Royal Netherlands Institute of Chartered Accountants

NBA

CSR Cyber Security Raad

CYBERSECURITY HEALTH CHECK

- MEDIUM-SIZED COMPANIES -

Appeal

This is the Cyber Security Health Check - a tool that allows you to gain an insight into cyber security within your organisation. This Health Check is primarily aimed at medium-sized companies and also serves as a guide for auditors when conversing with clients about the issue of cyber security.

The Health Check has been developed by four major auditing firms (Deloitte, EY, KPMG and PwC) upon request from the Cyber Security Council (CSR). The Royal Netherlands Institute of Chartered Accountants (NBA) is using this brochure to make the Health Check available to its members and other interested parties. The Health Check is not an exhaustive list, but is intended as a good starting point for identifying and mitigating the main cyber security risks.

The chairman of the NBA, Marco van der Vegte, emphasises the signalling and cautionary role of accountants when it comes to cyber security. “Accountants address the reliability and continuity of ICT systems during their auditing and advisory activities, which means it is very important to identify potential cyber risk. In this case, people are often the weakest link: that is why culture and behaviour deserve extra attention. This Health Check will enable more detailed discussions about the issue of cyber security.”

Co-chairman of the Cyber Security Council, Jos Nijhuis, continues: “There can also be weak links in the supply chain. For instance, your organisation can be threatened if suppliers do not adhere to certain underlying norms”. Nijhuis is pleased with the Health Check and the collaboration with accountants that preceded it. “Tackling cyber crime is not an easy undertaking. Comprehensive and unrelenting public awareness about risks in this field is needed to improve cyber security in the Netherlands.”

IDENTIFICATION

- [ ] Has responsibility for cyber security been accepted at board level and is cyber security periodically discussed by directors?
- [ ] Is there transparency within your organisation with regards to your 'crown jewels' (web-shop, operational financial data, personal details of customers, etc.) and what impact a cyber attack could have on these crown jewels?
- [ ] Have the main cyber risks and threats been identified and are they periodically evaluated from a strategic, financial, operational, reputation and compliance (e.g. GDPR) perspective, also by third parties?

Risk
The relevant threats are not acknowledged. This will create ambiguity about risks to which the company is exposed and measures that must be taken.

PROTECTION

- [ ] Do your employees receive refresher training at least once a year to remain up-to-speed with recent developments and security-related do's & don'ts in their jobs (both IT and non-IT)?
- [ ] Have the following basic IT hygiene measures been taken by you as well as any third parties:
  - patch management (updating, testing and installing software);
  - access management (incl. revoking access rights for users after job changes or departures);
  - creating back-ups. Are they performed periodically and is their effectiveness tested on a regular basis?
- [ ] Does your organisation implement effective measures for network segmentation, end-point security and (D)DoS mitigation? Are systems robust enough and is 2FA (e.g.: password and code via SMS) used for authentication on sensitive systems?

Risk
Unauthorised persons are able to enter your organisation. For example, after employees click links in phishing e-mails, whereby malware infects their (insufficiently patched) endpoints and then freely spreads through the (insufficiently segmented) network to other work stations and servers.

DETECTION

- [ ] Does your organisation use logging (log files), possibly aggregated centrally? Are these files also actively analysed so incidents can be monitored?
- [ ] Is your organisation capable of detecting future threats, for example, by implementing monitoring software on computers, servers and/or networks?
  - Ransomware (WannaCry, Petya);
  - Viruses and Trojans (Remote Access Tools);
  - Theft of information (commercial secrets);
  - Unauthorised access to servers and/or information.
- [ ] Does your organisation assess the effectiveness of implemented security measures by performing security tests, such as:
  - Vulnerability scans: automatically scanning internet-based systems and applications for the presence of well known vulnerabilities and configuration errors.
  - Penetration tests: security tests on internet-based systems and applications and/or office automation.
  - Red teaming: under certain scenarios, hackers attempt to gain unauthorised access to your information.

Risk
Incidents are not noticed on time, which means it is impossible to respond appropriately and prevent incidents (and their impact) being repeated.

RESPONSE

- [ ] Has your organisation compiled a communication plan to punctually and adequately inform stakeholders (like the legal department, the press, suppliers, customers, personnel, the government, Personal Data Authority, etc.) about cyber incidents?
- [ ] Has your organisation compiled a crisis plan to restrict the impact of cyber incidents and eventually resolve the incidents themselves, while clearly assigning roles to specific people?
- [ ] Does your organisation periodically practice (e.g. once a year) responding to simulated cyber incidents and do you discuss the results at board level so the communication and crisis plan can be improved?

Risk
Inadequate response means the impact of cyber incidents is more serious than necessary.

RECOVERY

- [ ] Has your organisation compiled a recovery plan, which allows you to duly resume your business operations (before damage becomes too severe)?
- [ ] Do you have appropriate back-up facilities, so you can quickly and efficiently restore compromised systems to their normal status, and do you test them on a regular basis?
- [ ] Does your organisation have processes and resources that allow you to learn from encountered cyber incidents, so they can be prevented in the future, detected sooner or dealt with in a more effective manner?

Risk
Inadequate recovery means the impact of cyber incidents is more serious than necessary.

General instructions

- For each question, indicate whether the matter has been sufficiently implemented in your organisation; basing yourself on how things stand at this moment in time.
- Discuss this questionnaire with colleagues and/or your accountant.
- Potential risks for each category have been described below.

Cyber security: awareness is the most effective weapon

Cyber crime, which is the counterpart of cyber security, is big business. Rogue organisations earn a lot of money by hacking companies. Sometimes it is merely a matter of time before organisations encounter cyber crime. And such cases can normally be attributed to human failings. It is thus important to consider how organisations can protect themselves against cyber crime. However, there is no such thing as absolute security, and awareness among directors and employees is still an important weapon in this fight.

Cyber Security Health Check

Accountants can play an important role when raising awareness, by asking appropriate questions about cyber security. The Cyber Security Health Check, which was compiled by several auditing firms (Inge Philips (Deloitte), John Hermans (KPMG), Douwe Mik (EY), Gerwin Naber (PwC)) for the Cyber Security Council, is an important tool when doing so. It aims to be the starting point for discussions between accountants and clients when addressing the issue of cyber security. The eventual aim is to improve digital resilience and defence, and to be able to respond quickly.

NBA: public relevance of theme

This brochure is the NBA's way of proactively addressing its role concerning important public themes, like that of cyber security. This includes identifying risks that could have a negative impact on the economy. That is why the NBA previously published its Public Management Letter entitled 'From hype to approach' about the risks of cyber security (May 2016). The Cyber Security Health Check is thus a logical follow-up step.

Useful downloads/links

Download the ‘Cyber Security Guide for Boardroom members’ published by the Cyber Security Council.

Download NBA’s Public management letter about cyber security.

MAATSCHAPPELIJKE RELEVANTIE

This brochure is part of the Accountancy Change Agenda; an NBA initiative aimed at ensuring the public relevance of the accountancy profession. The purpose of our profession is to improve the reliability of information. Accountants can do this when dealing with financial statements, business processes, credit reports or tax returns. This will not only allow us to improve the financial prosperity of individual organisations, but also the economic performance of our society in general.