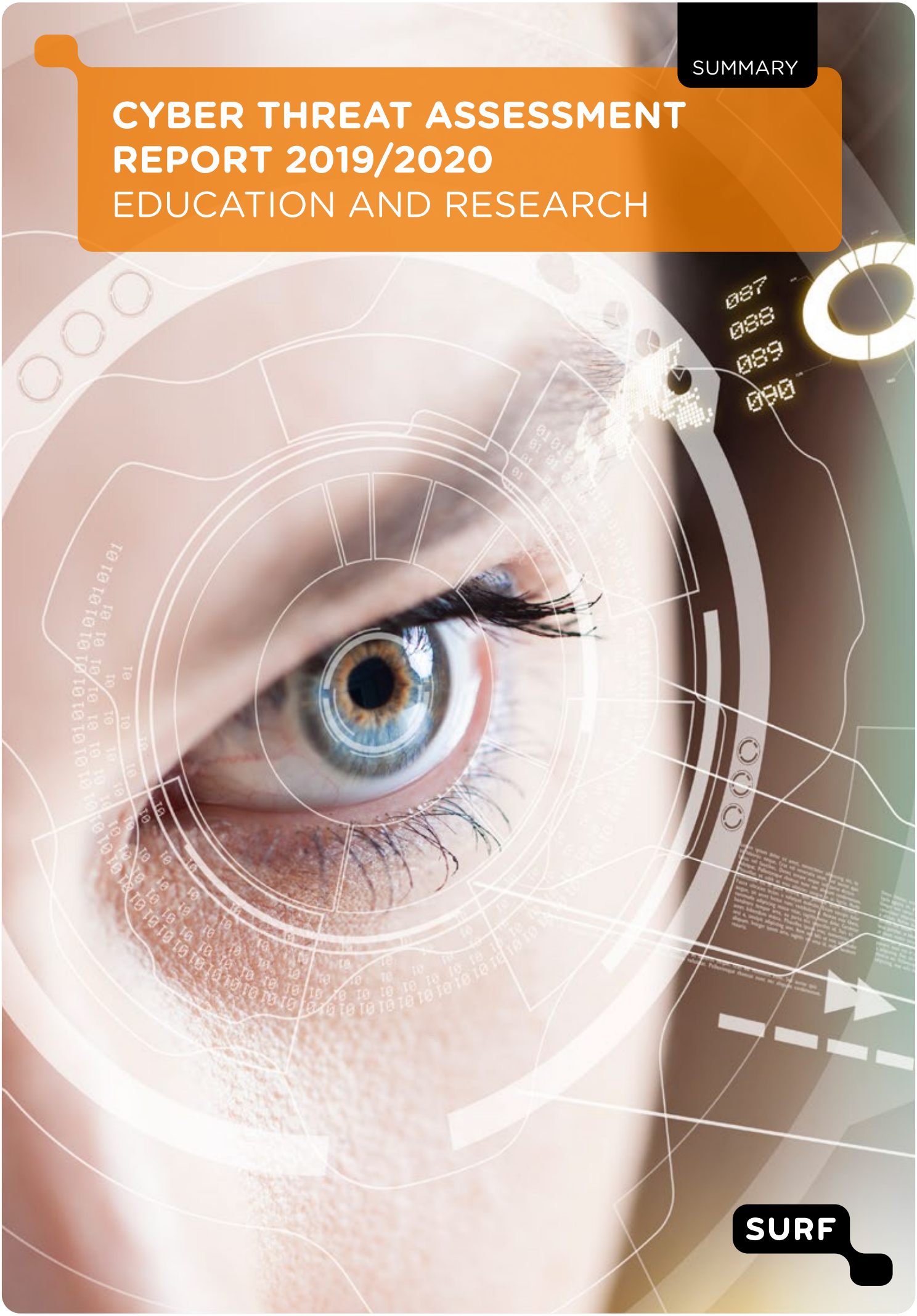
SUMMARY

CYBER THREAT ASSESSMENT REPORT 2019/2020

EDUCATION AND RESEARCH



SURF

TABLE OF CONTENTS

PREFACE
OPENNESS, ALERTNESS AND TRUST

The new decade has just begun. Looking back, we see that every decade has its own global tensions and security issues. Think of the world wars in the first half of the last century, the Cold War that followed, not to mention the terrorist attacks of 9/11 and thereafter. History repeats itself, but never in the same way.

The same is true in ICT. Fifteen years ago, we had never heard of DDoS attacks, yet now they are a well-known phenomenon. And a new category of cyber-attacks is emerging: many organisations are confronted with ransomware attacks, including Maastricht University in the recent past.

ICT offers more and more possibilities as it is strongly interwoven with primary processes, also in education and research. Cyber-attacks are becoming increasingly ingenious and complex, and it is no longer just whiz kids and nerds who are behind them. Cyber-attacks are also now an instrument of state actors, or at least they allow these attacks. As a sector we have to act together against such actors. We start by exchanging knowledge in order to learn from each other in a structured way. This Cyber Threat Assessment report is an example of such information exchange and co-operation.

As a sector, the publication of this cyber-threat assessment report does not complete our work. We have to get to work! We need to collaborate more often, not just within the usual networks but also beyond. Incidents such as the attack on Maastricht University demonstrate that every institution must do its homework when it is not under attack. We must collaborate to understand the risks and impact of cyber-attacks, understand attack-vectors and eliminate vulnerabilities. When a site is under attack, we need to get to work immediately with information as it becomes available at any given time. This requires openness on the part of the institution at the time it is attacked. It requires fellow institutions to be alert, to not sit back, but to keep monitoring their own systems. And it requires all of us to *trust* the agreements we have made with each other to collaborate and exchange information.

If we all use this Cyber Threat Assessment Report as a guide, we will at least have a good start in doing our homework!

Jan Bogerd
Chairman of the Executive Board, HU University of Applied Sciences Utrecht

Erwin Bleumink
Member of the board, SURF

1. INTRODUCTION

In this summary of the Cyber Threat Assessment 2019/2020 - education and research, SURF highlights the main points of the complete report[1]. We look back at 2019 and ahead to 2020 and consider which trends we saw in 2019 in the education and research sector. Which threats manifested themselves in the education and research sector? And what do we expect for 2020 and what is included in the institutions and organisations planned annual budget[2] for cybersecurity?

1.1 Purpose of the report

The Cyber Threat Assessment report aims to paint a global picture of the state of information security and the protection of personal data in the education and research sector. It was created as a result of voluntary participation in a survey and is not necessarily based on institutions' official data.

1.2 Methodology

To gain insight in the kind of incidents that have actually happened, and which risks are most relevant for educational and research institutions compared to 2018, we conducted a survey among member institutions during the fall of 2019[3].

We identified various trends by consulting public sources such as the annual report of the AIVD[4] [1], the annual Cyber Security Assessment Netherlands [2], the NCSC's Cyber Compass 2019 [3], and publications of the Scientific Council for Government Policy [4]. In addition, we consulted a number of international reports such as the Verizon Data Breach Investigations Report [5], the ENISA Threat Landscape Report [6] and "The cyber threat to Universities" of the NCSC (UK) [7].

1.3 Reading Guide

In the next chapter we briefly discuss the results of the survey. In chapter three we mention a number of cyber security trends, in chapter four we discuss the institutions' resilience, and in chapter five we conclude with a number of recommendations. Finally, in chapter six you will find four focus areas for management to consider.

[1] *https://www.surf.nl/files/2020-02/surf-cyberdreigingsbeeld-2019-2020.pdf (in Dutch)*
[2] *The organisation's planned annual budget contains the planned activities that are included in the budget for the year in question.*
[3] *From November 5th to 25th, 2019*
[4] *General Intelligence and Security Agency, the Dutch Secret Service*

2. SURVEY – RESPONSE AND RESULTS

When we carried out the survey, we approached 178 institutions, and of these fifty-seven completed the survey on time. We discuss part of the results from this Cyber Threat Assessment: the results in the areas of Governance, Awareness and Risk perception for 2020.

2.1 Response

The distribution of respondents by type of institution is as follows:

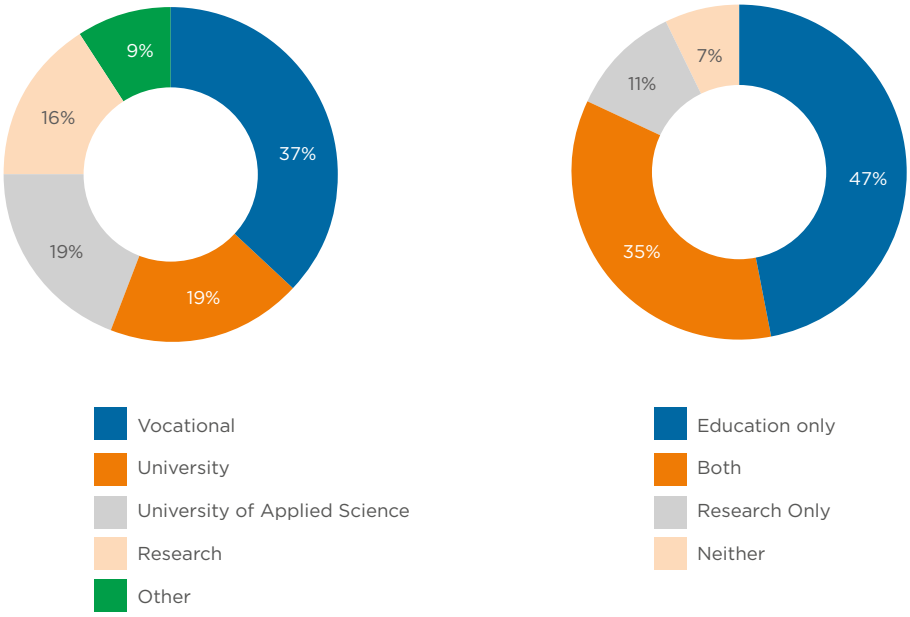


Figure 1: Respondents by type of institution and distribution between education and research

The majority of respondents (approx. 70%) were security officer:

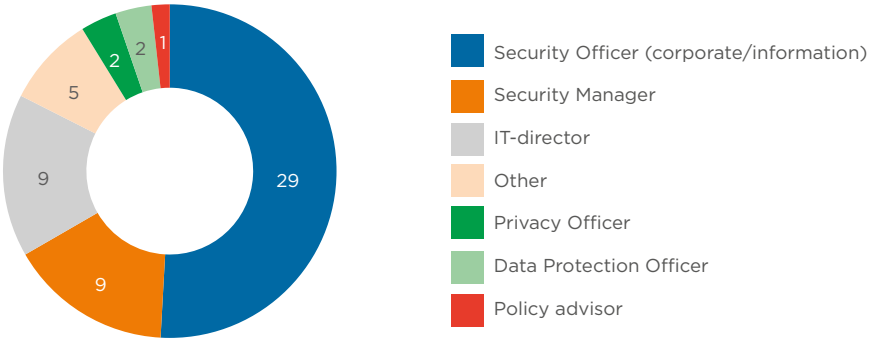


Figure 2: Respondents' role

2.2 Results

Governance

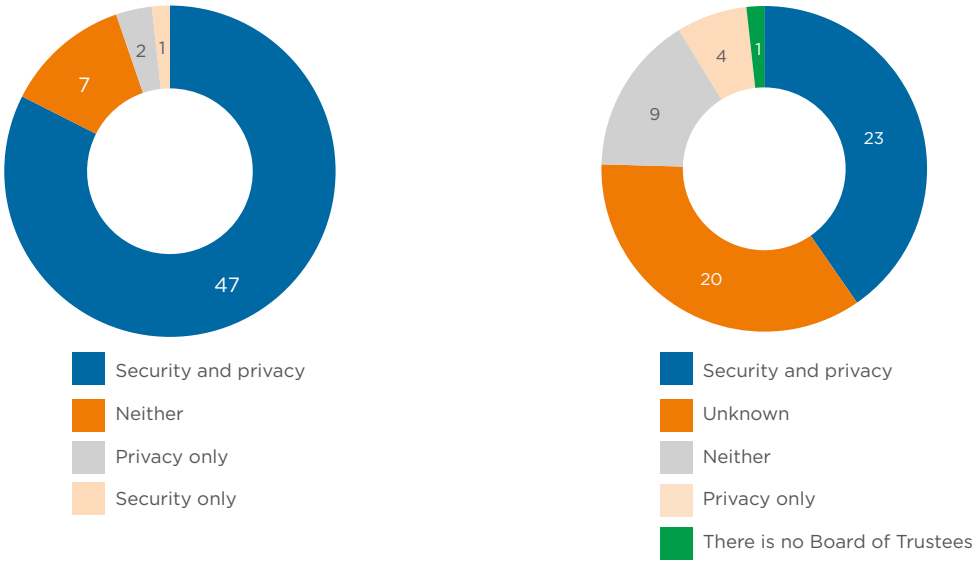


Figure 3: Regular reporting to management (left) and to the board of trustees (right)

Figure 3 illustrates that management is periodically informed of both security and privacy incidents. In the event of a serious incident, a large proportion of institutions (93%) the board of trustees is immediately informed.

Resources[5]

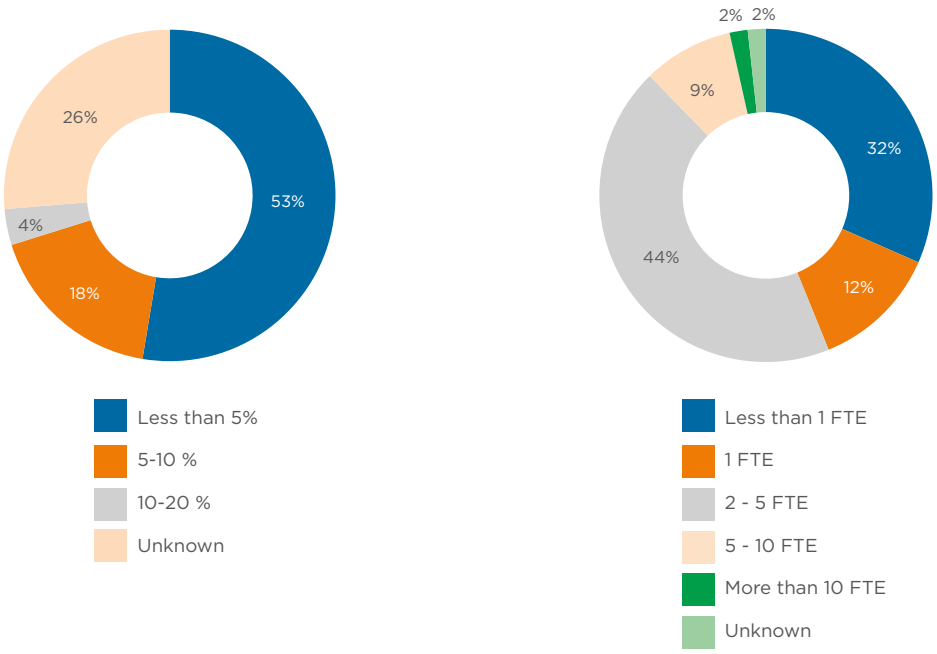


Figure 4: Percentage of the IT-budget (left) and FTEs (right) allocated to security & privacy

[5] *Based on respondents' estimates*

Compared to last year more resources have become available for information security. A large portion of institutions has 2-5 FTEs allocated to information security (figure 4). The number of FTEs also depends on the size of the institution:

FTEs	number of employees	number of students
More than 5 FTE	3.500 - 7.000	25.000 - 45.000
2 - 5 FTEs	1.000 - 6.500	8.500 - 45.000
1 FTE	400 - 3.000	4.000 - 30.000
Less than 1 FTE	100 - 850	1.000 - 8.000

Table 1: Relationship between FTEs and institutions' size

Awareness

Figure 5 illustrates that in many cases (at almost 70% of the institutions) new personnel, including teachers and researchers, do not receive awareness training when they start their job. Less than half of the institutions structurally provide general awareness training or awareness training aimed at specific groups:

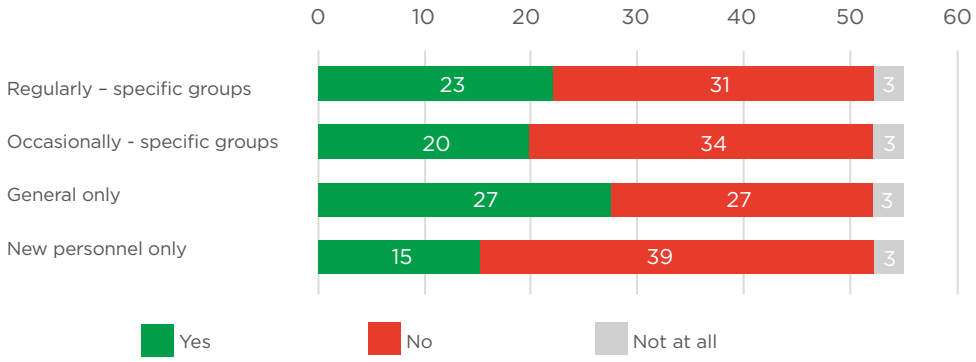


Figure 5: Awareness campaigns

Figure 6 shows that about 70-75% of the institutions consider information security and privacy in projects, purchasing and tenders:

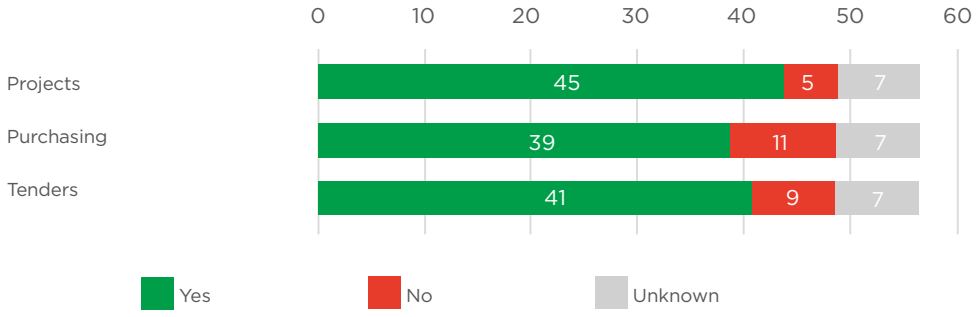


Figure 6: Attention for information security and privacy

Risk perception

The standard method for determining risk level is to take the product of the probability of damage and its consequences: risk = probability * impact. In the survey the respondents estimated probability and impact. The results are shown in the graphs below (see Figure 7 - 9).

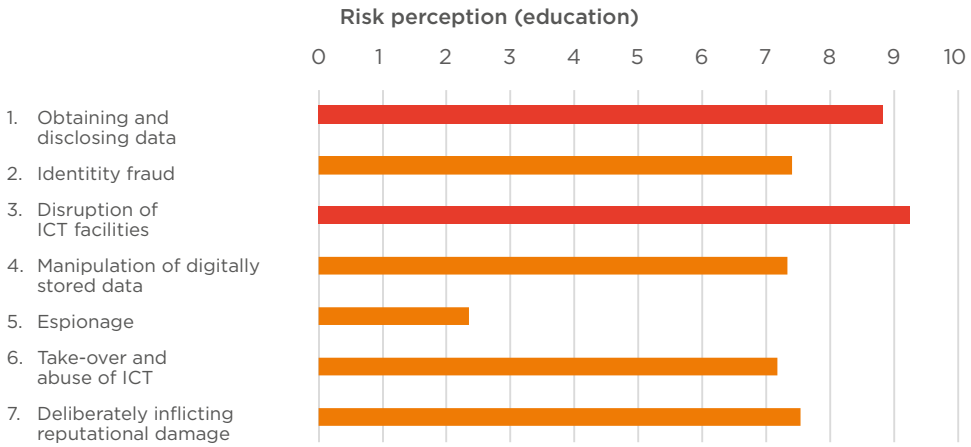


Figure 7: Perception of the risk categories (education)

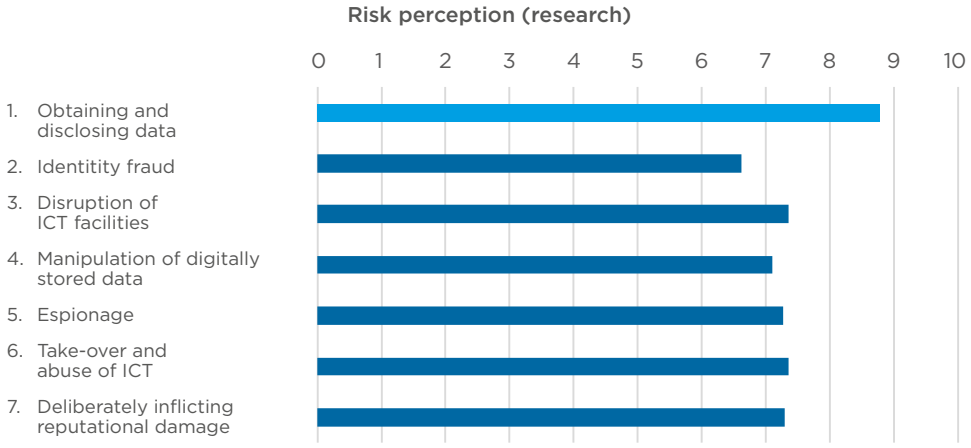


Figure 8: Perception of the risk categories (research)

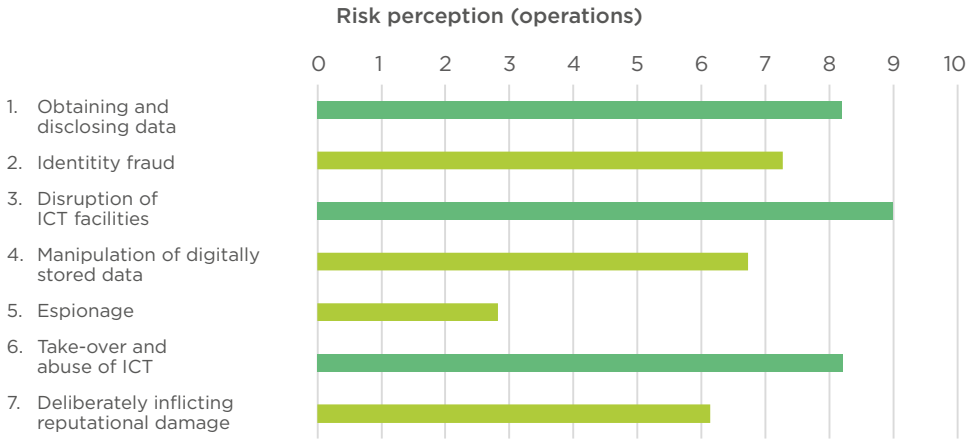


Figure 9: Perception of the risk categories (operations)

Figures 7 - 9 illustrate that:

- for education *Obtaining and disclosing data* and *Disruption of ICT facilities* are considered the highest risk,
- for research *Obtaining and disclosing data* is regarded as the highest risk,
- for business operations *Disruption of ICT facilities*, *Obtaining and disclosing data* and *Take-over and abuse of ICT* are seen as the highest risks, and
- With the exception of research, espionage is **not** considered a high risk.

3. CYBER SECURITY TRENDS

This chapter gives a short overview of the most important cyber security trends in the past year (2019). Also, we list the trends for this coming year (2020).

Trends for education and research

Based on the survey there are no significant changes in the type of threats that the respondents identified compared to 2018. Just like in 2018, in 2019 a slight increase for the risk categories *Obtaining and disclosing data*, *Identity fraud* and *Disruption of ICT facilities* was identified. In the public sources we consulted this trend has been identified for other sectors as well.

Increasing threats

We expect there to be a further increase in threats in 2020, not only to educational organisations, but also to research institutions. We expect ransomware and phishing to be the most common type of attack.

Actors

When we combine all threat types, the survey shows that our constituency considers (h)activists/cyber vandals the most likely actors, followed by professional criminals and insiders (figure 10). This picture is slightly different from the picture painted in the Cyber Security Assessment Netherlands 2019 [2], in which state actors and professional criminals are mentioned as the most likely actors. The NCSC UK also mentions these as most important for universities [7]. The reason why this is different from the survey results requires further investigation.

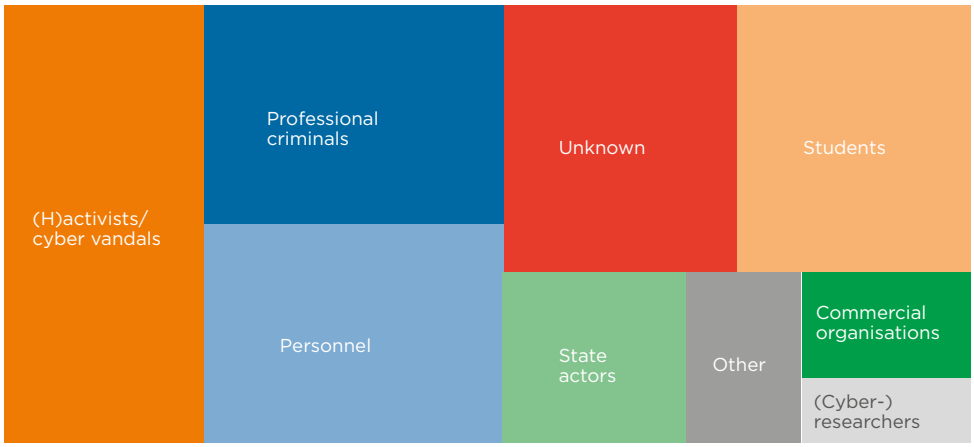


Figure 10: Most likely actors for all risk categories combined

4. RESILIENCE OF EDUCATIONAL AND RESEARCH ORGANISATIONS

The cyber resilience of educational and research organisations is not yet as good as it needs to be. However, this is also true in other sectors. Both the NCSC [2] and the WRR [4] mention that cyber resilience in the Netherlands is substandard in all sectors. For instance, the Netherlands Court of Audit reports in its 2018 report on accountability [8] that the central government itself does not have its information security in good order. Increasing complexity and connectivity of the ICT landscape puts further pressure on the resilience to attacks.

Assessment of resilience in the education and research sector

Respondents assess the cyber resilience of their own organisation on average with a sufficient score (6.3 on a scale of 0-10). This is a slight increase compared to 2018 (5.5). Based on these results, we propose that, despite progress, there is still room for further improvement in cyber resilience at educational and research institutions.

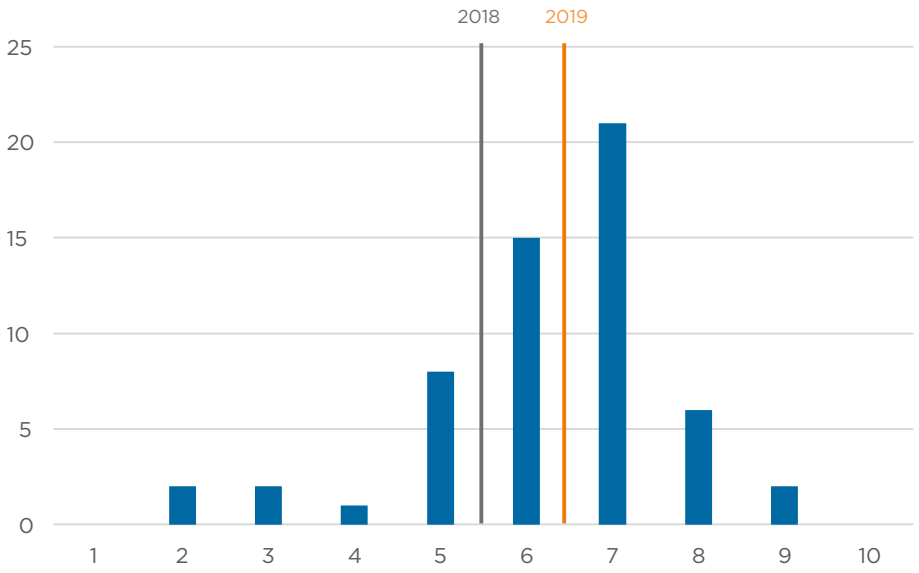


Figure 11: Institutions' own estimate of cyber resilience

To reduce risks, it is absolutely necessary to increase resilience. Connectivity and complexity in organisations are still increasing while basic measures are sometimes lacking. The business model of cyber criminals is still lucrative. They use relatively simple means to inflict major damage on organisations. For some criminals, money is the main motive. For state actors, obtaining knowledge or economic advantage is the main motive to attack organisations. Increasing resilience is the most important means to combat these threats.

5. CONCLUSIONS AND RECOMMENDATIONS

Generally speaking, the Cyber Threat Assessment 2019/2020 does not deviate much from the Cyber Threat Assessment 2018. However, the number of incidents continues to rise, ultimately causing the threat to increase. This requires organisations to continue their effort to increase their resilience. This chapter contains conclusions and recommendations for the education and research sector in order to increase their resilience.

Awareness is an important pillar for resilience

People remain a weak link because of their lack of knowledge and susceptibility for deception. Therefore, institutions need to put a lot of effort into both using training and raising awareness of users.

Bring risk profile for cloud use up to date

Institutions increasingly use cloud applications provided by a small number of large non-European players, which gives rise to new threats for the availability and confidentiality of data. Because of diverging legislation or geopolitical tensions, situations may develop where these suppliers are no longer able to fulfil their obligations to their customers. In addition, an interruption in their services can have major consequences for the primary processes of their customers.

Organisations should act together to identify the risks and find solutions

High investments and highly qualified expertise are necessary

Measures to increase resilience require major investment. However, budgets for information security are always under pressure. After all, these measures always come at the expense of the primary process: education and research.

To be able to adequately resist threats sufficiently highly qualified expertise is necessary. The survey identifies a shortage of capacity as one of the main vulnerabilities. However, the demand for well-qualified expertise is high and the supply low. Here too, cooperation and pooling can help provide a solution.

Expand cooperation

Collaboration is crucial to deal with the growing threats. Already a lot of collaboration and knowledge sharing within the SURF context exists, for example in communities such as SCIPR and SCIRT[6], via SURFcert[7] and with the Safe and Open Higher Education Platform[8]. To make the education and research sector as a whole more resilient to cybercrime, cooperation on the following topics is required:

- sharing information and threats,
- sharing expertise in the field of cyber security,
- setting up security monitoring and logging (SIEM), possibly extending to full-fledged SOC functionality (Security Operations Centre),
- cooperation in cyber security exercises (such as NOZON / OZON) or Red teaming.

Collaboration between institutions helps us to work more efficiently and to overcome the recognised shortages of capacity and expertise.

[6] *SCIPR – SURF Community for Information Security and Privacy, SCIRT – SURFnet Community of Incident Response Teams (https://www.surf.nl/en/security-communities-working-together-on-security-and-privacy)*
[7] *https://www.surf.nl/en/surfcert-247-support-in-case-of-security-incidents*
[8] *https://www.integraalveilig-ho.nl/english-2/*

6. REFLECTION FOR MANAGEMENT

Based on the results of the survey and the trends that were identified, we propose a number of focus areas for management (also see figure 12). This should help management define policy and strategy for their organisations.

- What is your level of ambition in the areas of cyber resilience and integrated safety and security management?
- What is your information position regarding cyber incidents and how do you monitor cyber threats?
- What does the cyber risk profile of your organisation look like, which risks are you prepared to accept and to what extent, and does it fit with your accountability?
- Does your institution have an integrated safety and security management policy and to what extent does the information security policy fit with it?

Figure 12: Focus areas for management reflection

SOURCES

#	Author(s)	Title	Publisher	Year	URL	Accessed
[1]	General Intelligence and Security Agency	**Annual Report 2018**	AIVD	2019	https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018	16-10-2019
[2]	National Coordinator for Security and Counterterrorism	**Cyber Security Threat Assessment Netherlands 2019**	NCTV	2019	https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/nieuws/2019/juni/12/csbn-2019-ontwrichting-ligt-op-de-loer	20-09-2019
[3]	National Cyber Security Centre Netherlands	**Cyberkompas 2019**	NCSC	2019	https://www.ncsc.nl/aan-de-slag/cyberkompas	16-12-2019
[4]	The Netherlands Scientific Council for Government Policy	**Preparing for Digital Disruption (summary)**	WRR	2019	https://www.wrr.nl/onderwerpen/digitale-ontwrichting/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting	10-09-2019
[5]	Verizon Business	**Verizon Data Breach Investigations Report 2019**	Verizon	2019	https://enterprise.verizon.com/resources/reports/dbir/	13-08-2019
[6]	European Union Agency for Cybersecurity	**ENISA Threat Landscape Report**	ENISA	2019	https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018	05-09-2019
[7]	National Cyber Security Centre UK	**The cyber threat to Universities**	NCSC (UK)	2019	https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities	16-12-2019
[8]	The Netherlands Court of Audit	**Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde (In Dutch only)**	Algemene Rekenkamer	2019	https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde	10-01-2020

COLOPHON

Authors
Bart Bosma *(SURF)*
René Ritzen (*SURF*)

Editor
Dr. Linda Cornwall (STFC UKRI)

Coordination
Yvonne Klaassen (*SURF*)

Design
Vrije Stijl, Utrecht

Photography
Istock

May 2020

This report has been produced in part thanks to contributions of the feedback group consisting of:

Bas Roset	*Kennisnet*
Dietmar Timmerman	*Saxion University of Applied Sciences*
Eric van den Beld	*Saxion University of Applied Sciences*
Maarten Veldhuis	*Rijn IJssel*
Marcel van der Kolk	*HU University of Applied Sciences Utrecht*
Martijn Bijleveld	*SaMBO-ICT*
Pamela Mercera	*VU Amsterdam*
Peter Berndsen	*National Institute for Public Health and the Environment (RIVM)*
Raoul Vernède	*Utrecht University*
Rienk de Vries	*Albeda College*
Roeland Reijers	*University of Amsterdam*
Sebastiaan Kamp	*Erasmus University Rotterdam*

Driving innovation together

Universities, universities of applied sciences, senior secondary vocational education (MBO) institutions, research institutions and university medical centres collaborate within SURF on ICT facilities and innovations, thus enabling improved and more flexible education and research. We do this by providing the best possible digital services, by encouraging sharing and exchange of knowledge and, most of all, by constantly innovating! This way, we are contributing to a strong and sustainable knowledge economy in the Netherlands.

SURF