Annual information security monitor

April 2020

DeNederlandscheBank

EUROSYSTEEM

Introduction

DNB has for several years conducted supervisory reviews on the the quality of information security of banks, pension funds and insurers. Since 2010, these reviews have been based on periodic self-assessments completed by the institutions subject to our supervision. As a tool to aid the completion of these self-assessments, we updated the Good Practice[1] and accompanying Q&A for Information Security in 2019.

The information security assessments completed by pension funds and insurers form the basis for this annual Information Security Monitor. The Information Security Monitor was first published in 2019. The supervisory activities with banking institutions have shown that the outcomes of the 2019 information security supervisory reviews are relevant for the entire Dutch financial sector.

In addition to the supervisory reviews completed by DNB supervisors in 2019, this Information Security Monitor has been supplemented with information from answers to standard requests for information[2] and ongoing account supervision, and information from other sources. For example, we receive reports of cyber incidents and through the TIBER programme we are engaged in testing several institutions' on their resilience to cyberattacks. As chair and co-chair of working groups within both the European Banking Authority (EBA)[3] and the European Insurance and Occupational Pensions Authority (EIOPA)[4], DNB has played a role in developing the European Guidelines in the field of IT and Cyber Security. The results from these working groups have been included in this document where relevant.

The six most important observations from this Information Security Monitor for financial institutions are as follows:

1. Cyber hygiene and vulnerability management in particular will remain vital.
2. Security testing contributes to the continuous improvement of cyber resilience.
3. Remain in control when outsourcing activities and do not delegate responsibility to others.
4. Prevention alone is not enough, the focus should extend to cooperation, detection and response.
5. Be aware of your role as management board in information security.
6. Pay attention to specific risks that arise as a result of the COVID-19 pandemic.

In addition to these recommendations, the Information Security Monitor shows that institutions have been working together more frequently. We view this as a vital step forward for the financial sector in effectively combating cyber threats.

1 https://www.toezicht.dnb.nl/en/3/51-203304.jsp
2 IT-SREP and SBA-NFR
3 European Banking Authority
4 European Insurance and Occupational Pensions Authority (EIOPA)

Contents

1 Observations resulting from the Information Security Monitor

Cyber hygiene and vulnerability management in particular will remain vital

Prevention alone is not enough, the focus should extend to cooperation, detection and response

Security testing contributes to the continuous improvement of cyber resilience

Be aware of your role as management board in information security

Remain in control when outsourcing activities and do not delegate responsibility to others

Pay attention to specific risks that arise as a result of the COVID-19 pandemic

Cyber hygiene remains vital

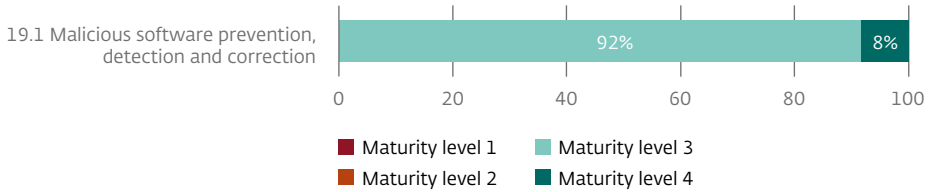
Proper hygiene in cyber security is especially vital in combating cyber threats. Cyber hygiene refers to the definition, application and maintenance of cyber security standards (requirements) and baselines (minimum requirements). Among other things, these standards and baselines apply to measures regarding the mitigation of the impact of malicious software. The control measures #19.1 through #19.3 from the Good Practice for Information Security relate to cyber hygiene and have been reviewed in greater detail in the information security supervisory reviews.

The impact of cyber threats in the form of, for example, malicious software such as malware or ransomware, can be considerable to the operational management of institutions. Only a short time ago, institutions experienced the impact of a vulnerability in the Citrix infrastructure, which caused many institutions to temporarily cease use of this infrastructure for remote working. The impact of this would have been even greater if it had coincided with the current COVID-19 crisis.

The next possible improvement step for institutions could be to focus more on preventive technical measures. In general, institutions have already the necessary provisions (tools) in place to deter malicious software (prevention), to track malware (detection), or to disarm it (correction). Also see figure 1, which is composed of the results from the Information Security supervisory reviews in 2019. We see this as a step in the right direction. In our reviews we also concluded that preventive technical measures such as network segmentation and hardening[5] of systems is presently applied to a relatively limited extent. The next possible improvement step for institutions could be to devote greater attention to these preventive technical measures.

Figure 1 Maturity level regarding managing Malicious Malware Attacks 2019

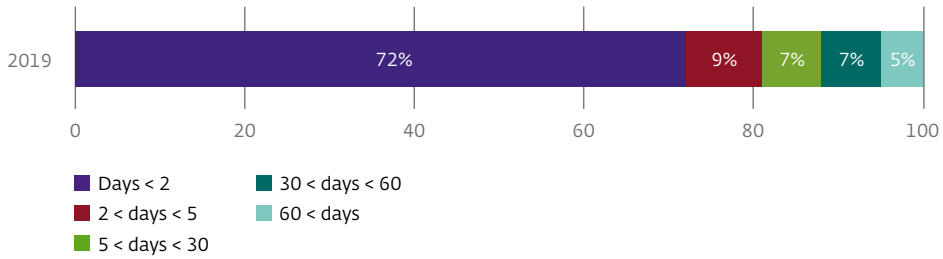
In percentages



We have observed a backlog in the follow-up of vulnerabilities found within institutions' IT systems. See also figure 2, which shows the lead time in patching systems of the investigated institutions. We observed that 28% of critical patches were not implemented within two days. Institutions should be aware of the risks resulting from failing to promptly spot and mitigate vulnerabilities.

Figure 2 Critical systems patched for critical weaknesses

In percentages

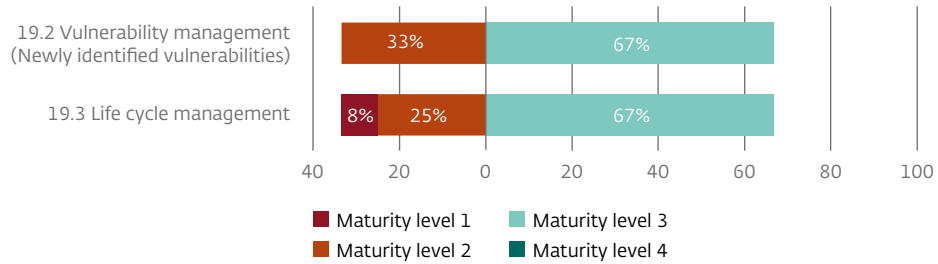


5 The purpose of system hardening is to eliminate information security and cyber security risks to the greatest extent possible, by removing excess functionalities and/or software from the operating system or by disabling them.

The use of end-of-life systems is often commonplace and/or institutions simply do not have the required insight into the life cycle of the applications they use. The result is that suppliers no longer offer support for the applications used, making these applications especially vulnerable to cyber and continuity threats. We also observed this in our supervisory reviews, as shown in figure 3 on life cycle management. In addition to the timely implementation of patches to minimise vulnerabilities, phasing out dated software and ensuring a proper separation in the network (network segmentation) could be good measures to further mitigate cyber risks. This not only applies to software in the IT infrastructure but also to other business-related applications. Another factor is that design principles such as 'security by design' are often not used in older applications, making them inherently more vulnerable than applications that were designed according to these principles.

Figure 3 Maturity level regarding Vulnerability and Life Cycle Management

In percentages



Furthermore, we have observed that institutions are often specifically targeted, and these digital attacks are focused on specific individuals, departments or assets. We used to consider that having 'general' information security measures in place was sufficient. By way of analogy, we used to think that securing our house with better locks than our neighbours was sufficient, whereas nowadays we know that is no longer enough. It is therefore important for institutions to determine on a structural and risk-based assessments basis the impact of the vulnerabilities on their own specific IT assets. In the Good Practice for Information Security, examples are given in which the institution determines its own risk response based on its tolerances and monitors the follow-up. Estimating which vulnerabilities are the most relevant and require a response appears in practice to be a challenging task for institutions. Cooperation in this area between institutions and within the sector is vital, but is to date insufficient.

The TIBER programme shows that analyses of cyber security threats are also increasingly relevant to vulnerability management. In order to prioritise which vulnerabilities require a response, it is necessary to identify the following aspects: which threats exist, which IT assets are available to the institution that can be used against which type of attacker, and which methods are used to reach, manipulate and/or damage those specific IT assets.

Examples mentioned in the Good Practice for Information Security include:

- The institution has implemented tools for the automatic detection and blocking of viruses, worms, malware and spyware, such as modern firewall technology, virus scanners, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).
- Log files from the systems are sent to a Security Incident and Event Monitoring (SIEM) system for the purposes of analysis and response/action.
- The institution constantly monitors whether firewalls, virus scanners, IDS and IPS are up-to-date and reports this on a monthly basis.
- The institution monitors whether service providers ensure that firewalls, virus scanners, IDSs and IPSs and their infrastructure are up-to-date. The service provider reports this to the institution.
- In its configuration management database (CMDB), the institution has included the replacement schedule for applications and replaces them on this basis.

Security testing contributes to continuous improvement

Security Testing conducted as realistically as possible can provide the institution with insight into the measures it has taken, and can be focused on various aspects of the institution's operational management. In the supervisory reviews performed by DNB, specific attention was devoted to testing by the institutions of their comprehensive system of information security and cyber security measures using scenario testing. Also see figure 4 with regard to control #22: Testing.
A scenario test can be aimed at discovering weaknesses in the IT infrastructure or in human behaviour and human actions, but can also be aimed at testing the continuity measures of IT systems (testing of the IT continuity plan). Effective testing by the institutions depends to a significant degree on the selection of the most suitable testing method. We have seen testing methods that vary from simple desk-based exercises to simulated attacks performed in the most realistic way possible. A number of institutions have already performed these realistic tests, for example by simulating mitigating measures surrounding DDoS attacks. We recognise the importance of testing the effectiveness of mitigating measures in a controlled manner.

Institutions should ensure that tests are regularly performed in a recurring cycle, for example as part of a larger testing programme throughout the chain. We have observed that structural embedding of information security and cyber security throughout the chain of institutions is sometimes lacking. We see plenty of opportunity for conducting scenario tests more effectively (and throughout the chain), thereby simulating a more realistic scenario.

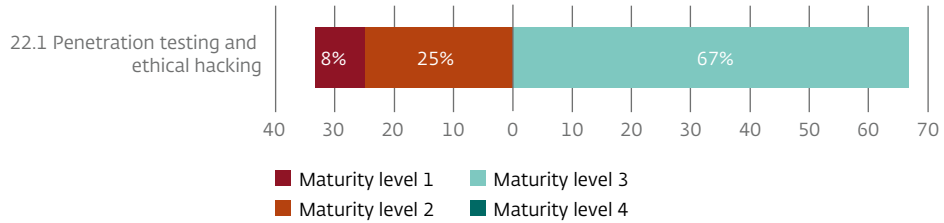
The integrated continuity of the operational management of institutions increasingly depends on a large group of service providers and subcontractors. Institutions could involve their chain partners more in setting up and performing the tests mentioned previously.

DNB's supervisory reviews have also revealed **two other risks** in addition to the above:

- **The quality of the penetration tests performed varies strongly** in terms of the rationale, scope, depth and the reporting. It is our opinion that in the penetration test supplier market, there is great variety in terms of quality and that institutions may find it quite challenging to obtain a clear picture of this market. It is important that institutions pay extra attention to selecting qualified external parties should they wish to hire them to conduct penetration tests.
- **So far, Business Continuity Management is overly focused on conventional scenarios** such as emergencies or fires. BCM policy and testing should be more focused on locations, people (key persons), IT and subcontractors and take into account other present-day threats. Also consider the impact of malware, ransomware and a pandemic on the continuity of operational management.

Figure 4 Maturity level regarding Testing 2019

In percentages



A number of institutions communicate specific expectations with regard to the performance of penetration tests (justification of the investigation, scope, depth, etc.) to suppliers to promote consistency and ensure the quality of the security tests performed. High-quality penetration tests in practice contribute to a significant degree to the improvement of technical measures and the reduction of information security and cyber security risks. Through clear communication with service providers and by managing expectations, the quality of penetration tests is consistently assured and the quality required by institutions is in line with the actual quality of the penetration tests. Service providers with existing policy on the performance of penetration tests could use this to manage the institutions' expectations. This could be done in the following ways: by determining quality criteria for penetration tests, translating those criteria into agreements with service providers and, where possible, to perform additional testing by the institutions.

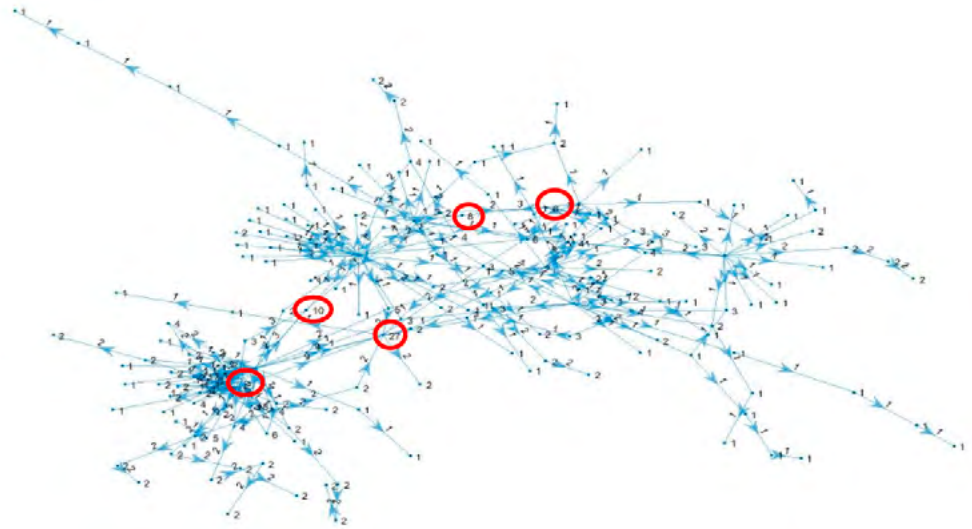
Remain in control when outsourcing activities and do not delegate responsibility to others

We would like to emphasise that the institution remains ultimately responsible for the activities performed by the service providers. This also applies to ensuring that measures with regard to information security and cyber security function properly. In recent years we have observed a trend that outsourcing of critical functions or activities is on the rise within the financial sector. This increases the dependence on service providers in the chain and as a result the need for cooperation between service providers and subcontractors in that chain.

DNB has appealed to institutions to be more aware of possible concentration risks. One way is by asking service providers critical questions with regard to the impact of emergency situations (Business Continuity Management) on service provision. Another way is by developing initiatives such as a pooled audit (see box).

At the same time, there are opportunities when multiple institutions use the same service provider. This allows institutions to show a united front to the service provider for example, based on their joint interests. For example by requesting joint security tests and audits and by demanding the implementation of sound security practices with regard to information security and cyber security. We also call on institutions to increase cooperation for the purpose of determining minimal requirements for information security measures for service providers (including subcontractors).

Concentrations in the chain of various major suppliers of IT infrastructure, data centre services, application management and core processes were shown through a survey conducted among insurers.

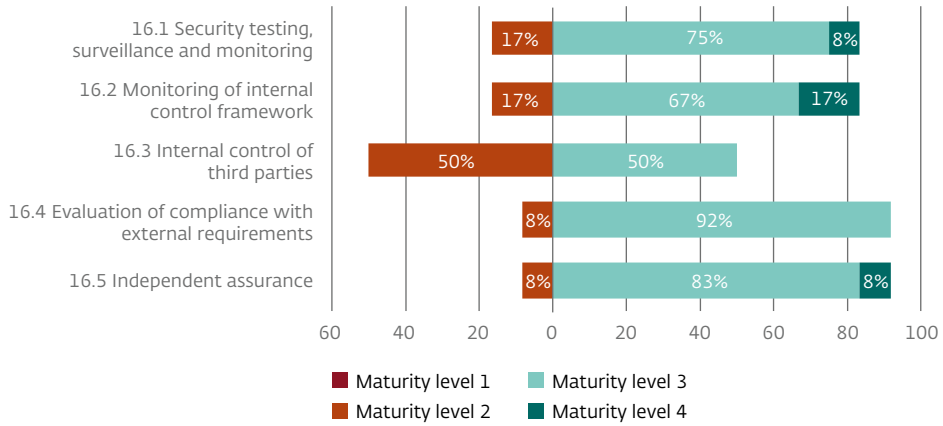


DNB's supervisory reviews have also revealed **three other risks** in addition to the above:

- **Not all institutions havae properly mapped out their critical or important subcontracting chains.** In our Good Practice for Information Security we state that we check to see if institutions have processes in place to at least ensure that they are fully aware of the IT chains that pertain to critical processes that they have the information they need about subcontracting and that proper contractual agreements are in place with service providers.
- **There is a risk of institutions becoming complacent based on the assurance reports.** There is room for improvement for institutions with regard to the use of assurance reports. The supervisory reviews show that an increasing number of service providers are able to hand over assurance reports on the quality of their services and their own internal controls. Also see figure 5 control #16.5, monitoring. There is room for improvement with regard to the use of these reports. It appears that institutions are not adequately performing checks on the type of assurance provided to ensure that it is suitable for the subcontracted activities (operating effectiveness of a measure provides more certainty than existence and design alone). The scope/control measures of the report could also be aligned better with the scope/measures of the subcontracted services. In addition, institutions should be more clear on how user considerations from assurance reports have been embedded in their own organisation and on the impact of any findings from assurance reports on the institution's own organisation.
- **Monitoring of chain partners' information security measures on an operational level is limited.** Also see figure 5 and control measures 16.1-16.5 from the Good Practice for Information Security. Examples include data from institutions and their customers that are no longer stored on their own IT infrastructure, but instead to the systems of chain partners and cloud providers. Clear agreements and proper accountability information are therefore prerequisites for institutions to ensure proper control and monitoring of information security and cyber security measures at service providers.

Figure 5 Maturity level regarding Monitoring 2019

In percentages



Example of a Pooled Audit

Under regulation, EU financial institutions are required to ensure unrestricted audit rights and capability to perform audits in case they outsource material workloads to cloud service providers. As a result, Deutsche Börse initiated a collaborative cloud audit group (CCAG) in 2017 in order to comply with these regulatory requirements. The collaborative audit group performs such audits in a collective manner, significantly reducing the effort for both financial institutions and cloud service providers. This industry-wide initiative includes large EU financial institutions and insurance companies. The CCAG's first successful pooled audit on Microsoft Azure was completed in 2018.

Cooperation, detection and response are becoming much more important

Prevention alone is not enough these days; the emphasis has now shifted more towards detection and response. As indicated in observation 1 Cyber hygiene, preventive measures in the area of information security and cyber security serve as the solid foundation needed to withstand related threats. We see an increase in the importance of measures in the area of detection and monitoring. This is because the question is no longer 'is the institution at risk in terms of information security and cybersecurity?' but 'How does the institution act in the event of an actual cyberattack or incident?'.

The manner and speed with which institutions and their service providers are capable of recognising attacks, withstanding them and/or mitigating their impact is becoming increasingly important. DNB supervisory reviews show that, once access to the institution has been gained, people with malicious intent are able to gain access relatively easily to adjoining components of the institution's IT infrastructure, or that of its service providers. The recent ransomware attacks on various companies have shown that the impact of a long-term attack can be considerable. By further integrating systems and networks, an undesired side-effect arises: increased vulnerability in terms of information security and cybersecurity.

Major service providers are already offering tools and working methods for detection and monitoring. From what DNB has observed, it appears that institutions are currently only making limited use of the available tools and methods. Examples include advanced behavioural tools that are able to detect deviating behavioural patterns of employees on the network. Setting up a professionally-run Security and Operating Centre (SOC) might also be an option.

A Security and Operating Centre (SOC) could contribute to boosting the detection and monitoring facilities of the institution. Due to an institution's limited size, an SOC of this kind might be a bridge too far. As a result, a number of institutions are purchasing SOC services from commercial operators. In addition, several institutions are looking into the option of setting up a joint SOC.

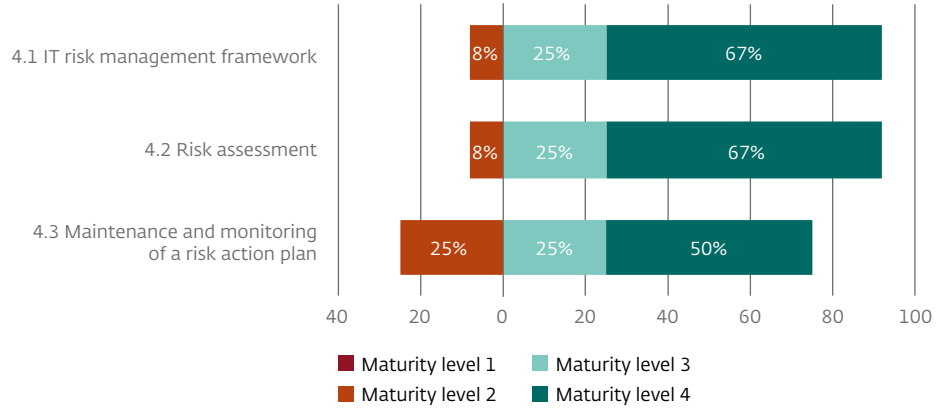
Collaboration with other institutions, also across borders, is becoming more important. Exchanging information about digital attacks and finding ways to detect and neutralise these attacks increases the sector's overall resilience. In terms of information, institutions often have access to only a piece of the puzzle. Information exchange would lead to a more complete overview which will then lead to a tightening of institutions' own control measures.

Responsibility of the management board

In order to properly assess threats in the area of information security and cyber security, the board members need to have a high level of technical expertise. The supervisory reviews show that over half of all institutions have an adequate maturity level with regard to control measures for the Risk Management Cycle. For this purpose also see figure 6 and control measures 4.1-4.3 from the Good Practice for Information Security. We also see that there is scope for institutions to improve the process of identification of risks related to information security and cybersecurity in a more structural manner and to discuss this at management board level. Is the board aware of the most important 'crown jewels' in the organisation and which range of preventive, detection and responsive measures are most suitable for the protection of these assets? Does the board possess the required expertise to make the necessary choices?

Figure 6 Maturity level regarding Assess and manage IT Risks 2019

In percentages



Although we have observed improvements, interviews with institutions demonstrate that the limited knowledge within executive and management boards concerning these threats is something that requires attention. Lack of expertise can lead to executive and management boards' inability to fully comprehend the risks of cyber threats and the effectiveness of the associated measures. This may result in the implementation of the wrong or inadequate measures. The right level of expertise contributes to giving the right level of priority in determining and implementing the necessary measures. The control measures from the Good Practice for Information Security can help to lay the foundations, but the work is never finished. For the specific targeted attacks as described in observation 1, Cyber hygiene, continuous improvement is a requirement. Proper information security consists of continuously analysing, testing, learning, improving and prioritising resources.

Management and executive board members are responsible for their own expertise regarding information security and cyber security to ensure they possess sufficient countervailing power in terms of their own organisation and outsourcing partners. One example is that board members complete training courses and programmes to improve their understanding of the most important IT risks and control measures relevant to their institution and to ensure they possess basic knowledge of information security and cybersecurity. Where necessary and appropriate, the institution may decide to bring in external expertise for specific areas. Finally, it is important that board members lead by example in terms of awareness of risks in the area of information security and cybersecurity and compliance with measures (tone-at-the-top).

The Good Practice for Information Security includes a few good examples per area for how board members can best carry out their roles. The supervisory reviews have shown that not all board members were fully aware of the expectations regarding their roles. DNB will also pay closer attention in assessment interviews to the level of expertise of executive board members in this area.

Pay attention to specific risks that arise as a result of the COVID-19 pandemic

In March and April of 2020, DNB completed an inventory of business continuity and cyber risks within the Dutch financial sector (insurers, pension funds, banks, payment institutions) and important service providers. This inventory was prompted by the coronavirus outbreak (COVID-19) which resulted in activation of measures (pandemic scenarios) by financial institutions and changing working conditions.

This inventory included the following actions:

- more contact moments with institutions that are crucial to our financial stability, such as the major insurers and pension funds and asset managers to discuss indicators and incidents in the area of Business Continuity Management (BCM) and cyber incidents;
- performed a check at major banks (SSM) based on the 'ECB letter on Contingency preparedness in the context of Corona';
- specific information obtained from external audit firms (and IT auditors);
- a data request was sent to major third-party service providers and big tech companies to learn more about the effectiveness of their BCM measures, emergency scenarios and the potential increase of cyber incidents;
- the CISOs of major institutions were specifically approached for the purpose of gaining an overview of the threat risk in the sector.

This inventory now clearly shows the following risks and associated points for attention of the financial institutions. In the coming months, DNB will continue working on this inventory and log and analyse any indications of problems in the sector.

- **Increased risk that the vital infrastructure will become temporarily inaccessible or less accessible as a result of DDoS attacks or attempts at hacking or extortion.** Dependence on the internet for remote working makes the threat of DDoS attacks even more relevant. Working remotely also requires increased capacity in order to keep network equipment up and running. As a result, the required capacity to detect malicious activities and take the necessary action has come under pressure. Attention for monitoring and detection of malicious activities will continue to be vital, as well as taking timely action to address vulnerabilities.

- **An increase of the risk of digital attacks by attempts at phishing and CEO fraud and other forms of fraud in both business and private environments.** Attackers are quick to take advantage of current trends, particularly in the case of attacks related to social engineering. There are several criminal enterprises, for example, such as the Eastern European group TA505, who have exploited the COVID-19 situation to increase phishing emails and have used the absence (due to illness) of key officials to further their attempts at CEO fraud. Institutions can act on any attempts to use the COVID-19 crisis for criminal activities by focusing more on raising awareness.

- **An increase in the risk of unduly paid invoices and other sums.** As a result of remote working, internal checks such as the four-eyes principle are coming under pressure and could be performed less carefully. Institutions could prevent the unlawful payment of funds by focusing more on security awareness and by making additional automated or human checks on invoices and outgoing cash flows mandatory, for example through the application of data analysis techniques.

- **Workarounds increase the risk of digital intruders.** The boundaries between home life and work are blurred as a result of working from home, which increases the risk of non-compliance with information security policy and may result in data leaks and/or other issues. Sending sensitive company information to personal email addresses or devices has therefore become an additional point of attention for institutions.

- **An increase in the risk of operational problems due to a rise in employee absence, including IT security staff and employees of the Security Operations Centre (SOC).** An additional risk to the SOC's operations is a combination of a large amount of external connections to the company network, lower operational staff levels and an increase in cyberattacks. This must be considered in addition to the SOC's current activities, in which proper security logging and monitoring are already a point of attention.

- **An increase in the risk that vulnerabilities within the IT environment are not addressed in a timely fashion because improvements and patches are either not implemented or implemented at a later time.** As a result of the increased workload associated with the effects of the pandemic, necessary upgrades and improvements for applications and IT infrastructure are being postponed. The SOC's activities should therefore be classified as vital.

- **Increased risk that the usual quality and/or security level of service providers cannot be guaranteed as a result of short and long-term staff absences.** One potential issue, for example, might be ensuring the accessibility of VPN connections provided by the service providers. Concentration risks at subcontractors are also at play due to the fact that an issue with one IT Service Provider could have a broad impact. Some institutions may need to have more awareness of the growing responsibility associated with a greater dependence on external service providers.

- **Increased risk of not identifying the reasons why control measures fail on time or later than usual.** Multiple institutions have indicated that they struggle to complete reports on time (including controls testing, annual reports and Financial Assessment Framework statements). Due to time constraints or reduced operational staff (for example as a result of illness) standard control measures may come under pressure or mitigating measures may not be not implemented in a transparent manner. This may prove to be an operational risk in the longer term. It may be important to continue to pay attention to the performance of proper risk management. Another point of focus is recording proper audit trails, so the efficacy of control measures can be shown (retroactively) and to ensure that employee actions remain traceable.

- **Increase of the risk of insufficient monitoring of high authorisations/rights for employees of institutions.** Due to absences (sickness, termination of contracts, no staff replacements, etc), working employees are currently assigned additional responsibilities and tasks that they may not be suitable for or that are not necessary or desired considering their current role. The temporary additional rights assigned to these employees must be carefully considered (based on risk analysis) and properly monitored. This does not always happen, resulting in possible security risks. This issue also has an impact on the operation of IT General Controls.

In our newsletter (https://www.dnb.nl/nieuws/dnb-nieuwsbrieven/nieuwsbrief-verzekeren/nieuwsbrief-verzekeren-maart-2020/dnb387742.jsp) we explain what we expect from supervised institutions in the context of business continuity management.

2 Outlook

As a result of the continuing developments in the area of information security and cyber security, institutions are required to pay continuous attention to upgrading and maintaining the level and design of their information security systems. In the coming years, DNB will use various review methods concerning information security and cyber security within the sector. The review methods form a coherent framework and are self-reinforcing. The methods are described below.

2.1 Sector-wide Analysis of Information Security (SWA-IS[6])

This concerns a sector-wide data request based on the Good Practice for Information Security in which institutions score the Maturity levels of the 58 controls and identify risk indicators based on a survey and a self-assessment. In principle, institutions do not supply supporting documentation for this analysis.

2.2 Information Security fundamental supervisory review

The Information/ Security fundamental supervisory review is the standard Information Security review DNB has performed since 2010 among a selection of institutions. Input based on the SWA-IS assessment contributes to the selection of institutions for the Information Security fundamental supervisory review. This review focuses on the presence of an Information Security foundation at institutions including outsourcing. Institutions submit a self-assessment, based on the Good Practice for Information Security, fully substantiated with documentation and complete with an independent validation (by, for example, an internal or external auditor or key function holder). We evaluate the self-assessment and the accompanying documents and perform a 'challenge' on location with regard to the reported maturity level levels. This review will result in a report with findings and feedback on the maturity levels assessed by DNB.

2.3 In-depth Information Security/cyber supervisory review

The In-depth Information Security/Cyber supervisory review is conducted among a limited number of institutions and is customised based on the insights from the Information Security foundation. A shift is taking place from a controls-based to a threat-based review. For each in-depth review, we will determine which components of the Information Security assessment framework are most effective for in-depth on-site challenges. For this purpose, DNB has access to review techniques such as data analysis and process mining.

6 "SWA-IS; in dutch known as the SBA-IB (*Sectorbrede Analyse Informatiebeveiliging*).

In addition to these review methods, we will be giving specific attention to the cooperation between institutions, which we view as vital for the financial sector in combating cyber threats.

Feedback loop Good Practice Information Security

In the context of this Good Practice, DNB wants to work with the sectors on setting up a feedback loop in which institutions can provide input to keep the examples up to date.

DNB has set up an email address for this purpose: info@dnb.nl. We are enriching the Good Practice based on anonymised results from our supervisory reviews and expect institutions themselves to collect and provide examples during meetings with DNB (including seminars). Cooperation between financial institutions is vital in mitigating cyber threats. If you have useful examples that might be beneficial to other institutions, we would like to receive them. The Good Practice for Information Security will be updated in 2020 and we would be happy to include new and useful examples provided by you.

3 Background Information Security Monitor

3.1 DNB's Information Security reviews

DNB has been reviewing the quality of information security and cyber security within in the financial sector for several years. Since 2010, these supervisory reviews have been based on periodic self-assessments completed by the institutions subject to our supervision. As a tool for performing these self-assessments, we updated the Good Practice and accompanying Q&A for Information Security[7] in 2019.

DNB conducts information security supervisory reviews among a selection of insurers and pension funds to determine the maturity level of Information Security management at those institutions. The observations from these reviews form the basis for this annual Information Security Monitor.

The Information Security Q&A shows that in accordance with Section 3.17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*), in conjunction with Section 20 of the Decree on Prudential Rules for Financial Undertakings Undertakings (*Besluit prudentiële regels Wft – Bpr*), and Section 143 of the Pensions Act (*Pensioenwet – Pw*) in conjunction with Section 138 of the Mandatory Occupational Pensions Scheme Act, institutions under DNB's supervision must have appropriate procedures and measures in place to control IT risks. These procedures and measures aim to safeguard the integrity, continuous availability and security of electronic data. In this context, "appropriate" means that the procedures and measures are based on the nature, scale and complexity of the risks associated with the institution's activities, and on the complexity of its organisational structure.

In order to comply with this provision, institutions take measures to control their information security based on a risk analysis. The control measures control measures are not limited to technological solutions (Technology), they must also address human actions (People), processes and facilities.

Institutions must also periodically and demonstrably evaluate the design, existence and operating effectiveness of control measures as part of their risk management process (risk management cycle), in order to deal with constantly changing information security risks and cyber threats. They must improve or replace any control measures that are not up to standard. The institutions must set up their Governance and Organisation in a way that allows them to manage this process. They must be in control regarding the outsourcing of information security and must test their level of resilience to cyberthreats.

In addition, institutions assess the design, existence and operating effectiveness of control measures on a regular basis as part of their Risk management cycle in order to deal with constantly changing information security and cybersecurity risks. They improve or replace any control measures that are not effective. Institutions set up their Governance and Organisation in such a way as to steer this process.
Also, institutions ensure that they are in control of information security and cybersecurity regarding outsourced activities (Outsourcing) and that they test their resilience to cyberthreats.

7 https://www.toezicht.dnb.nl/en/3/51-203304.jsp

This Good Practice for Information Security document provides institutions with practical tools and guidance, such as control measures and examples, to ensure the integrity, continuous availability and security of electronic data processing in accordance with statutory provisions.

In the 2019 supervisory reviews, specific attention was paid to the tools with regard to the 'role of the management board' and four new control measures that were introduced in the Good Practice for Information Security in 2019. These are:

1. Employee awareness: Actively promoting employee awareness in the area of cyber risks.
2. Vulnerability management: Actively monitoring and resolving vulnerabilities in the IT structure and in IT applications.
3. Application Life Cycle management: Ensuring timely maintenance and phasing out of applications, so as not to compromise the desired information security level.
4. Penetration testing and ethical hacking: Testing the institution's resilience against cyberthreats.

This focus on vulnerability management, testing of resilience and the role of the board can be seen in the most important observations in this Information Security Monitor.

The employee awareness control measure is generally fully implemented by financial institutions and, as a result, does not feature in our most important observations. It is however an important point for consideration in the current coronavirus pandemic. For more information, see the observation that contains additional points for consideration in light of the coronavirus pandemic.

3.2 TIBER and incident reporting

In its role as a central bank, since 2016, DNB has been working with the sector on the TIBER-NL programme which was developed to increase the resilience of financial institutions against cyberattacks. Relevant experiences and information gained from this programme were also included in this Information Security Monitor.

Conceived in 2016, the first version of the Threat Intelligence Based Ethical Red Teaming framework (TIBER-NL) was released in the Netherlands in 2017. Hack tests on production systems based on current threat intelligence are a key component of the programme. The framework describes how the Netherlands' most important financial institutions can request to voluntarily be assessed in terms of their resilience against current, highly-advanced cyberattacks. The conducted tests are coordinated by DNB. The development of documentation within the framework is done in close cooperation with both the parties from the financial sector and parties from the security sector. The goal is to increase the cyber resilience of the most important financial institutions in the Netherlands.

TIBER-NL is aimed at institutions that form a part of the core financial infrastructure; only banks at first, but since 2018 insurers and pension funds have also been included. The project was set up in cooperation with the sector and is also partly funded by the sector.

In the last three years, the framework has been used successfully to conduct around 20 tests in the Netherlands. The framework was adopted by the ECB in 2018 and will be implemented in a number of European countries. With the implementation of TIBER in other European countries, international cross-border tests have become possible.

A new version of the TIBER framework was recently published.[8] The most important adjustment to the framework concerns the alignment of the intelligence about the institution (what could the attacker use?) and the test scenario performed. More emphasis has been placed on learning from experiences once the test has been completed. This allows the institution to discover which areas need to be strengthened in the defence against cyberattacks.

In addition to the overview and experiences obtained from TIBER, this Information Security Monitor is also based on experiences with reported incidents. For the purpose of this Information Security Monitor, the scope was broader than just the incident reports received by DNB. The main source on which this Information Security Monitor was based, was an overview of incident reports and threat assessments from EUROPOL's OSINT dashboard and the Dutch FI ISAC.

3.3 European Banking Authority (EBA) and European Insurance and Occupational Pensions Authority (EIOPA)

In recent years, cyber risks have become an important topic for international regulatory authorities. Consider the G7 (the Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector and Fundamental Elements for Threat-lead Penetration testing), the BIS Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (IOSCO, report by the Cyber Task Force), the Financial Stability Institute (Cyber lexicon), BCBS (Cyber-resilience report: Range of practices) and IAIS (Application Paper on Supervision of Insurer Cybersecurity).

The European Commission also requested that European Supervisory Authorities – ESAs) more explicitly address cyber topics in their guidelines. In 2019, the European Banking Authority (EBA) published Guidelines on IT and security risk management. Shortly before the consultation, the European Insurance and Occupational Pensions Authority (EIOPA) published the draft version of Guidelines on information and communication technology (IT) security. Both sets of guidelines provide instructions for the sector on how to organise their Information Security. The guidelines were aligned where possible.

DNB's Good Practice for Information Security is in line with both EBA and EIOPA guidelines.

In recent years, DNB has played an active role in the working groups that have drawn up the guidelines and are more broadly involved with IT and Cyber within both EBA and EIOPA. The views and experiences gained from these and other domestic and international working groups have been included in this Information Security Monitor where relevant.

8 https://www.dnb.nl/binaries/TIBER%20NL%20Guide_tcm46-387212.pdf

Appendix 2020 Threat Assessment

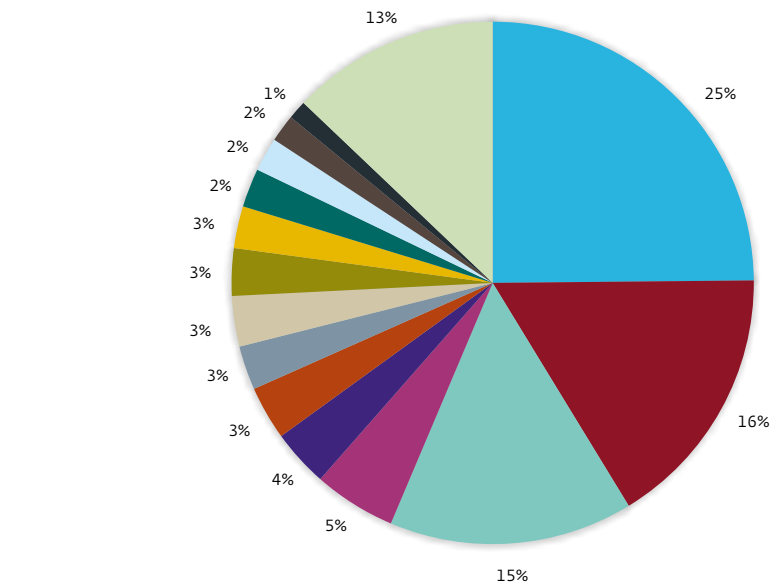
There are numerous possible threats to cyber security. Too many to include here. Based on the information and experiences gained from the sources used for this Information Security Monitor, we believe the following threats in particular could occur most often, have the highest chance of success and have a potentially significant impact on the financial sector in 2020.

The EC3 – part of the European Cybercrime Centre van EUROPOL – issues weekly automated (OSINT) and open-source-based dashboards containing general attack techniques used in various sectors. The various dashboards issued in the last year (2019/2020) have shown that phishing is an attack technique used most frequently in information security incidents. There are two forms of phishing: aimed at a large group (phishing) and aimed at specific persons within an organisation (Spear Phishing). DNB has observed that both attack techniques also occur frequently at financial institutions. In terms of Spear Phishing in particular, we have established that increasing use is made of the sale of personal data, sometimes obtained from leaks, sometimes available online, from other companies, social networks or websites. This information is used in combination with social engineering: a method used to manipulate people into giving up sensitive information about their employer.

In addition to information about attack techniques from the OSINT dashboards, we have also observed that financial institutions may be vulnerable via subcontracting parties (service providers) and those who have access to or are part of their core infrastructure. Examples include service providers such as cloud storage providers, infrastructure providers and data centres, call centres, payment systems and workplace facilities. Via service providers, financial institutions could be the direct target of a digital attack or could be affected by a digital attack aimed at the service provider of which the financial institution then becomes an unintended victim as well.

Figure 7 Attack techniques OSINT in the previous year

In percentages



Source: various dashboards from the past year (2019/2020) from OSINT EUROPOL. The dashboard were created based on various sources on the above-mentioned topics within a certain period of time.

Concentration risks arise in the context of certain service providers. This is due to the fact that a small number of service providers works for a large number of financial institutions. These operators are especially appealing targets for attackers. This concentration of service providers gives attackers potential access to multiple financial institutions at once. An attack that knocks out one concentrated service provider also allows attackers to impact a large part of the financial sector. Remaining in control of outsourced tasks is therefore also incredibly important for financial institutions in this regard.

In addition to external threats, we would also like to focus attention on relevant internal threats from employees within the own organisation. There are three different types of these threats.

1. Internal employees can intentionally obtain authorised or unauthorised access to relevant internal systems and steal, manipulate or tap information from these systems. Examples include employees who are seeking personal gain or employees who may be dissatisfied due to a reorganisation. There have also been cases of employees who have infiltrated financial institutions from criminal organisations.
2. Increasingly frequently, well-meaning employees are manipulated by criminals who pretend to be colleagues or supervisors and are tricked into providing data or access to systems. CEO fraud is a good example.
3. Due to the fact that employees are increasingly working from home, internal threats associated with potentially vulnerable VPN connections, laptops and mobile phones are on the rise. Employees are spending more time working remotely; not just from home but also on public transport, in public areas and in the offices of customers. This also increases the risk of potential loss and theft of devices, allowing vulnerable VPN connections to become more easily accessible.

For well-meaning employees working remotely, awareness programmes intended to increase focus on the safe use of devices and handling of sensitive data may prove useful. In the case of employees with malicious intent, specific tools need to be used to help detect deviating behavioural patterns on the network.

Once access has been gained, for example though one of the above-mentioned methods, we see that in addition to stealing and manipulating data, extortion for financial gain using ransomware is on the rise. Long-term infiltrations of bank systems or other systems by highly-advanced attackers can also be observed. Attackers use this time to gain insight into the institutions and use stepping stones to achieve their intended goals.

Which threats are relevant to individual institutions depends on the specific environment in which an institution operates. Each institution has its own internal landscape or system landscape and provides specific services. In order to successfully withstand the specific threats facing institutions, an overview is required of the most relevant threats. For more in-depth information, see the header 'Cyber hygiene remains vital'.

Disclaimer

This Good Practices document comprises a set of non-binding recommendations. It sets out our expectations regarding observed or envisaged behaviour in policy practice that reflects an appropriate application of the rules regarding information security and cybersecurity.

We encourage institutions under our supervision to take our expectations as well as their own specific circumstances into account in their considerations and decision-making, without them being obliged to do so. Our Good practices documents are indicative in nature and therefore do not alter the fact that some institutions require a non-standard, more strict application of the underlying count.