4.2 The purchase and use of software by organizations

Growing numbers of processes in our society and within organizations are being undertaken by digital means. As a consequence, dependency on digital systems and the software that these systems contain is growing both for organizations and for society as a whole. Because software will always contain vulnerabilities, it is essential for organizations to take the inherent risks into account when purchasing and using software. The questions discussed here are: how do organizations that purchase and use software, such as municipalities, hospitals and companies, deal with the risks involved in the purchase and use of software? Which dilemmas and obstacles play a role?

4.2.1 Relationships on the software market

The extent to which risks are managed when purchasing software with vulnerabilities is limited by a number of factors. This became clear from interviews with various organizations. One of these factors is the relationship between manufacturers and end users on the software market. The software market is characterized by information asymmetry.[150] Software manufacturers have more information about the composition of the products than customers. It is often not possible for them to identify the composition and quality of software. This is because manufacturers generally demonstrate little transparency as regards the structure of their products. Moreover, many organizations do not have the necessary knowledge or capacity to be able to evaluate the information, even if a manufacturer does offer the necessary insight.

This information asymmetry makes it difficult for customers to assess the quality and safety of software. As a result, they mainly assess products according to the elements they are able to check, such as price, functionality and ease of use. As a consequence, manufacturers compete with one another on these elements as there is no point for them to invest in the safety of the products. There are no legal provisions to compensate this information asymmetry by transferring liability from customer to manufacturer.

The software market is controlled by a small group of large manufacturers. The market power of a number of manufacturers means that for certain functionalities, there are only a few products available from a select group of suppliers, for example for operating systems such as Windows and macOS or office software packages such as Microsoft Office. In many cases, manufacturers offer standard packages and customers have few possibilities for matching these to their own wishes or requirements. This is because the software market is a global market which can hardly be influenced by users in the Netherlands alone. Influencing such a global market requires a larger power block, for example at EU or UN level, or based on joint actions by end users.

When vulnerabilities are discovered in software products, the manufacturer sets to work to develop a patch for those vulnerabilities. Developing this solution requires the manufacturer to spend resources. Many of the costs and risks in the event of vulnerabilities are borne by the user of the software. The user incurs costs in mitigating and patching systems. In addition, the user incurs costs if its operations are shut down, for example following an attack. If the user is insured against cyber incidents, in certain cases, the

150 Anderson, R. and Moore, T., *The Economics of Information Security*, Science 314, October 2006.

insurer will reimburse part of the costs incurred by the organization. Generally speaking, the risks of damage as a result of vulnerabilities in software are mainly borne by the user of the software. These factors together mean that the software market is described by experts as a failing market because of the asymmetric relationship between manufacturer and customer.[151]

4.2.2 The purchase of software

The customer purchases software based on a functional need to manage tasks or processes by digital means. After identifying this functional need, the user looks at the possibilities available on the market to meet its need. When selecting a product, a range of wishes and requirements play a role, such as the functionalities offered by the software, ease of use, price and security.

Formulating safety and security requirements and checking products according to those requirements

As discussed in section 4.1, at present there are limited possibilities to obligate manufacturers to safeguard cybersecurity in their products. This places an additional burden on the customers to test the products for safety and security, when purchasing software. Because of the information asymmetry on the software market (see subsection 4.2.1), customers often purchase software on the basis of a functional need, while safety and security aspects play a more minor role.

To be able to formulate the correct safety and security requirements, the organization that uses the software needs knowledge of the relevant requirements, for its situation. The user also needs information about the product to be able to assess the extent to which the product satisfies those requirements, and how this should be interpreted for its situation. If an organization is able to specify the correct requirements but is unable to check them, it is not possible for the organization to assess whether software actually satisfies the safety and security requirements.

There are broad differences in the extent to which organizations impose safety and security requirements on the software products they purchase. Some, mainly larger organizations do have the appropriate knowledge available to them, to impose requirements and to check them. One commonly imposed security requirement is the authority to carry out penetration tests.[152] Other, generally smaller organizations are unable to impose the correct safety and security requirements because they do not have access to the necessary knowledge and resources, or do not recognize the importance of doing so. In addition, manufacturers do not always allow penetration tests to be carried out on their products, because the process involves certain risks. For example, if penetration tests are carried out in a cloud environment, there is a risk that the test will cause damage or threaten the availability of the environment. In addition, when carrying out penetration tests or reverse engineering[153], it is possible to work out how a software product is built, and for example to ascertain details about a specific algorithm.

151 Anderson R., *Security Engineering*, 2020.
152 A pentest is a security check whereby an external test for vulnerabilities is carried out, followed by an attempt to hack the system via these vulnerabilities. See chapter 2.
153 Reverse engineering is investigating a product to determine its functioning and structure.

Because of the competition on the market, manufacturers are not keen to release this information. As a result, manufacturers often impose conditions and restrictions on penetration testing. It is therefore not common practice that customers be permitted to carry out penetration tests on the software they use. One way in which customers are able to ensure that they are permitted to carry out penetration tests is by including this as an explicit requirement in their contract with the supplier. In interviews, a number of organizations indicated that although they include penetration tests as a standard requirement in contracts, it sometimes takes considerable persuasion to allow this requirement to be included in the negotiations with product suppliers. Larger organizations with greater cyber maturity generally do have penetration tests carried out on their systems. There are also organizations that, if they do discover a vulnerability in software widely used in their sector, pass on this vulnerability to the sector organization. Subsequently the sector organization can raise the question of the vulnerability on behalf of all affiliated organizations, with the product manufacturer.

Although imposing safety and security requirements and checking those requirements is not carried out as standard, there are examples of specific sectors in which organizations impose compulsory safety and security requirements on software products and suppliers. The Dutch Ministry of Defence, for example, imposes strict safety and security requirements on suppliers that carry out work on its behalf. These requirements are laid down in the General Security Requirements for Defence Contracts (ABDO) scheme. The Military intelligence service MIVD also checks whether suppliers comply with this scheme. Financial institutions also impose strict safety and security requirements on the products they commission. By means of its procurement policy, the national government also aims to improve the cybersecurity of software. To assist government organizations in formulating safety and security requirements, the Government Cybersecurity Procurement Requirements wizard (ICO wizard) was developed. The ICO wizard is a tool for government organizations, but its use is not compulsory, and it offers no indicators as to how end users can check the requirements imposed. Moreover, the ICO wizard provides nothing more than a list of requirements, from which organizations can make their own selection. It is up to the organization itself to make the correct selection, and that is something that requires expertise that not every organization can call upon. In addition, the organization itself is required to assess the product, something that also requires knowledge and cooperation from the manufacturer.[154]

154 Ministry of Defence, *General Security Requirements for Defence Contracts 2019*, February 2020; Ministry of Economic Affairs and Climate Policy and ministry of Justice and Security, *Roadmap for Digital Hard- and Software Security*. April 2018;
The ICO wizard is a tool developed for government organizations based on the Government Information Security Baseline (BIO), to encourage demand for digitally safe software, and to create an incentive for manufacturers to place digitally safe products on the market. Within the ICO wizard, organizations can select the requirements they consider applicable to the procurement of software, see: https://www.bio-overheid.nl/ico-producten

Procurement requirements by governments abroad: US Executive Order
In May 2021, an Executive Order[155] was issued in the United States in which a series of measures are specified aimed at improving national cybersecurity.[156] As well as a number of measures relating to information sharing, the reinforcement of capacity in the event of incident management and learning from incidents, the Executive Order also aims to improve the safety of software.

One of the measures taken in the Executive Order is to impose standards on software used by federal governments. Within the Executive Order, federal governments are required to impose safety and security requirements on software suppliers. If the parties fail to satisfy these requirements, they will no longer be able to supply software to American federal government organizations.

As a rule, the imposing and monitoring of safety and security requirements on manufacturers by organizations is non-binding. There are no appropriate regulations. The extent to which it does take place therefore depends on the organizations themselves. Not every organization has the expertise available to impose the appropriate requirements on software, and to subsequently check whether the products satisfy those requirements. There are no safeguards in the system to ensure that products satisfy particular requirements.

4.2.3 Use and maintenance phase of software within organizations

As discussed in chapter 2, organizations are able to take a number of measures to secure their systems and to prepare for incidents. The NCSC recommends several basic measures that organizations can take to counter cyberattacks. Examples include patch management, firewalls, network segmentation and detection capabilities. In the Cyber Security Assessment Netherlands 2021, the NCTV concludes that although the resilience of organizations is improving, it is not yet at a sufficiently high level. Not all organizations have taken the basic measures.[157] How can we better understand the reason why organizations do not always take these basic measures? This is partly due to the ability to take measures, and partly due to biases in the way people in organizations view the risks of cyberattacks.[158] Below we discuss the dilemmas relating to these measures.

Dealing with the dependency on software

Using software and being dependent on that software always entails risks. It is impossible for end users to fully mitigate these risks, but it is essential that they first have a clear picture of the risks in order to make any assessment. One way of reducing the dependency on a product is to implement a redundant system by using software products from different manufacturers. However, it is not realistic for every organization to implement all systems redundantly, because it demands extra resources. If an organization operates

155 An Executive Order is a decree issued by the president, with the same powers as a law
156 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, accessed on 14 July 2021.
157 National Coordinator for Security and Counterterrorism, *Cyber Security Assessment Netherlands 2021*, June 2021. https://www.security.nl/posting/710981/Cybersecuritybeeld+Nederland%3A+al+tien+jaar+lang+de+basis+niet+op+orde
158 Meyer, R. en H. Kunreuther, *The Ostrich Paradox*: *Why we underprepare for disasters*, 2017.

different systems from different suppliers, it is also possible that those systems are unable to work together effectively (compatibility issues). In certain cases, end users deliberately do decide to implement their systems redundantly, for example for vital systems that facilitate crucial processes, or if the consequences of system unavailability are considerable.[159] As regards system dependency on a specific product within a network, there are many differences in how organizations have structured their networks. In an interview, one organization explained that it had structured its systems in such way that there is no single point of failure; as a result, if a system fails, other systems and processes are able to continue. Another organization told us that its network consists of a number of products on which many of its processes depend. In that situation, if a system fails, many of the processes within the organization cannot continue.

In dealing with the dependency on software, it is essential to gain an insight into the risks involved in using a particular product, and the related system dependencies. When an organization is aware of its critical systems, and has a clear understanding of its dependencies, it is in a better position to assess the risks of the measures that need to be taken in an incident, and in preparation for an incident. Generally speaking, there is a big difference between organizations in the extent to which they have an overview of their systems. Above all larger organizations tend to have a (reasonably) clear picture of the systems they operate, and the current versions. They record this information, for example in a Configuration Management Database (CMDB). Whenever a vulnerability is published, they can check the database to see whether the vulnerability applies to their organization and whether they need to implement a patch. Because they understand their systems and dependencies, they are also more easily able to prepare a more precise risk analysis of what would happen if the system were to be shut down. At other (often smaller) organizations, it is clear that they do not always have a complete overview of the systems they use. The risk of this situation is that if a major vulnerability is discovered, these organizations are unable to take the necessary action (in time) and run the risk of becoming compromised. In addition, these organizations are unable to make a complete risk analysis of the impact of a system shutdown.

Mapping out and maintaining a clear picture of the systems and system dependencies requires capacity, and the entire organization must recognize the importance of keeping this overview up to date. For organizations with limited capacity, obtaining a complete picture of all systems and the intersystem dependency can be a challenge. The organization structure can also make it more difficult to obtain a complete picture of all systems in use. The Inspectorate of Education identified this as one of the relevant factors following the ransomware attack at Maastricht University.[160] Universities are characterized by a multi-layered administrative structure with different administrative bodies, each responsible for their own information security. This makes it a challenge to obtain a clear overview of the complete network of IT systems. In addition, chain dependencies can make it difficult to generate a picture of the complete system and the dependencies. Many organizations work together with external suppliers or supply chain partners. As a

159 Jacobs, D., '*7 factors to consider in network redundancy design*', https://searchnetworking.techtarget.com/tip/7-factors-to-consider-in-network-redundancy-design, accessed on 16 July 2021.
160 Inspectorate of Education, *Cyberattack Maastricht University*, May 2020.

result, processes within an organization can be (partly) dependent on the systems used by external parties, as for example was the case in the Kaseya occurrence (see 3.3.5).

Patching

As a rule, software is not a static product but continues to develop following the purchase moment. In addition, the cyber risk and threat landscape is not static either, and equally continues to develop. When vulnerabilities are discovered in software, manufacturers develop patches to correct them (see section 4.1). At present, it is primarily the responsibility of the organizations that use the software to implement these patches to repair the vulnerabilities on its systems.

However, patching also engenders risks and requires consideration. Because of the large number of patches published each year (some organizations are required to implement up to a 100,000 patches a year), it is not always possible for an organization to install the patches in time. Because of the large number of patches per year, organizations have difficulties to have a complete and up-to-date overview of vulnerabilities in their systems. To simplify this, organizations can purchase scanning services. These scanning services scan for known vulnerabilities. But not all vulnerabilities are able to be scanned, and the list of vulnerabilities that is scanned is often incomplete. In addition, smaller organizations usually do not have the resources to purchase such scanning services. They often rely solely on the NCSC advices. In these circumstances, organizations cannot patch everything in time. It is therefore inevitable that known vulnerabilities, including critical ones, are not patched.

The large amount of vulnerabilities also apply considerable pressure on organizations to implement the patch process in the required manner, and to consider which vulnerabilities require immediate action. The incapacity of organizations to patch vulnerabilities in time, according to penetration testers at Positive Technologies, makes it easier for attackers to hack company networks. Patching requires knowledge of systems and staff capacity within organizations. As well as patching systems, IT staff have numerous other tasks that also have to be carried out. At every organization, it is a question of deciding whether to continue day-to-day operations, or to immediately switch to patching systems. End users are sometimes reticent in immediately implementing patches, because there is a risk that following the patch, systems will no longer function correctly or may even fail, which will have consequences for the organization's normal operations. In addition, it is possible that the patch will not or will only partially repair the vulnerability.[161] Interviews revealed that this consideration is particularly difficult for smaller organizations because they have limited resources to deploy additional capacity for system patching.

As described above, because it can be a challenge for organizations to obtain a complete picture of all the systems in use, it is possible that organizations fail to patch a vulnerability because they lack an up-to-date overview of which software is operated where, which version is affected and whether or not a patch is necessary to be able to guarantee the

161 Nichols, S., *You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that,* The Register, August 2020.
'The Nightmares of Patch Management: the Status Quo and Beyond', Trend Micro, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond, consulted on 14 July 2021.

security of the systems. Moreover, it is not always clear to organizations precisely which components make up the software they are using, because software is closed source in many cases. In other words, the source code is not accessible to the customer, and the manufacturer is reticent about revealing the software architecture. In addition, much software is based on open source components that contain critical vulnerabilities, without organizations being aware of this situation.[162] As a result, organizations can be vulnerable, without being aware of it themselves.

It is also important for the entire organization to recognize the importance and urgency of patching. It is not always clear to organizations that they can be attacked without an attacker specifically targeting their organization. A vulnerability in software on a server that is connected to the Internet is like honey to a bee, for attackers. These attackers automatically scan all servers containing vulnerable software, in the hope of identifying servers that will enable them to hack into systems of organizations. Research shows that organizations often base their actions on past experiences with updates.[163] Many published vulnerabilities are not actively exploited by attackers. Whenever organizations wait before patching vulnerabilities not used for attacks, it will have no consequences for the organization. As a consequence, organizations may tend to underestimate the importance of a rapid response to future vulnerabilities.

According to manufacturers and experts, transferring software to the cloud can be a solution for ensuring that systems can be patched in time. This is known as a Software as a Service (SaaS) solution.[164] Because the software is then managed by a manufacturer, the advantage of SaaS is that patches can be tested and applied more quickly. This eradicates the time between the release of a patch and its application, so that customers always have the latest patches, quickly. In the case of SaaS, the application of patches becomes the responsibility of the manufacturer rather than the customer.

Transferring software to the cloud, however, also brings with it risks and considerations for an organization. The disadvantage of SaaS solutions is that in the event of a vulnerability all servers will become vulnerable, since they all operate on the same version. Furthermore, the manufacturer is the only party able to do anything about the situation; the organization has no role to play. If organizations manage their own systems, they are in control of patching, mitigation and shutting down systems. In addition, when taking up a cloud service, the organizations have no understanding of the nature of the product. Moreover, an organization becomes less flexible, and the possibilities for software adaptation are restricted. Automatic updates to SaaS solutions can also threaten the continuity of systems, or even introduce new vulnerabilities. Organizations then have no control whatsoever over these risks. Another consideration for an organization is that in the event of an incident, the systems are held by the manufacturer. The manufacturer has the most in-depth knowledge of the product, and is therefore the ideal party to be

162 *'Veel kritieke lekken door open source in standaard apps'* (Numerous critical leaks due to open source in standard apps), AG Connect, https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps, 5 August 2021.

163 Rajivan et al., *Update now or later? Effects of experience, cost, and risk preference on update decisions, Journal of Cybersecurity,* 2020.

164 In SaaS, software is offered as an online service. Via the Internet or via VPN, the end user is granted access to the software managed by the provider.

able to analyse its software, in the event of an incident. The manufacturer can then assist the organization in investigating whether it has been affected, and solving the problem.

On the other hand, organizations sometimes do not want to share information with external parties, for example because it is not permitted, or because they do not want to risk their information ending up outside the organization. It is also possible that the organization does not want to link a system to the Internet because of the nature of that system. In that case, SaaS is not a solution, and it is up to the organization to physically manage (part of) its own systems.

The regular patching of software introduces new problems. If an organization fails to patch, it may be opening itself up to the risk of a security breach that can be automatically traced by external parties. Due to the large and ever growing number of patches, patching all vulnerabilities is not manageable for all organizations. Moreover, for organizations, the necessity of (rapid) patching is not always clear. Offering software from the cloud shifts the responsibility for patching to the manufacturer, but also entails risks for organizations that use the software.

Prevention and detection

In addition to patching, an organization can also take a series of other prevention and detection measures, to protect its network, for example installing a firewall, introducing network segmentation and monitoring systems. Each of these measures does engender risks and considerations for an organization.

One measure for restricting external access to the systems of an organization is to install a firewall.[165] The challenge with firewalls is that they must be installed in such a way that they prevent undesirable activity but do not inadvertently also prevent desired activity. In addition, the correct rules and policies must be implemented, and it is important that these aspects be checked and updated periodically. This too demands knowledge and capacity from an organization. A firewall can also introduce risks, if an organization does not have the appropriate knowledge about exactly what the firewall does. As a result, the organization may have no understanding of whether its systems are unnecessarily open to traffic.[166]

To limit the impact of a potential incident, organizations can segment their network. The risk of segmentation is that if a network consists of too many segments, it can take a great deal of time and money to manage the network.[167] Implementing segmentation in a network is a process that requires numerous adjustments, that is costly and that can

165 A firewall is a machine located between the network and the Internet, that monitors traffic and filters out possible harmful traffic.

166 https://www.insightsforprofessionals.com/it/security/firewall-management-challenges-how-solve-them, accessed on 22 July 2021; AlgoSec, *Firewall Management: 5 challenges every company must address – an AlgoSec Whitepaper,* 2015.

167 *'Hazardous Network Segmentation: when more isn't better',* AlgoSec, https://www.algosec.com/blog/hazardous-network-segmentation-when-more-isnt-better, accessed on 22 July 2021.

disrupt the primary processes of an organization. It is also difficult for organizations to find staff with the necessary skills and expertise.[168]

As well as more preventive measures like firewalls and segmentation, many organizations also invest in detection capacity and system monitoring. On this basis, organizations are able to detect suspicious activity when it takes place. The challenge for organizations is correctly setting the level of detection. If this is not the case, suspicious activity may go unnoticed, or an activity can be incorrectly detected as suspicious (false positives). In other words, the fact that detection systems are in place does not guarantee that all suspicious activity will be observed. In addition, organizations must have the knowledge to be able to interpret the activity, and to know how to respond when they do detect activity by an attacker. This demands capacity and expertise from the organization. For vital operators and national government organizations, it is possible to sign up to the National Detection Network (NDN). The NCSC passes on indicators to the participants in the NDN, to enable them to recognize a potential attack. To be able to be part of the NDN, organizations must have already implemented their own monitoring process. Direct participation in the NDN is only open to national government and vital operators.[169]

One trend that is emerging in the world of cybersecurity is the growth in investment in detection capabilities, as compared with prevention.[170] It is often emphasized in the security world that it is not possible to prevent all attacks, so it is worthwhile above all to invest in detection and response. This attitude was also clear in a number of the organizations we spoke to, that had invested primarily in detection and response. However, investing in detection does not always offer guarantees, as discussed above. The systems at one of the organizations interviewed, for example, failed to detect the attack via the software vulnerability, as a consequence of which the organization was compromised. To ensure the most secure system possible, multiple layers of security and protection are needed, in terms of both prevention and detection and response.

4.2.4 Managing cybersecurity in organizations

Capacity and expertise

All the measures referred to above require capacity and knowledge from organizations. The extent to which an organization has access to this capacity and knowledge depends on the size of the organization and its cybersecurity maturity level. Smaller organizations have limited capacity and knowledge in the field of information security. Generally speaking, in the course of this investigation, we saw major differences in the extent to which organizations take measures to prevent incidents, and the extent to which they are prepared for incidents. A municipality with a limited budget, for example, has little capacity for information security and IT, in general. Within such organizations, the CISO

168 Holt, M., *Security Think Tank: Benefits and challenges of security segmentation,* Computer Weekly, https://www.computerweekly.com/opinion/Security-Think-Tank-Security-segmentation-benefits-and-challenges, accessed on 15 July 2021.

169 Ministry of the Interior and Kingdom Relations and ministry of Security and Justice, *Handreiking voor implementatie van detectie-oplossingen (Guide for the implementation of detection solutions),* October 2015.
Certain organizations such as healthcare institutions, municipalities, educational institutions and water authorities can sign up to the NDN, indirectly, via the sectoral CERTs. See: https://www.ncsc.nl/actueel/weblog/weblog/2020/het-nationaal-detectie-netwerk-voor-een-private-organisatie.

170 https://www.youtube.com/watch?v=3IDiqYil2lQ, accessed on 16 July 2021.

is the only member of staff actively involved in information security. Due to these capacity limitations, the IT department often finds it difficult, for example, to bring the organization's CMDB up-to-date, and to implement all the necessary patches in time. At the other end of the spectrum, financial institutions have hundreds of cybersecurity professionals on their books. They have the capacity and expertise to thoroughly take the basic measures, and to anticipate and respond to incidents.

We also observed major differences between organizations in terms of the extent to which they implement IT activities themselves, or opt for outsourcing. Organizations outsource tasks because they do not have sufficient expertise and capacity within the organization to carry out those tasks themselves. Due to this lack of expertise and capacity, however, they also do not always have the necessary knowledge to determine whether the party to which they have outsourced the tasks in question in fact delivers good service.

In general, there is a shortage of expertise in the cybersecurity market. This has been a problem for years, and no end is in sight. The entire IT sector is experiencing a tight labour market, for example, in July 2021, thirty percent of the vacancies for IT programmers and IT developers were not able to be filled. One of the causes of this shortage of expertise is that professionals feel undervalued, and that starting a career in the cybersecurity domain is difficult. The growing number and complexity of attacks also means that many professionals suffer stress and burnout problems.[171] The risk of this situation is that the capacity shortfall is only set to grow. During the Citrix incident, it was also apparent that the demand for cybersecurity professionals outgrew the supply, resulting in security companies not being able to help every organization in need of expertise. Incident response capacity is fragmented through sectoral CERTs and each organization needs its own capacity and expertise regarding preventive measures. Expertise is not or rarely bundled and is therefore fragmented.

Urgency

The extent to which an organization recognizes the importance and urgency of taking measures and is able and willing to deploy the necessary resources also plays a role in the resilience of an organization. In government organizations like municipalities, unlike in private organizations, the administrators themselves are unable to determine how resources are spent. Instead, they are accountable to the municipal council, which in addition to cybersecurity, must also take account of any number of interests, as well as having been made responsible for many municipal tasks, that also take up resources. To make matters worse, IT is often taken for granted by public administrators and parliamentarians, despite the fact that they do not understand everything the processes involve. It is often more attractive to spend money on things that deliver a tangible result, than on preventing problems. After all, if a problem is prevented, the result remains out of sight.

It also became clear from interviews that in certain organizations, the position of the CISO in the organization when the Citrix occurrence took place was weak, so that it was

171 ESG & ISSA, *The Life and Times of Cybersecurity Professionals 2021 – Volume V*, July 2021; ABN Amro, Stand van TMT, September 2021; *VMware, Global Incident Response Threat Report*, 2021.

not possible to make a meaningful contribution to the successful management of the incident. At one of the organizations we spoke to, the CISO was not able to convince the IT department to decide to implement mitigation measures, at the time of the occurrence. As a consequence, the organization was compromised. In response to this incident, the position of the CISO within the organization was reviewed and reinforced, so that in the future, it will be easier to notify the management of incidents. At many of the organizations we spoke to, it is clear that the sense of urgency to invest in cybersecurity grows following an incident of this kind.

Individual risk

The risks that emerge in the event of software vulnerabilities are at present mainly seen as individual risks that have to be managed by each organization, operating individually. The operating principle in the Dutch system is that every public and private organization is responsible for its own digital resilience. Most organizations do not have to account for this. Medium-sized and large companies and organizations must have an annual audit of the annual accounts, in order to demonstrate their accuracy. An IT statement is currently not part of this audit report, even though having IT security sorted out is important for the continuity of an organization. The professional association of IT auditors has recently proposed to include an IT statement as a permanent part of the auditor's report.[172]

If incidents occur as a result of vulnerabilities in software, they tend to impact many organizations and individual citizens. As a result, vulnerabilities represent a collective risk to society as a whole. Individual organizations have only limited options to manage these risks, themselves, depending on the capacity and expertise available to them. Every year, the costs of cyberattacks are rising. More and more organizations are taking out cyber insurance to insure themselves against the damage and losses caused by incidents. Nonetheless, only a small portion of SME enterprises are insured against cyber incidents.[173] Because the costs of cyber incidents are continuing to rise, the premiums for cyber insurance are rising, too. Whenever an incident takes place involving a vulnerability in software used by many organizations however, the collective costs for the incident will be so high that they can never be borne by the insurers.

Insurers are expected to play a positive role in promoting cyber hygiene by setting requirements for the measures organizations must have in place to be covered for cyber incidents. At the same time, the role of insurers has also been criticized, and it is questioned whether they promote good cyber hygiene, because insurers cover ransomware payments and because security measures taken by organizations are not checked. Recently, this has changed, ransomware payments are no longer always covered by insurers.[174]

172 NCTV, *National Cybersecurity Agenda*, April 2018; Van Gils en Van Wijnen, 'Nieuwe IT-check kan voorwaarde worden voor krediet', FD, 11 August 2021.

173 Hiscox, *Hiscox Cyber Readiness Report 2020*, 2020; https://www.trouw.nl/economie/het-aantal-cyberaanvallen-groeit-explosief-maar-echt-ongerust-zijn-bedrijven-niet~b332e73e, consulted on 29 July 2021.
https://www.rtlnieuws.nl/tech/artikel/5000096/cyberverzekering-hacken-ransomware-gijzelsoftware-ddos-citrix, consulted on 29 July 2021.
Modderkolk, 'Vooraanstaande ict-beveiligers: 'Ransomware gaat richting nationale crisis, overheid moet meer doen' ('Leading IT security advisors: Ransomware is becoming a national crisis; government needs to do more'), *De Volkskrant*, August 2021.

174 Verzekeraars deinzen terug voor ransomware', *AG Connect*, *https://www.agconnect.nl/artikel/verzekeraars-deinzen-terug-voor-ransomware*, 25 May 2021.

At present, there is no collective basis for helping organizations to increase their resilience. It is up to each individual organization to build up a basis of resilience, using the knowledge and capacity at their disposal.

Due to the asymmetric relationship between manufacturers and customers in the field of software security, users are usually unable to impose safety and security requirements and make the right assessments themselves, when purchasing software. There are possibilities for organizations to consciously deal with the risks of software, but not every organization has the knowledge and capacity to impose and check the appropriate requirements. There are no generally applicable rules concerning the control of software, that require manufacturers to satisfy specific safety and security requirements.

As concerns prevention and preparation for incidents, there are major differences in the level of resilience of organizations. Many measures require a risk assessment. Not all organizations have the expertise and capacity to sufficiently implement the appropriate measures, or fail to recognize the urgency of deploying their capacity for this task. Every organization is independently responsible for its own digital resilience. There is no collective foundation available, to assist organizations in increasing their digital resilience.

4.3 Incident management (response)

The occurrences described in chapter 3 show clearly that the time between the reporting of a software vulnerability and an attack being launched on vulnerable organizations is limited: ranging from a month to just a few days or even zero days. In the previous sections, we discussed the factors that influence the way in which manufacturers prevent and respond to software vulnerabilities, and what organizations that use software do to prevent their digital systems suffering security leaks as a result. In this section, we deal with the factors that influence how the various stakeholders such as manufacturers, organizations and public and private incident managers tackle the incidents in order to limit the consequences.

4.3.1 Information flow

Following the announcement of a vulnerability, it is crucial that the relevant organizations be informed as directly and as quickly as possible. Organizations that use the software need information that is as precise and reliable as possible, in order to determine quickly how to respond in order to manage the risks; organizations unable to independently arrive at such a consideration need advice that they can follow. Manufacturers and incident managers want to know how many and which organizations are vulnerable and how they are being attacked, so they can take the appropriate measures and offer support and/or advice. This information can be collected from a variety of sources such as manufacturers, voluntary and commercial security investigators, CERTS via coordinated