'Narrowing the cyber resilience gap'

Advisory opinion on cyber resilience among Dutch small and medium-sized enterprises

CSR
Cyber Security Council
Cyber Security Raad

'Narrowing the cyber resilience gap'

Advisory opinion on cyber resilience among Dutch small and medium-sized enterprises

Addressed to:

The Minister of Justice and Security
The Minister of Economic Affairs and Climate Policy

Cc:

The State Secretary for Kingdom Relations and Digitalisation

CSR
Cyber Security Council
Cyber Security Raad

May 2024

INTRODUCTION

This advisory opinion was prepared in response to the request of the Minister of Justice and Security dated 31 January 2023, in which she asked the Cyber Security Council (referred to below as the council) to advise on the cyber resilience gap between organisations. This gap refers to the large differences in cyber resilience between forerunners (organisations that have balanced their cyber resilience measures with the threat) and stragglers (organisations for which this is not the case). The council addresses a wide range of issues in this advisory opinion, including the minister's questions. The aim of the advisory opinion is to empower the government with concrete recommendations to work with industry associations, IT and telecom suppliers and SMEs to help reduce and, where possible, bridge the cyber resilience gap.

The essence of the advisory opinion
This advisory opinion focuses specifically on small and medium-sized enterprises (SMEs), as there seem to be relatively many stragglers in that domain. At the heart of the advisory opinion are three main themes, which are elaborated in more detail below:

1. Bring about a targeted, structural and unified approach to improve the cyber resilience of SMEs. From a public-private partnership and under the central government's direction, this could create more cohesion between various initiatives. It can also help increase cooperation within and between networks.
2. Provide appropriate tools for SMEs through known and accessible channels to enable each organisation to achieve an optimal level of cyber resilience. Those tools range from basic measures and metrics for mapping resilience levels, to help in conducting risk assessments.
3. Encourage companies to increase their cyber resilience and take measures for improvement (or have them taken). Make use of the approach outlined above, the tools offered and existing products of IT and telecom suppliers. Forthcoming EU legislation, while a driving force in this regard, only affects a part of SMEs.

The starting point here is to reach all SMEs (i.e. not just the stragglers who are potentially most at risk) and to base the approach on the actual needs and perceptions of entrepreneurs within SMEs.

Positioning and accountability
This opinion is partly based on a study[1] conducted by Deloitte for the council. This study is largely based on literature review and consultation with SMEs, SME representatives, public parties, industry associations and private SME network partners. This made it possible to gain in-depth insights into SMEs' struggles with cybersecurity.

[1] See the report 'Cyberweerbaarheidskloof - Aanbevelingen voor een cyberweerbaar mkb en het verkleinen van de cyberweerbaarheidskloof in Nederland'. Deloitte May 2024

Parallel to Deloitte's study, TNO (commissioned by the Ministry of Economic Affairs and Climate (EZK)) also conducted the study 'Safe Digital Entrepreneurship'[2] on the motivations for entrepreneurs to invest or not to improve their cyber resilience. The TNO study is largely complementary and elements from it are also relevant to this council advisory opinion.

Why specifically SMEs?
SMEs are the backbone of our economy and indispensable for all major societal transitions. 70% of Dutch people also work in SMEs. An optimally cyber resilient SME is therefore important for the entrepreneurs themselves because of business continuity (without business, no earnings) and possible reputation damage, but also for society because of system continuity (sales market and earning power of the Netherlands).

SMEs are varied: they range from companies in the manufacturing industry to suppliers of parts and semi-finished products and from service providers to retailers. Also, many Dutch companies within SMEs supply foreign customers or partners, or they are multinational themselves. This covers medium, small and micro businesses, up to the sole proprietorship. Cybersecurity is not always at the forefront of people's minds and activities are mostly focused on the company's core business. Companies often lack an understanding of cybersecurity risks and do not always take sufficient resilience measures. Similarly, a business owner may view the consequences of cyber attacks or incidents as acceptable business risk and not take preventive action for this reason.

Because of the above, the council sees four reasons to focus this advisory opinion specifically on SMEs:
1. Many of the products and services of SMEs are widely used in society and society depends on uninterrupted service from SMEs.
2. The high quality level of many different products and services unfortunately makes SMEs a demonstrably rewarding target for attacks by cyber criminals and state actors.
3. Companies are becoming increasingly interconnected in value chains. The weakest link in a chain can provide unwanted access to other companies. Those weak links can also be found in SMEs.
4. The larger companies tend to have in-house cybersecurity knowledge and mobilise financial resources. Among SMEs, this is much less the case.

Companies within SMEs are an integral part of the digital ecosystem. Apart from the measures entrepreneurs themselves have to take to increase their cyber resilience, small businesses in particular rely heavily on their IT and telecom suppliers. The upcoming Cyber Resilience Act (CRA) enshrines the principle of providing secure products and services in European regulations. Implementing this Act in the Netherlands will unburden entrepreneurs more and gradually increase the cyber resilience level of their businesses.

Document structure
The three main lines of the advisory opinion are elaborated on below. To this end, the council first describes the most relevant cybersecurity developments, including the playing field with the most relevant actors from the perspective of SMEs. Through a description of the current and desired situation, a number of general recommendations follow to permanently increase the cyber resilience of companies and help reduce and, where possible, bridge the cyber resilience gap. Finally, some targeted advisory opinion to the relevant ministers is given.

Developments

[2] Hof, T., Van der Kleij, R., & Mergler, S. (2024). Secure digital business: Understanding motivations and barriers through target group segmentation. TNO report 2024 R10701.

Threat and risk

The annual Cybersecurity Assessment Netherlands (CSBN) shows that the cyber threat is current, growing in size and damage caused, and is not going away. The rise of artificial intelligence (AI), besides providing opportunities for more advanced security, also poses new risks: cyber attacks are increasing in scale, with more chances of infection. As a result, detection, response and recovery are also becoming increasingly difficult and require specialist knowledge and skills concentrated in larger organisations including IT and telecoms providers.

SMEs are targeted by digital attackers. The cyber threats come mainly from attacks by criminals and (in some sectors) state actors. Geopolitical tensions have made such cyber attacks the new normal. State actors deploy these means against a very wide range of targets, which also seriously affects SMEs. Research has additionally shown that it mostly involves extortion via *ransomware*[3], or stealing or copying intellectual property. This covers both office automation (IT) and operational technology (OT), also known as Industrial Automation and Control Systems (IACS).

The latter systems control a physical component and are common in the process industry. This technology is also prevalent in the manufacturing industry, especially with the rise of digitalisation in this sector (´smart industry´). This brings complex challenges to cybersecurity. Continuing and keeping such business processes safe requires specific knowledge and different forms of cooperation[4].

The business risk a suboptimal[5] cyber resilient company faces from these attacks is the (partial) shutdown of production or services and possible reputational damage. This has an impact on the company itself, but also on customers, suppliers and other supply chain partners. The consequences of suboptimal cyber resilience in the event of materialising risks are then felt more widely in society. There is a risk that the consequences of an attack could render a company unviable in the slightly longer term.

European and national legislation and frameworks

Various types of legislation and directives, mostly enacted within the EU and to be implemented nationally, should ensure that we as a society are sufficiently resilient against cyber threats. Of particular interest in the context of this opinion is the European Network and Information Security directive[6] (NIS2 directive), which aims to improve cybersecurity for a wide range of organisations within the EU. This directive was published in late 2022 and is effective for all member states from 17 October 2024. In the Netherlands, it has yet to be implemented through a new version of the Network and Information Systems Security Act (Wbni). This EU legislation on digitally secure products and services (CRA) is also highly relevant in this context.

The NIS2 directive should contribute to greater uniformity and a higher level of cyber resilience across all companies and organisations identified as critical or important. It involves both a duty of care for a secure network infrastructure and service, and a duty of notification for organisations in case of cyber incidents. Implementation also involves the designation of *incident response organisations* and supervisors, with their different roles, powers and responsibilities.

For SMEs, only a limited number of companies are *directly* affected by the NIS2, but there are also companies that are *indirectly* affected by the NIS2. Indeed, companies directly covered by the NIS2 must impose cybersecurity requirements on their supply chain, which is mostly SMEs. The NIS2 directive, because of its mandatory nature, will be a powerful driver for businesses identified as

[3] See CBS cybersecurity monitor, 2022/2023: https://www.cbs.nl/nl-nl/publicatie/2023/31/cybersecuritymonitor-2022
[4] See also the council's earlier advisory opinion on OT/IACS: CSR Advies 'Industrial Automation & Control Systems (IACS)' - CSR-advies 2020, nr. 2 | Advies | Cyber Security Raad
[5] "Suboptimal" here means that a company's cyber resilience level is not in line with the risks it is willing to take, or that these risks are not clear or not defined.
[6] See NIS2 directive: https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555&qid=1707471344352#d1e1300-80-1

essential or important. This will also apply to companies that are part of the supplier chain of these organisations. There is also a third group within SMEs that will *not* have additional requirements imposed under the NIS2. Within SMEs, there is a need for education and additional information on the exact separation between organisations directly, indirectly or not covered by the directive.

The introduction of the Digital Resilience Business Promotion Act (Wbdwb) is at an advanced stage[7]. This law gives the Digital Trust Centre (DTC) the powers to inform and advise organisations *not* covered by the current Wbni on specific vulnerabilities, threats and incidents, which may affect their network and information systems. Generally, this mainly concerns SMEs.

Playing field

SMEs have to deal with a multitude of actors, organisations and agencies that can set frameworks regarding their cyber resilience. These may include legal requirements, requirements from chain partners, IT service providers or (public and/or private) resource providers. The most relevant initiatives in the cybersecurity playing field for SMEs are discussed below.

Government

The government has a stimulating and driving function for SMEs. Usually, this means creating framework conditions to enable the actions of other players. This includes entering into public-private partnerships and offering support to initiatives already developed. The government's role mainly involves setting strategic direction, establishing frameworks and translating EU legislation for national implementation.

Seeking to increase the digital resilience of the Netherlands, strengthen the cybersecurity system and tackle digital threats, the government launched the Netherlands Cybersecurity Strategy (NLCS) in 2022, including an accompanying action plan. This indicates the following for SMEs[8]:

1. *NCSC and DTC are developing new products and services that include a focus on embedding cybersecurity in the risk management process, crisis preparedness, incident response and thematic advice. These differentiated and data-driven information and knowledge products and services are made available to organisations collectively and in a low-threshold manner appropriate to the maturity level.*
2. *The creation of a first version of central registries for cybersecurity-related information (i.e. type of ransomware, vulnerabilities).*
3. *Encourage the use of tools, such as risk scans, products and security advice, including action perspectives, among SMEs including through trade associations, such as with the public-private platform Samen Digitaal Veilig, or 'Together Digitally Secure'.*
4. *One set of basic measures is formulated and promoted by the government for voluntary use by organisations.*

The council has previously indicated that the government should take a firm directing role with regard to the implementation of the NLCS, including providing clarity on mutual expectations in the public-private partnership[9].

Initiatives from partnerships

In collaboration between private parties and in a public-private context, many initiatives are already being undertaken (through a promoting role of the DTC) to improve the cyber resilience of companies (in a general sense). This is where the 'big helps small principle' comes in. MKB-Nederland and VNO-

[7] At the time of publication of this advisory opinion, the Senate has yet to agree to the bill; the House of Representatives passed the bill on 19 March 2024.
[8] NLCS action plan, p.14: https://www.rijksoverheid.nl/documenten/publicaties/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022---2023
[9] See CSR Adviesbrief over de Nederlandse Cybersecuritystrategie - Minister van Justitie en Veiligheid | Advies | Cyber Security Raad

NCW have teamed up in the Digitally Safe Together project[10], together with the Ministries of Justice and Security and Economic Affairs and Climate. The Chamber of Commerce (CoC) has a LinkedIn portal for advice and referral to government agencies. Furthermore, Brainport Eindhoven has developed CyRa[11] (Cyber Rating), in collaboration with industry (including companies that are also members of the CISO Circle of Trust established in 2022), FERM Rotterdam, the MKB Cybercampus and TÜV Nord Netherlands.

The above partnerships play an important role in providing information and advice to SMEs. There is a high density of them in the Netherlands, offering opportunities to continue building a 'network of networks'. This is in line with the intended further development of the current National Coverage System (LDS) into an umbrella 'cyber resilience network'. This brings together initiatives in the areas of prevention, information and knowledge exchange, crisis preparation, incident handling, as well as learning and practice. Trade associations and other collaborations can play an important linking role in this towards SMEs.

Initiatives from private service providers

Depending on the resources available and the nature of the business, many SMEs outsource their cybersecurity to third parties. This may involve the services of IT and telecom providers, which includes cybersecurity. Those services offer suitable opportunities for companies to put their basic hygiene in order. This means that business owners can opt for virus and malware protection[12], as well as purchase additional security solutions.

When more specialised knowledge and expertise is needed, SMEs can engage a cybersecurity firm (in addition to the solutions mentioned above) to manage the digital environment. This concerns parts of the complete palette of prevention, detection, response and recovery, combined with the prior performance of an adequate risk analysis. Larger companies generally pay more attention to this. Purchasing such services can yield a premium discount when buying cybersecurity insurance, offered by insurers and banks, sometimes in combination with a cybersecurity company.

For companies that have their basic hygiene in order and need more specialised knowledge and expertise, but do not have sufficient financial scope themselves to engage with a cybersecurity company, there is the option of seeking expert advice on an ad hoc or structural basis under a contract. This often involves technical analysis and additional advice, so that the company can take charge of its implementation itself.

Learning from other countries

Although national structures and strategies differ in the international arena, threats and vulnerabilities are generally cross-border. Countries face the same issues and the applicable EU laws and regulations are identical. The Netherlands can learn from successful or promising initiatives from other countries, despite the fact that solutions may differ between countries. This is especially true for like-minded countries that have similar digitisation rates, for example. The council recommends that specific findings[13] from these countries, for example on certifications or labels, or on subsidy schemes, be taken into account when taking such measures.

The current situation

Deloitte's research shows that, on average, companies within SMEs implement fewer measures and carry out less frequent risk analyses compared to business as a whole. Also the recent WODC report *Evaluation Framework and Zero Measurement Netherlands Cybersecurity Strategy*[14] indicates with regard to the implementation of the NLCS that the involvement of SMEs calls for additional attention.

[10] See Samen Digitaal Veilig
[11] See About us - Cyra - Cyberrating
[12] Suppliers cannot activate this by default without explicit permission due to laws and regulations.
[13] Deloitte's report also provides pointers for this, see Appendix I.
[14] See Evaluatiekader en Nulmeting Nederlandse Cybersecuritystrategie (NLCS) | Rapport | Rijksoverheid.nl

Deloitte's research reveals several internal and external obstacles experienced by companies within SMEs that stand in the way of increasing their level of cyber resilience. Interviews show that three internal obstacles cause the most problems:

- There is insufficient cyber awareness and knowledge
- There is insufficient understanding of the risks and possible courses of action
- It is difficult to determine how much and what to invest in.

Following on from this study, the council offers some additional observations, which characterise the current situation and stand in the way of the optimal cyber resilience of SMEs:

- The initiatives launched in recent years by the government, partnerships and trade associations are often not specifically aimed at SMEs, a particular sector, or a type of company.
- There is little or no understanding of the effectiveness of the tools offered.
- The set of tools on offer is unclear, not very coherent and does not sufficiently align to the needs of SMEs. The offer emphasises risk identification and insight creation, with less focus on standard solutions available for entrepreneurs.
- The tools offered focus mainly on preventive (substantive) measures, and not on being prepared for an incident and how to respond to an incident to minimise/make the impact.
- Some entrepreneurs deliberately take the risk of not investing further in their cyber resilience.
- For fear of reputational damage, companies sometimes refrain from notifying a cyber attack or incident, or reporting the matter to the police. This has resulted in other potential victims not being warned or able to be protected in time[15].
- Not all notifications or police reports can be taken up by the police and Public Prosecution Service due to a lack of capacity. However, notifications and police reports are crucial because they contribute to a clearer image of current cybercrime trends and developments. This enables more effective and efficient use of capacity.

The study further shows that SME entrepreneurs consider achieving a level of cyber resilience that is optimal for them primarily as their *own* responsibility, commensurate with their own entrepreneurial risk. The council endorses this, but in order to set this up properly, there is also a responsibility on their IT and telecom suppliers and other trusted partners, as well as the need for underlying products they use to be demonstrably sufficiently digitally secure.

Some companies also see a clear coordinating, facilitating and connecting role for the government, such as when it comes to raising awareness, providing concrete action perspectives that fit the precise context of SMEs and help in determining what to invest in. This includes support in identifying the requirements that their IT and telecom suppliers and/or cybersecurity companies must meet, and pointing out the standard security solutions available.

Optimal situation

In an optimal situation, the Netherlands has an SME sector within which companies are aware of cyber security risks and their potential impact on their business processes. Those companies can make their own risk assessments for taking or arranging cybersecurity measures and are able to decide for themselves what investments they need. In this situation, companies are offered the necessary low-threshold information, education and advice. This implies that the identified obstacles – as described above – have been removed.

If a company falls victim to cybercrime, there is an *incentive* to report an attack and/or file a police report. Also, information about vulnerabilities is shared with other companies to alert potential

[15] The study shows that within SMEs in the UK, outsourcing IT leads to a reduction in incident reporting. Whether this is also true in the Dutch context is unknown and could be investigated further.

victims. The organisation resulting from the merger of the DTC, NCSC and CSIRT-DSP has an important role to play here as a centre of expertise and information hub. Through this merger, all organisations in the Netherlands – large or small, public or private, vital or non-vital – will be provided with appropriate information and knowledge by a single institution. More specifically, according to the council, an optimal situation could be shaped as follows:

- Government, industry associations or partnerships offer companies appropriate help to remove obstacles in improving their cybersecurity.
- The tools are easily accessible; distribution ideally takes place from a single point of contact, through knowledge centres and linking organisations in the ´network of networks´ mentioned above.
- SMEs are therefore able to analyse risks and companies open to cybersecurity improvements can take appropriate action. As part of that, they can purchase digital products and services whose security level matches that risk assessment.
- Besides IT and telecom suppliers, other parties in the immediate vicinity of SMEs act as boosters by drawing extra attention to cybersecurity measures. This applies, for example, to trusted partners such as insurers, banks, the Chamber of Commerce, accountants and auditors.
- There is a monitoring system for digital resilience, which explicitly includes a place for SMEs. This will make it possible to monitor how SMEs' cyber resilience is evolving and whether the tools offered are having the desired effect.

ADVISORY OPINION

The prosperity of the Netherlands benefits from thriving SMEs. Optimal cyber resilience is a prerequisite for this. Within SMEs, however, we see significant differences, in terms of forerunners and stragglers in cyber resilience. Some companies knowingly accept major cybersecurity risks as part of their overall business operations and will not improve in the short term, while others are willing but lack awareness and knowledge. Therefore, achieving the optimal situation is not a beaten track and requires joint efforts. Along the aforementioned three main lines, the council provides some general advice for improvement below.

1. **The government ensures an SME-specific, structural and unified approach through building the ´network of networks´, based on existing structures and clear assigned responsibilities.**
2. **The government, trade associations and partnerships provide appropriate resources through accessible channels.**
3. **Through public-private partnerships, the government encourages companies within SMEs to increase their cyber resilience together with trusted partners as much as possible, prompting them to act directly or indirectly (e.g. through trade associations).**

Re 1. Ensure an SME-specific, structural and unified approach.

The current approach to increasing cyber resilience of SMEs shows valuable initiatives, but consistency in their organisation is still largely lacking. Building a ´network of networks´ from existing structures, with the government working with trade associations, other partnerships and linking organisations, is crucial for this.

Targeted
The multitude of agencies make it confusing for SMEs to easily gain and maintain an overview of information, tools or advice on cybersecurity. It is therefore necessary to bring more structure to the network of parties playing a role in the cyber resilience of SMEs.

The organisation resulting from the merger of the DTC, NCSC and CSIRT-DSP should take a central and coordinating position in its implementation, focusing on all necessary cybersecurity activities of organisations: prevention, detection, incident response, and promoting recovery and learning capability. On the one hand, this involves sharing and resharing information on threats, incidents and vulnerabilities to SMEs and/or their partners (IT and telecom suppliers, cybersecurity companies) and on the other, the function of a counter and knowledge centre for tools and advice on the importance of cybersecurity and the measures to be taken. The intended further

development of the National Coverage System into an umbrella cyber resilience network provides good starting points for this, including in reaching SMEs.

Structural
Cooperation within this network should be structural in nature, with clear roles and responsibilities. It is very important to periodically evaluate whether measures and initiatives are effective in structurally increasing the cyber resilience of SMEs; here, too, the goodwill and/or awareness of the entrepreneurs concerned will play a role.

Trusted partners of SMEs that work with them on a structural basis have the opportunity to bring the taking of (additional) cybersecurity measures to the attention of their customers, and also make demands on them. The same applies to an organisation, such as the Chamber of Commerce, which can make novice entrepreneurs in particular aware of their own responsibility and raise awareness of cybersecurity risks.

Uniform
SMEs generally experience high regulatory pressure, while entrepreneurs are primarily concerned with running their business. Making the broad palette of cybersecurity measures as clear as possible calls for a unified approach. Customisation may be necessary, for example when a company or sector has a special risk profile because of their sensitive information or intellectual property. If specific tools need to be tailored to those companies, it may be necessary to differentiate by sector, chain or region. Trade associations and specific partnerships play an important role when differentiation is needed.

Re 2. Offer appropriate assistance to all SMEs, through accessible channels.

As described in the Deloitte study, appropriate help can be provided to SMEs through a strong link between the central merger organisation mentioned in point 1 and network partners who are close to SMEs' businesses. This should lead to a compact and uniform set of basic measures. These tools should focus on performing a risk analysis that allows the company to move from its current to its optimal cyber resilience level. That covers the complete range of tools for prevention, detection, incident response, recovery and learning.

With the necessary support and education, existing metrics for mapping cyber resilience levels from the private sector, such as CyRa, as well as various tools from the DTC, can serve as a basis and de facto standard to arrive at a practical interpretation that suits the needs of SMEs. This aligns closely with the aforementioned four actions from the NLCS that directly address SME resilience.

This does require a reduction in the current number of tools and the council recommends a guide developed through public-private partnership to help trade organisations and their members find the most appropriate tools. Moreover, a mechanism is needed that periodically evaluates tools for the value of their contribution to the cyber resilience of customers.

IT and telecom suppliers and cyber security firms play an important role in increasing cyber resilience within SMEs, for example by informing customers about vulnerabilities and implementing appropriate solutions for them. In particular, buyers need help in selecting ICT suppliers that have sufficient cybersecurity knowledge and expertise and can therefore be a valuable partner in this area. This could be facilitated by linking up with a quality mark for IT suppliers under development within the Centre for Crime Prevention and Safety (CCV). Using

standard tools to ask the right questions and requirements of suppliers is also a good option, such as the checklist for Service Level Agreements made available by the DTC.

Re 3. Encourage and prompt action.

Improving the approach and the supply of tools are important steps, but several factors play a vital role in achieving improvement: motivation among entrepreneurs, support through the trusted partners in their environment, and an appropriate supply of secure products and services from IT and telecom suppliers.

Deloitte's study did not show that companies that actively seek tools or education are unable to find the necessary information adequately and, therefore, that this is necessarily where the biggest gains can be made. The pre-eminent challenge is to also reach those entrepreneurs who by their nature see no reason to take action, regardless of the quality and findability of tools. This group sometimes deliberately disregards the risk of data theft, downtime or even bankruptcy due to a cyber-attack.

It is imperative that companies at all levels within SMEs are aware of the importance of cybersecurity, take appropriate measures for it and, in addition, carry out a periodic risk analysis. If entrepreneurs experience incentives from their chain partners and are suppliers to other (larger) companies, for example, they are more likely to act accordingly.

Based on the above, the council recommends taking into account the various factors that explain the behaviour of entrepreneurs and determine whether they act or not. The TNO study 'Safe Digital Business' gives clear pointers for this and also suggests a number of interventions depending on those behavioural factors. Drivers to act can also vary by type of organisation and are related to aspects such as knowledge, opportunity and motivation.

Companies not directly or indirectly covered by the future NIS2 are more likely to be stragglers in terms of the cyber resilience gap. The council recommends paying extra attention to this large group of companies through incentives. Trade associations or alliances can play an important role here through education, training and learning from incidents that occur among fellow entrepreneurs in the same sector. The targeted use of grants can also help, in line with some recent processes of the DTC. Despite the fact that this will only reach a limited group of companies, there is a desire to continue experimenting with it.

TARGETED RECOMMENDATIONS

The recommendations below are intended to give substance to the aforementioned three main lines. They are aimed at the government and through the government on the market. In this regard, public-private partnerships are the cornerstone for strengthening the cyber resilience of SMEs. This involves a concerted effort to narrow the current cyber resilience gap between frontrunners and stragglers, bridging it where possible and strengthening SMEs across the board.

Objectives and actions of the NLCS aimed at protecting SMEs should be given extra attention and energetically pursued. This prevents unnecessary risks, is of great importance for society as a whole and promotes a stable contribution of SMEs to the earning capacity of the Netherlands. To flesh this out, the council has produced the targeted advice below.

As part of a **targeted, uniform, structural approach**, the council advises the ministers of Justice and Security (JenV) and Economic Affairs and Climate (EZK) jointly as follows:

1. From the current cooperation of NCSC, DTC and CSIRT-DSP, work incrementally towards a single point of contact and knowledge centre in the new organisation, which also provides targeted support to SMEs. Also encourage target and victim notification for SMEs and notifications and/or police reports. Pay extra attention to the adequate deployment of resources for this purpose.

2. Join the forces of organisations by expanding the ´network of networks´ in public-private partnerships (where big helps small) and include trusted partners of SMEs, such as accountants and the Chamber of Commerce. Besides developing information and knowledge products for SMEs, the use of standard available solutions from IT and telecom suppliers is crucial.

3. From 2025, initiate annual measurement of SMEs' cyber resilience and the impact of measures and initiatives taken. Use the recently published baseline measurement and also link this to the annual NLCS progress report. Specifically address the actions related to SMEs.

The council advises in the context of providing **appropriate help**:

To the ministers of JenV and EZK jointly:

4. Give the new central merged organisation the lead in public-private partnerships to better tailor the supply of tools to increase cyber resilience to the needs of SMEs. Have this picked up in consultation with SME Netherlands, among others. Initiate their harmonisation before the end of 2024, aimed at reducing the current number of different tools.

5. On a voluntary basis, work towards resource standardisation and make it as accessible as possible. There are several options for this, such as CyRa (Cyber Rating). Also encourage the use of existing OT standards and the generic ISO27001 security standard (as a possible top up for

CyRa), and measure the effectiveness of these tools. Take into account (future) EU marks and implement upcoming EU regulations for safe products and services as soon as possible.

6. Encourage the use of (differentiated) tools and the adoption of basic measures within sectors. An accessible guide aimed at industry organisations is essential for this. This also applies to the security of OT systems (or IACS) within SMEs; base it as much as possible on standard available solutions. Make use of existing partnerships in this regard.

To the EZK minister:

7. Ensure that the already initiated development of a quality mark for IT suppliers (in collaboration with the DTC and industry associations) is effected, including cybersecurity requirements, and that the CCV energetically takes up its implementation. If possible, harmonise such a label with future EU developments in this area.

The council advises in the context of **promoting and prompting action**:

To the ministers of JenV and EZK jointly:

8. Consider launching a broad social public awareness campaign in collaboration with private parties. The overarching message here is that entrepreneurs, too, need to adapt to the further digitalising society, with cybersecurity a key focus. Also use the TNO research 'Safe Digital Business' to effectively influence behaviour.

9. Commit to timely implementation of the NIS2 directive in the Netherlands and specifically encourage SMEs in taking measures to comply with these requirements. Also pay attention to companies not covered by the current Wbni or future NIS2, using the forthcoming legislation (Wbdwb) for information sharing and support as a starting point.

The Hague,

On behalf of the Cyber Security Council,

Theo Henrar
(Acting) Co-chair CSR

Pieter-Jaap Aalbersberg
Co-chair CSR