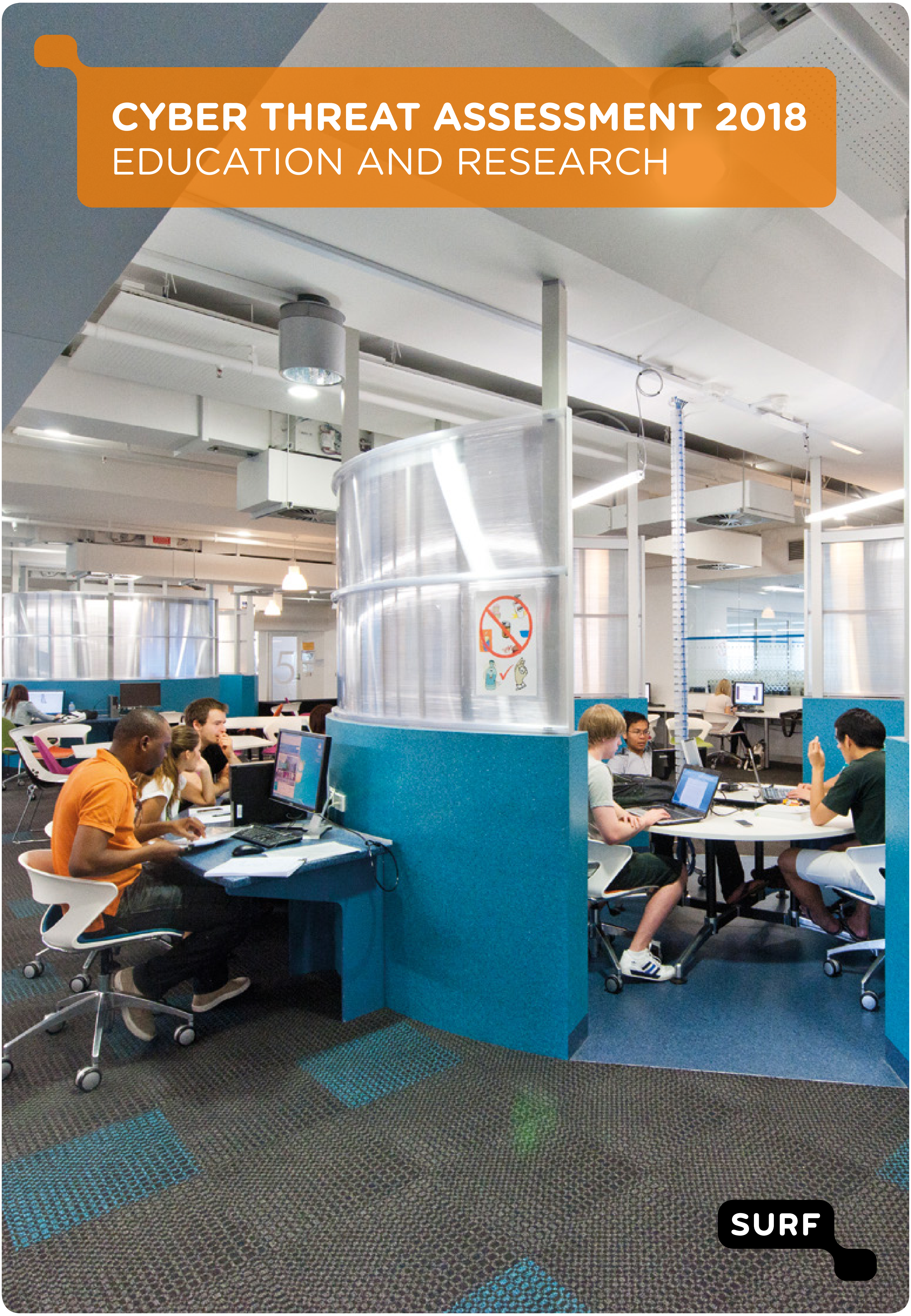
CYBER THREAT ASSESSMENT 2018
EDUCATION AND RESEARCH



SURF

CONTENTS

FOREWORD

ICT is vital for education and research. We are seeing a rapid growth in digital learning methods, increased digital cooperation with partners, and more and more digital data being exchanged across borders. Digitisation is widespread and offers unprecedented opportunities for education and research. For example, SURF provides high-performance computing, big data processing and cloud services for its members. This contributes to a flourishing and innovative knowledge infrastructure. In order to take full advantage of these opportunities in the long-term, it is necessary to have confidence in these digital solutions. At the same time, the threats posed by digitisation are increasing and directly affect the heart of our education and research.

This is the 5th edition of the Cyber Threat Assessment report for Education and Research, which aims to provide insights into developments that are relevant to our sector. The basis for this analysis was created by conducting a survey of institutions affiliated to SURF. The main conclusion of the survey is that the information position on cyber risks needs to be improved because it is intertwined with the primary process and because of the impact it causes if a cyber security incident occurs. The report also provides an up-to-date picture of the cyber risks experienced by institutions. In reality, this picture will differ from one institution to another and will raise questions about the situation at the institutions.

It is crucial that the management of the institutions addresses these questions. This report challenges directors with stimulating questions and focus points. How is your institution prepared for cyber threats? What are your ambitions? What do you know about cyber incidents at your institution? These are questions of great relevance to all of us. Taking basic measures and offering safe products and services is not always self-evident. Institutions also assess their own resilience as insufficient or, perhaps worse, they do not even know where they stand. It is up to the managers of institutions to develop a vision with regard to cyber security, or to incorporate their vision into the broader framework of integrated security as described, for example, by the 'Integral Safety in Higher Education Programme'.

In concrete terms, this calls for the further development of promising initiatives such as 'security-by-design' and 'privacy-by-design', and for participation in cyber crisis exercises such as OZON, that SURF organises every two years, in order to improve its own resilience. This year OZON was very successful again, with a lot being learned and institutions exchanging knowledge and experiences. A successful example of joint action to improve our resilience as a sector.

Looking back at five years of publishing the Cyber Threat Assessment report, we see constant changes in the threats that are coming towards us and a further increase in the complexity of the application landscape at institutions. Institutions are increasingly dependent on digitisation, so there is a need for increased vigilance and growing importance of proactive measures.

Together with the biennial SURFaudit benchmark, this report contributes to raising awareness at all levels about the state of information security in the education and research sector, so that institutions know what to do to become more resilient, to counter threats, and to make full use of digitisation.

Erwin Bleumink, *SURF board member*
Marjolein Jansen, *Vice-Chairperson VU Amsterdam*
and *SURF Cyber Security Ambassador*

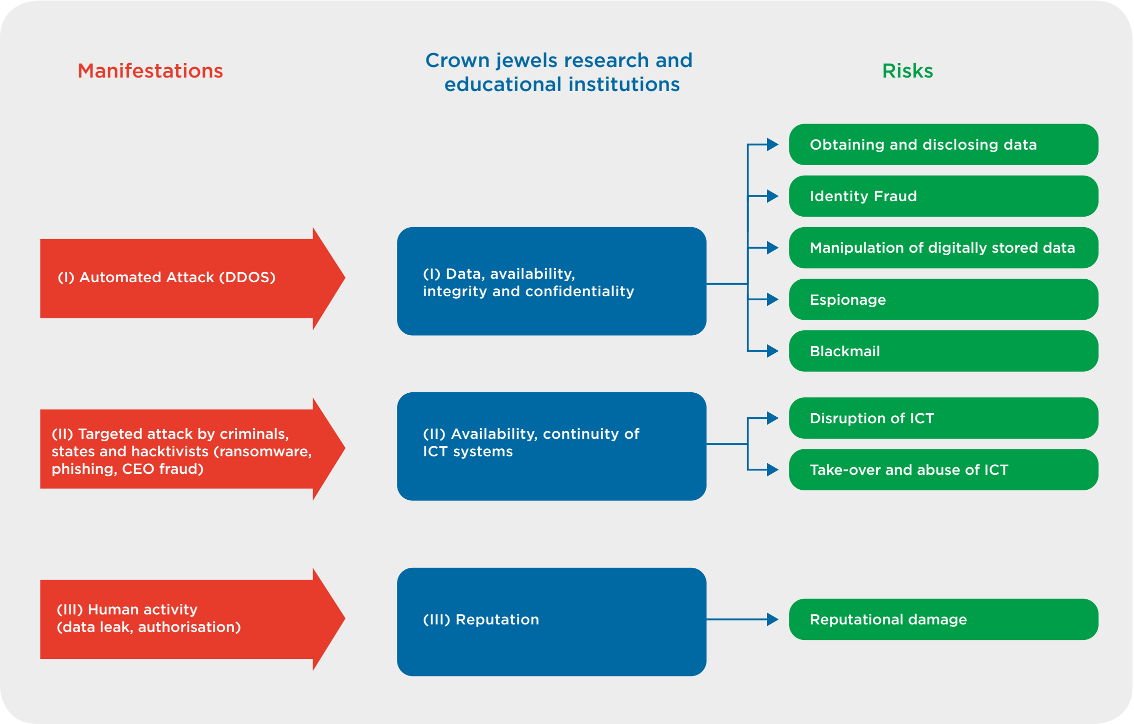
SUMMARY

General

This Cyber Threat Assessment report provides information to administrators, security and privacy officers of Dutch research and educational institutions about developments in the field of cyber security that took place in 2018. In addition, we conducted a survey to map out the risk perception of the institutions and to get an idea of incidents that have occurred in the following risk categories:

1. Obtaining and disclosing data
2. Identity fraud
3. Disruption of ICT
4. Manipulation of digitally stored data
5. Espionage
6. Take-over and abuse of ICT
7. Deliberately inflicting reputational damage

The following figure illustrates the manifestations of threats, the risks and which crown jewels they influence:


Manifestations
Crown jewels research and educational institutions
Risks
(I) Automated Attack (DDOS)
(I) Data, availability, integrity and confidentiality
Obtaining and disclosing data
Identity Fraud
Manipulation of digitally stored data
Espionage
Blackmail
(II) Targeted attack by criminals, states and hacktivists (ransomware, phishing, CEO fraud)
(II) Availability, continuity of ICT systems
Disruption of ICT
Take-over and abuse of ICT
(III) Human activity (data leak, authorisation)
(III) Reputation
Reputational damage

General trends observed in 2018 in terms of cyber threats

As in previous years, criminals use malware to achieve their goals. Ransomware is a widely used tool and several organisations have been affected by infections. Furthermore, denial-of-service attacks occur regularly, with varying effects, and hacking attacks are still carried out to gain access to internal systems. Apparently, the effectiveness of phishing is still large enough to occur on a regular basis.

Criminals are mainly interested in financial gain: data are money. Research and educational institutions are also in possession of valuable data, ranging from personal data to research data. On the one hand, when basic security measures are not properly in place, criminals can easily gain access to internal systems. On the other hand, if control and logging are not properly organised, it is difficult to determine what is happening on the network and on internal systems. In addition to external parties, internal staff can also cause problems, whether intentionally or not.

Cyber threats that institutions have encountered in 2018

The perception of the risk to which institutions are exposed has changed considerably: the risks are estimated to be much higher than in the past. Whereas in previous years, risks were estimated to be low, now most risks are estimated to be medium-high. This may be due to the introduction of the GDPR on 25 May 2018. While this date came close, institutions paid a great deal of attention to the protection of personal data. They have also set up procedures to report data leaks, should they occur, to the Data Protection Authority in due time. As a result, institutions have been giving more attention to the governance of information security and to the need for measures to protect information.

The top 3 cyber threats vary by sector. For education and business operations, the ‘Disruption of ICT’ is the most important risk. The reason is that this threat has a fairly direct effect on the continuity of the primary (educational) process. For the research sector, ‘Obtaining and disclosing data’ is the most significant risk. This threat also directly affects one of the crown jewels of institutions, namely the intellectual property/integrity of research and personal data. ‘Deliberately inflicting reputational damage’ is also seen as an important risk.

When answering the question about the frequency with which incidents took place, it is striking that many respondents to the survey indicate that this is not known. This reinforces one of the conclusions of the SURFaudit benchmark report indicating that the ‘control and logging’ cluster scores low. In the case of a risk such as ‘Disruption of ICT’, the number of ‘unknown’ responses is actually low, probably because all institutions have an incident registration system and disruptions will be reported quickly.

Current trends that receive full attention are the constant occurrence of denial-of-service attacks, the use of BYOD and the use of the Internet of Things (IoT).

Measures taken by institutions to improve their cyber resilience

In most of the institutions that took part in the survey, information security is on the agenda of the Executive Board and, to a lesser extent, has the attention of the Supervisory Board as well. All institutions have an approved information security policy, but sometimes they fail to evaluate it and keep it up to date.

The resilience of institutions scores well in the survey:

- MBO (secondary vocational education) institutions score above average,
- Universities of applied science (HBO) show a mixed picture with a few outliers downwards (scores 2 & 3 on a scale of 1 - 10), and
- Universities and research institutes score slightly above average (5.5).

The extent to which participants in the survey rate threats as being under control is ‘average’, although ‘Espionage’ and ‘Deliberately inflicting reputational damage’ are rated significantly lower.

Management dialogue

To promote management dialogue on cyber security, and based on the results of this Cyber Threat Assessment report, we have included five questions on the topics ‘cyber risk profile’, ‘ambitions’, ‘information position’, ‘cyber security policy’ and ‘evaluation’. These questions can be used by administrators - in consultation with their Corporate (Information) Security Officer, faculty directors, the Supervisory Board - to discuss the cyber risks and cyber resilience of their own institution.

INTRODUCTION

1.1 Background

Since 2014, SURF has been monitoring the main developments in cyber threats to research and educational institutions on an annual basis. The SURF Cyber Threat Assessment report provides an up-to-date overview of trends and threats. This version builds on previous editions of the Cyber Threat Assessment report, but focuses on developments that took place in the recent period (from January 2018 to January 2019).

With the Cyber Threat Assessment report, SURF informs the administrators, security, and privacy officers of Dutch research and educational institutions on developments that are taking place, so that they can further improve their own information security and privacy protection.

Institutions are faced with various security issues. The Integral Safety Programme for Higher Education (IV-HO) distinguishes eight security topics, ranging from social security and alarming behaviour to internationalisation. [1] Institutions see cyber security and privacy as the most serious threats, according to the Higher Education Threat Analysis 2018. In concrete terms, this concerns data leaks, data manipulation and identity fraud, loss of intellectual property and damage to image. [2]

The SURF Cyber Threat Assessment report focuses on cyber security, which is part of the 'Privacy and Cyber Security' theme in the IV-HO Threat Analysis:

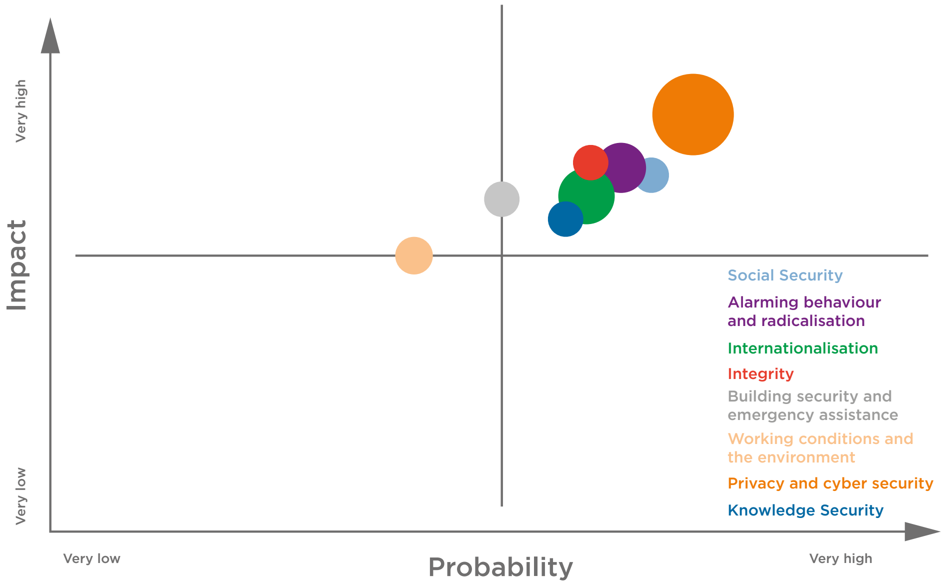


Figure 1: Threat matrix from the Higher Education Threat Analysis of IV-HO. [3]

The new edition: cyber survey among educational institutions

Previous editions were largely based on public sources such as reports from the National Cyber Security Centre (NCSC) and Verizon and discussions with security officers of institutions; in this edition, we asked employees of research and educational institutions involved in privacy and ICT about cyber threats. In addition, we have attempted to involve more MBO (secondary vocational education) institutions in the Cyber Threat Assessment.

1.2 Cyber threats, crown jewels and manifestations

As a framework for analysis, we use the model below:

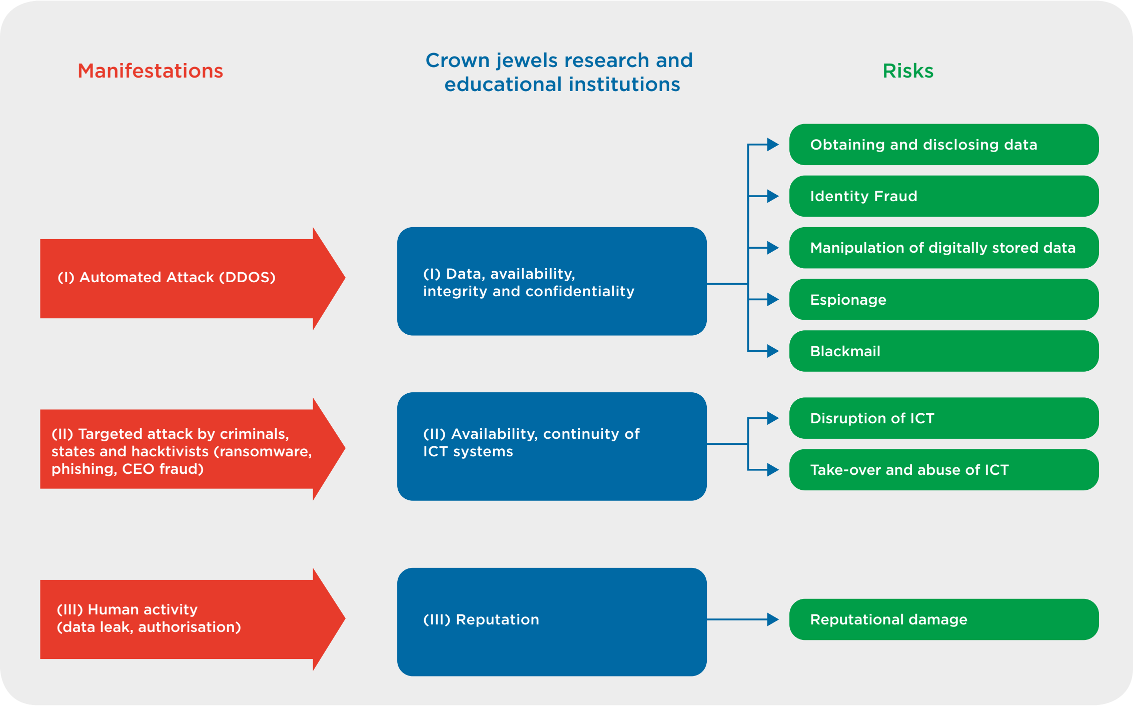

Manifestations
Crown jewels research and educational institutions
Risks
(I) Automated Attack (DDOS)
(I) Data, availability, integrity and confidentiality
Obtaining and disclosing data
Identity Fraud
Manipulation of digitally stored data
Espionage
Blackmail
(II) Targeted attack by criminals, states and hacktivists (ransomware, phishing, CEO fraud)
(II) Availability, continuity of ICT systems
Disruption of ICT
Take-over and abuse of ICT
(III) Human activity (data leak, authorisation)
(III) Reputation
Reputational damage

Figure 2: Manifestations, crown jewels and risks

This diagram illustrates the effects of the manifestations of threats and of the risks on the crown jewels. We also briefly discuss measures against these cyber risks that affect the resilience of institutions.

Crown jewels

Institutions consider the availability, integrity and confidentiality of data, the continuity of education, research and business operations, and reputation as their crown jewels:

	Crown jewels	Examples
1	Data (availability, integrity, confidentiality)	Personal data (students, employees)
		Personal data in the context of research/databases, including special personal data such as ethnicity, religion and medical data.
		Intellectual property
2	ICT facilities (continuity of education, research and operations)	Student Information Systems, etc.
		Student administration
		Websites (general, departments, events)
		Security
		Building climate control
3	Reputation (damage to reputation)	Reputation is based on the undisturbed and secure operation of ICT facilities and on the integrity and availability of data. Reputation is at stake in the event of (large-scale) incidents that may involve negligence, such as non-compliance with the GDPR, inadequate information security or incident response.

Table 1: Risks

Risks that manifest themselves can affect the availability, integrity and confidentiality of data, the continuity of education, research and business operations and the reputation of institutions. In this report, we use the seven categories of risks defined in previous editions of the Cyber Threat Assessment report (see also Appendix 1):

1. Obtaining and disclosing data
2. Identity fraud
3. Disruption of ICT
4. Manipulation of digitally stored data
5. Espionage
6. Take-over and abuse of ICT
7. Deliberately inflicting reputational damage

Manifestations

Cyber risks for MBO schools (secondary vocational education), universities of applied sciences and universities can manifest themselves in various ways (see Figure 2):

- Automated attacks (such as DDoS)
- Targeted attacks by criminals, states and other individuals and groups (such as ransomware and espionage).
- Human action - intentional or unintentional (resulting in loss of data).

Consequences

Consequences arise, for example, when data is obtained (theft), manipulated or viewed unlawfully (espionage), identity fraud is committed or institutions are blackmailed. But also when ICT facilities are taken hostage and/or disturbed.

Resilience

Institutions can protect themselves against digital attacks and disruptions in various ways, depending on the risk profile of the institution concerned. For information security, ambition levels are available that serve as guidelines for information security and privacy (see also: SURFaudit-benchmark). [4] In addition to prevention, aimed at preventing cyber incidents, institutions can also invest in detection, incident response and crisis management.

1.3 Approach

For the purpose of this Cyber Threat Assessment report, SURF conducted a survey among employees of MBO institutions, Universities of applied sciences, Universities, and other SURF member institutions, who are professionally involved in information security issues, such as security & privacy officers. The survey was conducted among members of SCIPR and SCIRT and the MBO institutions via the MBO Information Security & Privacy steering committee.

SCIRT is the community of members of Computer Security Incident Response Teams (CSIRTs) of institutions affiliated with SURF. The aim of SCIRT is to achieve synergy within the field of security experts of the institutions affiliated with SURF. SCIRT is the premier place where operational security experts discuss current security challenges and exchange the latest tips & tricks.

SCIPR is a community of practice in which information security officers and privacy officers from the SURF members work together to improve professional information security and privacy. SCIPR stands for SURF Community for Information Security and Privacy. Its aim is to improve information security and privacy at education and research institutions. One of the ways SCIPR does this is by developing policy and guidelines.

The platforms work together. SCIPR deals with security policy and governance, SCIRT with more operational matters.

The MBO Information Security & Privacy steering committee is a joint venture under the auspices of saMBO-ICT, in which Kennisnet and SURF also participate. The aim of the steering commitee is to develop knowledge and share experiences.

The survey contained questions about the most significant cyber threats and about measures to improve cyber resilience. A total of 35 respondents completed the survey, divided over 28 institutions, including both small and large institutions. It also included institutions that only carry out research, institutions that only offer education and institutions that do both. Not all institutions answered all questions.

Vocational education and training ('MBO')	3
Higher professional education ('HBO')	14
Scientific education ('WO')	7
Research	3
Unknown	1

Table 2: Number of institutions per sector

Security officer/manager	17
Privacy officer	5
Head of IT	4
Policy officer/advisor	4
Other	5

Table 3: Number of respondents per function

To validate the design and results of the survey, we set up a feedback group of interested employees from research and educational institutions. We used the input from the feedback group in the survey and incorporated its feedback in this report.

To identify trends, we consulted authoritative publications and retrieved information from SURF's own datasets, such as those of SURFcert.

1.4 Cyber Threat Assessment report 2017

Cyber Threat Assessment report 2017: main points

The following trends emerged in the Cyber Threat Assessment report 2017:

1. Professional criminals and state actors continue to constitute the greatest threat and cause the most damage.
2. Resilience in individuals and organisations does not keep up with the proliferation of the threats.
3. The increasing digitisation of citizens (and therefore also of students, teachers, researchers and other staff at education and research institutions) is changing the threat landscape.
4. Denial-of-service attacks will continue, but can be kept under control.
5. Malicious parties are still taking advantage of vulnerabilities, including on mobile devices, to gain access to critical systems. [5]

Cyber Threat Assessment report 2018: compared to previous editions

The above trends continued unabated in 2018. An important difference with the previous edition of the Cyber Threat Assessment report is the effect of the introduction of the General Data Protection Regulation (GDPR) mid-2018. The GDPR has attracted a great deal of attention from institutions and in the past year institutions have taken measures to comply with the GDPR. The focus on the GDPR is a possible explanation for a different perception of cyber threats: conceivably, participants will estimate threats to be more serious than in previous years. Also, we adopted a different approach in 2018. However, for the sake of continuity we have maintained the seven threats from previous editions.

Nevertheless, cyber threats are extremely dynamic. The 'colour' of the Cyber Threat Assessment report will vary from year to year. For the first time, a more quantitative assessment of threats has been carried out in this edition. The assessment of threats therefore differs from previous editions. In this edition, a broader target group has been consulted. In addition to research institutions, universities of applied sciences and universities, MBO (secondary vocational education) institutions participated in the survey.

1.5 Document structure

Chapter 2 provides an overview of the most important current cyber trends.
Chapter 3 focuses on the main cyber threats to research and education institutions. The focus is both on the *perception* of threats and on the actual occurrence of cyber incidents.
Chapter 4 deals with the cyber resilience of institutions, i.e. the extent to which they are prepared to prevent and respond to cyber threats.
Chapter 5 contains the most important highlights from this report and points for reflection that managers can use for the dialogue on cyber risks and resilience within their own institution.

2. TRENDS

This chapter provides an overview of the most important current cyber trends. They are derived from authoritative reports and information provided by SURF. The following topics are addressed: methods, motives, actors and digital resilience. In addition, an overview is given of data leaks and incident reports at SURF.

2.1 Methods: ransomware, DDoS and hacking

- Although cybercriminals are still successful with tried and tested attack techniques, [6] the complexity of attacks is increasing. [7]
- Ransomware is the most common form of malicious software; using ransomware obviates the need for cyber criminals to steal data, their only aim is to block the use of data and systems. The most important reason for its popularity is: it is easy to use, low-risk for the attacker and appears to be very effective. [6] Although the exact damage is not clear, the estimated amount of ransomware damage is approaching 5 billion U.S. dollars in 2017. [8]
- Cyber-attacks are easy to carry out. There is a thriving online business, offering infrastructure, attack tools and techniques for a fee. This makes it relatively easy to carry out an attack, even for actors other than, for example, states. [9] According to the National Cyber Security Centre, this will lead to an increasing number and intensity of threats. These attacks are highly arbitrary, affecting citizens and various other (business) sectors. It is expected that the randomness of attacks will decrease and attacks will be more targeted in order to optimise profits. [8]
- Website defacements continue to occur, although the impact of such attacks is minimal. [8]
- Ransomware remains a prominent threat, although growth appears to be slowing down. A new revenue model for criminals, and therefore a possible future threat, is cryptojacking, the misuse of bandwidth and computer resources for cryptomining that can lead to the disruption of ICT facilities. [8] However, according to experts, it depends on the price of crypto coins that has fallen recently; a higher price makes it more interesting as a business model.
- Many breaches occur with stolen credentials. [8] Collecting login information (credential harvesting) is increasingly taking place in cloud applications, which are also used by institutions more often.
- Currently, cyberactors make extensive use of e-mail as a tool to disseminate malicious software or for phishing purposes. [8]
- In nearly half of all incidents in which data is stolen, hacking is used as a method. [6]

2.2 Motives: monetary gain, data as a commodity

- Three quarters of attacks are committed for financial gain. [6] That means that in fact all the data in possession of institutions have value. Data are worth money, this is something that is important to realise.
- There is a great deal of interest in personal data among various types of actors. Cyber attacks are being carried out in order to obtain this data. The data is used for credit card and identity fraud, among other things. [9]

- According to Verizon's Data Breach Investigations Report, [6] attacks within the education sector are mainly motivated by financial motives (70%), followed by espionage (20%) and fun (11%). [6] This illustrates that educational and knowledge institutions also have access to data from, for example, employees and students or research databases that are financially appealing to cybercriminals.
- The most common data to be compromised is personal data, followed by payment data and medical data. [8]
- Cyber attacks target agencies and individuals that are poorly protected or prepared. [6] Since cyber attacks in many cases take place at random, they can hit anyone. That makes those who don't prepare themselves also extremely vulnerable. [6]
- Cyber attacks are and will continue to be a profitable way of achieving specific (personal, economic or ideological) goals. The impact and proceeds of cyber attacks are growing under the influence of increasing digitisation. [9]

2.3 Actors: criminals and states/persons

- A large majority of digital attacks (73%) are committed by so-called outsiders, such as criminals and states. Nearly a third of attacks are carried out by insiders. [6] For example, IT administrators, temporary employees and users who have access to sensitive data. The risks involved here include data leaks because of carelessness or negligence and deliberate leakage of data. [10] This risk is difficult to detect and counteract because insiders often have legitimate access to confidential data. The 'insider threat' is often underestimated and is also more difficult to detect.
- Commercial institutions and public authorities in particular are targeted by state actors. [7]
- In addition to criminals and states, hacktivists, cyber criminals and insiders can cause disruption to business processes and theft of information. [9]

The Dutch ICT security company Fox-IT warns against the ransomware SamSam. This new form of ransomware first sabotages the backups and then locks the original files. It appears that dozens of companies in the Netherlands have already been affected by this ransomware. There are as yet no Belgian victims known to Fox-IT. [11]

2.4 Digital resilience: basic measures and unsafe products and services

- The National Cyber Security Centre (NCSC) warns that the digital resilience of the Netherlands is at risk. Organisations are vulnerable, even to attacks by simple means. The NCSC reports that incidents could have been prevented by taking basic measures, such as the timely implementation of security updates. Furthermore, increasing complexity and connectivity in the ICT landscape lead to vulnerabilities. [9]
- The National Cyber Security Centre warns against digitally unsafe products and services. According to the NCSC, they are a fundamental cause of many cyber incidents. It concerns, for example, the fact that suppliers do not (or no longer) make updates available and that it is not, or not easily, possible to install updates. [9]
- Most organisations do not have sufficient knowledge and skills to counter threats effectively. [7] An additional risk is that employees see cyber security primarily as the responsibility of the IT department, although cyber incidents are regularly related to human errors, such as the opening of spam mails or the frequent use of the same passwords. Also, IT still operates much too independently and too little in connection with other (staff) services and users, so that they do not strengthen each other sufficiently. [12]

- A concern among experts is the inability of institutions to secure sufficient qualified and specialist IT personnel. [12] The increased complexity of the field of work and the high demand in the market for such personnel lead to fierce competition to recruit and retain good specialists.
- There is a strong increase in the use of cloud services. [13] SURF is also experiencing an increase, as evidenced by the number of users of cloud services such as SURFcumulus (approximately 100 customers) and Microsoft Office 365 via SURFmarket (from around 100 at the end of 2017 to over 200 at the end of 2018). This makes these services an interesting target for hackers. [14]
- The ICT landscape of organisations is becoming increasingly complex, driven by increasing connectivity, organic growth and long lifespan of ICT systems. Add to this the increased use of cloud services and it is clear that it is becoming more difficult to keep track of and control over the ICT landscape. [9] The lack of a good understanding of one's own ICT systems within institutions is therefore seen by some experts as an underestimated risk. This concerns questions such as: where is our most sensitive data located, and how is our network architected? [12] According to Fox-IT, monitoring networks and endpoints is becoming increasingly critical as attackers use tools that are present on the networks and computers already. This requires insight into which tools and behaviours are different and which are not. [14]
- Security measures cost time and money, and the direct benefit of such preventive measures is either impossible or difficult to demonstrate. This can lead to conflicts of interest between, for example, greater resilience and the ease of use for individual users, or between the continuity of processes and the implementation of measures and security updates. These conflicts of interest can counteract the digital resilience of institutions. [9]
- If an attack is effective, there is little time to take preventive measures. This means that confidential data can be compromised within seconds or minutes. [6]

2.5 Reports of data leaks

On 25 May 2018, the General Data Protection Regulation came into force. The GDPR requires organisations to report a data breach to the National Data Protection Authority (AP). In 2018, a total of 20,881 reports were made to the AP, a sharp increase compared to previous years. The figure below shows the type of data leaks.

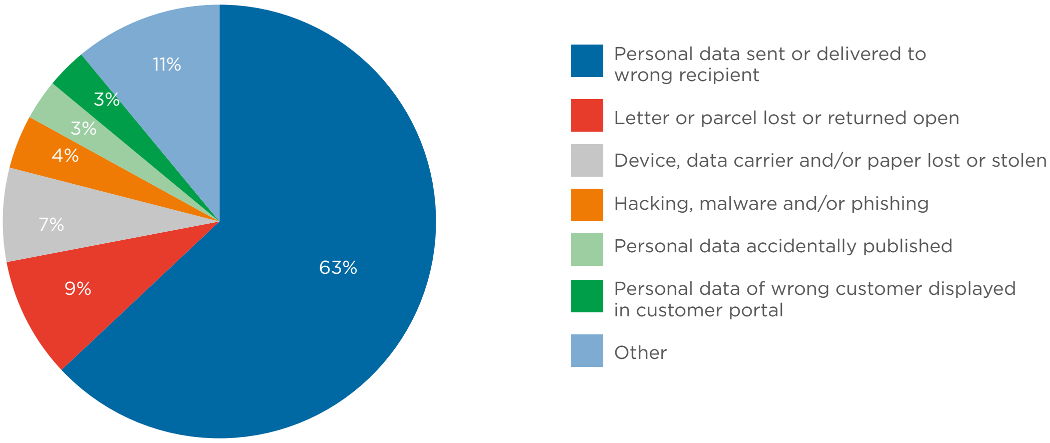


Figure 3: Types of data leaks [15]

In most cases, this involves sending or handing over personal data to the wrong recipient, for example by sending an e-mail with sensitive personal data to the wrong recipient. Name, gender and contact details are the most frequently leaked data. The Dutch DPA received more than 6000 reports of leaked medical data and social security numbers. Data leaks caused by hacking and phishing are particularly common in healthcare. For example, this could involve organisations that are bombarded with fake e-mails that seem to come from a reliable party, such as a business partner. By clicking on links or opening fake e-mails, there is a risk that a virus such as ransomware, which requires payment, will be installed. [15]

2.6 Trends observed at SURF

SURFcert

SURFcert offers affiliated institutions 24 x 7 support in the event of security incidents. Incoming reports are registered and categorised. When SURFcert starts dealing with a report, it becomes an incident. Some notifications are generated automatically when certain threshold values are exceeded.

All reports handled by SURFcert are distinguished as follows (see Appendix 2):

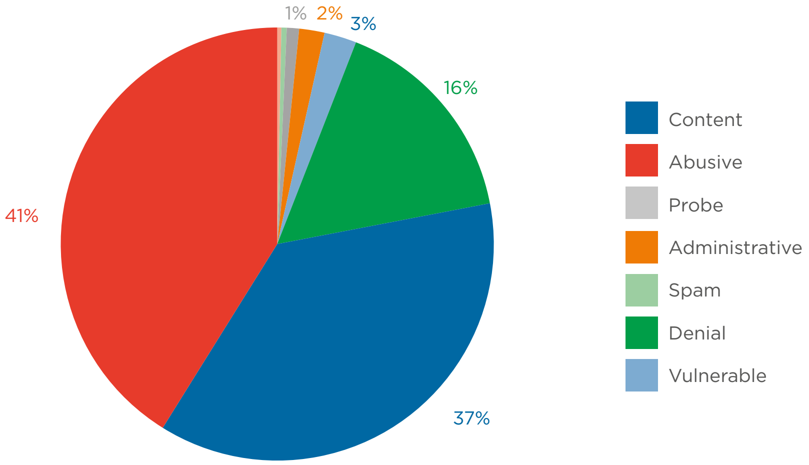


Figure 4: SURFcert type of incidents

Almost 80% of the incidents relate to systems at institutions that contain vulnerabilities known to SURFcert (vulnerable - 37%) and to systems that contact IP addresses that are known to be associated with malware (infected - 41%). The third major category of incidents (denial - 16%) relates to systems involved in a DDoS attack, usually as victims, sometimes as perpetrators, for example by searching for booter[1] services.

The following chart shows how many DDoS reports were received by SURFcert in 2018:

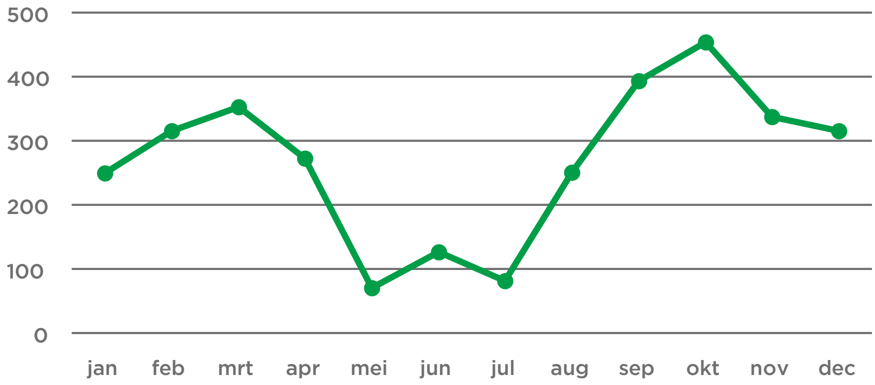


Figure 5: SURFcert; DDoS reports received (per month)

The figure above illustrates that there is a dip in the summer months, while more reports are received from January to April, and many more from August to December. Overall, the number of reports of DDoS attacks remains high throughout the year.

SURFmailfilter

SURFmailfilter checks and filters all incoming and outgoing e-mail for viruses, phishing and spam. At least 95% of spam is detected. About fifty of the institutions affiliated with SURF use SURFmailfilter.

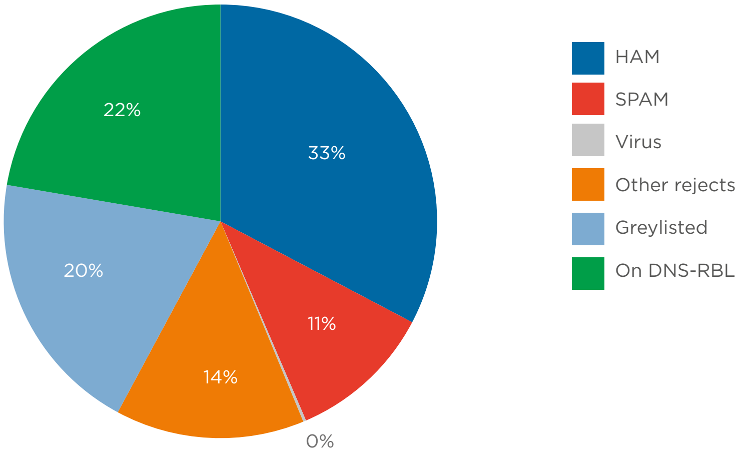


Figure 6: SURFmail filter; filtered e-mail categories

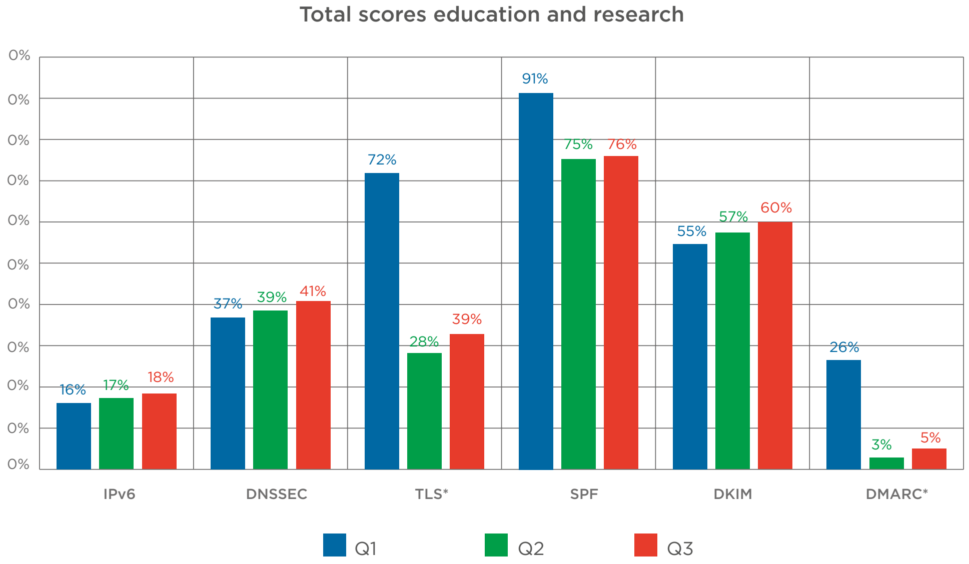
[1] A booter or stresser service, also known as DDoS-for-Hire, offers denial-of-service attacks. Many are offered as legitimate test tools over the Internet at low cost (See e.g. https://www.booter.pw/#pricing).

More than half of the mail (56%: On DNS-RBL, Greylisted and Other rejects) is blocked. The amount of mail that SURFmailfilter handles per day is normally between 2 and 5 million messages (with a peak of 20 million messages per day in December 2018 as a result of a spam run).

IV-measurements

Every six months, the Dutch Standardisation Forum carries out measurements against a number of Information Security Standards, the so-called IV-measurements. [16] The standards have been established by the Standardisation Forum and are on the so-called comply-or-explain list. This is a list of standards with which the (semi-)government must comply when purchasing and setting up ICT systems. SURF participates in the forum and spin-offs such as the Secure E-mail Coalition (VEC).

In this context, SURF has been carrying out quarterly IV-measurements for the education and research sector since April 2018. The measurement looks at IPv6 adoption, DNSSEC, TLS (according to NCSC guidelines), SPF, DKIM, and DMARC (the last 3 are secure e-mail standards). The chart below shows that there still is room for improvement, but that an upward trend* is also apparent:



Figuur 7: IV measurements 2018 (from April 2018)

*Note: Internet.nl adjusted the measurements and the calculation of the score after the Q2 measurement. As a result, the results of the TLS and DMARC measurements seem to have deteriorated.

3. CYBER THREATS EDUCATION AND RESEARCH

In the survey, we asked about a number of aspects of information security. In this chapter, we will look at institutions' risk perceptions, how often threats have actually occurred, to what extent there has been a change compared to 2017 and how much attention has been paid to a number of developments.

3.1 Risk perception

In the survey, we asked about the probability of a threat manifesting itself and about the impact of a threat if it manifested itself, both on a scale of 1 – 5. In addition, we make a distinction between the three columns education, research and business. In Table 5: Risk perception 2018, the risk perception is determined by multiplying the values for likelihood (L1 – L5) and impact (1 – 5). To determine when a score is high, medium and low risk, the following risk matrix has been established after discussion in the feedback group:

Impact:	1	2	3	4	5
L1	1	2	3	4	5
L2	2	4	6	8	10
L3	3	6	9	12	15
L4	4	8	12	16	20
L5	5	10	15	20	25

< 5 = Low **5-10** = Middle **> 10** = High

Table 4: Risk matrix

Risk perception 2018: Likelihood * Impact	Education	Research	Business operations
1. Obtaining and disclosing data	9,6	11,6	8,4
2. Identity fraud	10	8,1	9,2
3. Disruption of ICT	12,2	9,5	10
4. Manipulation of digitally stored data	8,2	9,7	8,4
5. Espionage	2,8	8,7	3,1
6. Take-over and abuse of ICT	10	9,1	9,9
7. Deliberately inflicting reputational damage	10,3	9,9	7,2

Table 5: Risk perception 2018

For education, the **top 3 risks** are (based on the numerical score):

1. Disruption of ICT (high)
2. Deliberately inflicting reputational damage (high)
3. Identity fraud/Take-over and abuse of ICT (medium)

The risk that scores lowest (and significantly lower than the other threats in the education sector) is espionage.

For research, the **top 3 risks** are (based on the numerical score):

1. Obtaining and disclosing data (high)
2. Deliberately inflicting reputational damage (medium)
3. Manipulation of digitally stored data (medium)

Whereas espionage scores low as a risk for the education and business operations sectors, this is not the case for the research sector. In this sector, espionage is considered to be a medium risk. The threats are all close to the highest risk category.

For business operations, the **top 3 risks** are (based on the numerical score):

1. Disruption of ICT (medium)
2. Take-over and abuse of ICT facilities (medium)
3. Identity fraud (medium)

The risk that scores lowest (and significantly lower than the other threats for business operations) is espionage.

Risk perception various sectors

Looking at the risk perception of different sectors, we notice that generally speaking the risk perception of the secondary vocational education (MBO) institutions is lower than the risk perception of universities and universities of applied sciences. This may be related to the assessment of one's own cyber resilience, but also to the notion that MBO institutions are not the sought-after target of cyber actors. Further clarification is desirable here. The research sector (universities of applied sciences and universities) assesses the risks higher across the entire spectrum of threats.

Risk perception compared to previous years

The risk perception of the threats in 2018 is clearly higher than in previous years. It is striking that in previous editions the threat of deliberately inflicting reputational damage of all sectors scored low. The introduction of the GDPR, with the risk of fines for non-compliance, may have led to a higher perception of the risks among institutions in 2018.

Risk perception 2017	Education	Research	Business operations
1. Obtaining and disclosing data	M	H	H
2. Identity fraud	H	M	L
3. Disruption of ICT	M	M	M
4. Manipulation of digitally stored data	H	L	L
5. Espionage	L	H	L
6. Take-over and abuse of ICT	L	M	M
7. Deliberately inflicting reputational damage	L	L	L

Table 6: Risk perception 2017

3.2 Actual occurrence of threats

This section provides a picture of the actual occurrence of threats: the frequency with which incidents have occurred in the past 12 months.

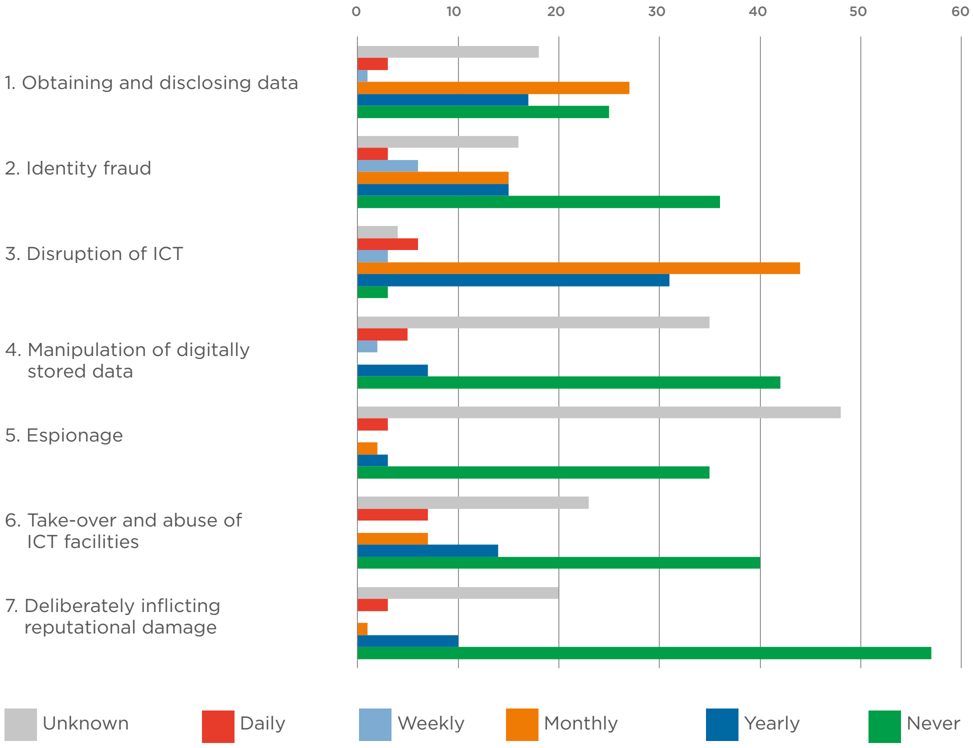


Figure 8: Incidents per threat (sum of education, research and operations)

Striking in Figure 8 is the large number of respondents who indicate that a number of threats have not manifested themselves at all, including reputational damage, the manipulation of digitally stored data and the take-over and abuse of ICT facilities. Apparently, these risks are managed well. Threats such as the disruption of ICT and the obtaining and disclosing data occur on a monthly basis. There are good mechanisms for reporting them, for example, incident registration systems are widespread and each institution has procedures for reporting data leaks.

It is also striking that a fairly high number of respondents indicated that they did not know how often incidents occurred. This applies in particular to espionage and manipulation of digitally stored data. The limited view of incidents is in line with the results of the 2017 SURFaudit benchmark, [4] which showed that the cluster 'control and logging' scores much lower than the maturity level recommended by SCIPR.

It should be noted that detecting threats such as espionage or data manipulation can be complicated (and may only come to light in case of a red-handed act or when the data files are checked specifically). This is in contrast to the disruption of ICT, which is more likely to have consequences in the physical reality: the malfunctioning of e-mail traffic and websites and the limited accessibility of systems. The chance of detection is greater.

Newsitem: Espionage

Dutch universities victims of Iranian hackers

In March it was announced that the United States had charged nine Iranian hackers with digital espionage at universities. Dutch universities are also reported to have been victims (which universities are not known). According to the United States, the hackers have stolen a total of 31 terabytes of documents and data: these are mainly scientific documents and other intellectual property. [17]

News article: human action

Data leak at Saxion University of Applied Sciences

In May, the data of 5100 students of Saxion University of Applied Sciences were publicly available for at least 24 hours. This includes the name, address, place of residence and e-mail address of the students, plus the books they ordered. During e-mail contact, a tab containing the students' personal details was accidentally sent along, after which these details were made public. [18]

3.3 Changes in cyber threats compared to 2017

Below are the results on whether cyber threats compared to 2017 have increased, decreased, remained the same or that this is not known. It should be noted that:

- the threat of obtaining and disclosing data, and identity fraud has increased the most
- and that manipulation of stored data and espionage have increased the least.

It should also be noted that the development of cyber threats is often not clear or known to the institutions.

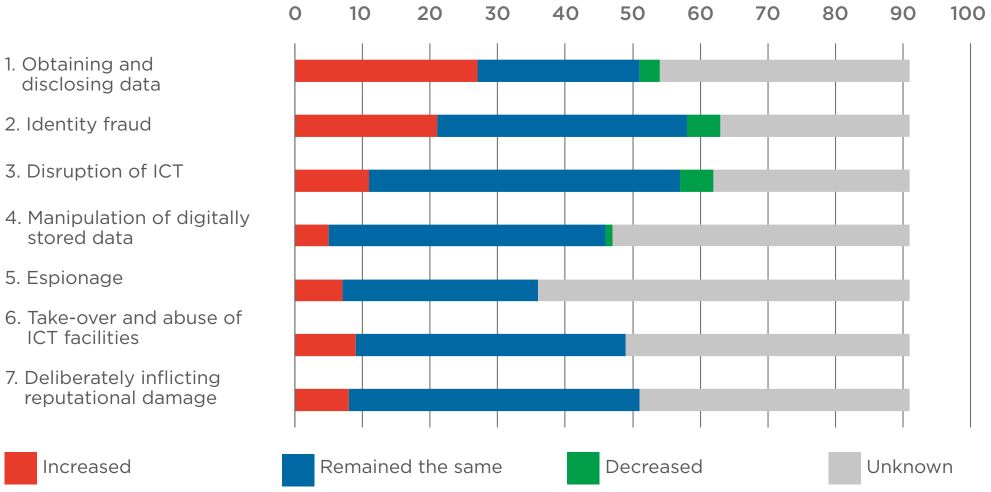


Figure 9: Changes in cyber threats compared to 2017

3.4 Focus on current trends

Institutions also pay attention to current trends in the field of ICT, because these may eventually have consequences for information security. In the survey, the participants indicated that they paid particular attention to DDoS attacks, Bring Your Own Device (BYOD) and Internet of Things (IoT). There is limited focus on developments such as Supervisory Control and Data Acquisition (SCADA)[2] and Blockchain.[3]

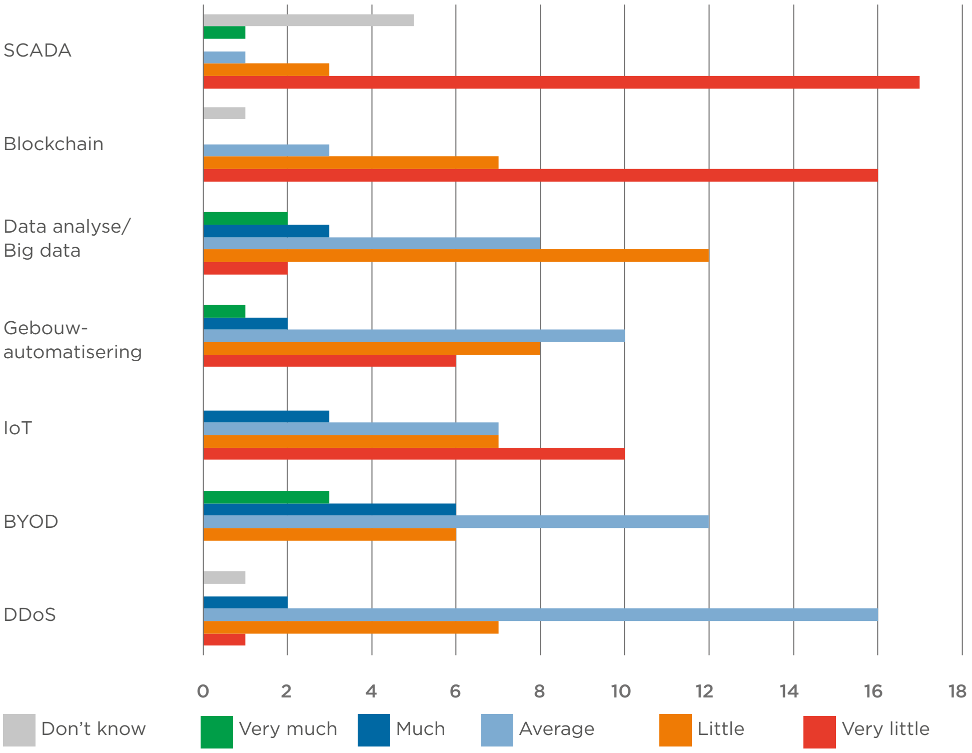


Figure 10: Focus on developments.

News article: human action

Mail bomb Avans University of Applied Sciences

A student from the Avans University of Applied Sciences accidentally sends an e-mail with a survey to a large group, creating a mail bomb: many people react to each other, so that all those e-mails end up in the hands of thousands of recipients. The e-mail addresses were visible to all participants. [19]

News article: human action

Personal data disseminated by mistake at the University of Twente

In May, an electoral list is mistakenly added to an e-mail sent to all students of the ITC department. The document contains personal and confidential information. The incident was immediately reported to the Data Protection Authority. [20]

[2] SCADA is the collection, processing and visualisation of machine measurement and control systems in large industrial systems.
[3] Blockchain is a system that can be used to record data such as transfers and personal deeds.

4. CYBER RESILIENCE

In this chapter, we will discuss the organisation of information security and how much attention it receives in the organisation.

4.1 Governance: management focus on information security

A majority of the respondents indicated that information security is on the agenda of the Executive Board and is explicitly included as a management portfolio.
This is in line with the results of the 2017 SURFaudit benchmark for the 'organisation and policy' cluster. Generally, institutions score well on having a policy approved by the management. However, they score less on the periodic (re-)assessment of the effectiveness and adequacy of information security policy. [4] The latter is important in view of the dynamics and changes that occur in threats and the environment in which institutions operate.

Information security on the agenda of the Executive Board

Yes	20
No	5
Unknown	2

Information security as the portfolio of the Executive Board

Yes	15
No	9
Unknown	3

At about half of the institutions, cyber security is also an item on the Supervisory Board's agenda, although a similar number of respondents also indicate that they do not know whether this is the case.

Information security on the Supervisory Board's agenda

Yes	12
No	2
Unknown	13

4.2 Organisation of information security

Capacity

Below are the results on the question of how much capacity your own institution has for information security in FTEs. No institution has more than 10 FTEs for information security; one institution has 5-10 FTEs, followed by 14 institutions with 2-5 FTEs. Although the required capacity depends on various variables (size, complexity, interests), no less than seven institutions indicate that they have less than 1 FTE at their disposal for information security.

The feedback group mentioned that awareness and knowledge at the tactical and operational levels within the institutions is a concern, as the organisational structure of the institution is seen as an obstacle to the implementation of information security policy.

Available information security capacity (in FTEs):

🟦	**< fte**	7
🟥	**1 fte**	2
🟩	**2 – 5 fte**	14
🟧	**5 – 10 fte**	1
🟦	**> 10 fte**	0
⬜	**Unknown**	3

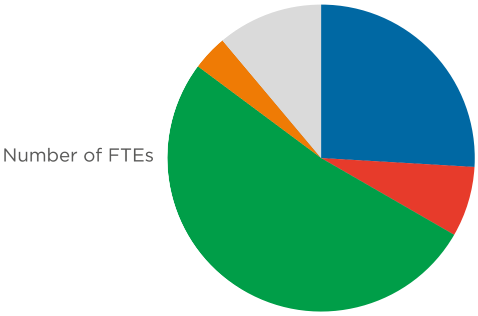


Figure 11: Number of FTEs for information security

Budget

Below are the results of the question about the available budget within the own institution for information security:

- Five institutions spend more than 200,000 euros a year on information security.
- Eight institutions have less than EUR 50,000 available for information security on an annual basis.
- For six participants it is unknown what budget is available.

🟦	**< €50k per year**	8
🟥	**€50k - €100k per year**	4
⬜	**€100k - €200k per year**	4
🟧	**> €200k per year**	5
🟦	**Unknown**	6

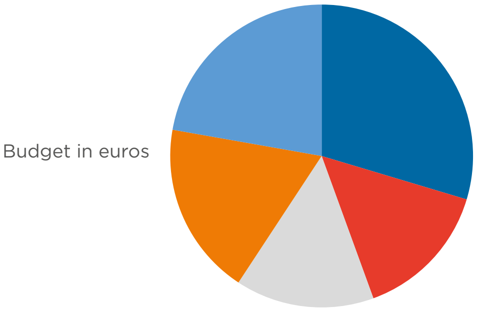


Figure 12: Available budget for information security

The budget for information security (as part of the total ICT budget) of the institutions is between 1 and 5% for eleven institutions. Fourteen participants did not know the percentage of budget that is available for information security.

These numbers are well below the so-called ‘10% standard’ that the Cyber Security Council advocates in its report ‘The economic and social need for more cyber security – Keeping dry feet in the digital era’. A global analysis shows that globally on average 10 percent of the IT budget is spent on cyber security and privacy measures. The Committee recommends that this standard be adopted as a guideline for Dutch government and other public institutions. [21]

Available budget for information security (as a percentage of the total ICT budget):

🟦	< 1 %	1
🟥	1 - 5%	11
⬜	5 - 10%	1
🟧	10 - 20%	0
🟦	> 20%	0
🟩	Unknown	14

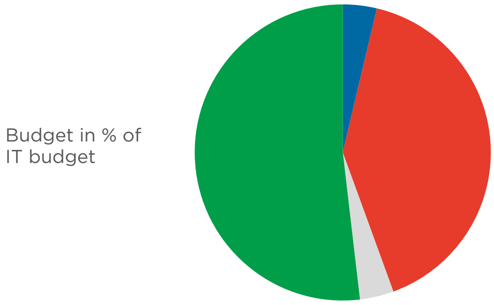


Figure 13: Investment in information security

Corporate (Information) Security Officer

Six institutions indicate that they do not have a CISO (or CSO). The reason given is the size of the organisation. When asked whether the CISO (or CSO) has sufficient mandate and capacity to monitor and advise independently, opinions are divided:

Sufficient capacity and CISO/CSO mandate?

Agree	10
Disagree	11
No CISO	6

Where is information security in place?

Fifteen institutions indicate that information security is not the task of the IT department or its employees alone. However, eleven institutions indicate that this is the case: within these institutions, information security is primarily the task of IT. This supports the trend depicted in chapter 2, in which experts point out that information security is seen by employees as an ‘IT thing’. But they also point out that IT still operates very independently and that there is too little cooperation with other services. [12]

Information security is the primary task of IT:

Yes	11
No	15
Unknown	1

An example showing that various services and departments play a role in cyber resilience, is the national cyber crisis exercise OZON. 50 institutions participated in this exercise in 2018. The aim was to test cyber resilience. [22] [23] The simulated cyber scenario started relatively innocently, but slowly expanded into a real “cyber crisis” with impact in many areas: in addition to IT and CERT, departments, legal, communication and management.

4.3 Cyber resilience

Investments in cyber resilience

Institutions mainly invest in firewalls and in the awareness of their own employees. But also in raising employee awareness, which is good in view of the institutions' low score on this in the 2017 SURFaudit benchmark. [4] It appears that the institutions are devoting more attention to the training of their staff on policies and procedures, and instructions for contractors. On the other hand, hardly any investments are made in the awareness of external parties, participation in the national cyber crisis exercise OZON* and the so-called Computer Emergency Response Team (CERT).

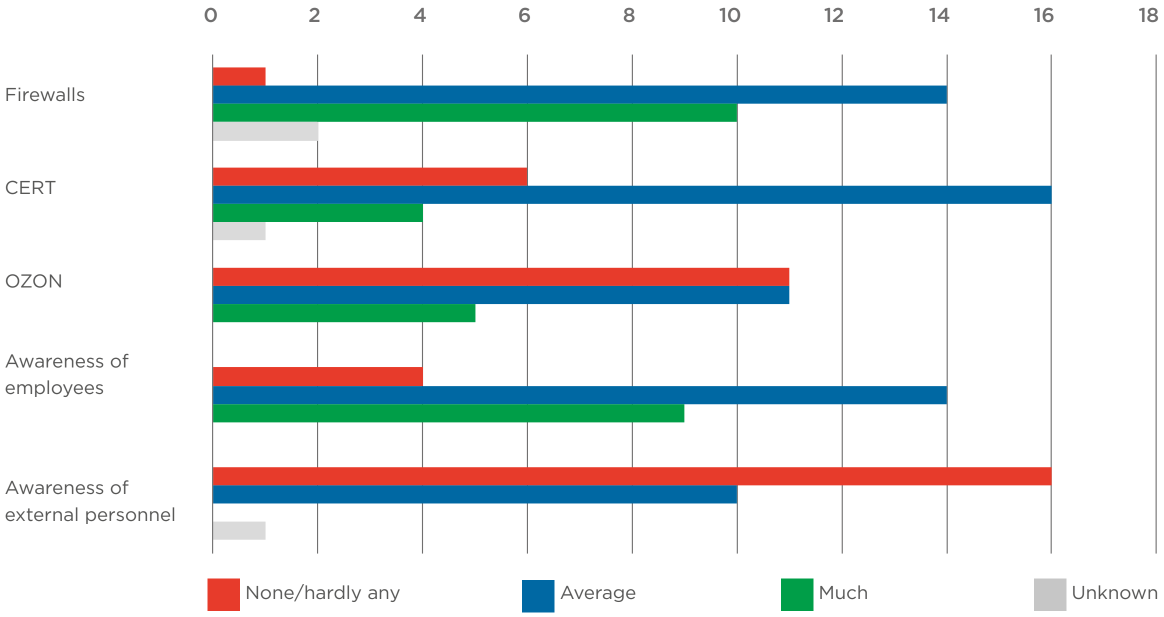


Figure 14: Investment in cyber resilience

* Note: The low investment in the cyber crisis exercise OZON mentioned here does not seem to be in line with the actual participation in OZON, in which 40 of the 50 participating institutions have registered at a silver/gold level, which has required a significant investment in in terms of time and manpower.

In addition, institutions indicate that they invest in:

- checks that the policy adopted is being implemented (SURFaudit),
- performing Pentests, which provide insight into the status of an IT organisation,
- zoning and central logging/monitoring,
- new CISO,
- governance,
- support in resources of programmes to increase resilience and improve awareness.

Assessment of own cyber resistance

Respondents assess their own organisation's cyber resilience on average with barely sufficient score (5.5 on a scale of 0-10). This is in line with the results of the 2017 benchmark, in which institutions scored below the recommended level for all clusters. [4] Based on these results, there is room for further improvement of information security within institutions.

One institution assesses its own resilience with a score of 8, six institutions give themselves a score of 7 and nine institutions a score of 6:

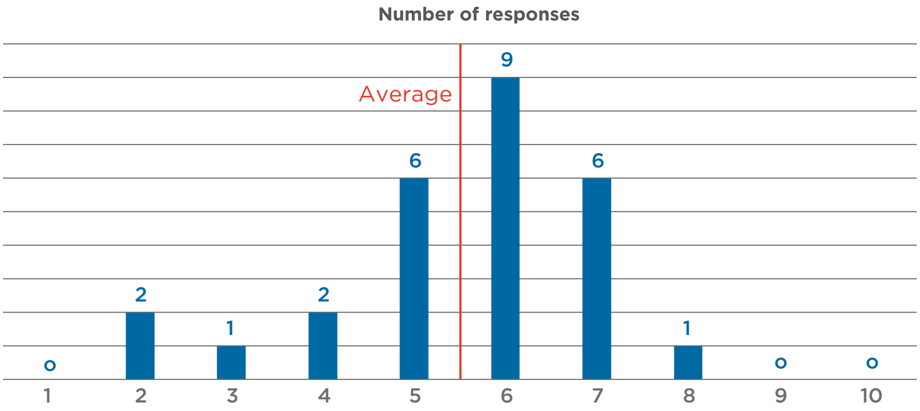


Figure 15: Number of responses per resilience level (survey)

Also, the fact that the secondary vocational schools (MBO) that have answered this question estimate their resilience to be relatively high (7) stands out. This may be related to their perception of risk: the MBO institutions have a low estimate of the risks for their own institution. In addition they cooperate very well in the area of IT and specifically information security.

Vulnerabilities

The respondents indicated the available capacity and expertise, the complexity of ICT systems and the awareness of students as significant vulnerabilities, including:

- specialised knowledge and staff training required,
- hiring specialists,
- ownership of information and regulation (authorisation) and
- awareness through the introduction of the GDPR.

This is in line with the trend depicted in chapter 2, in which the concern was shared that many organisations lack the knowledge and skills to effectively counter threats. [7]

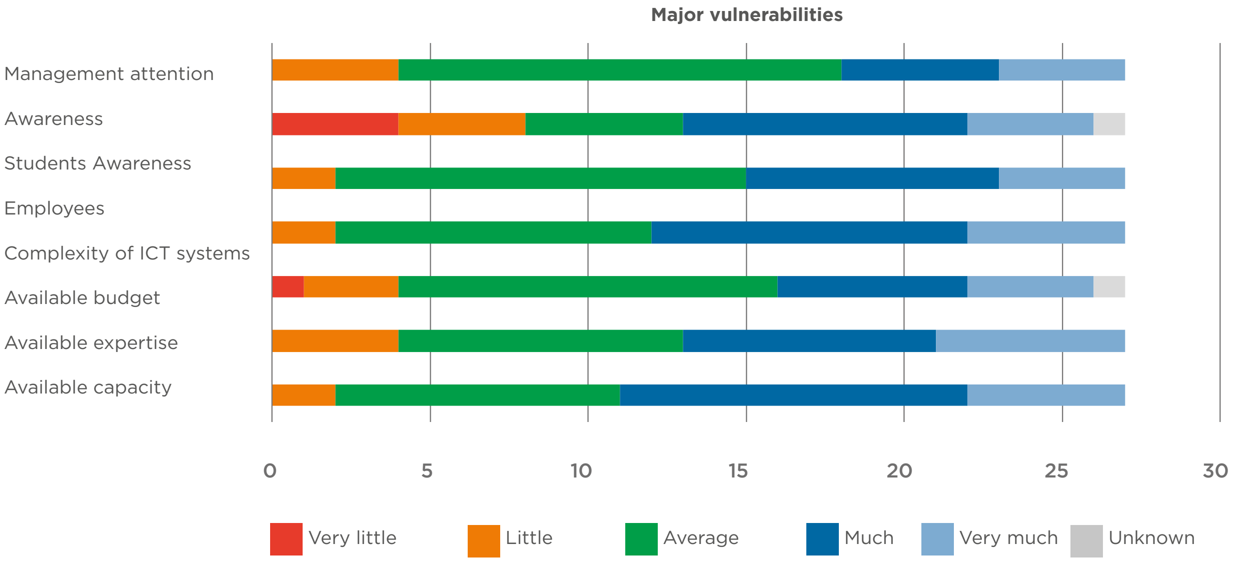


Figure 16: Relevance of vulnerabilities

News article: Phishing mails

Phishing mails at the University of Groningen
On New Year's Day, employees and students of the University of Groningen receive an e-mail with the subject 'SAFETY INFORMATION!'. The mail seems to come from the ICT department and contained a link to a website where the username and password of the university account have to be entered for verification. [24]

Phishing mails at the University of Twente
On Monday 19 March, the University of Twente received reports of phishing e-mails sent to employees of the university. The subject of the mail is 'Migrate,' which makes the phishing extra tempting as the university is busy migrating the Exchange/Outlook environment at that moment. [25]

Threats under control

The threats that respondents felt were best controlled were:

- Disruption of ICT (score 6.3)
- Take-over and abuse of ICT (score 5.9)
- Manipulation of digitally stored data (score 5.9)

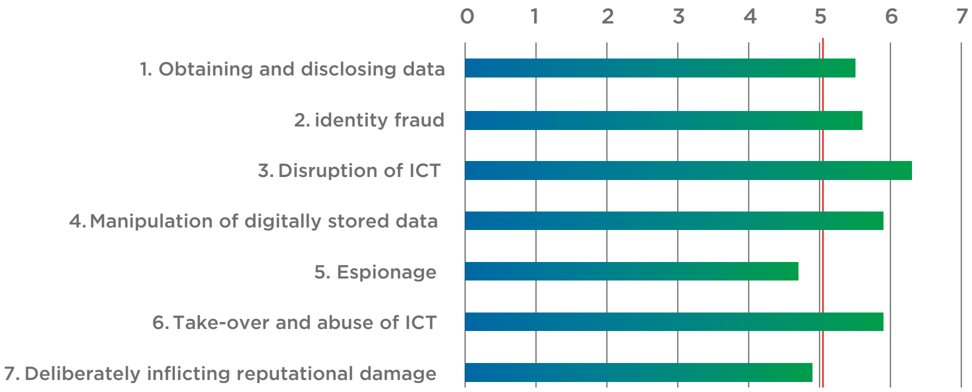


Figure 17: Degree of threat control (on a scale of 1 – 10)

The institutions regard espionage and deliberately inflicting reputational damage as the threats that are the least under control. They score lower than 5 on a scale of 10.

5. HIGHLIGHTS AND REFLECTION FOR MANAGEMENT

In this concluding chapter, we will focus on some of the highlights of the cyber threat assessment report (taken from chapters 2 to 4) with the purpose of informing administrators about current cyber trends and risks. Finally, we provide five points for reflection that managers can use for the dialogue on cyber risks and resilience in their own institutions.

5.1 Highlights for management

1. **The risk perception of cyber threats in 2018 is clearly higher than in previous years.** It is striking that in previous editions the threat of deliberately inflicting reputational damage in all sectors scored low. The introduction of the GDPR, with the risk of fines in the event of failure to comply, may have lead to a higher perception of the risk among institutions in 2018.

2. **The cyber threat top 3 varies by sector.** For education and business operations, the disruption of ICT facilities is the most important threat. Therefore, this threat has a fairly direct effect on the continuity of the primary (educational) process, a crown jewel. For the research sector, obtaining and disclosing data is the most important threat. This threat also directly affects a crown jewel of institutions, namely the intellectual property/integrity of research and personal data. Reputational damage is also seen as an important threat.

Risk perception 2018: Likelihood * Impact	Education	Research	Business operations
1. Obtaining and disclosing data	M	H	M
2. Identity fraud	M	M	M
3. Disruption of ICT	H	M	M
4. Manipulation of digitally stored data	M	M	M
5. Espionage	L	M	L
6. Take-over and abuse of ICT facilities	M	M	M
7. Deliberately inflicting reputational damage	H	M	M

Table 7: Risk perception 2018

3. **Disruption of ICT, take-over and abuse of ICT, and manipulation of digitally stored data are threats that are best controlled.** The institutions regard espionage and deliberately inflicting reputational damage as threats that are the least under control.

4. **In addition to criminals and states, hacktivists, cyber criminals and insiders can cause disruption to business processes and theft of information.** As the complexity of attacks increases, cybercriminals benefit from tried-and-true attack techniques such as hostage-taking software, DDoS and hacking.

5. **The information position on cyber incidents is very limited.** The limited information position of institutions about cyber incidents stands out. A significant number of the institutions have no insight into the number of incidents that take place, which is cause for concern. It may be that the respondent in question has no insight into this, but it may just as well be that incidents are not registered or, more alarmingly, are not noticed. This makes the ICT facilities and data of institutions vulnerable. In addition, a better information position can help institutions to take risk-driven measures.

6. **There are concerns about the order of basic measures and about digitally insecure products and services.** The concerns expressed earlier about the digital resilience of organisations are still an issue. [21] This year, the National Cyber Security Centre once again draws attention to the vulnerability of institutions and calls for basic measures to be taken, such as the timely implementation of security updates. This is necessary, bearing in mind the increasing complexity and interconnectedness of ICT facilities.

7. **Overview ánd management of their own ICT landscape are becoming increasingly difficult for organisations.** Because of increasing connectivity, organic growth of ICT systems and the growing use of cloud services, having and maintaining an overview and control of the ICT systems and facilities are becoming increasingly complex.

8. **On average, institutions rate their own cyber resilience with a low rating.** Participants rate their own institution's digital resilience with an average of 5.5 (on a scale of 0-10). This is in line with the results of the 2017 benchmark, in which institutions scored below the recommended level for all clusters. [4] Among the major vulnerabilities mentioned by the institutions are the the available capacity and expertise, the complexity of ICT systems and the awareness of students and staff. The budget for information security as part of the total ICT budget is well below the so-called '10 percent standard' of the Cyber Security Council. [21]

5.2 Points for reflection

Cyber security requires a joint effort on the part of ICT specialists, legal experts and privacy staff. Regular staff, teachers and students can contribute by adopting best practices and instructions on authorisation, privacy, password management and software updates. However, in view of the possible impact of cyber risks on institutions[4], management involvement is a must. For the purposes of the management dialogue on cyber security, we have included five questions for the board table, fed by the results of this Cyber Threat Assessment report.

These questions can be used by managers (in consultation with their Corporate (Information) Security Officer, directors of services and faculty directors, Supervisory Board) to discuss the cyber risks and resilience of their own institution.

Topic	Explanation	Management reflection
Cyber risk profile	The impact of cyber threats depends on the risk profile of institutions.	What does your cyber risk profile look like?
Ambitions	Institutions can prepare themselves for cyber threats in different ways. Guidelines and recommended maturity levels are available via SCIPR/SURFaudit.	What is your level of ambition in terms of digital resilience?
Information position	There is limited insight into the numbers and impact of cyber incidents at educational institutions.	What is your information position on cyber incidents?
Cyber security policy	In addition to information security, investing in detection and incident response pays off. This is based on the fact that 100% prevention of cyber incidents is unrealistic.	What are the cyber security policies of your institution and how are prevention and incident response balanced?
Evaluation	Dynamics in cyber threats call for periodic evaluation and reassessment.	How do you monitor cyber threats?

Table 8: Questions for reflection

[4] The COT, together with Erasmus University Rotterdam, evaluated the handling of a data breach in 2016. One of the findings concerned the management nature of such incidents. [26]

APPENDIX 1
CYBER THREATS

The seven threats and possible manifestations defined in previous editions of the Cyber Threat Assessment report:

	Type of threat	Manifestation of threat
#	Type of threat	Incident
1	Obtaining and disclosing data	→ Research data is stolen
		→ Privacy-sensitive information is leaked and published
		→ The blueprint of a research institution's set-up falls into the wrong hands
		→ Fraud committed through the acquisition of data on exams and assignments
2	Identity fraud	→ A student engages someone else to take an exam
		→ A student pretends to be another student or a staff member to gain access to exams
		→ An activist pretends to be a researcher
		→ A student pretends to be a staff member in order to manipulate grades
3	Disruption of ICT	→ DDos attack paralyses the IT infrastructure
		→ Critical research or exam data is destroyed
		→ A research institution's set-up is sabotaged
		→ Research resources are made unusable by malware (e.g., eLearning, or the network)
4	Manipulation of digitally stored data	→ Study results are falsified
		→ Manipulation of research data
		→ Adjustments to business management data
5	Espionage	→ Research data is stolen
		→ Intellectual property is stolen through a third party
		→ States check up on foreign students
6	Take-over and abuse of ICT	→ Setup of research institutes taken over
		→ Systems or accounts are misused for other objectives (botnet, mining, spam)
7	Deliberately inflicting reputational damage	→ Website is defaced
		→ Social media account is hacked

Table 9: Threats to education and research

APPENDIX 2
SURFCERT
TYPE OF INCIDENTS

#	Categories	Explanation
1	content	traffic that is filtered because of illegal content, such as illegal downloads
2	abusive	institutional traffic causing nuisance
3	probe	institution traffic to collect information
4	administrative	non-technical issues, including, for example, investigation requests
5	spam	spam traffic
6	denial	reports of systems involved in a DDoS attack
7	vulnerable	reports about institution systems where known vulnerabilities were found by SURFcert
8	infected	systems that contact IP addresses known to be associated with malware

Table 10: SURFcert type of incidents

BIBLIOGRAPHY

[1] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/over-ons/. [Opened 01 2019].

[2] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/wp-content/uploads/COT-Dreigingsbeeld-Onderwijs-2018.pdf. [Opened 01 2019].

[3] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/). [Opened 01 2019].

[4] B. Bosma, "Report SURFaudit benchmark 2017," [Online]. Available: https://www.surf. nl/kennisbank/2018/rapport-surfaudit-benchmark-2017.html. [Opened 01 2019].

[5] B. Bosma, „SURF Cyber Threat Assessment report 2017," [Online]. Available: https://www.surf.nl/kennisbank/2017/cyberdreigingsbeeld-2017-publicatie.html. [Opened 01 2019].

[6] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Opened 01 2019].

[7] ENISA, „Threat Landscape 2017," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. [Opened 01 2019].

[8] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Opened 01 2019].

[9] NCSC, "Cyber security Analysis Netherlands 2018: Digital threat in the Netherlands is increasing," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Opened 01 2019].

[10] Crowd Research Partners, „Insider Threat Report 2018," [Online]. Available: https://crowdresearchpartners.com/portfolio/insider-threat-report/. [Opened 01 2019].

[11] Computable, "Fox-IT warns of ransomware SamSam," [Online]. Available: https://www.computable.nl/artikel/nieuws/security/6524994/250449/fox-it-waarschuwt-voor-ransomware-samsam.html. [Opened 01 2019].

[12] Verdict Encrypt, „What Cybersecurity Risks Are Companies Currently Underestimating the Most?," 03 2018. [Online]. Available: http://verdict-encrypt.nridigital.com/verdict_encrypt_mar18/what_cybersecurity_risks_are_companies_currently_underestimating_the_most_34_experts_have_their_say#_blank. [Opened 01 2019].

[13] CBS, „CBS Cybersecuritymonitor 2018," [Online]. Available: https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018. [Opened 01 2019].

[14] Fox-IT, "The threats of 2017 and the trends of 2018," [Online]. Available: https://www.fox-it.com/nl/insights/blogs/blog/dreigingen-2017-en-trends-2018/. [Opened 01 2019].

[15] Dutch Data Protection Authority, 'Notification of data breaches: facts & figures 2018,' [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2018.pdf. [Opened 01 2019].

[16] Standardisation Forum, "Standardisation Forum," [Online]. Available: https://www.forumstandaardisatie.nl/. [Opened 01 2019].

[17] NU, "Dutch universities victim of Iranian state hackers," 23/03/2018. [Online]. Available: https://www.nu.nl/internet/5191589/nederlandse-universiteiten-slachtoffer-van-iraanse-staatshackers.html. [Opened 01 2019].

[18] NOS, "Data from Saxion University of Applied Sciences students on the street through datalek," 01/05/2018. [Online]. Available: https://nos.nl/artikel/2229926-gegevens-studenten-hogeschool-saxion-op-straat-door-datalek.html. [Opened 01 2019].

[19] Brabants Dagblad, "Mail bomb at Avans Hogeschool: hundreds of nonsense messages, thousands of e-mail addresses reached, but not visible," 24/05/2018.

[Online]. Available: https://www.bd.nl/den-bosch-e-o/mailbom-bij-avans-hoge-school-honderden-onzinberichten-duizenden-e-mailadressen-bereikt-maar-niet-zichtbaar~af4f7d43/. [Opened 01 2019].

[20] Tubantia, “UT is e-mailing personal details of 500 students around,” 29/05/2018. [Online]. Available: https://www.tubantia.nl/enschede/ut-mailt-persoonlijke-gegevens-van-500-studenten-rond~ab17c443/. [Opened 01 2019].

[21] Cyber Security Council, “The economic and social need for more cyber security, 2016,” 09/2016. [Online]. Available: https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf. [Opened 01 2019].

[22] SURF, “Cyber crisis exercise OZON,” [Online]. Available: https://www.surf.nl/diensten-en-producten/surfcert/cybercrisisoefening-ozon/index.html. [Opened 01 2019].

[23] Tweakers, “OZON 2018 - A look behind the scenes at a major cyber-principle exercise,” 06/10/2018. [Online]. Available: https://tweakers.net/reviews/6605/ozon-2018-een-kijkje-achter-de-schermen-bij-een-grote-cyberincidentoefening.html. [Opened 01 2019].

[24] Computable, “RUG tightens security after phishing,” 03/01/2018. [Online]. Available: https://www.computable.nl/artikel/nieuws/security/6273951/250449/rug-scherpt-beveiliging-aan-na-phishing.html. [Opened 01 2019].

[25] University of Twente, “Phishing mail warning,” 19 03 2018. [Online]. Available: https://www.utwente.nl/nieuws/!/2018/3/201267/phishing-mail-waarschuwing. [Opened 01 2019].

[26] L. v. d. Varst, “Dynamics around a new crisis type: lessons from the response to a data breach at Erasmus University Rotterdam,” 04/12/2017. [Online]. Available: https://www.linkedin.com/pulse/dynamiek-rond-een-nieuw-crisistype-lessen-uit-de-op-van-der-varst/. [Opened 01 2019].

COLOPHON

Authors
Bart Bosma
(SURFnet)
Laurens van der Varst
(COT Institute for Security and Crisis Management - an Aon Company)

Editors
Jan Michielsen
(SURFnet)

Design
Vrije Stijl, Utrecht

Print
Drukkerij Libertas Pascal

Photography
QUT Science and Engineering

Februari 2019

This report has been produced partly thanks to contributions from the feedback group consisting of:

Maarten Veldhuis	*Rijn IJssel*
Roeland Reijers	*University of Amsterdam*
Marcel van der Kolk	*Utrecht University*
Hendrik Jan Buist	*Utrecht University*
Rob van Duin	*The Hague University of Applied Sciences*
Edwin Hubers	*University of Applied Sciences Leiden*
Rienk de Vries	*Albeda College*
Remon Klein Tank	*Wageningen University & Research*
Bart van den Heuvel	*Maastricht University*
Eric van den Beld	*Saxion University of Applied Sciences*
Matto Franssen	*University of Groningen*
René Ritzen	*Utrecht University*
Dubravka Marović	*Leiden University*

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