Follow-up recommendations *Vulnerable through software: lessons following security breaches by Citrix software*

Report publication date: 16 December 2021

1 About the report

The Dutch Safety Board investigated security breaches created through vulnerabilities in manufacturer Citrix's software. On 17 December 2019, Citrix disclosed a vulnerability in its software and published temporary measures that organizations using the software could take to mitigate the risks. Both the manufacturer and volunteer security researchers from the Dutch Institute for Vulnerability Disclosure (DIVD), among others, searched the internet to see which Dutch organizations were still using vulnerable software and were at risk of being attacked. They shared this information with the National Cyber Security Centre (NCSC). The NCSC immediately alerted the part of the Dutch users it considered itself responsible for: government departments and vital organizations. Other organizations were not alerted by the NCSC.

Attackers were able to penetrate digital systems on a large scale of organizations that had not taken measures, or had not properly taken measures. If they have remained undetected, these attackers have unauthorised access to these organizations' systems and data to this day. Meaning that they can trigger an attack at any time, with disruptive effects on business processes, service delivery, privacy and security.

The incident shows that Dutch public and private organizations are vulnerable to cyber-attacks and that there is no national structure within which all potential victims of cyber-attacks are warned in time. This investigation by the Dutch Safety Board shows that vulnerabilities in software lead to unsafety for organizations that use software, and for those who depend on them. The gap between digital dependence and the size of the threat on the one hand, and society's resilience against it on the other, is growing. Quick and fundamental action is needed to prevent society from being disrupted.

Therefore, the Safety Board issues seven recommendations in this report. The first recommendation aims to increase response capacity in the short term. The six following recommendations aim, in the longer term, to strengthen the public and private system and introduce incentives to create a system in which manufacturers and customers continuously work on making software more safe and secure.

The Safety Board recommends setting quality requirements for software at the European level to force software manufacturers to take responsibility for the safety of their product. The Safety Board advises governments and industry to join forces. By working together, they can strengthen their position towards software manufacturers and make better use of their scarce

expertise. Within the government, the monitoring of digital security can be regulated in the same way as the monitoring of the conduct of prudent fiscal policy is laid down in the Government Accounts Act. The Board also recommends that larger companies and organizations should be required by law to account for how they manage their digital safety and security.

The following parties responded to the recommendations, in order of receipt:

- Chamber of Commerce (CoC), 21 March 2022;
- Union of Dutch Water Authorities (UvW), 14 April 2022;
- VNO-NCW, also on behalf of MKB-Nederland, 10 June 2022;
- Business Software Alliance (BSA), 16 June 2022;
- Citrix, 24 June 2022;
- Cabinet, through the Ministers of Justice and Security (JenV) and Economic Affairs and Climate (EZK), and the State Secretary of the Interior and Kingdom Relations (BZK), 10 October 2022.

The full responses of the addressed parties can be found on the DSB website.[1]

Despite reminders, the following addressed parties did not send a response to the recommendations addressed to them: the European Commissioner for the Internal Market and the European Commissioner for "A Europe Ready for the Digital Age", Association of Netherlands Municipalities, Agriculture and Horticulture Organization LTO Netherlands, the Interprovincial Consultative Council; and software manufacturers Ivanti, Fortinet, F5 and Palo Alto. That the parties did not respond is a missed opportunity to show what they are doing to improve digital safety and security.

This note contains a general conclusion on the follow-up of recommendations, followed by a summary of the response received for each recommendation and a conclusion on their follow-up.

[1] A number of parties, among which the CoC, UvW and VNO-NCW, did not explicitly receive a recommendation, but the Board has written to them as being relevant parties within the system.

2 General conclusion on follow-up

Society is vulnerable to cyber attacks because of its increasing dependence on digital systems. The potential consequences of these attacks can be disastrous for individual organizations, or even for national security as a whole. Organizations have a responsibility to ensure safety and security when using digital systems. In doing so, they partly depend on how manufacturers fulfil their responsibility for safety and security. This also requires an effort from governments, regulators and non-governmental organizations.

To enhance safety and security, the Board has issued recommendations to relevant stakeholders, both nationally as internationally. Their responses demonstrate that the relevance is recognized by the parties. In general terms, the cabinet states that cybersecurity is a task for the international community. To cope with this, the cabinet has created the current Netherlands Cybersecurity Strategy (NLCS) with accompanying Action Plan. It forms the strategy for the next six years, until 2028. The cabinet thus appears to be working on cybersecurity in the Netherlands. However, the cabinet's response shows that it will take several years (until 2026) until all preconditions are in place to be able to alert all organizations as quickly and effectively as possible. Manufacturers point to customer responsibility and the lack of a level playing field. It is not clear at this stage what effect European horizontal regulation will have on this dynamic.

The Board finds it hopeful that the parties express several intentions and name actions they (plan to) take. However, the gap between cyber threat and resilience is continuously widening. The Board therefore calls on the parties to continuously accelerate action to increase digital safety and security.

The Board further stresses that safe and secure software is first and foremost the responsibility of software manufacturers and requires them to take collective action. Manufacturers should invest more to continuously improve the safety and security of software, commit to this continuous security improvement and offer customers insight into the security of the software.

In this note, the Board discusses the individual responses and again urges all parties to act quickly and fundamentally to prevent society from being disrupted by cyber-attacks.

3 Follow-up by recommendation

Recommendation 1

To the Dutch Cabinet and organizations in the Netherlands that use software[2]

> Ensure in the near future that all potential victims of cyber attacks are alerted quickly and effectively – solicited and unsolicited - so they can take measures for their digital safety and security. To this end, bring together public and private response capacity and ensure sufficient mandate and legal safeguards.

Cabinet response

In a comprehensive policy response, the cabinet answers the question of how it deals with the Safety Board's recommendations. The response to recommendation 1 is arranged thematically. For the sake of clarity, the Board maintains this arrangement below.

Organization of cybersecurity information sharing

The cabinet states that within the so-called National Coverage System (hereinafter: LDS or the system), general information on digital security and specific risks can be shared. The aim of the system is to enable all organizations in the Netherlands, public and private, to increase their level of resilience and strength through information sharing. The cabinet calls the system "young" (established in the 2017-20 government period) and expresses its intention to "further develop" the system in the coming years through the Netherlands Cybersecurity Strategy (NLCS). Of importance in this respect is that the cabinet calls the system "effective and efficient with clear points of contact", without losing sight of its own responsibility.

Fragmentation, as identified by the Dutch Safety Board, should be "avoided as much as possible", according to the cabinet. A scoping exercise was carried out in 2022 for the

[2] For practical reasons, the Safety Board writes to the government in its role as purchaser through the State Secretary of the Interior, the Interprovincial Consultative Council, the Association of Netherlands Municipalities and the Union of Dutch Water Authorities. The other organizations, including healthcare, education, vital providers and the rest of the business community, the Board writes to the other organizations through the Dutch Confederation of Netherlands Industry and Employers (known as VNO-NCW), MKB Nederland (umbrella organization for Dutch enterpreneurs) and Netherlands Agricultural and Horticultural Association (LTO Nederland), which are involved in the SER.

services involved to achieve integration.[3] The services - the NCSC, DTC and CSIRT DSP[4] - have that intention. According to the cabinet, the results of the scoping exercise were positive, which recently led to the further elaboration of the integration in a so-called programme plan. A separate letter to parliament shows that the full integration of the said services should take shape between 2024 and 2026.[5] The NLCS and the accompanying action plan contain actions that the cabinet additionally proposes to take to further develop the system.[6]

An important point for the cabinet to note is that the so-called Cyber Info/Intel Cell (CIIC) was established in 2020. This is an information-sharing partnership between the General Intelligence and Security Service of the Netherlands (Algemene Inlichtingen- en Veiligheidsienst AIVD), Netherlands Defence Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst MIVD), NCSC and the Public Prosecution Service. According to the government, this link is in line with the Board's recommendation to better bring private and public response capabilities together.[7] The cabinet aims to establish a cooperation platform in which information can be shared, analysed and distributed and has commissioned research to this end.[8]

Bottlenecks central government powers of information sharing

The cabinet states that it agrees with the Board's recommendation that undesirable legal obstacles around information sharing should be removed. To this end, in 2021, the cabinet conducted an inventory of legal powers. The inventory led to the cabinet's intention to amend the Network and Information Systems Security Act (Wbni). The aim of the legislative amendment is to enable "as optimal as possible" information exchange by the NCSC and other organizations. The bill aims to give the NCSC broader powers to be able to provide threat and incident information (if relevant) to other organizations. This will allow more organizations to be alerted (directly or switched) when necessary, the cabinet said. The bill passed the House of Representatives on 4 October 2022 and will be presented to the Senate this year. The government mentions the Digital Trust Centre. The DTC informs and advises about 2 million

---

[3] Parliamentary letter from the ministers of JenV and EZK, "Implementing programme plan tracks integration CSIRT-DSP, DTC & NCSC", reference: 4196464, 13 September 2022. In it, the ministers stated, "The outcomes of this exploration contribute to more synergy and counteracting fragmentation within the government cybersecurity landscape and the desire for closer cooperation and integration. The ambition is to jointly form a new organization that is the national centre of expertise, information hub and CSIRT in the field of cybersecurity".

[4] Resp. National Cyber Security Centre, Digital Trust Centre, Computer Security Incident Response Team for digital service providers.

[5] Letter to parliament from Minister of Justice and Security and Minister of Economic Affairs and Climate Policy, "Implementing programme plan tracks integration CSIRT-DSP, DTC & NCSC", reference: 4196464, 13 September 2022.

[6] See in particular Chapter 3 of the NLCS, pp. 24-30.

[7] The DSB notes that this partnership currently consists only of public organizations.

[8] Results of the research can be found in: P. Oldengarm and L. Mooy, “Cyclotron: Gezamenlijk sneller en gerichter delen van informative rondom (dreigende) cyberincidenten in publiek-privaat verband”, 31 May 2022.

non-vital companies in the Netherlands how to improve their digital resilience. To improve tasks and powers of the DTC, the bill "promoting digital resilience of companies" was drafted, among other things.[9] According to the cabinet, non-vital companies will be actively informed about serious digital threats and vulnerabilities known to the government since the summer of 2021.[10]

The cabinet concludes its response to this recommendation by noting that it is not yet possible to warn potential victims in all cases. This applies, for example, when personal data are involved (under the General Data Protection Regulation, among others). Therefore, the cabinet, under the coordination of the Ministry of Justice and Security, is launching a study to determine "in which way target and victim notification from non-criminal sources can be further shaped." These actions are also included in the NLCS action plan.

Finally, as regards sufficient statutory regulation of tasks and powers, the topic of "scanning" in relation to the NCSC is important. According to the government, the NCSC's statutory task is to conduct technical investigations into threats and incidents, and to inform and advise central government-affiliated organizations and vital providers about them. For that task performance, the NCSC also scans for vulnerabilities in digital systems of the said organizations, when possible without invading the organizations' systems. However, the NCSC does not have the legal authority to scan without permission to penetrate such systems. The European NIS2 Directive (see also recommendations 2, 6 and 7 below) leads to adaptation of the NCSC's scanning powers. Thus, the NCSC is allowed to scan for vulnerabilities if organizations give permission, or if no intrusion into the organization's systems is made.

Response Union of Dutch Water Authorities (Unie van Waterschappen, UvW)
The UvW states that it endorses the recommendation. The Water Authorities - individually and collectively - recognise the increasing digital dependence. The subject is high on their administrative agenda, the UvW states. Since 2017, the Water Authorities have joined the CERT-WM[11]. This enables them to cooperate with other parties, including Rijkswaterstaat (Public Works), in the event of cyber-attacks. According to the UvW, this has proven its added value in recently discovered vulnerabilities, including Apache Log4j.[12] In the coming months,

[9] The Council of State has given a positive opinion on this bill. It will be presented to the House of Representatives this autumn.
[10] In its report, the DSB referred to the announcement by the Ministry of Economic Affairs on 13 September 2021 that the DTC was launching a pilot to actively inform companies about digital threats. According to that announcement, it involved 40 companies In the fourth quarter of 2022, the pilot consists of 57 companies. https://www.digitaltrustcenter.nl/pilot-dtc-informatiedienst (The Netherlands has 1.9 million companies of which more than 400 thousand are BVs, source: CBS)
[11] Computer Emergency Response Team Water Management.
[12] In December 2021, a serious vulnerability was found in open source component log4J, which is used worldwide in numerous especially business software packages to log data traffic. This led to

the Water Authorities will examine the further development of the CERT-WM into a more central and proactive body. The UvW states that the Water Authorities regularly test their digital resilience through cyber exercises, and through audits by a certified external agency. However, the UvW also notes that information security costs more and more money and scarce capacity. Therefore, the UvW welcomes the Board's recommendation to address the issue (inter)nationally. The UvW also notes that cooperation with other governments "is still very fragmented". Good cooperation with the relevant ministries of Justice and Security, Infrastructure and Water Management, Interior and Kingdom Relations and Economic Affairs and Climate Policy costs the Water Authorities a lot of time and energy, according to the UvW. It therefore calls for more coordination on information security within the Dutch government.

Response VNO-NCW (also on behalf of MKB-Nederland)
VNO-NCW and MKB-Nederland say they welcome the recommendation. According to the parties, information sharing is crucial for companies to better arm themselves against cyber-attacks. The parties consider it a "highly undesirable situation" that the NCSC does not as yet have the mandate to share incident or threat information with non-vital organizations, thus preventing them from taking timely protection measures. VNO-NCW and MKB-Nederland mention a number of developments that make them "hopeful", including in particular legislative and regulatory changes in the Netherlands and the EU that broaden information sharing and explorations for more and better cooperation.[13] VNO-NCW and MKB-Nederland say they are hopeful about these developments, but at the same time worry that they have not yet been fully implemented. This worries VNO-NCW and MKB-Nederland: receiving information does not necessarily make society safer. According to the parties, it should also be acted upon. VNO-NCW and MKB-Nederland state that they contribute to following the recommendation by, among other things, educating their members, for instance by activating industry organizations to actively bring digital security to their attention. They have started a project entitled "Digitally Secure Together" to help smaller companies in particular.

VNO-NCW and MKB-Nederland think further exploration is necessary to see where and how (response) capacity can be brought together effectively and efficiently. This is because, in their view, the response differs from one organization to another, depending on the role and specific services within the "digital ecosystem". The employers' organizations argue that the Safety Board has not included in its report a definition of what it understands by 'response capacity', but assumes that it understands it broadly.[14] Under conditions, the parties favour bringing the

---

what experts called and cyber pandemic, an immeasurable number of systems potentially invaded by attackers.
[13] Examples cited include: the amendment of the Network and Information Systems Security Act to give the NCSC a broader mandate to share expanded information; the new notification obligation of the Telecom Act 11a.2(4); the Network and Information Security Directive.
[14] The Board defines "response capacity" in the report, section 2.5 as: "incident management: these are the activities that are undertaken when an incident has actually occurred".

NCSC and the DTC closer together. VNO-NCW and MKB-Nederland saw the public-private cooperation that took place during the Log4j episode as an example to be repeated.

Conclusion on follow-up
The recommendation will not be followed up in the short term. The cabinet has expressed its intention to follow up the recommendation, as shown in the response letter. It is important that these intentions are translated into concrete actions aimed at *all* organizations in the Netherlands as soon as possible.

The cabinet describes a number of organizational measures, such as integrating organizations and proposals to enable wider information sharing. The cabinet's action plan shows that the actions needed to alert all potential victims as quickly and effectively as possible will take years (until 2026). However, the cabinet does link realising the ability to warn all potential victims separately from broader initiatives (as mentioned in the *Cyclotron report*). This suggests that the central government wants to achieve results as soon as possible precisely on the issue of this first recommendation. This is a positive sign.

Despite the cabinet's promised continued attention and further development of the system to alert organizations in time, the gap between cyber threat and resilience is continuously widening. The societal need for is evidenced, among other things, by the step taken by a number of multinationals active in the Netherlands to set up their own organization to share information among themselves about impending cyber attacks.[15] The rest of the Dutch business community has to wait for the cabinet and other parties to settle a number of legal and technical issues in the coming years.

The reaction of other parties, such as employers' organizations VNO-NCW and MKB-Nederland, also shows that they consider the pace of measures to improve cyber security in the Netherlands too slow. In the meantime, voluntary security researchers, through organizations such as the Security Meldpunt, DIVD and the Clean Networks Platform, continue alerting as many organizations with vulnerable servers as possible: for instance, DIVD has sent just under 60,000 alerts in 2020 and over 170,000 alerts so far in 2022.[16] The cabinet does not mention these initiatives in its response but focuses on its own role. It calls on the government to facilitate such parties better and faster.[17]

---

[15] In addition to ASML, the NL CCoT foundation consists of ABN AMRO, Ahold Delhaize, Akzo Nobel, ING, KPN, Philips, Rabobank and Shell. NS has indicated that it would also like to participate. The foundation is working closely with the National Cyber Security Centre (NCSC) on this. Source Article from https://fhi.nl/nieuws/nauwe-samenwerking-in-stichting-helpt-asml-enandere-multinationals-cyberweerbaarheid-te-verhogen/
[16] Source: https://www.divd.nl/
[17] See also the Slingelandt lecture by Michel van Eeten, professor of cybersecurity at TU Delft. https://www.bestuurskunde.nl/2019/11/14/blussen-met-nullen-en-enen-cyber-rampen-cyberexceptionalisme-en-de-rol-van-de-overheid/.

Recommendation 2

To the European Commissioner for the Internal Market and the European Commissioner for a Europe Fit for the Digital Age:

Ensure that your initiatives to legislate for safer and more secure software lead to a European regulation that establishes the responsibility of manufacturers and provides insight to buyers of software in how manufacturers assume this responsibility.
Establish that manufacturers are liable for the consequences of software vulnerabilities.

Response of the Internal Market Commissioner and Eurocommissioner for a Europe Fit for the Digital Age:

Both Eurocommissioners did not send a response to the DSB on the recommendations addressed to them. Reminders and contact with the Dutch Permanent Representation and a number of Dutch (former) MEPs to obtain a response had no effect. However, the Board was invited to contribute the report to an Impact Assessment initiated by the European Commission for the purpose of the *Cyber Resilience Act*. The Dutch Safety Board found and analysed policy intentions and measures in public sources, which can be related to our recommendations to the Eurocommissioners.

The European Commission published a proposal for new horizontal legislation, the *Cyber Resilience Act*, in September 2022. This bill covers all products with digital elements, regulating both hardware and software. The proposed law is a so-called EU regulation and will thereby be directly applicable in all EU member states. The law imposes requirements on manufacturers regarding digital security in their products, both when developing them[18], and when vulnerabilities are found. The bill requires manufacturers to quickly and effectively fix vulnerabilities during the lifetime of a product (with a maximum of five years) and notify customers. In addition, products must have a "declaration of conformity", which means they must meet the specified requirements before being placed on the European market. Manufacturers will be obliged to share information on the composition of their products with their customers, and to provide understandable information to customers on the safe use and configuration of the product.

Cabinet response

Although this recommendation was not addressed to the Dutch cabinet, it did respond to it. The cabinet also did so in respect of recommendations 3 and 4 (see below). The cabinet stated that it had brought these recommendations to the attention of the European Commission. The cabinet wants to "play an active and stimulating role" towards the European Commission and software manufacturers to take measures to increase cross-border digital security.

[18] Some software development requirements include that products should be delivered without known vulnerabilities and with a 'secure by default' configuration.

Specifically, the cabinet proposes to do this public-privately by developing and applying cybersecurity certification schemes of ICT-related products, services and processes under the European *Cyber Security Act* and *Cyber Resilience Act (CRA)*. In negotiations on the CRA, the cabinet is pushing for "the clearer placement of a duty of care for cybersecurity on manufacturers and suppliers" to strengthen the position of customers.

Conclusion on follow-up
The recommendation will be partially followed up. The European *Cyber Resilience Act* (as yet a proposal, so not yet implemented) has the potential to ensure that it is no longer optional for manufacturers to invest in digital security of their products if they want to operate in the European market. The Act also gives customers clearer insight into what manufacturers are doing about product security, as well as what the products consist of. However, the European Commission does not stipulate in this proposal that manufacturers are liable for the consequences of software vulnerabilities. Excepted are very specific cases where the consequences have resulted in physical injury. A number of other aspects mentioned in the recommendation's explanatory memorandum do not appear in the CRA, namely: mandatory participation in so-called *bug bounty programmes*, *lesson-sharing*, and the organization of independent audits. The Board appreciates the government's commitment to (continue to) bring the recommendations to the attention of the European Commission. Attention to continuously improving security inside and outside the Netherlands and Europe will benefit from this.

Recommendation 3
To software manufacturers collectively[19]:

> Develop good practices with other manufacturers to make software safer and more secure. Include a commitment to these practices in contracts with your customers.

Citrix response
In response to this recommendation, Citrix shares a number of good practices the company has developed in response to the incident under investigation, such as collecting contact information from their customers and a call home feature of the software. The manufacturer also states that it strongly supports cybersecurity standards for manufacturers when it comes to software development, as wide adoption makes standards more effective and improves cybersecurity across the board. Citrix itself uses several standards, including NIST, ISO, Common Criteria and SOC2, but as an individual manufacturer is only one link in a larger chain.

[19] This recommendation is addressed to all software manufacturers. For practical reasons, the Safety Board writes to the manufacturers involved in the incidents described by this investigation and the (members of the) industry organization Business Software Alliance

Business Software Alliance (BSA) response
In its response, BSA indicates that software development is "a complicated process". According to the industry association, software often contains numerous components with many lines of code, so while error-free code should be a goal, it is not realistic. BSA thus confirms the findings of the Dutch Safety Board as contained in its report. BSA indicates that many parties play a role in software security, that the safe use of software often lies with the buyers of products, and that the responsibility to manage the risks should also be placed there. BSA claims to have developed a so-called *secure software framework* for industry stakeholders -from manufacturers to customers -to evaluate and communicate security.

Conclusion on follow-up
The recommendation is not followed up. Citrix and BSA state that they support and follow (existing) standards for the development of secure software. Citrix and BSA do not commit to complying with these standards in agreements with their customers. Industry organization BSA places the responsibility for secure use of software mainly on the customers. Finally, the parties do not address the sector-wide development of good practices. The Dutch Safety Board reiterates here that safe and secure software is first and foremost the responsibility of software manufacturers and that it is necessary for them to take collective action. The Board states in the report that manufacturers should invest more to continuously improve the safety and security of software and offer customers insight into the security of the software.

Recommendation 4
To software manufacturers collectively[20]:

> Warn and help all your customers as quickly and effectively as possible when vulnerabilities in software are identified. Create the framework conditions necessary to be able to warn your customers.

Citrix response
Citrix claims to publish "*security bulletins*" about vulnerabilities. The company additionally gives certain customers advance announcements about vulnerabilities. Citrix states that they encourage their customers to provide "security contact details", but that the initiative to do so lies with the customer.

Business Software Alliance response
BSA indicates that so-called coordinated vulnerability disclosure is well developed in the industry. The party does not address manufacturers' warning of customers in the response.

[20] Ibid.

Conclusion on follow-up
The recommendation will not be followed up. Citrix is willing to warn customers who sign up for it. The other manufacturers contacted have not responded to the recommendation. Industry body BSA does not address manufacturers warning customers after they have identified a vulnerability, in defiance of the flaws identified in the DSB report.

Recommendation 5
To the State Secretary of the Interior and Kingdom Relations and the Minister of Economic Affairs and Climate Policy (for the benefit of all organizations and consumers in the Netherlands)[21]

> Encourage that Dutch organizations and consumers jointly formulate and enforce safety and security requirements for software manufacturers. Ensure that the government plays a leading role in this. Proceed on the basis of the principle: collective cooperation where possible; sector-specific where necessary.

Cabinet response (State Secretary of the Interior and Kingdom Relations and Minister of Economic Affairs and Climate Policy)
The cabinet states that it embraces the recommendation. According to the cabinet, the recommendation is in line with ongoing and planned efforts by the government. The cabinet stated that the government sees it as its task "to set a good example by means of a pioneering role, to strengthen its role as a good principal and thus also to stimulate a general movement in the market towards developing and offering secure ICT products and services". The cabinet calls the government "an important market player" because all government organizations collectively purchase many ICT products and services every year. To help achieve the objectives mentioned in the recommendation, the so-called Cybersecurity Government Procurement Requirements (ICO) programme provides tools to this end, such as sets of procurement requirements and a basic process description. According to the cabinet, government policy aims to give ICO a permanent place in the overarching procurement process of all Dutch governments. In time, the sets of standards will become mandatory and "translated" in line with European laws and regulations, in particular the Cyber Security Act, the cabinet said.

Regarding consumer protection, the cabinet mentions that since April 2022, the Implementation Act is in force, which specifically implements the European directives "sale of

[21] Because of the relevance of safe and secure software for end users (including consumers), the Consumers' Association should also be involved. And the Chamber of Commerce for support to organizations.

goods" and "supply of digital content" in the Netherlands.[22] The laws and regulations should make buying and selling goods and digital content safer and easier. Specifically, the government cites the example that it gives consumers the right to (security) updates to software "as long as they can reasonably expect them". These laws and regulations will be supervised by the Consumer and Market Authority (ACM). In this context, the cabinet further mentioned that "wirelessly connected devices" entering the European market from August 2024 must comply with legal cybersecurity requirements. If the products fail to do so, they could be taken off the market and banned. The Telecom Agency is monitoring this.

The cabinet concludes its response regarding this recommendation with the intention to strengthen the position of software users by anchoring security requirements for manufacturers in the European CRA. Finally, in consultation with industry organizations, the Ministry of Economic Affairs is exploring how it can stimulate clear contractual agreements between suppliers and customers.

Chamber of Commerce response
The KVK states that it recognises the recommendation by pointing out the importance of providing information and advice on digitisation. However, the KVK states that it is "not a logical party" to support this. The KVK gives as its reason that this would go far beyond the legal role the KVK actually has. Branch organizations are, according to the KVK, the most appropriate organizations to take a pioneering role in information provision and advice.

Conclusion on follow-up
The recommendation is being partially followed. The cabinet is working on legal requirements that manufacturers must comply with. As far as Internet-connected consumer products are concerned, the ACM will supervise and enforce manufacturers' compliance with legal requirements. For business software, this is not yet regulated, but the government sees possibilities to start regulating this through the *European Cyber Resilience Act*. The Board considers the point made by the cabinet about consumers' right to get software updates a valid one, but at the same time stresses that safety and security should be front-end requirements. After all, an update is an after-the-fact repair, the potential insecurity is already a fact by then. As for the ICO programme and the point with scarce expertise, the Dutch Safety Board considers that each organization would then still have to assess for itself whether the products meet those procurement requirements. So just having a set of procurement requirements will

[22] In its policy response, the government states: "This law introduces new and clarifies existing rules that make the buying and selling of goods and digital content, including across borders, safer and easier, and it makes explicit, among other things, a mandatory update regime for digital content and tangible goods with a digital element. Consumers will thus be entitled to (security) updates as long as they can reasonably expect them. The seller/trader will have to make arrangements with a third party, such as the manufacturer or a software provider, who can provide the updates. The exception is when the trader explicitly informs the consumer at the time of purchase that they should not expect updates, and the consumer agrees to this."

not help you as a company or small government organization. In short, the question remains how the government is going to collectively enforce these requirements (or have them enforced). The role the government sees for itself here - as a pioneer and good client - is no small ambition.

The KVK does not see a role for itself to support organizations in this process, as this would lie outside their statutory remit and would better suit trade associations. The Dutch Safety Board sees opportunity in the Chamber of Commerce Act for the KVK ton indeed play a role.[23] The Board considers it necessary for customers to join forces so that they can strengthen their position towards manufacturers and jointly deploy scarce cyber security expertise as efficiently and effectively as possible.

Recommendation 6

To the Dutch Cabinet:

Create a legal basis for the management of digital safety and security by the government, by analogy of the Dutch Government Accounts Act (*Comptabiliteitswet*).

Cabinet response

According to the cabinet, the Ministry of the Interior and Kingdom Relations is systemically responsible and therefore standard-setter for the government's creation of (legal) frameworks for the digital security of the Netherlands. There will be a duty of care for information security, as well as government-wide supervision. The cabinet regulates the aspects of duty and supervision in the forthcoming Digital Government Act (WDO) and other relevant regulations. In this regard, the government mentions the NIS2 directive, which requires member states to bring central governments under the scope of the directive. The cabinet wants the national implementation of the directive for public authorities to run parallel with regulating the aforementioned duty of care and supervision.

The cabinet states "to achieve an unambiguous, simple and harmonized system" "in which appropriate inter-governmental enforcement" has a place. To specify this, the cabinet states that a requirement for an annual IT report and statement will be included in the WDO to support supervision. According to the cabinet, this "strengthens horizontal oversight and facilitates vertical accountability." Until the mandatory IT declaration is included in the WDO, the Ministry

[23] Chamber of Commerce Act: There is a Chamber of Commerce whose purpose is to promote economic development by providing information and support in the field of entrepreneurship and innovation to persons running a business or considering setting up a business. Currently, the Chamber of Commerce already advises on what entrepreneurs can do to reduce the risk of a cyberattack and which laws and regulations are relevant to them in that area. The CoC works with the DTC, among others.

of the Interior and Kingdom Relations will experiment with it in consultation with all four layers of government. The cabinet says it will take the initiative Europe-wide and internationally to make the developed products the standard, if the experiments are successful.

Conclusion on follow-up
The recommendation will be followed up. Among other things, the cabinet will regulate a duty of care for information security and government-wide supervision in the WDO and/or other appropriate regulations.

Recommendation 7
To the Dutch Cabinet:

Require all organizations to uniformly account for the way they manage digital safety and security risks.[24]

Cabinet response
First of all, the cabinet mentions that there are major differences between organizations and sectors, so accountability should be proportional to managing digital security risks. The cabinet is implementing the aforementioned NIS2 directive into national legislation. Among other things, the directive requires providers to implement adequate security measures and to report incidents. Such matters apply specifically to sectors "with high societal importance", such as "providers of essential and important entities". More sectors are now covered than under its predecessor, such as healthcare. Small and medium-sized enterprises are not covered, even though they include companies that have a high impact on their customers' digital security risks. The cabinet recognises that it is important for all organizations to manage digital risks. Accountability for this has parallels with accountability for other types of risks, according to the government. The cabinet considers it important to link up with existing structures set up for cyber security.

The cabinet sees two options for following up on this recommendation: in the management report through statutory anchoring in the annual accounts law, or by tightening the so-called *Corporate Governance Code (CCG)*. As for the management report, the cabinet does not consider it proportional to make this mandatory by law, as it would apply to only two to four per cent of Dutch companies (public traded). Non-public traded companies, the vast majority of Dutch companies, do not have this duty "due to the proportionality of the associated administrative burden." The CCG contains principles and provisions for encouraging good

[24] It makes sense to align with existing structures and obligations in the 2016 Comptabiliteitswet 2016 (applicable to public authorities), Civil Code (non-listed legal entities), further regulations on auditing and other standards (NV COS) from the NBA and harmonised legislation for public limited companies from the EU.

governance in listed companies. According to the cabinet, many other organizations apply the CCG voluntarily. Therefore, the cabinet has brought this recommendation to the attention of the socalled CCG Monitoring Committee.

Conclusion on follow-up

The cabinet endorses the purport of the recommendation, but assumes voluntariness. The recommendation will therefore not be followed up for the time being. The aspects mentioned by the cabinet around proportionality are aimed at shareholders.[25] In terms of information security, companies without shareholders also have important responsibilities towards other companies in the chain. Thereby, the extent of the risk they cause for others doing business with them is not necessarily proportional to their size, but to the function they fulfil in the process of their customer or business partner. Consider, for example, a small organization that provides a payment system or manages a digital platform for a group of affiliated organizations.

Time should tell whether the ultimate goal (that most companies are accountable for how they manage their digital security risks through their annual report) will be achieved with voluntary application of the CCG. Incidentally, the recommendation included more starting points for how control and accountability can be shaped, including a unified mandate for CISOs. The cabinet does not address most of the mentioned starting points.

[25] The Board used the term "unambiguous" in its recommendation. The term "proportionate" would have been more appropriate, to be mindful of the wide variety of organizations and sectors and ditto ways of accountability.