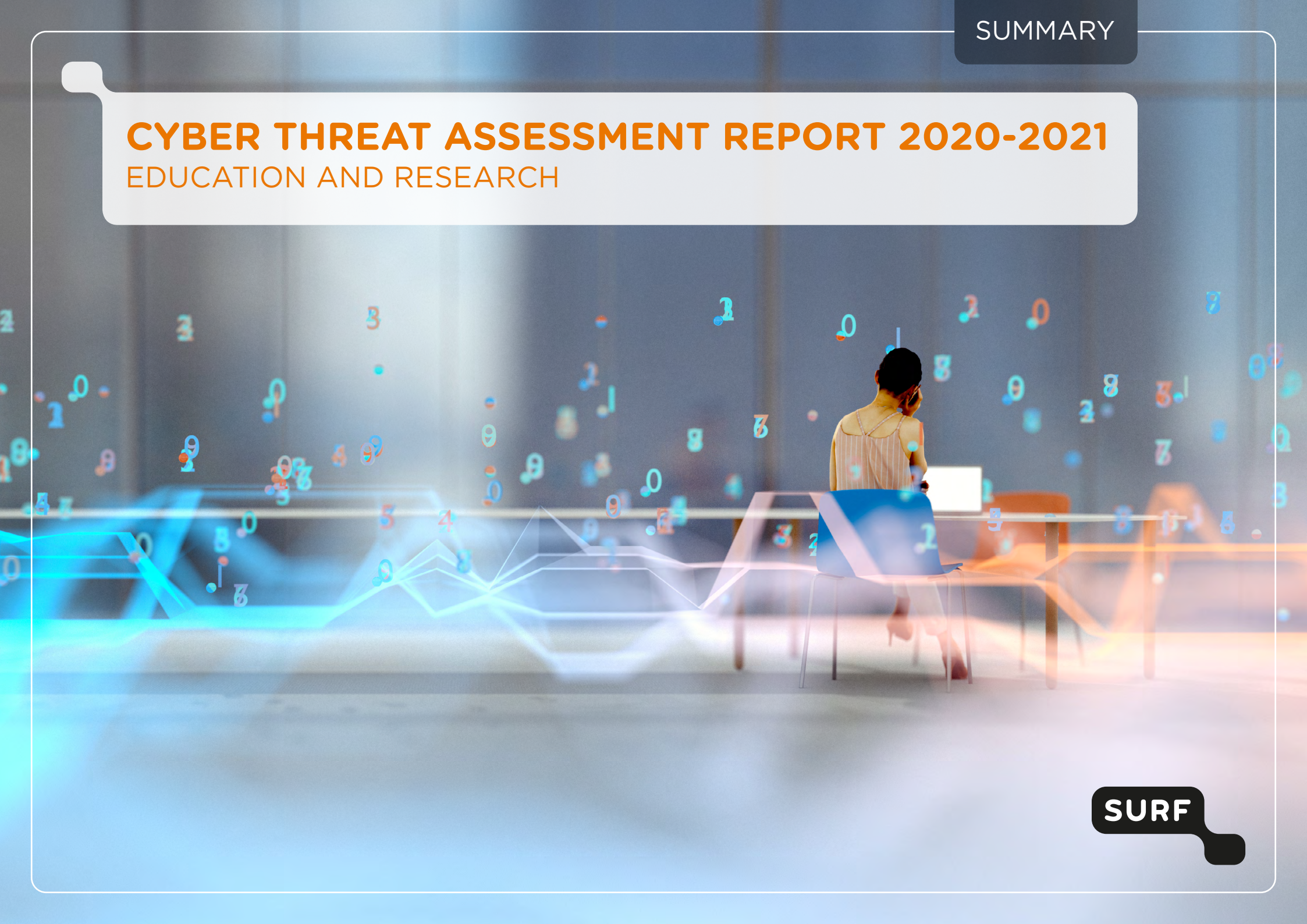
SUMMARY

# CYBER THREAT ASSESSMENT REPORT 2020-2021

## EDUCATION AND RESEARCH



SURF

# PREFACE **RESILIENT TOGETHER**

When the previous SURF Cyber Threat Assessment report was produced, the ransomware attack on Maastricht University had not yet occurred. The Christmas week of 2019 and the first weeks of 2020 have taught us that a threat can develop from a chimera, a notion, into a real crisis. A crisis that is not only of great significance for the institution concerned, but also has an impact on an entire sector.

Welcome to the SURF Cyber Threat Assessment Report 2020-2021. It strikes us that, on average, institutions assess the cyberthreat to be higher than in 2019. Of course, this is not the case only because of the incident at Maastricht University. Working from home as a consequence of the covid-19-lockdown and the many incidents that have been reported in the media in 2020 contribute to this as well. These incidents are also a clear indication that external parties, criminals and state actors see more opportunities to achieve their goals through cyberattacks. In many ways, 2020 was a wake-up call.

Our sector's exposure to cyberthreats has changed and many institutions have made more resources available to strengthen their resilience. In addition to taking responsibility as individual institutions, all parties are also taking their responsibility on a cooperative basis.
For example, institutions have taken the initiative to set up a joint 24/7 Security Operations Centre: SURFsoc was launched in early January 2021. Another example is the joint approach taken by the institutions to fulfil the need for external assessment of their security maturity (SURFaudit): the first results of the external benchmark can be expected in the first quarter of 2021.

In short, although physical get-togethers have been virtually impossible since spring 2020, we observe a growing enthusiasm in the SURF community for collaboration and the exchange of information. And through that intensive collaboration, we improve the security of the digital infrastructure of the education and research sector in the Netherlands together across the board.

Also, cybersecurity has become a mainstay on the political agenda in 2020. The collaboration between the National Cyber Security Centre and four sectoral CSIRTs, including SURFcert, has been laid down in a ministerial ruling in early 2020. The cross-sector motto is 'Resilient together'. In its letters to the House of Representatives about 'Safeguarding Knowledge in higher education and science' and about 'Collaboration with China in Education and Science', the government took steps to improve the safeguarding of knowledge at educational and research institutions. And in December 2020, the Dutch Secret Service (AIVD) disrupted Russian espionage activities at higher education institutions.

In other words, we consider the developments in the area of cyber resilience as positive. At the same time this Cyber Threat Assessment report also shows that there is still reason for increased monitoring of the dikes. The OZON2020 exercise, postponed to March 2021 because of the covid-19 pandemic, can serve as a litmus test for this. Hopefully, in retrospect we will be able to report in 2021 that it has been a year of raising dikes and crisis exercise rather than a year of cyberattacks.

**Nick Bos**
*Vice-chairman of the Executive Board Maastricht University*

**Jet de Ranitz**
*Chair of the SURF Executive Board*

# TABLE OF CONTENTS

# 1 INTRODUCTION

In this Cyber Threat Assessment report 2020-2021 for education and research, we look back on 2020 and forward to 2021. We map out which trends manifested themselves in the education and research sector in 2020 and the threats that have occurred. Also, we look forward to the trends we expect in 2021.

**Headlines**

- **The number of incidents has increased again, particularly the number of phishing attacks. The complexity of incidents has also increased.**
- **Greater dependence on a limited number of large cloud providers from outside the EEA makes education and research vulnerable.**
- **Increase in threats from state actors requires more attention to the safeguarding of knowledge.**
- **Increased complexity and sophistication of threats makes investing in awareness and training of users crucial.**
- **Expertise and resources are still scarce. Collaboration on the topic of cybersecurity within education and research as well as beyond, is as important as ever.**

## Covid-19 pandemic and ransomware incident Maastricht University

The covid-19 pandemic and the ransomware incident late 2019 at Maastricht University have largely set the 2020-agenda. Because of the covid-19 pandemic, institutions had to switch to online education and working from home overnight. To be able to do this quickly, the use of cloud services has increased even more.

The incident at Maastricht University prompted many institutions to speed up the introduction of additional security measures to increase their resilience.

The survey shows that many institutions have paid more attention to awareness of staff and students. On the technical side, many institutions introduced multi-factor authentication and VPN, and focused more on patch management and backing up their data. Despite the covid-19 pandemic, most institutions were able to continue with these projects.

## Incidents

The number of incidents increased again in 2020. Especially the number of phishing attacks has risen sharply. Ransomware attacks in the Netherlands in general did not show a sharp increase, however, there was an increase in the ransom amount attackers demanded.

A number of incidents in 2020 show that the education and research sector in the Netherlands is as vulnerable as ever. In addition to the ransomware incident at Maastricht University, there were a number of high-profile incidents that disrupted the continuity of processes at several other institutions. At the University of Amsterdam, for example, a malfunction meant that almost 6,000 examinations could not be held at the scheduled time and at the University of Groningen, a few hundred online exams could not be held because of an ICT malfunction.

## Trends

Phishing incidents clearly indicate that cybercriminals do extensive research on the organisations they want to attack. For instance, they target specific officials within the organisation.

To facilitate online education and working from home, institutions are deploying new tools, including tools for video conferencing and online proctoring. For this, they usually engage cloud services. As a result, institutions have become even more dependent on a limited number of large cloud providers, which can disrupt

continuity in the event of a disaster. Also, the fact that the European Court of Justice declared the EU-US Privacy Shield invalid could ultimately lead to continuity problems.

The survey shows that many institutions have made additional investments in measures to increase resilience. For instance, a large number of institutions are interested in and connecting to SURFsoc, which went live early 2021.

Institutions have a growing focus on safeguarding knowledge. Partly because of the changing international relations, they assess the exchange of knowledge in collaborations or the participation of some foreign students in a different way now. The Ministry of Education, Culture and Science coordinates the development of instruments to support educational and research institutions in safeguarding knowledge.

### Actors

The survey shows that institutions consider professional criminals as the most important actors, followed by (h)activists/cybervandals. Meanwhile, there are strong indications within the education and research sector that state actors are penetrating institutions more frequently. This has led the government to provide a set of measures for safeguarding knowledge.

### Other results of the survey

Compared to 2019, the 2020 survey shows no major shift in the types of threats observed. *Obtaining and disclosing data*, *Identity fraud* and *Disruption of ICT facilities* are still the most common threat categories. *Takeover and abuse of ICT* has increased in 2020.

### Budget and capacity

Almost half of the institutions spent less than 5% of the total IT budget on information security. Note that compared to 2019, the percentage 'unknown' has increased slightly.

Almost half of the institutions indicate that they have between 2 and 5 FTEs available for information security. This is a slight increase compared to 2019.

### Awareness

Most institutions conduct regular awareness campaigns. About a quarter of the institutions indicate that new employees receive awareness training upon joining the company.

### Security and privacy by design and involvement of the security and privacy officers in projects

Over 80% of the institutions pay attention to security and privacy by design. The involvement of the security officer or privacy officer in new projects has also improved compared to 2019.

### Risk perception

For the seven risk categories, the risks are rated higher than in 2019 for the processes education, research and business operations. *Deliberately inflicting reputational damage* is the sole category for which the risk is estimated slightly lower for all three processes. Espionage is also rated slightly lower for the educational process and business operations.

We asked survey participants to estimate the risk of *Dependency on cloud services* and added this as the eighth risk in Table 1 (page 9). Institutions are increasingly moving their data and applications to the cloud, which creates a different risk profile. For example, it is much more difficult to determine the state of information security of the cloud services themselves. And often the data is located outside the EEA, which means compliance with the GDPR is at risk. There is also a limited number of cloud service providers, which gives them a monopoly position. In addition, these providers are mainly based in the US.

# 2 HIGHLIGHTS

In this Cyber Threat Assessment report, we build on the previous editions. We use public sources such as the Verizon Data Breach Incident Report and the ENISA Threat Landscape to see which trends there are. In the fall of 2020, we conducted a survey to gain insight in the type of incidents that have actually taken place and to see which risks are most relevant for the education and research sector.

## Incidents

In 2020 a number of incidents made the news:

- **Maastricht University**
  This incident at the end of 2019 affected the entire sector. All universities decided to have an external auditor perform a cyber assessment using the SURFaudit framework. The university organised a symposium to share what happened, why they acted the way they did and the lessons learned. A number of universities initiated setting up a Security Operations Centre together with SURF.
- **Citrix vulnerability**
  In the beginning of 2020 a hospital, a municipality and several ministries announced they had detected intrusion attempts into Citrix systems as a result of vulnerabilities. Organisations in the education and research sector had to take action to prevent them from being hacked as well.
- **Privacy Shield invalid**
  In July 2020 the European Court of Justice struck down the EU-US Privacy Shield for the transfer of personally identifiable information from the EU to the US.
- **Exams interrupted**
  At the University of Amsterdam and the University of Groningen students were unable to participate in exams because of ICT-disruptions. In Amsterdam the authentication system was faulty, in Groningen the e-learning environment was overloaded. The next day the application Proctorio failed in Amsterdam, which forced the university to postpone exams again.

## Trends

The year 2020 was marked by the outbreak of the corona virus.

- **Covid-19**
  The covid-19 pandemic caused a severe lockdown in the Netherlands starting March 13, 2020. As a result, face to face education was prohibited overnight. Organisations in the education and research sector had to scramble to enable online and distance learning.
- **Survey results**
  Compared to 2019 we do not observe major differences. The most common threats still are *Obtaining and disclosing data*, *Identity fraud and Disruption of ICT facilities*. The risk level for *Take-over and abuse of ICT* increased in 2020. The number of threats has increased again, especially phishing attempts. It is worth mentioning also that criminals investigate their targets thoroughly before launching an attack.
- **Vulnerabilities on the rise**
  According to the National Vulnerability Database[1], the number of vulnerabilities was more or less stable between 2010 and 2016. In 2017 however a steep increase occurred that has continued thereafter (figure 1 on page 8).
- **Dependency on cloud services**
  To facilitate online education and working from home, organisations in the education and research sector increasingly deploy new tooling, including tools for video conferencing and online proctoring. Most of these are delivered as a cloud service by a limited number of large cloud providers.
- **Safeguarding knowledge**
  Safeguarding knowledge (protection of intellectual property) is a new focal point for the sector. Organisations assess the exchange of knowledge during partnerships with other institutions and the role of foreign students differently. Also, undesired transfer of knowledge and technology has come under closer scrutiny because of changed international relations.

1 https://nvd.nist.gov

Table 1 **Risk perception and dynamic**

| Risk Category | Education | △ | Research | △ | Operations | △ |
|---|---|---|---|---|---|---|
| 1 Obtaining and disclosing data | Very high | ↑ | Very high | ↑ | Very high | ↑ |
| 2 Identity fraud | High | ↑ | Medium | ↑ | High | ↑ |
| 3 Disrupting of ICT facilities | Very high | ↑ | High | ↑ | Very high | ↑ |
| 4 Manipulating digitally stored data | High | ↑ | Medium | ↑ | Medium | ↑ |
| 5 Espionage* | Low | — | Medium | ↑ | Low | — |
| 6 Take-over and abuse of ICT | High | ↑ | High | ↑ | Very high | ↑ |
| 7 Deliberately inflicting reputational damage | Medium | ↓ | Medium | ↓ | Medium | ↓ |
| 8 Dependency on cloud services | Very high | ○ | Medium | ○ | High | ○ |

△ Change in 2020 compared to 2019

↑ Significant increase

↑ Increase

— No change

↓ Decrease

↓ Significant decrease

○ No comparison

** The uncertainty is greatest for espionage (36% of the respondents do not know whether the risk has increased or decreased)*

Figure 1 **Number of CVE registrations since 2010**

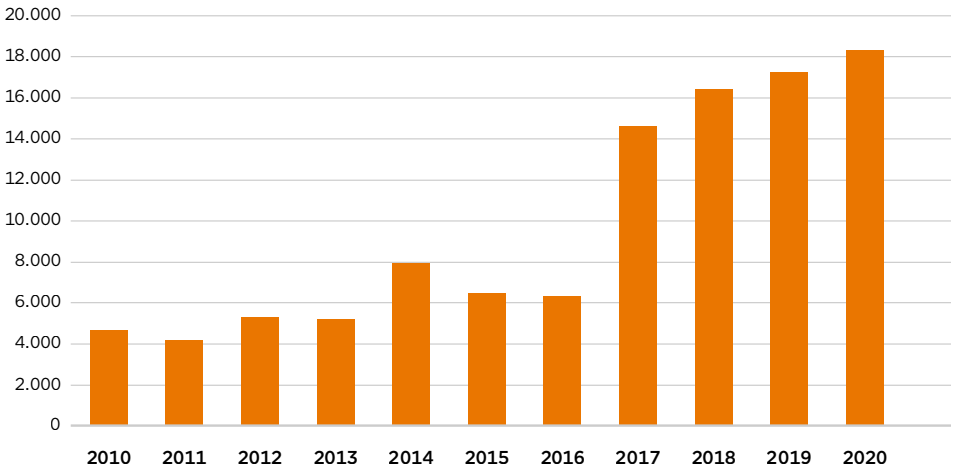
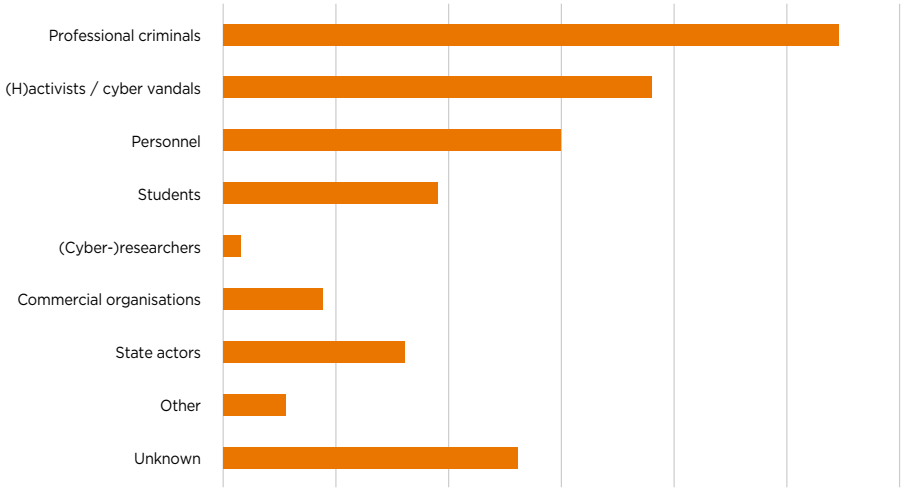



Figure 2 **Actors mentioned most often**




## Actors

The actors that are mentioned most often in the survey for all threats combined are *professional criminals* followed by *(h)activists/cyber vandals*. But the education and research sector is catching up on the national trend that state actors are becoming more prominent as well.

## Survey outcome

Next you will find the most important results of the survey we conducted in the fall of 2020.

### Governance

The majority of organisations report about the state of information security and privacy to the executive board, certainly in case of a serious incident (figures 3 and 4).

Figure 3 **Reporting to the executive board**

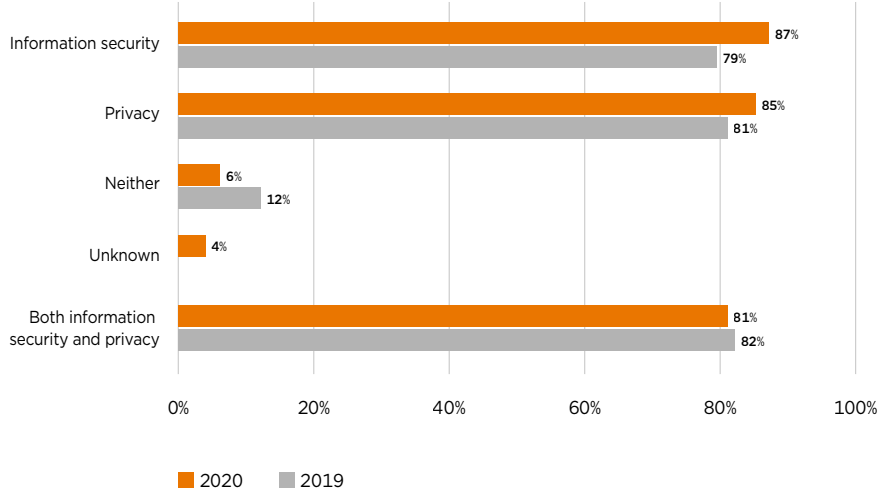


Figure 4 **Reporting when a serious incident happens**

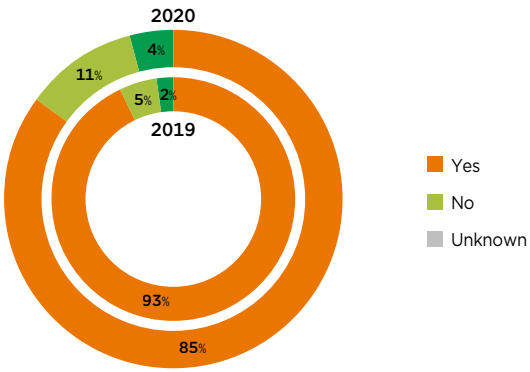



Figure 5 **Reporting to the supervisory board**

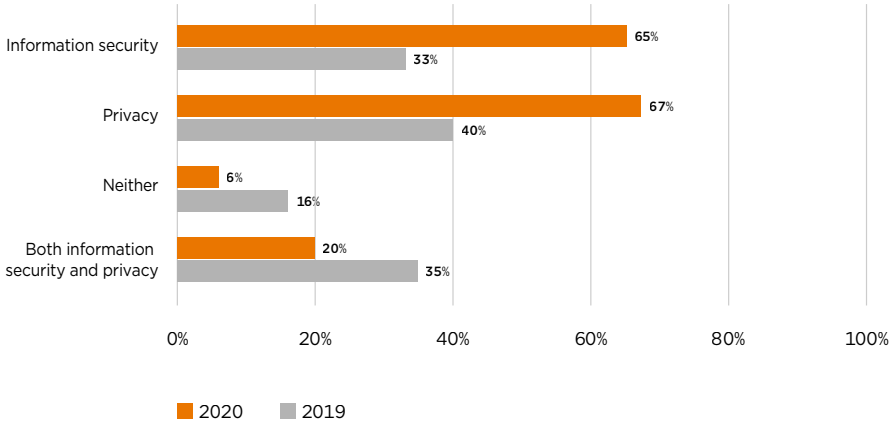



Figure 6 **Attention for information security and privacy in the annual report**

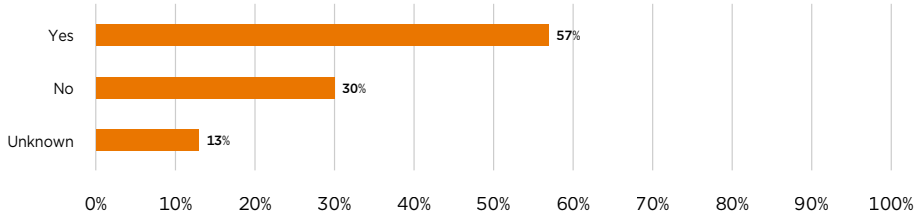
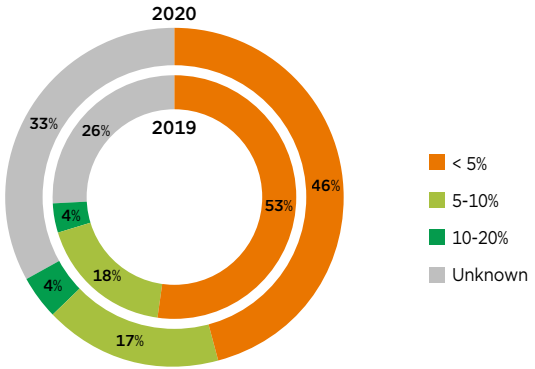



Figure 7 **Budget for information security as a percentage of the total IT budget**




With respect to reporting to the supervisory board, the percentage of institutions reports has almost doubled since 2019 (figure 5).

In 2020, more than half of the institutions mentions information security and privacy in their annual report (figure 6). Almost half of the institutions spends less than 5% of the total IT-budget on information security and privacy (figure 7). Also note that this is a slight decrease since 2019 and that the percentage 'unknown' has increased a bit.

When we distinguish institutions by size, a relation between size and number of FTEs available for information security becomes apparent (table 2).

Table 2 **FTEs in relation to the institution's size**

| FTE | Number of employees | Number of students |
|---|---|---|
| **More than 10 FTE** | 2,100 | 20,000 |
| **5 - 10 FTE** | 1,150 - 6,100 | 10,000 - 46,000 |
| **2 - 5 FTE** | 80 - 7,500 | 5,000 - 40,000 |
| **1 FTE or less** | 400 - 2,600 | 2,600 - 23,000 |

## Resilience

The survey results indicate that respondents consider investments in operational security sufficient. Awareness of students and contractors, and having or using a Security Operations Centre however lag behind. In figure 9 you find an overview of the respondents' opinion with respect to the degree of investments in technical and non-technical measures.

On average, respondents rate the resilience of their organisation in 2020 a 6.5 (on a scale of 0-10), slightly higher than in 2019 (also see figure 10).

Figure 8 **Numbers of FTEs available for information security for universities, universities of applied sciences, vocational schools and research institutes**

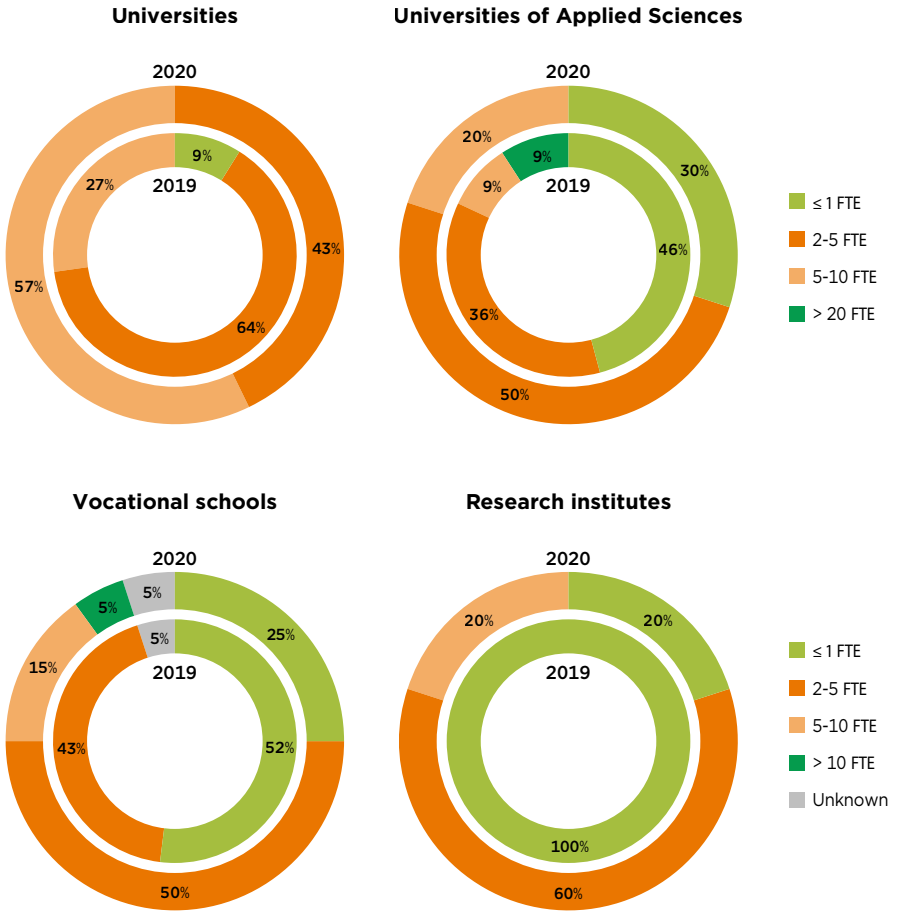


Figure 9 **Investments in security measures**

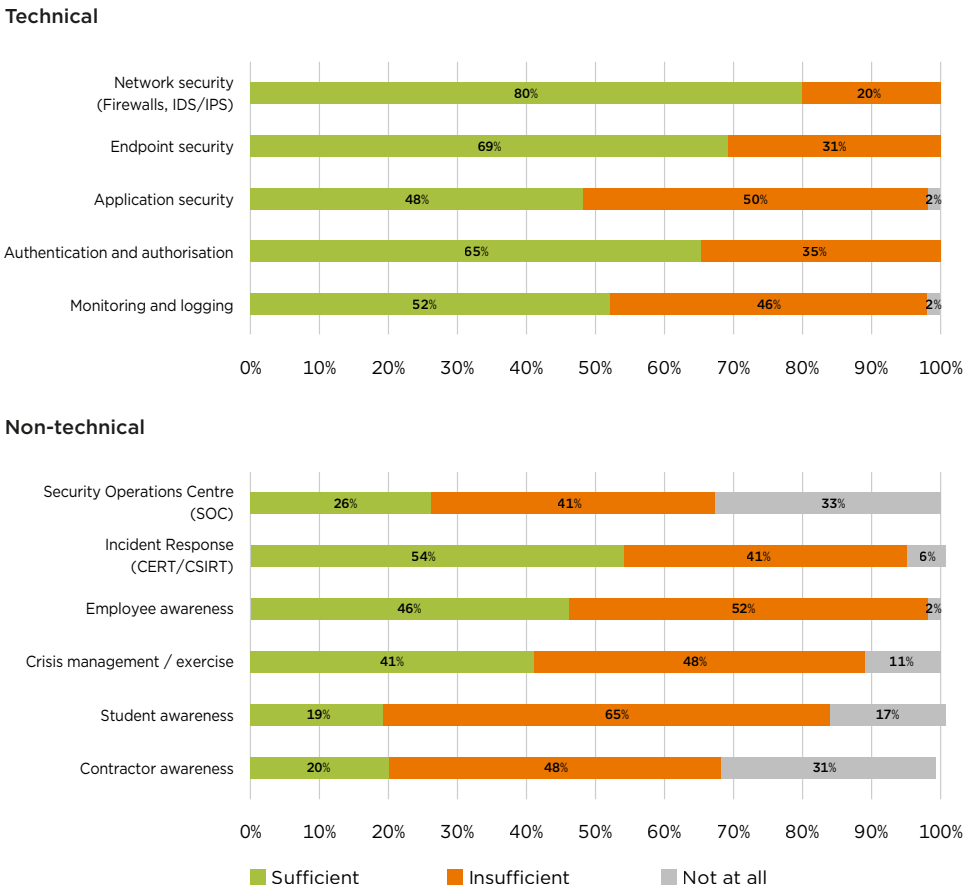
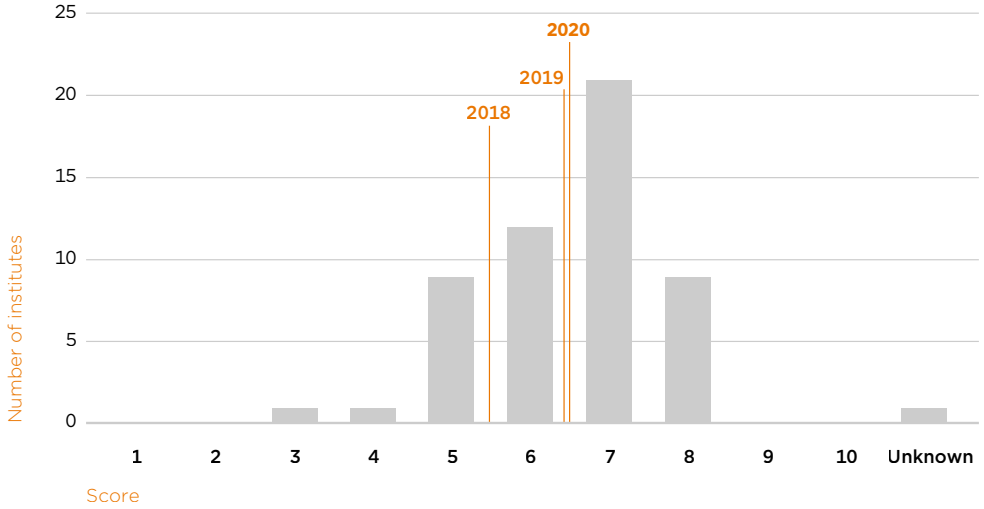



Figure 10 **Resilience in 2020 and average per year**



# 3 REFLECTION AND CONCLUSIONS

### Increased dependency on cloud providers

Cloud services are increasingly used for online education, online proctoring and working from home. This has increased the dependency on a limited number of large cloud providers. A number of disruptions at these large cloud providers show that the Dutch education and research sector is still vulnerable. In addition, the invalidation of the Privacy Shield by the European Court of Justice means that institutions must consider these aspects of their use of cloud services when drawing up their risk profiles.

### Safeguarding knowledge

The increase in threats from state actors require institutions to invest even more in safeguarding knowledge and in expertise in the area of cyber security.

### Awareness and training of users increasingly crucial

The number of phishing attempts has risen significantly and the methods are becoming much more sophisticated. Investing in training and awareness is becoming increasingly crucial, so users also become more resilient to the latest threats.

### Cooperation

We notice increased cooperation, both within the sector and outside. University security officers have started the U-CISO panel in which they pool knowledge and exchange information confidentially. Within the VSNU (Association of Dutch Universities), data protection officers work together. At the initiative of the universities, SURF started to set up a security operations centre (SURFsoc) in 2020, in close collaboration with the universities and one University of Applied Sciences. This is a good example of making optimum use of the expertise available in the sector and efficient use of resources.

At the national level, cooperation in the field of incident response exists since the beginning of 2020 within the LDS (National Detection/Response System), a collaboration between the National Cyber Security Centre (NCSC) and sectoral partnerships, CERTs, and other public and private parties. SURFcert represents the education and research sector. The aim of the collaboration is to exchange information and knowledge about, for example, vulnerabilities and threats.

There will be a huge shortage of cyber security expertise in the coming years. In addition, it is to be expected that after the covid-19 pandemic, financial resources will become scarcer. This reinforces the need for further cooperation in order to deal with the increasing number of threats.

# COLOFON

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

**Editor**
Jan Michielsen (SURF)

**Coördination**
Yvonne Klaassen (SURF)

**Design**
Studio Koelewijn Brüggenwirth BNO, Den Haag

**Photography**
iStock

Februari 2021

**This report has been produced thanks to contributions of the feedback group consisting of:**
Alex Peeters – Helicon Opleidingen
Bart van den Heuvel – Maastricht University
Bram Bogers – Onderwijsgroep Tilburg
Dietmar Timmerman – Saxion University of Applied Sciences
Donny Toebes – Graafschap College
Erik van den Beld – Saxion University of Applied Sciences
Erwin Elieveld – VU Amsterdam
Gert Douma – Hanze University of Applied Sciences
Jurrian Wijffels – Fontys University of Applied Sciences
Ludo Cuijpers – Vista College
Martijn van Hoorn – CITAVERDE College
Martijn Bijleveld – SaMBO-ICT
Pamela Mercera – VU Amsterdam
Peter Vermeijs – MBO Raad
Raoul Vernède – Utrecht University
Roeland Reijers – University of Amsterdam
Sebastiaan Kamp – Erasmus University Rotterdam

Driving innovation together