CSR Cyber Security Council

CYBERSECURITY GUIDE FOR BOARDROOM MEMBERS

CYBERSECURITY AT STRATEGIC LEVEL

Our society is rapidly digitalising, and we are all reaping the benefits. Our country is a leading knowledge economy and a digital port. But there are also downsides. Personal data, bank credits and business secrets are stolen, identify fraud is committed and hackers disrupt our critical processes.[1]

Society expects organisations to keep their digital services in good order. In particular, critical processes and infrastructure have to be protected against digital (and other) threats. Nobody wants to see society disrupted by a cyber incident. Public and private organisations in the critical infratructure are therefore expected to be resilient and responsive in the event of an incident taking place.

A sound approach to cybersecurity affects all aspects of your organisation: at the top (organisational structure) and across its breadth (service). It therefore presents a pre-eminent strategic challenge for the boardroom. Your IT department does of course also play an important role, but you are the person who sets the parameters at strategic level for the formulation, implementation, monitoring and maintenance of your organisation's cybersecurity policy. This is not a one-off matter, but a continuous process.

Incidents are having an ever-greater impact. They not only affect your organisation and your partners in the chain, but could also affect you personally. Therefore we would like to refer to the Cyber Security Guide for Businesses 'Every business has duties of care in the field of cybersecurity'. Digital resilience calls for and deserves the same attention as your organisation's financial and operational health.

This guide will help you to gain an insight into how you can put cybersecurity in place in your organisation.

For the Cyber Security Council,

Jos Nijhuis, co-chairman
Dick Schoof, co-chairman

Cybersecurity means taking steps to prevent damage being caused by IT being disrupted, interrupted or abused and, if such damage is caused, repairing it.
The damage could involve: impairing the reliability of IT, limiting availability and breaching the confidentiality and/or integrity of information stored in the IT system and its origin.

1 Critical processes are processes that could result in severe social disruption in the event of their failure or disruption. The term 'critical sectors' was used in the past. Since not all processes in a sector are critical, the current focus is on critical processes instead of critical sectors. Identifying critical processes allows the use of tools and scarce resources in a more efficient and targeted manner. (NCTV)

CYBERSECURITY GUIDE FOR BOARDROOM MEMBERS

The importance of cybersecurity in the critical infrastructure

As a company director your aim is to seize the opportunities that arise in your organisation and to minimise possible consequences of incidents. A cybersecurity policy helps you to establish both. Cybersecurity covers both aspects. Taking appropriate action is also part and parcel of your role as a company director. But this sometimes calls for an approach that is different from what you would take for other responsibilities. This guide, formulated by the Cyber Security Council, provides you with information about how to put cybersecurity in place at your organisation.

What are your options when it comes to cybersecurity?

To take the right approach to cybersecurity it is important to be aware of the risks your organisation faces. The next step is to make risk-based decisions. Finally, you steer the process that you initiate to make your organisation (digitally) secure.

Current insights into risks

Do you know what your most important assets (the ‘crown jewels’) are? Or: what is so valuable and important to your organisation that it must not fall into the wrong hands? And how do you protect it? What against? For you as a boardroom member it is relevant to know where the main threats come from. Only then can you put the right measures in place. It will be clear that there is no such thing as 100% security and that endlessly investing in cybersecurity is not a realistic option. However you can invest in cybersecurity according to the '10% criterion'.[2]

The CEO of Target - a major chain of department stores in countries including America and Australia - resigned when the credit card details were stolen online by cyber criminals. This underlines the point that security and privacy incidents have a serious impact on the CEO and the company’s image. What better reason to place cybersecurity on the boardroom agenda?

Risk-based considerations

There may be an apparent field of tension between your organisation’s economic interests and/or public function on the one hand and its digital security on the other. But the fact is that they go hand in hand. A cybersecurity incident could have such a serious impact on your organisation and potentially also for your chain partners, that by its very nature it affects your organisation’s economic interests and security. The question is where to place the focus. What should you mainly invest in? But also: what risks are you willing to accept? You necessarily have to make choices and weigh things up against each other. Make sure that you are structurally provided with relevant information so that you can continue to make risk-based decisions.

2 Verhagen, H. (2016), The economic and social need voor more cybersecurity, keeping "dry feet" in the digital era, The Hague

How do you put cybersecurity in place in your organisation?

Having structural access to relevant information for your risk-based assessments and decisions is a result of how you put cybersecurity in place at your organisation. We have given below a summary of possible job positions that could help you to organise clear tasks and responsibilities.

The precise form and titles of the positions may differ between organisations. The division of tasks is also affected by the size of the organisation. In some (smaller) companies several tasks are placed with a single person. It is important in such cases that no conflicts of interest come about and that tasks are separated where necessary. It is advisable to give the most senior company officer in charge of security an independent position.

The **Chief Information Security Officer** (CISO) holds an essentially advisory role for the company board and is charged with formulating and monitoring the physical and digital information security policy. The CISO should operate independently within the organisation and reports directly to the Supervisory Board. In some cases the CISO role is held by the Chief Risk Officer (CRO). In that case, digital security risks are included in the portfolio in addition to other risks.

The **Chief Information Officer** (CIO) is responsible the development and provision of digital facilities to the rest of the organisation. This officer has a key cybersecurity role and must be able to advise independently. In some organisations the CIO is a member of the Supervisory Board.

The **Data Protection Officer** (DPO). The General Data Protection Regulation (GDPR) applies as of 25 May 2018. Due to this regulation organisations are obliged to employ a DPO. The DPO is tasked to observe the proper use and compliance with the GDPR.

The **Supervisory Board** has a monitoring and advisory role. It is tasked with giving the Board of Management strategic advice on digital security and monitoring his activities in this area. Not all supervisory boards are sufficiently equipped for this task.
Additionally equipping them is therefore advisable with a view to raising the subject of cybersecurity to the organisation's highest level.

How do you structurally build on digital security?

Strengthen the management

- Take responsibility for digital resilience.
  This means showing leadership in formulating, implementing and maintaining the cybersecurity policy. This is not a one-off matter. It is a continuous process that calls for the board's attention.
- Appoint a portfolio holder on the board.
  The portfolio holder and the CISO define the objectives and frameworks, facilitate implementation and monitor the progress and enforcement of the cybersecurity policy. That does not absolve the other directors of their responsibilities!
- Structurally place cybersecurity on the boardroom agenda.
  Work on the basis of a report that is clear to you so that you know enough about your organisation's resilience.
- Make sure that all members of the Board of Management have the desired basic knowledge of cybersecurity.
  Cybersecurity is a distinct discipline with its own concepts and language. It is therefore important to provide your board members with sufficient basic knowledge so that they can keep each other, the CISO and other experts on their toes.
- Create an open atmosphere in your organisation. Employees must feel free to report abuses. This could be aided by operating rules of behaviour at your organisation. You should set a good example on this point.
- Make sure that cybersecurity is a regularly recurring topic of conversation with your chain partners and suppliers.
  The chain is only as strong as its weakest link. Incorporate measures and regulations for cybersecurity levels for processes, products, services and employers should be part of your convenants. It is also advisable to incorporate arrangements on how to act in case of incidents. Holding regular consultations will help to keep this subject on the agenda. This will raise awareness and promote safe behaviour.
- Use the checklist that forms part of this guide.
  It provides effective pointers for making your organisation as digitally secure as possible. It provides effective pointers for making your organisation as digitally secure as possible. You can also use the Cyber Security Guide for Businesses 'Every business has duties of care in the field of cyber security'. The Guide offers businesses better insight into the complex laws and regulations concerning duties of care. This guide also contains a checklist.
- Cybersecurity is incorporated in the revised version of the Dutch Corporate Governance Code (CGC)[3]. As a company director you define the strategic level of the framework. For the implementation of cybersecurity you can also use 'Advancing Cyber Resilience, Principles and Tools for Boards' from the World Economic Forum (WEF)[4].

3 https://www.mccg.nl/download/?id=3364

4 https://www.weforum.org/whitepapers/advancing-cyber-resilience-principles-and-tools-for-boards

Insider threat

Your employees must be reliable. They have access to important information to a greater or lesser extent. It is advisable to ask new employees to handover a certificate of conduct. During the employment you could have your personnel screened (periodically). Make sure that employees have the right authorisations based on their roles and tasks. And if those roles and tasks change, make sure that the authorisations are changed accordingly.
All authorisations of departing employees should be withdrawn immediately and the passwords should be changed. Not just their own passwords, but also those of general systems that they had access to. This serves to prevent undesirable situations.

It is important to train your employees on a regular basis and make them aware of the threats and risks your organisation faces so that they can take them into account.

DigiNotar is an originally Dutch company that issued SSL certificates. These certificates serve to identify websites and to protect web traffic. DigiNotar was hacked in 2011 and dozens of fraudulent certificates were made. DigiNotar kept quiet about the fact that it had been hacked for some time. The hacking had a huge impact.
National security was placed under threat because there was no longer any confidence in any DigiNotar certificates. This resulted in websites being inaccessible because Google and others automatically cancelled dubious certificates. The company DigiNotar no longer exists.

Security in the chain

A robust approach to cybersecurity concerns not only your own organisation, but also your chain of suppliers, contractors (and subcontractors), customers and, where applicable, end-users.
These parties are becoming increasingly interwoven and dependent on each other. This also increases the potential impact of a cyber incident. Directors and other company officers charged with cybersecurity among your chain partners are therefore important discussion partners for you. Hold regular consultations with each other on digital security in the chain. It is advisable to openly share relevant information about digital vulnerabilities in your sector. This enables all the organisations in the chain to take appropriate measures. Regular consultation also ensures that cybersecurity continues to occupy a high position on the agenda. This will raise awareness and promote safe behaviour.

Non-critical organisations can join the Digital Trust Centre (DTC). The DTC improves the information position of small and medium-sized businesses through a nation-wide network of information hubs by providing them with information on threats and advice on how to act.

National security

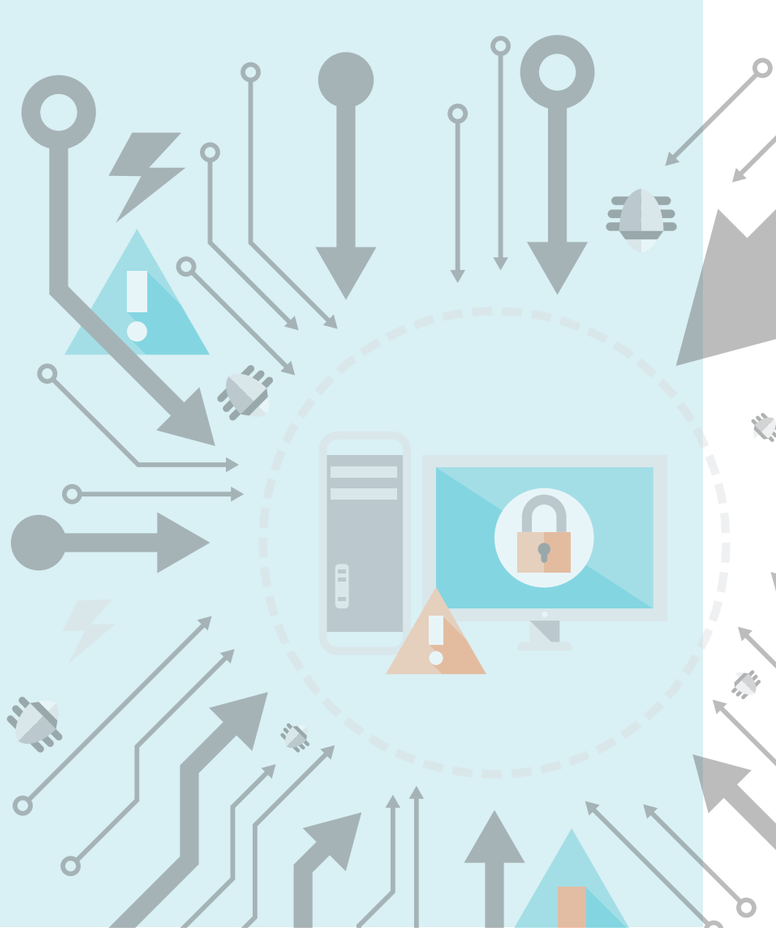
If your organisation carries out a critical process, a disruption and/or downtime could possibly cause social disruption or present a national security threat. In that case operational continuity is an extra big responsibility. Your day-to-day operational management therefore includes preventing cyber incidents and effectively responding should such an incident occur.

Synchronising physical and digital security

Cybersecurity is not always embedded in an organisation as a matter of course. And even when it is, it is not always at the same high level as physical security.
We also see that digital and physical security are by no means always geared to each other. Carefully guarding the front door while the 'digital' back door is wide open does nothing to improve your organisation’s security. Have departments work together in areas where there is common ground.

Use of the checklist

You want to tackle cybersecurity in order to make your organisation as digitally safe as possible. For that reason we have included a checklist in this guide. You can use it to help make your organisation digital resilient. It gives you pointers you can use to prepare your organisation for a cyber incident, to limit its damage and enhance its ability to recover. The list is not exhaustive and needs to be augmented for each organisation.



CHECKLIST

Cybersecurity guide for boardroom members

You want to tackle cybersecurity in order to make your organisation as digitally safe as possible. The checklist below could help you to make your organisation resilient. It gives you pointers you can use to prepare your organisation for a cyber incident, to limit its damage and enhance its ability to recover. The list is not exhaustive and needs to be augmented for each organisation.

Are we sufficiently prepared for a cyber incident?

- [ ] Is it clear which duties of care apply to our organisation? Did we take steps to make sure we act conform these duties?
  Explanation: You can also use the Cyber Security Guide for Businesses 'Every business has duties of care in the field of cyber security'. The Guide offers businesses better insight into the complex laws and regulations concerning duties of care. This guide also contains a checklist.
- [ ] Have we determined the necessary level of security in relation to the risks we face? And have we consciously chosen this level of security? Or: what is our *risk appetite* in the digital domain?
- [ ] Have we (well) invested, organised and provided enough to achieve and maintain this level of security?
  Explanation: Invest in cybersecurity according to the '10% criterion'.[5]
- [ ] Are we clear about which processes and systems are of vital importance and are we adequately monitoring them? What are our 'crown jewels' that we want to protect?
- [ ] Are we sufficiently able to avoid disturbing the forensic investigation that may have to be carried out in response to the incident? Do we know what to do to retain evidence?
- [ ] Have we introduced the right standards and guidelines at our organisation? Do the chosen standards reinforce each other? Do we want to have ourselves accredited?
- [ ] Are sufficient internal and external audits carried out? Do we make use of them and carry through the improvements?
- [ ] Are we connected to the National Detection Network (NDN)?
  Explanation: The NDN is a network of organisations in the critical sector that alert each other to matters such as vulnerabilities, malware and attacks. The network makes it possible to establish digital threats and risks more quickly and effectively. Anonymously sharing threat information enables the participants to take appropriate measures to prevent or limit the damage.
- [ ] Are we sufficiently linked up to other current initiatives that could promote security, such as Information Sharing and Analysis Centres (ISACs) and the Digital Trust Centre (DTC)?
  Explanation: ISACs organise regular meetings in each critical sector for technical experts from your sector, the Dutch General Intelligence and Security Service (AIVD), the National Police and the National Cyber Security Centre. At these meetings (mostly) operational and other information about cyber security subjects are exchanged verbally on a confidential basis. This makes it possible for all parties in the sector to take appropriate measures and prevent or limit damage.
- [ ] Have we introduced a Responsible Disclosure (RD) policy? Is enough capacity available to settle the RD matters?
  Explanation: Responsible Disclosure offers ethical hackers the possibility to report vulnerabilities they discovered. Organisations offer the opportunity to make an anonymously report on the website. Organisations are forced to repair the vulnerability and to thank the reporter for reporting it.
- [ ] Do we periodically (e.g. annually) test our digital and other security with a 'cyber exercise'; do we evaluate the outcomes and implement the necessary changes? Do we sufficiently draw the subject of cyber security to the attention of our personnel? Do we provide our personnel with sufficient (awareness) courses?
- [ ] Are our physical and digital security linked together where possible?

Are we sufficiently able to respond to an emergency?

- [ ] Do we have an efficient crisis structure, including escalation management and crisis communication with a hierarchy of spokespersons?
- [ ] Are we clear about which groups of (chain and other) partners could be affected by incidents and do we inform them promptly and correctly?
- [ ] Are we clear about which parties can help us to solve cyber incidents and are we maintaining close contact with them?
- [ ] Do we need to take out cyber insurance?
- [ ] Do we comply with the legislation such as the General Data Protection Regulation (GDPR) and the Cybersecurity Law?

Are we sufficiently able to recover from an emergency?

- [ ] Are our recovery procedures as they should be and does this form part of our Business Continuity Plan?
- [ ] Is our aftercare, including internal and external communication, as it should be? Have we set up an effective evaluation process with regard to 'lessons learned' and for carrying changes through?
- [ ] Have we set up a process that ensures the matter is reported to the police?

5 Verhagen, H. (2016), The economic and social need voor more cybersecurity, keeping "dry feet" in the digital era, The Hague

CSR Cyber Security Council

The Cyber Security Council (CSR) is a national, independent advisory body of the Dutch government and the business community (through the government) composed of high-ranking representatives from public and private sector organisations and the scientific community. The CSR undertakes efforts at strategic level to bolster cyber security in the Netherlands. The CSR's unique composition enables the council to approach priorities, constraints and opportunities from different angles. The CSR has two co-chairs: one on behalf of the public sector and one on behalf of the private sector.

First revised version, The Hague, April 2018

CSR Cyber Security Council