SUMMARY

RAND EUROPE

Digital resilience of Dutch organisations

Opportunities and challenges for measurability

Fook Nederveen, Erik Silfversten, Maria Chiara Aquilino, Scott Warnier

For more information on this publication, visit www.rand.org/t/RRA3700-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

Summary

Governments are becoming increasingly aware that incidents cannot always be prevented. Because of this, the term 'resilience' is being used more frequently in policy documents. Whereas in the past the focus was mainly on prevention, 'resilience' places greater emphasis on the continuity of a system even when a threat does lead to an incident. In the case of digital systems, the term 'digital resilience' or 'cyber resilience' is used. Digital resilience is of great importance, as societies and organisations are becoming increasingly dependent on technology.

Promoting the digital resilience of organisations is one of the priorities of the Dutch Cybersecurity Strategy (NLCS) 2022-2028. The aim is to minimise the identified imbalance between digital threats on the one hand and the degree of digital resilience of organisations on the other. However, there is currently no suitable resilience measure that the government can use to assess the degree of digital resilience of organisations. The lack of such information makes it difficult to determine whether resilience has actually increased, or to assess where investments and efforts have been effective and efficient.

The aim of this study was to provide insight into whether the digital resilience of Dutch organisations can be made measurable in a broadly applicable way by the National Coordinator for Security and Counterterrorism (NCTV). The hope is that, in time, it will become possible for the government to monitor changes in the degree of digital resilience of organisations, whether as a result of policy interventions aimed at increasing it or not. The study was conducted on behalf of the Research and Data Centre (WODC), an independent knowledge institute that falls under the Dutch Ministry of Justice and Security, and at the request of the NCTV.

This study is an exploration of the possibilities for measuring (aspects of) the digital resilience of organisations, which indicators can be used or developed for this purpose (preferably quantitative ones, in which everything with an ordinal scale is considered quantitative), and what these data can say about the state of the digital resilience of organisations. This explorative approach also means that this study does not seek to produce a detailed measurement method that the NCTV can then use. Instead, the advantages and disadvantages of different approaches are outlined, as well as the considerations that will determine the design of a possible future measurement tool.

This research is based on A) a small literature review, searching for studies focused on measuring digital resilience, B) interviews with experts, focusing on their practical experiences with measuring digital resilience, and C) internal workshops in which the findings of this research were discussed and implications analysed.

How can 'digital resilience' be defined?

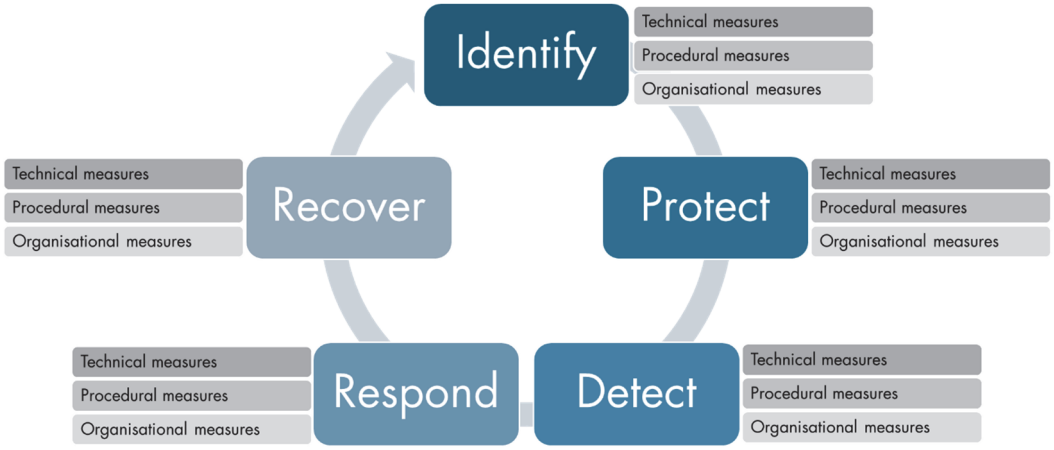
The NCTV defines digital resilience in the Dutch Cybersecurity Strategy 2022-2028 as:

> The ability to reduce relevant risks to an acceptable level by means of a set of measures to prevent cyber incidents and, if they do occur, to detect them, limit the damage and facilitate recovery. What constitutes an acceptable level of resilience is determined by a risk assessment. This can help with the selection of the right technical, procedural or organisational measures.

This definition has been taken as the starting point for this study to align with the Dutch policy environment. The Dutch government does not distinguish between 'digital resilience' and 'cyber resilience.' The latter term is also sometimes used by them, and the two terms are considered synonyms. However, there is still no clear consensus in the literature on the use and definitions of cyber and digital resilience. Some authors, for example, take a narrower view of resilience by limiting their definitions to the ability of a system to continue its functioning or to recover technically after attacks. In Dutch-language literature, the term '*veerkracht*' is also used for this narrower interpretation. However, the definitions of many other authors, as well as views in the broader field of resilience literature, are more in line with the broader view of the NCTV, in which resilience ('*weerbaarheid*') is seen as a continuous, cyclical process that includes both preventive and reactive and learning elements. This cycle is usually divided into phases such as identify, protect, detect, respond and recover, or variations thereof.

Various strategies, laws, and policy documents translate this broad concept into interventions, including technical measures (such as firewalls and backups), procedural measures (such as risk assessments and incident response plans), and organisational measures (such as training and governance). Literature and policy documents consider the phases of the resilience cycle to be interrelated sub-processes, each of which requires a combination of technical, procedural, and organisational measures.

Figure 1. The core components of digital resilience



What does the literature teach us about existing instruments for measuring the digital resilience of organisations?

Despite the increased focus on improving digital resilience, gaining insight into the degree of resilience is proving to be extremely complicated. Various technical, procedural, orgRRanisational, and external characteristics play a role. For example, technologies and threats are constantly and rapidly changing. In addition, technical systems are often too complex for people to fully understand or to test for all possible vulnerabilities in the system. There are also many aspects that play a role in digital resilience that are difficult to capture in indicators, such as the role of social relationships between employees and the workplace culture. Finally, digital processes are to a high degree connected and interdependent on processes outside of the organisation's control, meaning that incidents outside the organisation can directly affect digital resilience, e.g. through dependencies on suppliers.

Data is needed in all these areas to determine with certainty the direction in which an organisation's digital resilience is moving. There are currently no methods that provide such a complete picture. Nevertheless, methods have been developed that can be used to gain insights into aspects of the digital resilience of organisations. In this study, we identified and analysed 18 approaches. These fulfil various functions: they enable organisations to systematically monitor their development over time, identify current strengths and weaknesses, and/or pinpoint specific areas where further improvement is needed. However, only a few of these approaches cover all five aforementioned phases of digital resilience and all three types of measures. Most approaches focus on qualitative rather than quantitative indicators, emphasising descriptive assessments and subjective evaluations rather than numerical or data-driven measurement criteria. While they can provide valuable contextual insights and operational advice, they are often flexible frameworks that remain largely at a conceptual level and are applicable to organisations in different sectors and of different sizes, rather than detailed methodologies. The results are usually specific to an organisation but cannot be easily compared with the results of other organisations. Although most of these approaches do not explicitly address how unknown threats are taken into account, several instruments emphasise a proactive strategy for dealing with such uncertainties.

Little is known about the validity and reliability of these 18 approaches. No evidence proving that they accurately measure what they intend to measure or that they consistently produce meaningful results in different organisational contexts was found for any of these tools. This raises questions about the real value these frameworks offer and the extent to which they contribute to improving digital resilience. Furthermore, it is unclear which specific mechanisms would influence resilience, making it difficult to determine their effectiveness.

What do the answers to the above questions teach us about how digital resilience can be made measurable?

At present, there is no existing method readily available to generate the specific data desired to measure digital resilience. The methods identified and analysed in this study highlight the inherent trade-offs and tensions associated with conceptualising and measuring digital resilience at the organisational level. None of these methods are at the time of writing being used by a government for the purpose of measuring the

degree of digital resilience. Moreover, the methods identified are rarely used for this purpose alone. Other purposes include risk management, ensuring basic security measures, or compliance, which can indirectly contribute to a better understanding of resilience, even if that is not their primary purpose. All approaches identified in the literature have advantages and disadvantages and different strengths and weaknesses for measuring digital resilience. However, empirical data needed to test the validity of current measurement methods are lacking, making it difficult to say whether one method inherently performs better than another.

Nevertheless, the approaches analysed offer useful starting points for designing a future measurement method, depending on its ultimate purpose. If the goal is to build digital resilience at the organisational level and measure the implementation of basic digital resilience measures, the UK's Cyber Essentials program may offer a useful starting point. If the goal is to collect data and measure in more detail the readiness of organisations to identify, protect, detect, respond to, and recover from cyber incidents, then a more comprehensive assessment framework based on the NIST or ISO frameworks may be more appropriate. Finally, if the overall goal of the approach to measuring digital resilience is to collect and analyse comprehensive and sector-specific data on how organisations perform in real-life digital resilience contexts, an approach similar to the framework developed by TNO for organisations in the financial services sector is likely to be necessary.

All three of these use cases share important challenges. For example, they do not fully reflect the organisational context in which digital resilience exists. The organisation's risk appetite and investment thresholds, for example, play an important role in digital resilience. Another challenge is that 'complete' digital resilience – or maintaining full functionality over time – is not a static given. This can change as threats, demands, and expectations evolve. Moreover, effectiveness depends on the type and quality of information that organizations are willing to share.

Implications for the NCTV

Although developing a practical approach to measuring digital resilience at the organisational level presents challenges – such as the lack of evidence for the effectiveness of existing methods, the limited possibilities for automated or quantitative measurements, and doubts about the feasibility of the ambition to determine changes in the degree of digital resilience of organisations as a result of policy interventions - new insights into specific aspects of the digital resilience of organisations in the Netherlands could be gathered by collecting additional data. The NCTV would be best advised to proceed step by step, starting by developing a comparable benchmark for a specific component, such as an organisation's resilience after a cyber incident, and then expanding on this by assessing other aspects as well.

In the current situation, however, there is no legal mandate for the NCTV to require organisations to provide such data. Against this background, it is important that the NCTV remains cautious about creating new reporting obligations without a clear legal basis or policy necessity, given the costs this may entail for organisations. Any new data collection will primarily have to be carried out on a voluntary basis. To ensure that additional data collection complements is in line with existing legal mechanisms, existing initiatives and offers tangible benefits, such as useful insights or targeted support, it is important to consider how participation and involvement can be encouraged. It is also important to strike a balance between the type and amount of information requested from organisations and their limited resources.

One of these existing options concerns the reporting obligations under the Dutch Cybersecurity Act, which transposes the EU's NIS2 Directive. This law provides a framework for collecting information about significant cyber incidents that could affect the continuity or security of so-called 'essential' and 'important' entities. These reports will provide new data on the digital resilience of organisations that was not previously directly available to the government. Therefore, this reporting obligation offers an opportunity – to the extent permitted by law and feasible within the existing reporting obligations – to gain better insight into certain aspects of digital resilience that could guide future policy aimed at strengthening digital resilience in the Netherlands.