and asking them to insert it into their laptop. Our tests will give them a wake-up call.'

Alliander has also upped its use of cloud-based storage. Does this automatically increase the risk of cybercrime?

'Not necessarily, although we obviously keep a close eye on how well our cloud providers are maintaining the security of our client data. We've set up guidelines with Procurement on how this should be done and have concluded a processing agreement with these providers. This is in any case a requirement specified by the Dutch Privacy Protection Act.'

You've also worked with some of these partners to analyse the risks of cybercrime in the energy chain. Why and what emerged from it?

'Together with Shell, TenneT, Nuon and Gasunie, we scrutinised key critical IT systems, along with the associated cybercrime risks. You can only improve digital security within the chain if you work with all your suppliers and buyers. This is crucial, because technological progress is making us all increasingly interdependent. A security breach in one company could precipitate a security breach in another.'

What can each link in the chain do to improve security?

'First, you need to identify who is dependent on whom. What are the critical IT systems within the chain and what risks do the various partners have to contend with? The art is to decouple processes and then ensure the connections – the interfaces between these separate units – are extremely well secured.'

Rather like a firebreak in a forest?

'Exactly. We need to ensure that a "spark" can't jump across and set fire to another part of the forest. If one of the chain partners sustains a leak or is hacked, the rest of the chain mustn't be similarly affected. That's why we've created separate internal zones in our networks to keep out viruses or cyber-attacks and to prevent those that do get in from spreading.' ‹

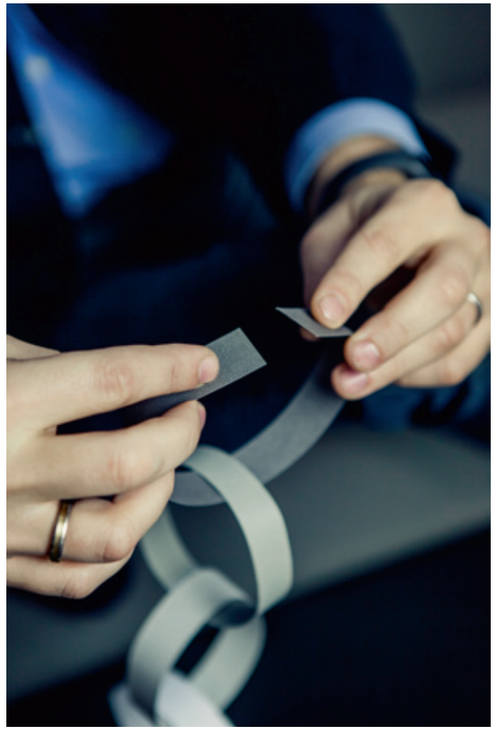
ALLIANDER
Sector energy
Product network management and electricity and gas distribution
Staff complement 7,240
Clients connected 5.7 million
Active in Gelderland, Noord-Holland, Flevoland, parts of Zuid-Holland and Friesland provinces in the Netherlands
Annual revenue approx €1.6 billion (2015)

Aad Dekker (57) studied electrical engineering at Delft University of Technology. He worked as an IT consultant for Baan, Multihouse, ASML and PTT Post before joining Robeco as Corporate Information Security Officer. In 2007, he was appointed CISO at Nuon. After the break-up of the company, he became Privacy and Security Officer for grid operator Alliander.

FROM TRUST TO CONTROL

VANDERLANDE INDUSTRIES
Sector manufacturing industry
Product logistical process automation at airports and for parcel services and distribution centres
Staff complement more than 4,500
Outlets in 105 countries
Annual revenue approx €988 million (2015)

After obtaining a degree in Information Technology at Eindhoven University of Technology, **Marcel Verbruggen** (39) began his career as a software engineer with KISS Solutions before joining Vanderlande as a Network Engineer in 2005. In 2012, he was appointed Security Officer and last year additionally took on the role of Privacy Officer.



For Dutch company **Vanderlande**, the cybersecurity of the logistical systems it installs for its global clients is crucial. After all, if these systems are undermined by hacking, the processes that depend on them will also grind to a halt. So how does Vanderlande optimise its cybersecurity measures?

The company's founder, Eddie van der Lande, started an engineering firm in Veghel, the Netherlands, in 1949. Now, nearly 70 years on, Vanderlande has evolved into a global market leader in baggage-handling systems and distribution centres. The company delivers parcel-sorting systems, automated logistical systems to Europe's biggest retailers and baggage-handling systems to more than 600 airports worldwide. Vanderlande continues to rapidly expand. In 2015, it took a record €1.5 billion in orders and it recruits an extra 700 employees each year.

Get into the cybercriminal's mind

Although Vanderlande is a typical manufacturing company, an increasing share of its revenue comes from services designed to ensure that its clients' systems continue to meet their requirements. Naturally, this includes cybersecurity, says Security and Privacy Officer Marcel Verbruggen. 'There is a serious potential risk that our systems, which are running at our clients' premises 24/7, could be hacked and may turn out not to be fully secure. It's our job to help the client minimise that risk. What specifically does this involve? My colleagues and I occasionally visit clients and prospects to discuss the cybersecurity of our systems with their IT teams. I always try to impress on them that they must constantly try to get into the mind of the cybercriminal, since that will allow you to stay ahead of them.'

Business models of cybercriminals

The advent of the Internet of Things is causing operations technology (the technology embedded in industrial networks such as those of Vanderlande) to progressively merge with information technology. Verbruggen explains: 'Until now, the two worlds were always separate, but this can't be sustained at a time when every appliance has its own IP address. This interconnectivity involves an inherent cyber risk, which confronts operations technology with the same threat – hacking and malware – that faces company IT environments.'

Verbruggen also points out that cybercriminals are becoming increasingly clever and skilful. 'Previously, such people would be sitting in a garret hacking in their spare time, but this has gradually evolved into major criminal gangs using substantial budgets to pursue sophisticated business models. What's more, we're seeing more state-sponsored malware and hacking. And I'm not just referring to Russia and China.'

Blackmail

These days, you can buy cybercrime as a standard solution online, says Verbruggen, 'complete with helpdesk numbers'. Unfortunately, this development means you can never guarantee that your systems are 100% secure. He says: 'Although most risks can be covered, some cannot.'

There is an upper limit when it comes to combating the risk of cybercrime, he adds. 'You need to make sure you don't restrict the flexibility and productivity of your employees. More important, though, is that as well as targeting security, companies should also focus on recovering quickly after a cyber-attack.' Verbruggen speaks from experience. Like many companies, Vanderlande was once targeted by ransomware – software used by cybercriminals to take files 'hostage', returning them only in exchange for a ransom. Verbruggen doesn't want to go into much detail, but says: 'We've never given in to this kind of blackmail. However, these are incidents from which we can recover relatively quickly and easily, partly by adopting a strict policy on central data storage and frequent back-ups of all centralised data, although this is time-consuming.'

Improve the control-based culture

The process of raising awareness of cybersecurity is not restricted to the workfloor, though. Senior management also has to take a lead, says Verbruggen. 'Our Executive Board is committed to the need for cybersecurity and has launched a relevant ISO certification process. We were helped by our corporate culture, because we've always been a family business with an extremely open, trust-based culture. This is a good starting point for information assurance and one of our strengths. That said, we still need to do more to move from a trust-based to a control-based culture.'

Earlier this year, Vanderlande launched an internal awareness campaign for all its employees. Only by repeating the message frequently can the company be certain that staff will fully internalise and act in accordance with it, Verbruggen argues. 'It's the same approach that's used by production companies to improve their physical safety record. For instance, we'll be sending out internal phishing emails purporting to be from the IT department, telling people they've got a virus and to give us their password. After all, that's what cybercriminals do. Later, we'll obviously confront them with the scam.'

Be careful when tendering

However, internal awareness alone will not save you, Verbruggen points out. It's equally important to address the cybersecurity of your supply-chain partners because they're exposed to similar risks. 'For example, if a department unilaterally decides to purchase technology from a supplier without involving the central ICT department, that could very quickly lead to trouble. In the past, we asked an external contractor to set up a website for our in-house Christmas celebrations, where employees could select presents for their children. To do so, however, they first had to enter some personal details, including their password. Unfortunately, the website turned out to be insecure. Thankfully, we were able to intervene in time, but it shows how even "innocent" initiatives can conceal major cyber risks if they're not adequately checked.' ‹

CYBERSECURITY: HOW DO YOU RATE YOURS?

What score does **Marcel Verbruggen** give Vanderlande's cybersecurity? 'A generous 7: 10 out of 10 is unattainable, but we're ultimately looking to achieve a respectable 9.'

'We still need to do more to move from a trust-based to a control-based culture'

'It's important to focus on a quick recovery after a cyber-attack'

‘TWO-FACTOR AUTHENTIFICATION IS A **MUST**’

Digitisation is turning large companies into gold mines for cybercriminals. How can the public and private sectors arm themselves to combat this cyber threat?

Lokke Moerel (51) is Senior of Counsel for international legal firm Morrison & Foerster. Earlier in her career, she worked as ICT Partner for Linklaters and De Brauw Blackstone Westbroek. Moerel is also Professor of Global ICT Law at Tilburg University in the Netherlands and a member of the Dutch Cyber Security Council.

CYBERSECURITY: HOW DO YOU RATE YOURS?

What score does **Lokke Moerel** give to the cybersecurity of Dutch business? 'A 3 (out of 10). Despite the cybersecurity measures taken by individual companies, our networks are so interdependent that, at present, we have few resources with which to counter malicious professional hackers.'

In reality, only a small proportion of all data leaks are caused by hackers and cybercriminals. Most are due to staff errors, such as losing an unencrypted USB stick, leaving a laptop somewhere or running a cloud application that hasn't been approved by their IT department. But here's the good news, says Lokke Moerel: slowly but surely, awareness is growing within organisations 'thanks largely to the Dutch Data Breach Notification requirements, which came into effect early last year'.

Moerel, a lawyer, has worked in the ICT and ICT security sectors for nearly 20 years. She is Senior of Counsel at US law firm Morrison & Foerster, which specialises in technology, and Professor of Global ICT Law at Tilburg University. Moerel was appointed a member of the Dutch Cyber Security Council in 2015.

Has cybercrime really grown so much in recent years or were companies already struggling with it several decades ago?

Moerel: 'Both. Twenty years ago, we had a number of information security cases. One involved a large IT firm losing the credit card details of its clients. They asked us to advise them on whether they should notify the clients concerned. Even then, the answer was "yes", because companies have an obligation to mitigate damages. Neglecting to notify your clients could constitute a tort. In another example, an executive director of a listed company had his briefcase stolen that contained company's interim quarterly results, and the thief could use this knowledge to trade on the stock market (insider trading). The difference between then and now is that these were isolated incidents. Nowadays, cybercriminals are systematically out to hijack confidential company information. The intensity, scale and professionalism of these criminals has grown enormously in recent years.'

'Ensure that you always have adequately encrypted, real-time back-ups'

How do you rate the existing cybersecurity awareness of companies?

'It can and should be a lot better. Private companies still aren't sufficiently aware of the dangers of ransomware and cryptoware, which criminals use to encrypt company data that's of no use to them but essential to the company. This data is only released when the company has paid a ransom. Pure extortion, in other words. The data that's "kidnapped" isn't in principle of any interest outside the company and therefore often isn't heavily secured. The solution is simple: ensure you always have securely encrypted, real-time data back-ups so you can always retrieve the data yourself.'

How do the leading Dutch companies score internationally in terms of cybersecurity?

'Most are highly ICT intensive and use centralised ICT systems to which their employees have access, wherever they are at a certain moment in the world. The downside is that because these companies are so highly digitalised, they are automatically more susceptible to cybercrime. Countries where ICT is still more locally organised or where processes are still paper based are less attractive to cybercriminals.'

The Dutch Cyber Security Council recently commissioned PostNL CEO Herna Verhagen to investigate the progress being made with cybersecurity in the Netherlands (see separate story, below left). What do you think of her report?

'It's very good, because it underlines the urgency of the issue for both the government and the private sector. Verhagen concludes that the government needs to take the lead in improving cybersecurity and argues in favour of a national action programme, including an investment agenda. She also recommends the appointment of a National Coordinator, such as we also have for the fight against terrorism. I fully endorse these recommendations, because we won't solve the problem without coordinated action. The Netherlands likes to present itself as a "safe place to do business" but it can't deliver on that promise without adequate cybersecurity.'

Verhagen also stresses companies' duty of care towards their clients.

'Rightly so. Consumers need to be confident they're buying a "cyber-secure" product. The point is a significant one: last autumn, the Dutch Consumer Association brought a civil law action against Samsung, based on its inadequate policy for updating software on Android smartphones. The Consumer Association claimed that Samsung was creating an unsafe situation for consumers because outdated software makes smartphones vulnerable to cybercrime. A ruling hasn't been handed down yet, but this case clearly shows that companies are now expected to adequately secure their products against cybercriminals.' Companies do realise this, but under pressure of 'time-to-market' adequate cybersecurity often suffers. The Dutch Cyber Security Council will shortly issue a guide what the cyber security duties of care are for ICT suppliers.

Are companies doing enough to improve cybersecurity with their partners in the chain?

Companies that are clearly dependent on other businesses or that work together closely with them more often carry out audits to check the adequacy of their chain partner's cybersecurity. It's in any case logical to do so, especially if you rely on other players to process your employee or customer data or to host your ICT systems. When companies do not have contractual relationships but still work in a chain, there is often still insufficient awareness of their chain dependency.'

The human element, the employee, remains the weakest link in the cybersecurity chain. Are careful training and ongoing refresher courses sufficient?

'They're indispensable, but they're not enough on their own. Securing access to a system using solely password protection isn't sufficient because there'll always be someone who will stick his/her password somewhere or who uses the same password for several systems. "Two-factor authentification" is a must for proper cybersecurity. What's more, simply building a firewall around your internal network and systems is no longer enough to keep cybercriminals at bay. What you should do now is put extra security cordons around the data you most want and need to protect. You should also permanently monitor your own network for any unusual or unexplained data movements that could implicate the presence of an intruder.' ‹

€15 BILLION WORTH OF **DAMAGE**

The following is a translated extract from the Verhagen report: 'Cybercrime costs the Dutch economy an estimated €15 billion per year, mainly in the form of monetary losses and the misappropriation of valuable intellectual capital. Other attacks involve sabotaging the services and processes of governments and key public infrastructure organisations. This could potentially result in large-scale social disruption – for example, if power plants, transport systems or flood defences are undermined.'

'Put extra security cordons around data you most want to protect'

‘THREE LINES OF DEFENCE’

Aloys Kregting (49) is CIO at AkzoNobel. He previously served as CIO at DSM, Numico and Unilever. He became a member of the Supervisory Board of Ordina in 2008 and joined the Supervisory Board of the University Medical Center (UMC) in Utrecht last year.

Cybersecurity is a top priority for Supervisory Boards. But how can their members get fully to grips with such an abstract concept? The answer is surprisingly simple: by properly immersing themselves in the subject, using the help of a ‘digital buddy’ if need be. And, above all, by continuing to ask plenty of questions…

Aloys Kregting has been in the ICT sector for nearly 30 years. Now CIO of AkzoNobel (having been CIO at DSM, Numico and Unilever), Kregting has twice won the CIO of the Year award. Understanding ICT and cybersecurity is as vital for Supervisory Boards as for anyone else in the company, says Kregting, who’s also a member of the Supervisory Board of Ordina and of UMC in Utrecht.

Are businesses sufficiently aware of the importance of cybersecurity?

Kregting: ‘Their understanding is certainly growing but levels of awareness vary from sector to sector. Organisations in the office automation and finance sectors are comparatively far advanced in cybersecurity, whereas those in manufacturing tend to lag further behind. The risk facing industry is that cybercriminals could potentially completely derail their processes from outside. And that could be highly dangerous. Five years ago, an external worm virus caused the temporary shutdown of a nuclear reactor in Iran. When I was at Numico, we produced clinical foods for patients with highly specific nutritional requirements. If you suddenly can’t supply this food because production has been brought to a standstill by computer hacking, it could cost lives.’

How good is cyber awareness in company boardrooms?

‘The subject appears more often now on the agendas of Executive and Supervisory Boards. Supervisory Board members are also increasingly being sought specifically for their ICT knowledge. I’m an example of that. It’s not a question of whether companies should digitally evolve but of when, and that incrementally increases their sensitivity to cybercrime straight away.’

How should companies organise their cybersecurity?

‘You should adopt a model based on three lines of defence, starting with the external audit, in which an external player assesses levels of cybersecurity. A contractor will, for example, send spam messages to employees and try to hack into the company’s systems so that it can see what happens and learn from it. The second line of defence is the internal audit, which has to be carried out by the ICT department responsible for cybersecurity. This involves drafting and implementing the organisation’s policy on cybersecurity and specifying how employees should behave. The third line of defence is all the staff on the work floor, who should be alert to identifying incoming spam before it does any damage. They also need to ensure that they never discuss sensitive company information in a crowded railway carriage or divulge passwords to third parties.’

What do you, as a Supervisory Board member, specifically do to oversee the company’s cybersecurity policy?

‘You have a duty to ensure that the management is taking all possible measures to identify the cyber risks and applying the appropriate mitigating action. You also have to keep on asking questions and calling management to account, not just by checking the policy as formulated but also by overseeing the ›

‘Digitisation is incrementally increasing commercial sensitivity to cybercrime’

‘Failing to address your ignorance is a form of negligence’

CYBER SECURITY SCORE:

Aloys Kregting: ‘Supervisory Board members score 6 out of 10 on cybersecurity knowledge. They know they need more IT knowledge to keep their supervision relevant.

external verification of cybersecurity measures. And ensuring that you are copied in on the results. You’ve got to immerse yourself in the subject for long enough to gain an accurate picture.’

A Supervisory Board member is still at arm’s length. Shouldn’t you in fact be visiting the workplace?

‘Making a personal tour of the premises gives you a much better sense of how employees deal with cybersecurity. For instance, how easy is it for you as a visitor to get through security? Do employees tend to have their password written on Post-it notes stuck to the side of their computer screens? Are sensitive documents left lying around on desks or on the shared printer? That kind of thing gives you a good idea of the corporate culture surrounding cybersecurity.’

Many Supervisory Board members seem ill-informed about cybersecurity. How do you ensure you’re not being fobbed off?

‘You should always scrutinise the results of external audits. I’ve got an extensive IT background, but some of my fellow Supervisory Board members are much less au fait with the subject. They’re aware of the threat but don’t know how to arm themselves against it. So they have to catch up on their knowledge in this area. This can be done through discussions with cybersecurity professionals or a “digital buddy” from within the firm itself. It’s what we did when I was at Unilever and it worked very well. If Supervisory Board members fail to address their ignorance and bury their heads in the sand, that’s a form of negligence.’

If a company has left something undone in relation to cybersecurity, isn’t the Supervisory Board responsible to some extent?

‘If you can’t show that you’ve adequately performed all your supervisory duties and have clearly been negligent, you could ultimately be held jointly and severally liable.’

As a member of the Supervisory Board of Ordina, how do you exercise supervision of its cybersecurity policy?

‘We’ve appointed a Supervisory Board audit committee to focus specifically on compliance, employee and client privacy and cybersecurity. The committee checks whether the company is properly addressing these issues and having itself externally audited. We then analyse the results of these audits. So far, this has always resulted in improvements in our cybersecurity policy.’

What are the biggest cyber risks facing an ICT organisation such as Ordina?

‘Ordina outsources many professionals to work for its clients and therefore mainly provides knowledge and innovation. It also offers a range of ICT services, so there’s always a degree of risk involved. The biggest risk for Ordina and many other ICT companies is the damage its image could sustain following a cyber leak.’ ‹

ARE WE IN FOR **A CYBERWAR?**

How does Aloys Kregting see the future? Does he think cybercriminals will always be one step ahead of companies? ‘I fear that they will be. After all, everything’s in their favour: businesses are digitising very rapidly and establishing ever more digital connections, which increases their vulnerability to an attack. At the same time, cybercriminals are becoming increasingly professional and have progressively more to gain from hacking. Companies really do need to get their cybersecurity in order as fast as possible. If ever there is a World War III, it will be a cyberwar in which countries will try to undermine each other by paralysing each other’s digital infrastructures. That’s why governments must take the lead in moving cybersecurity forward.’

‘Cybercriminals could potentially completely derail industrial processes’

SECURE YOUR DATA: **ALWAYS BE ALERT**

Data security is more important than ever. Cyber-attacks can inflict substantial damage on your organisation, such as the loss or theft of confidential information, reputational harm and heavy fines. But you don't have to battle these risks alone.

Good data security requires specialist know-how and that's something BDO can help you with. With a global reach of more than 1,400 offices in 158 countries and a staff complement of over 67,000 professionals, we have specific expert knowledge and can combine it throughout our network to offer genuine cross-border services.

Why BDO?

At BDO, we offer our clients new perspectives based on a focused and timely service based on effective coordination and teamwork within our global network. BDO is the answer if you are looking for:

- Centralised planning, management and control by our dedicated client teams with a proven track record.
- A customised client portal through which progress can be monitored.
- Timely and constructive feedback.

If you have any questions or want to find out more about this topic or about BDO, please contact:

Sandra Konings, Partner
BDO – Cybersecurity
sandra.konings@bdo.nl
Tel. +31 (0) 6 515 08 151

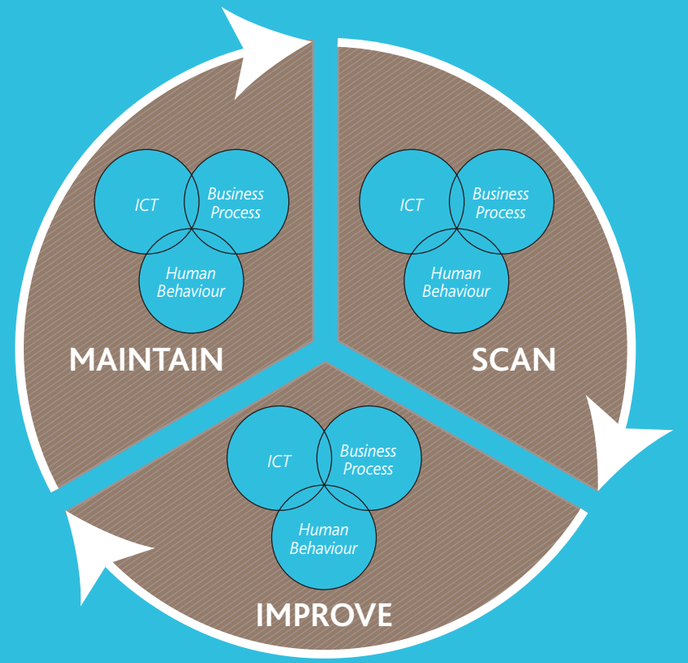
Robert van Vianen, Partner
BDO – Cybersecurity
robert.van.vianen@bdo.nl
Tel. +31 (0) 6 300 79 909

Jeffrey de Bruijn, Senior Advisor
BDO – Cybersecurity
jeffrey.de.bruijn@bdo.nl
Tel. +31 (0) 6 249 21 197

SECURITY FULL CIRCLE

BDO offers five different services to help improve your cybersecurity

- **Information security scan** to assess the current status of information security, taking into account your ICT environment, business processes and the behaviour of your employees.
- **Privacy scan** to scan the current status of the protection of privacy data, again taking into account ICT, business processes and human behaviour.
- **Improve information security and/or privacy** to implement the necessary security measures within ICT and your business processes and to raise awareness and change human behaviour.
- Maintain the current level of security by offering an Information Security Officer as a service to **detect** issues in time, ensure proper **response** and **recovery** and to continuously raise **awareness**.
- Maintain the current level of privacy by offering a Data Protection Officer as a service to **detect** issues in time, ensure proper **response**, **recovery** and **reporting**, and to continuously raise **awareness**.



THE WORLDWIDE
BDO NETWORK

BDO Countries

COUNTRIES
158

LOCATIONS
over 1,400

PROFESSIONALS
more than 67,000

REVENUE IN 2016
$7.6 billion

‘Companies spend millions of dollars on firewalls, encryption and secure access devices, **and it’s money wasted, because none of these measures addresses the weakest link in the security chain’**

Kevin Mitnick

‘There are **risks and costs** to a programme of action – but they are **far less** than the long-range cost of **comfortable inaction.’**

John F. Kennedy

WWW.BDO.NL/CORPORATECLIENTS

02/2017 – CC1702