From hype to policy

Public management letter concerning Cyber Security

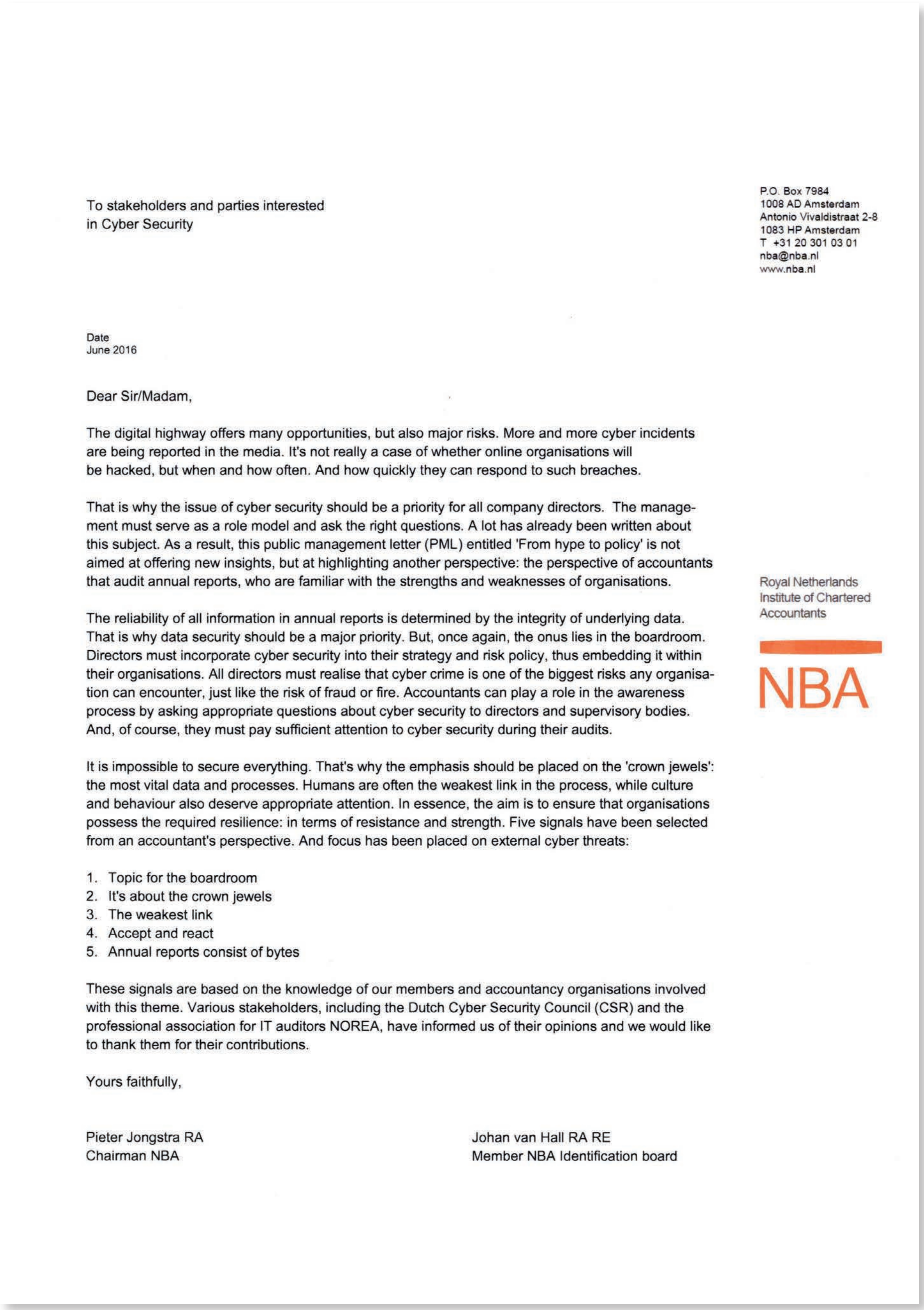
May 2016

NBA

Royal Netherlands
Institute of Chartered
Accountants

NBA

The NBA's membership comprises a broad, diverse occupational group of over 20,000 professionals working in public accountancy practice, at government agencies, as internal auditor or in organisational management. Integrity, objectivity, technical competence and due care, confidentiality and professional behaviour are fundamental principles for every accountant. The NBA assists accountants in fulfilling their crucial role in society, now and in the future.



To stakeholders and parties interested
in Cyber Security

P.O. Box 7984
1008 AD Amsterdam
Antonio Vivaldistraat 2-8
1083 HP Amsterdam
T +31 20 301 03 01
nba@nba.nl
www.nba.nl

Date
June 2016

Dear Sir/Madam,

The digital highway offers many opportunities, but also major risks. More and more cyber incidents are being reported in the media. It's not really a case of whether online organisations will be hacked, but when and how often. And how quickly they can respond to such breaches.

That is why the issue of cyber security should be a priority for all company directors. The management must serve as a role model and ask the right questions. A lot has already been written about this subject. As a result, this public management letter (PML) entitled 'From hype to policy' is not aimed at offering new insights, but at highlighting another perspective: the perspective of accountants that audit annual reports, who are familiar with the strengths and weaknesses of organisations.

Royal Netherlands
Institute of Chartered
Accountants

NBA

The reliability of all information in annual reports is determined by the integrity of underlying data. That is why data security should be a major priority. But, once again, the onus lies in the boardroom. Directors must incorporate cyber security into their strategy and risk policy, thus embedding it within their organisations. All directors must realise that cyber crime is one of the biggest risks any organisation can encounter, just like the risk of fraud or fire. Accountants can play a role in the awareness process by asking appropriate questions about cyber security to directors and supervisory bodies. And, of course, they must pay sufficient attention to cyber security during their audits.

It is impossible to secure everything. That's why the emphasis should be placed on the 'crown jewels': the most vital data and processes. Humans are often the weakest link in the process, while culture and behaviour also deserve appropriate attention. In essence, the aim is to ensure that organisations possess the required resilience: in terms of resistance and strength. Five signals have been selected from an accountant's perspective. And focus has been placed on external cyber threats:

1. Topic for the boardroom
2. It's about the crown jewels
3. The weakest link
4. Accept and react
5. Annual reports consist of bytes

These signals are based on the knowledge of our members and accountancy organisations involved with this theme. Various stakeholders, including the Dutch Cyber Security Council (CSR) and the professional association for IT auditors NOREA, have informed us of their opinions and we would like to thank them for their contributions.

Yours faithfully,

Pieter Jongstra RA
Chairman NBA

Johan van Hall RA RE
Member NBA Identification board

From hype to policy
TOP SECRET
2016
TOP SECRET
Annual report
1. Topic for the boardroom
2. It's about the crown jewels
3. The weakest link
4. Accept and react
5. Annual reports consist of bytes
CEO
Management

NBA

Contents

Hoofdstuk Pagina

From hype to policy 6

Signal 1: Topic for the boardroom 8

Signal 2: It’s about the crown jewels 10

Signal 3: The weakest link 12

Signal 4: Accept and react 14

Signal 5: Annual reports consist of bytes 16

Credits 20

From hype to policy

Cyber crime, which is the counterpart of cyber security, is big business. Mala fide organisations earn a lot of money by hacking companies, and amounts totalling tens of millions have become commonplace. The damage caused when American supermarket chain Target was hacked in 2013 amounted to a whopping 236 million dollars. In February 2016, hackers were able to transfer almost 1 billion Dollars from the Federal Reserve Bank of New York. Hackers had already amassed 81 million from four earlier attempts, and things only went wrong during the fifth attempt because a word had been spelled incorrectly.

DDoS attacks (Distributed Denial-of-Service) have been common knowledge for quite some time, and are aimed at crashing networks by overloading them. Banks have often been on the receiving end, although cable company Ziggo was also targeted last year. The hacking of personal photos on iCloud in 2015 showed that celebrities can also be targets for cyber crime. According to a recent study, there was almost a 40 percent increase in cyber security incidents in 2015.[1]

The overriding perception, that only large international companies are victims of hacking, is not accurate. SME's, civil society (including municipalities, hospitals and energy companies) and private individuals also fall foul of cyber crime. Even though they have a different risk profile, they are still exposed to the same threat. It is no longer a question of *whether* you will be hacked, but *when* and *how often*. There is no such thing as absolute security.

Cyber attacks can have far-reaching consequences. Not only due to the direct damage caused during the hack itself, but also due to the indirect damage. For instance, the theft of intellectual property, loss of customers and turnover, reputation-related damage, claims by victims or fines by external supervisory bodies. In addition, one must also consider the cost of (forensic) investigations, legal advice and initiatives aimed at recovering from incurred damage.

An issue of national security

The government also recognises the importance of cyber security. That's why, for example, the National Cyber Security Centre (NCSC) and the Dutch Cyber Security Council (CSR) were established a few years ago.

The NCSC is a partnership involving public and private organisations and focuses on the whole approach to cyber security. It is an information database and expertise centre, which also acts as the Computer Emergency Response Team (CERT) for the Dutch government. The National Cyber Security Operations Center (NCSOC) is an important part of the NCSC and can be accessed night and day for reports and assistance. The NCSC is organised by the National Coordinator for Anti-terrorism and Security (NCTV).

The CSR is the government's independent and strategic advisory body concerning cyber security issues in the Netherlands. The CSR released a *Cyber Security Manual for directors in April 2015*, which focused on three questions: what do directors consider when evaluating cyber security; how do they address the issue in their organisations; and how do they attempt to realise digital security? The CSR's work plan for 2016 bears a very telling heading: *The future is closer than you think*. One of the main findings in this programme concluded that awareness is still an important weapon in the battle against cyber criminality.

The NCSC publishes an insight into cyber security in the Netherlands (CSBN) every year. The most recent edition[2] shows that most incidents involved DDoS attacks, abuse

[1] Turnaround and transformation in cybersecurity. PwC, October 2015
[2] Cybersecuritybeeld Nederland (CSBN) 2015, September 2015

of user rights, access to sensitive data and the circumnavigation of security measures. This involves the NCSC examining the likelihood of abuse taking place and what kind of damage could be encountered. The publication also features a threat matrix, which highlights potential threats per target (governments, companies and civilians). The main threats are still phishing (sending fraudulent e-mails) and cryptoware (fraudulent encryption of files). The NCSC states that reliance on ICT and the internet continues to increase. Thankfully, better insights into cyber incidents are also being obtained so more specific cyber security measures can be implemented.

Obtaining the right perspective

An incorrect perception of cyber security could created due to the attention the issue receives, the many publications on the matter and the somewhat bombastic reporting in the media. It's as if countless organisations have been victims of cyber crime and are unable to anything about it. But, in reality, the picture is more balanced: a lot of damage can be prevented with the right approach. As the CSR highlighted, awareness is still an important tool and technology alone cannot resolve the problem. The most important issue is how cyber security can been embedded into the whole organisation. Directors, employees, regulators and internal and external accountants all have a role to play. Greater attention must be given to the crown jewels, culture and behaviour, awareness and training. Digital resilience must be improved; this is the ability to resist and respond quickly.

A natural role for accountants

Accountants encounter the issue of cyber security via various channels. From an auditing perspective, they must realise that the foundations of annual reports consist of bytes. The reliability of information is determined by the integrity of underlying data. That is why the role of accountants involves more than just confirming whether damage from cyber incidents has been correctly reported in annual reports or whether continuity has been safeguarded.

However, accountants can perhaps be most effective via their natural advisory function, by asking the right questions about cyber security. This will involve determining whether directors and supervisory bodies have enough awareness, and assessing whether cyber security has been given an appropriate place within strategy and risk policy.

Signal 1 | Topic for the boardroom

Almost every day, cyber incidents prove that major risks can be expected in cyber space. These risks could come from individual hackers as well as organised professional cyber criminals. It actually goes without saying that cyber security deserves the attention of all organisations that operate online.

The number of cyber incidents, and their severity, have increased so much recently that cyber crime could be a risk for every organisation. It could result in reputation or image-related damage, loss of income, fines or the release of intellectual property into the public domain. Due to increasing digitalisation in society, it is now very important to effectively secure valuable information. Not only has there been an increase in safety-related risks, but the number of incidents has also increased. Customers, the media, supervisory bodies and legislators have now also become more scrutinous. Customers have concerns about whether their information is suitably protected. Supervisory bodies are asking directors to be more vigilant and are assessing measures taken with regards to cyber security.

But legislators have also been active and more and more legislation has been passed to address this specific issue. An example of this is the mandatory notification of data breaches, which came into effect in 2016. Directors can now be held liable if they fail to take appropriate cyber security measures or if they fail to report data-related leaks. In addition, there may also be individual claims from victims themselves.

Cyber crime must be an active concern for every director, non-executive director and regulator. But this also applies to (semi)public organisations or directors/owners of SME's. The subject of cyber crime is nothing new, but is increasingly becoming a fact of life.

The media often paints a rather bombastic picture of cyber crime, as if many organisations are helpless victims of cyber criminals. Everything is tarred with the same brush, and this can lead to an unfounded sense of fear. But, in reality, the picture is more balanced. SME's have a different risk profile compared to multinationals or civil society, and need not worry about a lot of the incidents reported in the media. Their risks are manageable, although 100 percent security is actually an illusion. And attempts to realise this ideal are not only accompanied by high costs, but also lead to a false sense of security.

Cyber crime is a risk that deserves the same attention as, for example, the risk of fire or fraud. It is a risk that must be addressed in a structural manner by directors and company regulators, as part of an overall risk management process. It is an issue that accountants also need to address when auditing annual reports.

Negative example

Not my responsibility; we have a special department

During a board meeting at major international organisation A questions were asked about what actions the organisation takes with regards to cyber security. The CEO answered: we have a special department; it's not my responsibility. Shortly afterwards, A suffered a major cyber attack and did not possess the required resilience because not enough had been invested in cyber security measures in recent years. The incident caused A major damage.

Positive example

Cyber security as part of the risk model

At large ICT multinational B the risk associated with cyber security was identified as one of the organisation's strategic risks. It was discussed in the boardroom on a quarterly basis, using a dashboard showing the risks encountered by B. These discussions resulted in appropriate priorities being selected for investments and operations in the field of cyber security. This approach was consistent with B's risk profile and accompanying risk appetite.

RECOMMENDATION 1: As a director, ask the right questions

- Make cyber security an integral part of risk management.
- As a director, ask the right questions to the organisation:

1. What is the risk appetite and risk prioritisation?
   - What is the risk appetite for downtime, loss of data and privacy-related incidents?
   - How can this be determined and how can it be monitored (risk dashboard)?
   - Which is the most important data worthy of most protection? Which processes are essential for the future of the organisation?
2. How is cyber security organised within the organisation?
   - How is the first and second line of defense organized (at departmental level and in terms of internal inspections)?
   - What kind of reporting is adopted for cyber security risks?
   - How is coordination realised between various positions within the company?
3. Is there enough investment; are there any benefits?
   - Which planned investments in cyber security have been identified for the coming three years?
   - Will this be enough to achieve effective protection (in accordance with the risk appetite)?
   - How do the investments compare to those made by competitors?
4. Exactly how safe and resilient is the organisation at this moment in time?
   - What were the most relevant security and privacy incidents (also compared to similar organisations) during the past 12 months?
   - What were the learning points and what is the organisation doing differently in order to prevent new incidents?
5. Is the organisation becoming safer or unsafer?
   - Which critical statistics or KPI's are mentioned on the cyber risk dashboard?
   - Is the organisation realising identified cyber risk objectives?
   - How do cyber risk KPI's compare to those of competitors?
6. How are the risks of suppliers and other partners in the supply chain managed?
   - What is done to make sure external suppliers, their suppliers and other partners in the chain do not expose the organisation to unacceptable cyber risks?
7. How is cyber security ensured within products and services?
   - What approach is adopted to ensuring cyber security in existing products and services, and when developing new products and services?

Signal 2 |
It's about the crown jewels

The crown jewels of a company are most susceptible to cyber attacks because they result in the most damage or allow the biggest gains to be made. That is why investments in cyber security must focus on the crown jewels. But this will require a switch in risk-related thinking.

Digital crown jewels represent the highest value from a strategic, operational financial, legal and reputation perspective. They are an organisation's most vital sources of information, technologies or processes. In particular:

- an effectively functioning web-shop
- availability of operational and/or financial data
- the personal details of e.g. customers, patients, tenants or students
- intellectual property and research investments in the high-tech industry
- the operational technology in production organisations
- the continuity of services offered by an ICT service/ Cloud service provider

In practice, it is difficult to rank various sources of information, technologies and processes based on importance and value. All company resources are often treated in the same manner, which means the 'picnic set' is treated in the same way as the 'family silver'.

Parties with bad intentions include organised criminals, hacktivist and terrorists, but also national governments and even the company's own employees. They tend to be determined and patient, and often adopt well refined approaches. They focus on individuals, organisations and even entire sectors. Their primary goal often involves making financial gains or causing damage. And the most sought after target is the crown jewels. Attackers are continuously evolving so they can exploit vulnerabilities within digital systems. At the end of the day, the weakest link determines the quality of the whole system. If intellectual property, customer details or other valuable information is leaked, total impact often only becomes noticeable much later down the line. It can take months or even years for all negative effects to be identified.

In practice, many organisations invest in security products and services based on out-dated standard formats, which do not pay enough attention to the real crown jewels. This leads to an approach which is the same for all digital company resources, without making a distinction based on importance and value. It often pays little attention to punctually identifying and effectively addressing security incidents. Cyber security requires a completely different approach and manner of thinking: start by identifying the crown jewels, and then determine the value, risks and threats. Besides monitoring, security officers must also perform testing and assume overall control.

This insight will allow management to restate their organisation's risk profile. The aim is to reduce the damage caused by cyber attacks, and not to eliminate risks altogether. By continuously identifying new threats, organisation can be more effective in anticipating attacks and limiting the accompanying negative impact.

Negative example

Crown jewels accessible via the back door

Innovative company C established that blueprints and developed recipes had to be well protected. C wanted to thus prevent its competitors from getting their hands on important knowledge before it was ready for release. The critical data was stored in a separate segment of the network, with extra security, away from segments featuring less critical data. However, C was not fully aware of the interfaces between the various segments. This meant hackers could still access C's valuable information via a low-security component in the network.

Positive example

As long as the shop is open and customers are safe

Online retailer D was having difficulty deciding what needed to be done about the security and continuity of its web environment. A risk analysis, which was performed throughout the organisation, showed that inability to access the webshop and leaks involving customer details had the biggest impact. As a result, D decided to create a backup for its webshop framework and to improve security in the environment featuring customer details.

RECOMMENDATION 2: Identify the crown jewels

- Management must take the initiative when identifying and classifying the crown jewels.
- Identify where they are located, determine the level on reliance and who is able to access them.
- Do not only examine threats and opportunities from the organisation's perspective, but also from the perspective of people who may want to harm the organisation:
  - Who is interested in your crown jewels and why?
  - Where are the crown jewels located and how are they connected to external suppliers and partners?
  - Which methods and techniques will potential attackers use to access the crown jewels or to interfere with them?
- Prioritise measures based on value and risk. This insight will allow organisations to invest in measures that effectively help to protect the crown jewels and reduce the risk profile.

Signal 3 |
The weakest link

Cyber security risks are not just encountered via technology. Often employees tend to be the weakest link in the security chain. Attackers try to exploit social engineering when convincing employees to share business-critical data with them.

Social engineering is an increasingly popular trend used during attacks on organisations. It involves using psychological manipulation to exploit the sensitivities and goodwill of employees. It is used by hackers because it has a good chance of success and requires less technological know-how than other methods of attack. Illustrations of social engineering include:

- *Baiting:* attackers leave hardware, which is infected with malicious software (malware), at a location where it will definitely be found. This often involves USB sticks. This malware is then installed as soon as the hardware connects to the company network.
- *Phishing:* this involves sending a fraudulent e-mail, where the sender is portrayed as reliable.
- *Spear phishing:* similar to phishing, but involves using a tailor-made e-mail to specific companies or even specific employees.
- *Quid pro quo:* attackers offer something (discount, discount voucher, etc.) in return for personal information like login details.
- *Spam:* junk e-mail sent en masse. Some people still fall for this approach.
- *Tailgating:* This involves attackers walking behind employees into a secure environment; often secure company entrances. They sometimes claim to have lost or forgotten their entrance pass.

An attempt is made to gain employees' trust be specifically using templates, URL's, names of colleagues and business jargon they may be familiar with. This often involves exploiting fictional authorisation, tight deadlines or the greed of employees. Successful attacks result in hackers gaining access to company-related data which can be used to perform harmful actions. For example, stealing private information or fraudulently obtaining money.

The confines of traditional office environments are becoming more vague due to the increasing use of mobile devices, cloud-based storage and flexible workplaces. It has now become very difficult to make a distinction between office work stations, home work stations or work stations in internet cafés. This new way of working requires a completely different approach to data security and better awareness about social engineering.

An organisation's risk culture determines how the organisation deals with such risks. The risks associated with social engineering apply to all employees and everyone should be familiar with them. The best way to make organisations even more aware about these risks is to implement specific initiatives concerning risk culture. The first step involves acknowledging the risks faced by the organisation. Awareness can then be improved via specific training and information about social engineering. There must be a clear structure for reporting incidents. In practice, even though reports are submitted, they are not always followed up effectively.

The role played by management is crucial. Besides serving as role models, management must also set the right tone. This will help to improve awareness among employees and create an atmosphere where people address one another about potential risks. Appropriate behaviour must be positively stimulated. The management must continuously test, measure, evaluate and improve their organisation's culture and behaviour in the field of cyber security.

Negative example

It's probably fine

After being employed for a month, employee E receives an e-mail from the personnel department, saying some of his data are missing. The e-mail has come from an e-mail address with an unknown extension and is asking for his name, date of birth and a copy of his passport. E thinks this is strange because he had already provided these data when he joined the company. E asks his colleagues and it appears that all of them have received the same e-mail. E thinks it's probably fine and decides to send the requested data. A week later, he is no longer able to log into his account. His password appears to have been stolen and a hacker has gained access to the company system using his name.

Positive example

Identify false promises

A lot of employees at company F receive an e-mail from a web-shop, telling them that they can choose a Christmas gift worth 25 Euros on behalf of their employer. To take part in the promotion, all they have to do is click the link in the e-mail and enter a promotion code. A few employees do not trust the e-mail: the sending address is unknown, not every employee has received the e-mail and the promotion had not been announced in advance. Full of suspicion, the employees seek advice from the security officer. Upon closer inspection, the e-mail appears to be an attempt at social engineering. Potential damage was prevented because employees were alert and reacted quickly.

RECOMMENDATION 3: Also pay attention to culture and behaviour

- Realise that cyber security involves more than just ICT and technology; the human factor also plays an important role. So make sure the risk model pays enough attention to culture and behaviour.
- Management should set the tone when it comes to cyber security. Reward appropriate behaviour. Test, measure, evaluate and improve culture and behaviour relating to cyber security.
- Everyone can encounter social engineering. So make sure all employees are familiar with this phenomenon. Organise information sessions and training, and provide information via the intranet. Use concrete illustrations; this will help employees to better recognise cases of social engineering. Also establish a clear reporting procedure within the organisation.
- Take all reports about attempts at social engineering seriously. A casual attitude or failure to provide feedback could encourage people to no longer report incidents.
- Tactics used in social engineering are continuously changing. Social engineering must thus be a fixed part in any organisation's risk culture and risk analyses. The effectiveness of risk management in this area must be continuously tested and evaluated.

Signal 4 | Accept and react

Organisations must become digitally resilient so they are less vulnerable to cyber crime. Preventive measures alone are not sufficient. Attention must be given to detection and response. The same applies to internal and government accountant.

An appropriate mix of security measures must be adopted to protect the crown jewels. During various major hacks last year, it became apparent that organisations still relied too heavily on prevention. The idea that even higher walls lead to 100 percent security is now outdated. Employees are not enthusiastic about ever difficult and complicated measures. Organisations must accept that they will be hacked or have already been hacked. That is why measures focusing on detection and response are becoming increasingly important.

Detection is difficult if people don't know what they are looking for. So a good way to start is to identify the crown jewels and potential threats. This can then be used as a basis to define scenarios that could be followed by potential attackers. It is important for detection to not only be implemented around the outskirts of organisations, but also on internal paths that lead to the crown jewels. This is the best way to quickly identify potential intruders.

In order to successfully combat intruders, detection measures must identify unwanted behaviour as early as possible. The best thing to do is establish a security operating center, which collects reports on a daily basis and compares them to pre-defined scenarios. The response team can then react immediately once particular signals are received. This team can then quickly determine whether an incident has occurred or whether the report was just a false alarm. In case of an incident, as much information as possible will be gathered so a risk assessment can be carried out and follow-up steps can be identified. Already identified scenarios and action plans make sure the process is streamlined and efficient. Besides these scenarios, action plans and handbooks, it is also important to provide training about how to deal with incidents. This means not only training personnel at the security operating center, but also members of the organisation's general crisis team and even people at the top of the organisation.

However, fully manning a security operating center and having a well trained response team can be expensive. And not all organisations have the personnel and resources to set up such structures. Thankfully, solutions are available within the market. Various organisations are able to offer detection and response capacity via subscription-based systems.

The latest trend is to actively hunt for potential incidents. Incident detection takes place based on pre-defined scenarios and threats. However, these so-called hunting teams focus on identifying irregularities and abnormalities in received security reports. Abnormalities that cannot be immediately identified, could point to potential break-ins. Irregularities can then be tracked and break-in scenarios can be modified. Another example of preventive investigation involves 'red team' exercises. These tests are carried out by external cyber security specialists in order to check the operating effectiveness of implemented security measures.

It is important for accountants to not only be aware about prevention, but also about detection and response. Annual audits often focus on the effectiveness of preventive measures and the accompanying processes. However, audits can become even more beneficial if detection and response capacity is also checked. If accountants are not suitably equipped to perform such checks, they must collaborate with other specialists.

Negative example

Penny-pinching hinders awareness

Business G possesses a web-shop, which is used to sell its products. G manages the website in-house. G uses a content management system to easily add products and restate prices. G has no idea about what is going on in the surroundings because it does not possess enough technological know-how. It also fails to perform physical scans on web-shop files. This means G is unaware that hackers have been tracking payment traffic for a few weeks. The credit card data of all customers are then hacked. They appear on G's website and can be seen by everyone.

Positive example

Discovered on time

SME H has outsourced all administrative duties to its accountant X. X implements the very latest digital technology when performing these admin activities. The accountant adopts a fully automated approach when dealing with mutations in bank accounts. In addition, H also thoroughly checks these mutations personally on a daily basis. One day, H discovers that he has been the victim of skimming. However, because of the daily checks, damage was limited and the bank was willing to provide compensation.

RECOMMENDATION 4: Improve digital resilience

- Accept that cyber crime is an inherent risk, which simply accompanies the operations and risks of all organisations. Organisation and risk management must thus be defined accordingly.
- Focus on the crown jewels when taking measures against cyber crime. Besides prevention, also pay sufficient attention to detection and response.
- Improve digital resilience throughout the organisation - from the work floor to the executive directors. Ensure awareness and provide training. Learn from already reported incidents.
- Ensure sufficient capacity so security incidents can be dealt with in an appropriate manner. This could be realised via insourcing. Identify emergency scenarios in advance, appoint a crisis team and regularly perform checks so a better insight is obtained into potential vulnerabilities.

Signal 5 | Annual reports consist of bytes

When auditing annuals accounts, accountants assess risks to financial reporting and continuity, which include cyber crime and cyber security. This means accountants must be aware of control measures that are implemented for data integrity and security.

Cyber attacks can have a direct or indirect impact on organisations. Direct impact could, for example, involve attacks on operational processes. This could involve DDoS attacks, hacking of confidential data or fraudulent transactions. Indirect impact tends to be of a greater magnitude. For instance, the theft of intellectual property, loss of customers and turnover, reputation-related damage, claims by victims or penalties by external supervisory bodies. In addition, one must also consider the cost of (forensic) investigations, legal advice and initiatives aimed at recovering from incurred damage.

Cyber attacks can, both directly and indirectly, have an impact on an organisation's financial reporting and continuity. It is thus essential for accountants to pay explicit attention to cyber security during risk analyses. Naturally, this will involve risks concerning programmes and applications. However, the whole infrastructure must also be examine. Such infrastructure is becoming increasingly complex due to virtual workplaces, cloud storage, mobile solutions and internet interfaces. Accountants must ask themselves if they are capable of independently reaching conclusions about digital risks and measures. Do they possess the necessary expertise or are other specialists required?

If an elevated cyber risk is encountered, accountants can add supplementary activities to the audit strategy. These activities should specifically focus on areas where the accountant expects higher risks to be encountered. It is important for these activities to be in line with approaches adopted by hackers, so leaks can be effectively identified. They must thus focus heavily on implemented technology. Illustrations include penetration tests, evaluation of security log files and implementation of red team exercises.

It is standard procedure for accountants to focus on ICT security during their audits. However, it is not enough to simply check for set-up and implementation. Effective security and data integrity must be safeguarded at all times. Monitoring must be implemented to quickly detect potential exploitation of vulnerabilities (via the prevent-detect-react approach). The most important conclusions about an organisation's cyber security measures must be embodied in the management letter. According to article 2:393 section 4 of the Dutch Civil Code, accountants must at least mention findings about the reliability and continuity of automated data processing.

Accountants must also discuss their findings with directors and regulators (Supervisory board of Regulatory Council). Naturally, every year they must check to what extent their findings have been followed up. Accountants can perform their natural advisory role by also mentioning current cyber security risks in the management letter.

Negative example

Look beyond the annual reports

Accountant Y is responsible for auditing the financial statements of salary processor I. Y has primarily focused on salary processing applications when evaluating the financial data. He has only paid a limited amount of attention to the underlying infrastructure. Hackers are able to hack the infrastructure and access the databases. Data about the employees of customers is placed on the internet en masse. This causes many customers to cancel their contracts with I. It is unclear how long the hackers had been active. The media is critical about Y's failure to place greater emphasis on cyber security

Positive example

An unexpected outcome

When auditing financial statements, accountant Z decided to perform a hackers test at company J. Directors at J agreed to this. The cyber security specialists at Z then tried to enter J's web environment without informing J's employees. The hackers test was successful and the specialists were able to initiate large financial transactions in the system. However, tracks left by real hackers were also identified during the test. This immediately led to an investigation. It appears that hackers had carried out fraudulent transactions, which had led to millions of Euros disappearing. The systems had also been manipulated to avoid detection. Based on the investigation carried out by Z, security was improved and the financial transactions were reversed.

RECOMMENDATION 5: Have access to sufficient cyber know-how during an audit

- Differentiate between clients based on potential cyber security risks (low/medium/high). Use this classification to modify the audit strategy. When doing so, realise that the indirect impact of a security incident can be much greater than the direct impact. Organisations must be able to determine total damage as soon as possible.
- The audit strategy must not only focus on (administrative) applications, but must also check whether appropriate security measures have been incorporated into technology environment.
- Ask specific cyber security questions to clients, for example:
  - Is the organisation aware of the main cyber risks?
  - Does the organisation know what its crown jewels are?
  - Has cyber security management been designed to reduce the organisation's main risks and protect the crown jewels?
  - Does the organisation possess the technology, processes and people needed to punctually detect and appropriately respond to cyber attacks? Has a security operating center been set up?
  - Has incident management been designed to quickly respond to incidents (appointment of a multi-disciplinary team, including ICT, communication, operations and legal specialists)?
  - Does the organisation regularly check all aspects of cyber security?
- Define revised testing activities for areas where not enough preventive and/or reactive security measures have been implemented. If necessary, add cyber specialists to the audit team or request expertise.
- Mention the most important cyber security conclusions in the management letter. Each year, examine to what extent conclusions from the prior year have been followed up.

WORD
CRACKER
RE
CYBER
ENCRYPTION
TROJAN
IDENTITY
ER
THEFT
PRIVACY
S
NTRUSION
DETECTION

Summary of stakeholders' responses

At the request of the NBA the following stakeholders have responded to the public management letter. Their responses are summarized in this chapter.

Dutch Cyber Security Council (CSR)

The CSR is pleased that the NBA is paying attention to the important topic of cyber security. The CSR agrees that the management letter must be used to emphasise that cyber security is also a topic for the boardroom. In terms of the first signal, the CSR believes cyber security will always be the organisation's responsibility, even if ICT services are outsourced. Responsibilities must be clearly established and arranged at every level of the organisation, while directors oversee strategic management. When doing so, the aim should not only be to prevent incidents, but to also deal with incidents or accidents and to ensure recovery. The boardroom is also responsible for ensuring effective implementation and compliance with existing laws and regulations. Many companies are suffering from legacy problems. It is important for them to be aware of this and develop appropriate policy.

In terms of the second signal, the CSR feels companies can possess more crown jewels than they initially realise, e.g. Intellectual Property Rights. As far as the third signal is concerned, the CSR believes people are not the only weak link, because weak links can also be encountered in the supply chain. Suppliers that fail to comply with certain basic norms could present a risk to other organisations. That is why cyber security in the supply chain also deserves appropriate attention. Regularly conducting incident-related exercises, and involving the main stakeholders when doing so, could help to improve awareness among employees and remind them about agreed procedures. In terms of the fourth signal, the CSR believes the approach used by organisations should also involve mitigating cyber attacks, and it should be standard practice to report potential incidents.

Cyber security is an important topic within audits, and within the professional training given to accountants. The CSR recommends introducing a certain degree of standardisation in the cyber security audit process. Finally, the CSR believes it would be beneficial if accountants played an active role concerning cyber security in the boardroom.

NOREA

As a professional association for IT auditors, NOREA admires the initiative the NBA has taken to place the issue of cyber security on the agenda of directors and managers. NOREA feels the recommendation, that accountants can be most effective in the field of cyber security via their advisory role, does not go far enough. An accountant's expert role must involve more than just offering advice about information security and cyber security, and about reporting the risks. Accountants must use their audits to determine whether organisations are prepared for cyber incidents, so an adequate response can be identified and business data can be recovered to ensure business continuity. If accountants want to succeed in this task, they must possess ICT expertise or add ICT audit experience to their audit teams. In addition, NOREA specifically asks for internal audits to be used as a third line of defence.

When identifying information security policy, organisations must start off with a risk analysis so an appropriate scope can be identified. In relation to this, NOREA would like to highlight its Cyber Security Assessment Tool and web page about mandatory reporting for data leaks. NOREA will be pleased to collaborate with auditors from a variety of disciplines when dealing with the topic of cyber security.

Colofon

Sharing Knowledge

In the NBA Sharing Knowledge policy programme the expertise of accountants is collectively applied to signal risks early in social sectors or relevant themes. In doing so the emphasis is on governance, operations, reporting and audit.

The NBA has used this public management letter (PML) to present five recommendations about the theme of Cyber Security. This theme is the sixteenth topic to be selected by the Identification Board of the NBA. A work group featuring public accountants and advisers involved with the theme gathered and discussed anonymised findings. This was then discussed at a sector meeting with stakeholders. The Identification Board then gauged the signals from a social perspective and applied a social assessment to the signals. Stakeholders involved in the theme were willing to respond in writing to the PML. Coordination and final editing was provided by the Sharing Knowledge programme team.

Further information

A public management letter is one of the publications issued by the Sharing Knowledge policy programme. Open letters and discussion reports are also released. The NBA has released the following publications:

- 2016: Energy
- 2015: Curative healthcare and Hospitality
- 2014: Life Sciences and Banks
- 2013: VET colleges, Risk management and Transport & Logistics
- 2012: Municipalities, Tone at the Top and Charities
- 2011: Commercial Property, Pensions and Greenhouse Horticulture
- 2010: Insurance and Long-term Care

All publications are public and are intended for a wide audience.

Identification Board

prof. dr. mr. Frans van der Wel RA (chairman)
Gineke Bossema RA
Johan van Hall RA RE
mr. Charlotte Insinger MBA
Leon van den Nieuwenhuijzen RA
Carel Verdiesen AA

Cyber Security work group

drs. Tony de Bos RA RE CEH (EY)
ing. John Hermans RE (KPMG)
ir. Bram van Tiel RE (PwC)
drs. Marko van Zwam RE (Deloitte)

Sharing Knowledge Programme Team

drs. Robert Mul MPA (programme leader)
Michèl Admiraal RA (editor-in-chief)
Jacques Urlus RE CISA (coordinator)
drs. Jenny Dankbaar (secretariat)

Phishing
Shift

The last five years NBA published Public Management Letters (PML's) concerning specific sectors or themes.

Indications for Insurers
A sectoral management letter
Royal NIVRA, June 2010
Governance, a special skill
Public management letter for Secondary Vocational Education and Training
April 2012
NBA
Stacking tasks, piling risks
Public management letter for Municipalities
June 2012
NBA
Cease trading or carry on
Public management letter for Transport and Logistics
June 2013
NBA
Good cause, good story
Public management letter for the charitable sector
December 2012
NBA
Tell it like it is
Summary of the public management letter for the commercial property sector
June 2011
NBA
New perspectives for Dutch Healthcare
Summary of the public management letter for the long-term care sector
November 2010
NBA
Public management letter
Managing risks is a people's business
Risk management and reporting in large enterprises
November 2013
NBA
Your pension is uncertain
Open letter
February 2011
NBA
From craft to business
A public management letter for the Greenhouse Horticulture Sector
November 2011
NBA
From consolidation to trust
Public management letter for the banking sector
December 2014
NBA
Discussion report
Tone at the Top
Can accountants make a difference?
September 2012
NBA
Between science and business
Public management letter
October 2014
NBA
Moving towards trusted healthcare
Open letter for the curative healthcare sector
June 2015
NBA
Hospitable entrepreneurship
Public management letter for the hospitality sector
September 2015
NBA

Royal Netherlands
Institute of Chartered
Accountants

NBA

Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
P.O. Box 7984
1008 AD Amsterdam
The Netherlands

T +31 20 301 03 01
F +31 20 301 03 02
E nba@nba.nl
I www.nba.nl