

CYBER THREAT ASSESSMENT 2016

EDUCATION AND RESEARCH SECTORS



English version

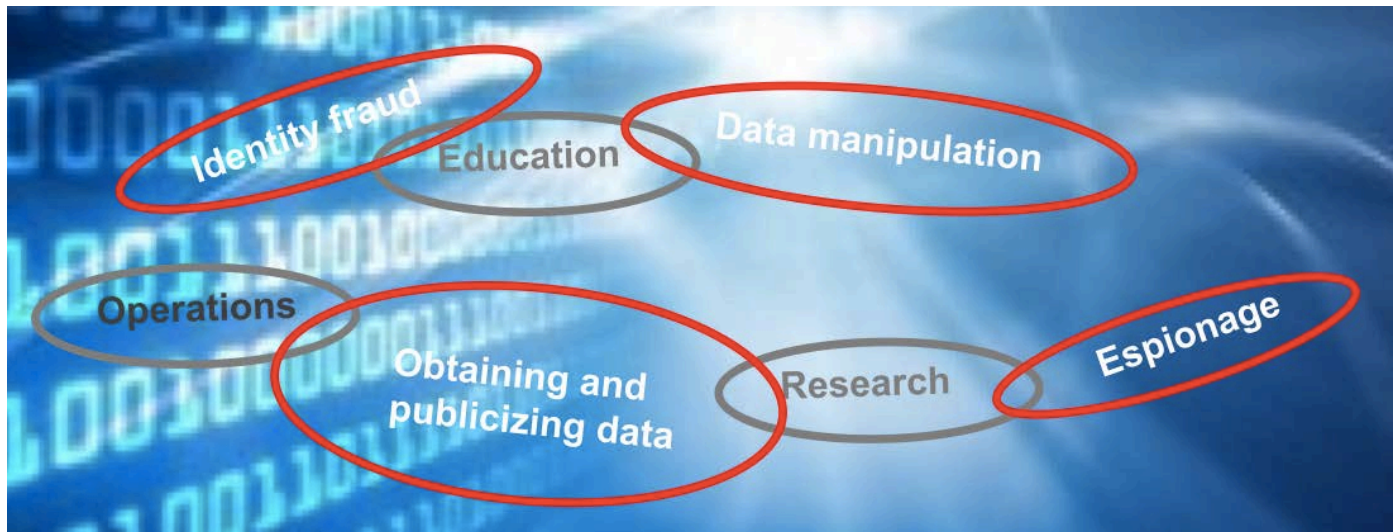
Author(s): Bart Bosma
Version: 1.0 (abridged)
Date: May/June 2017

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 - 787 30 00
admin@surfnet.nl
www.surf.nl/surfnet

ING Bank NL54INGB0005936709
KvK Utrecht 30090777
BTW NL 0089.60.173.B01



Preface

The reporting requirement for data leakage that went in effect on January 1st, 2016 was high on the agenda of security officers in education and research. Nevertheless, it seemed that no-one realized beforehand that the new reporting requirement would have so many consequences for handling personal data and for the way in which they should be protected.

Furthermore, since January 1st, 2016, the Privacy Authority (formerly the College for Protection of Privacy Data) has the power to impose heavy fines to violators. In this respect, the European General Data Protection Regulation, which will come into force in mid-2018, is the next hurdle to be taken. Then, even more stringent requirements for the protection of personal data come into force and, in case of non-compliance, even heavier fines will be given.

At the same time, we have seen a huge increase in the number of ransomware attacks in the education and research area, which could lead to data loss. Data leaks must be reported to the Privacy Authority, but they feel that the number of reported data leaks is low considering the total number of data processors in the Netherlands.

Cyber security is all over the news, and the SURF member institutions cannot avoid thinking about what they need to do to bring their cyber resilience to a higher level, thus lowering the risk of reputational and financial damage as much as possible. The cyber crisis exercise Ozon, organized by SURF in October 2016 shows that education and research institutions are very serious about cyber security. More than 200 employees from 30 affiliated institutions participated in the exercise. The exercise showed that the institutions are well prepared for attacks and that those involved are able to escalate to the administrative level within their own organization quickly. The exercise made the institutions realize more than ever that a cyber crisis is realistic and can have a major impact on the primary process.

To provide education and research institutions with insight into the major threats to the sector, and to make you understand what measures you could take to overcome these threats, we present to you the Cyber Threat Assessment 2016 report.

Erik Fledderus
CEO SURF

Table of contents

Preface	2
Summary	4
1 Main Findings	7
1.1 Cybercrime is on the radar	7
1.2 Impact of cyber threats.....	7
1.3 Trends	7
1.4 This report's purpose is to increase resilience	8
1.5 About this edition	8
1.6 Relationship with SURF-services	8
1.7 Reading guide	8
2 Threat landscape	9
2.1 Introduction: general threats	9
2.2 Threats for the sector education and research	11
3 Threats for each process	21
3.1 Introduction	21
3.2 Education process.....	23
3.3 Research process	26
3.4 Operations.....	29
4 Resilience	31
4.1 Introduction	31
4.2 Measures	31
5 Bibliography	35
6 Contributors	36

Summary

Increased focus on cybersecurity

Society is paying more attention to cybersecurity. Aside from the Cyber Security Assessment Netherlands 2016 report, published on September 5th, 2016, a number of other reports were published emphasizing the importance of a solid cybersecurity posture. Also, directors and board members are becoming more aware of cybersecurity, in part because of the addition of the data breach notification effective January 1st, 2016.

Enhance cybersecurity posture

This report shows which threats in the cyber domain, our digital world, are relevant to educational and research institutions and thus offers tools for organizations to enhance their cybersecurity posture.

Minimize risks

Because the reputational or financial damage caused by a cyberattack can be substantial, it is very important to minimize the risks. In table 1, the threats that are relevant for educational and research institutions are listed:

#	Type of threat	Manifestation of the threat	Risk level		
			Education	Research	Operations
1	Obtaining and publicizing data	<ul style="list-style-type: none"> Research data is stolen Privacy data is leaked and published Research blueprints of research institutions fall in the wrong hands Fraud by obtaining exam and exercise data 	MEDIUM	HIGH	MEDIUM
2	Identity fraud	<ul style="list-style-type: none"> Student has someone else take his/her exam Student impersonates another student or teacher to obtain exams Activist poses as a researcher Student impersonates teacher or employee to manipulate study results 	HIGH	MEDIUM	LOW
3	Disruption of ICT	<ul style="list-style-type: none"> DDoS-attack shuts down IT-infrastructure Critical research data or exam data is destroyed Setup of research institutions is sabotaged Educational resources are unusable because of <i>malware</i> (e.g. eLearning or the network) 	MEDIUM	MEDIUM	MEDIUM
4	Manipulation of digitally stored data	<ul style="list-style-type: none"> Study results are tampered with Research data is manipulated Operational data is changed 	HIGH	LOW	LOW
5	Espionage	<ul style="list-style-type: none"> Research data is tapped Intellectual property is stolen through a third party Foreign students under control of foreign state 	LOW	HIGH	LOW
6	Take-over and abuse of ICT	<ul style="list-style-type: none"> Setup of research institution copied Systems or accounts misused for other purposes (<i>botnet</i>, <i>mining</i>, <i>spam</i>) 	LOW	MEDIUM	MEDIUM
7	Deliberately inflicting reputational damage	<ul style="list-style-type: none"> Web site compromised Social media account hacked 	LOW	LOW	LOW

Table 1: Relevant threats for educational and research institutions

Most prevalent threats

For the education process manifestation of the following threats is most likely:

- *Manipulation of digitally stored data*
Mostly concerns study results and exam materials. Measures to counter data manipulation include cryptographic techniques to assure the integrity and confidentiality of the data.
- *Identity fraud*
With the increased use of digital forms of education and testing, being able to irrefutably establish someone's identity becomes more important. If there is no adequate assurance that someone's identity is correct, the risk of unauthorized access becomes high, for instance because it is possible to alter grades or steal exams.

For the research process manifestation of the following threats is most likely:

- *Obtaining and publicizing data*
During many research projects, sensitive data is processed and stored. Also, certain research can be socially sensitive. Measures to avoid obtaining and publication of this kind of data and information about sensitive research include using cryptographic techniques, proper access controls and a high level of cyber awareness.
- *Espionage*
Research institutions possess potentially valuable data and knowledge, which can be of high interest to both criminals and states. Although information is somewhat intangible as little is publicly disclosed, according to the AIVD's annual report and the NCSC's Cyber Security Assessment Netherlands 2016 report espionage is a fact in the Netherlands. Measures primarily focus on detecting attempts to break into the network and to exfiltrate data. They include system and network logging and log analysis to recognize patterns.

For the operations manifestation of the following threats is most likely:

- *Obtaining and publicizing data*
All kinds of sensitive data, including personally identifiable information (PII), are processed in the context of business operations. If they fall into the wrong hands, reputational damage can be immense and, additionally, overseeing authorities can issue heavy penalties. Measures to avoid the obtaining and publication of sensitive data and PII include cryptographic techniques, proper access controls and a high level of cyber awareness.

Resilience

This report is one of the deliverables of the SURF innovation program "Reliable and Safe Environment". The program's ambition is for SURF and its member institutions to be immune for cyber incidents and cyberattacks by 2018. Immune means that, in spite of incidents, the availability and reliability of information and systems remain at a high level and the cost of repair and damages are low. As a result, recovery is swift and doesn't come at the expense of an open and freely accessible internet.

To reach that goal, institutions should take measures to increase their cyber resilience. Traditional protection techniques such as firewalls are not effective anymore, because in many cases users are not located within the perimeter of the institution. Moreover, nowadays data are processed and stored in the cloud more often than not, which affects the type of measures that are required. Data classification is of the utmost importance to determine which measures are adequate to protect the data, before exchanging it among users or with users from other institutions or third parties.

Preparation

Before implementing any measures the institution's board should have a good overview of the general threat landscape, know which threats are relevant for the organization, be aware of the crown jewels of the organization and have an idea of which data are processed or stored in the cloud.

Furthermore, it is important for the board to know the status of its own institution's cyber resilience and to know the status of cyber resilience relative to other, similar institutions.

SURFaudit provides for the latter. The self-assessment based on the "Information Security Standard for Higher Education" (or the similar "Information Security Standard VET^{*}") is a good instrument for determining how cyber-resilient the institution is. In addition, every two years SURFaudit facilitates a benchmark, which enables institutions to compare their cyber resilience with that of similar institutions.



^{*} Vocational Education & Training

1 Main Findings

1.1 Cybercrime is on the radar

Society as a whole pays more attention to cybersecurity than before. For instance, the AIVD (the Dutch General Intelligence and Security Service) talks about it in their annual report [1], the NCSC (the Dutch National Cyber Security Centre) already mentions it since their 2011 Cyber Threat Assessment Report [2], the WRR (Netherlands Scientific Council for Government Policy) published in 2015 a report 'The public core of the internet' [3], which highlights cybersecurity, and on October 6th 2016, the Dutch Cyber Security Council published 'The economic and social need for more CYBER SECURITY – Keeping “dry feet” in the digital era' [4]. The latter is an independent public-private advice on the importance of cybersecurity for the Dutch economy and society. In summary, reports and advice on the subject abound.

Board members of institutions connected to SURF are becoming more aware of cybersecurity and cybersecurity figures more prominently on the board's agenda than ever.

1.2 Impact of cyber threats

If an attacker manages to access IT systems or the network, the impact can be immense:

- **Data Leak** – sensitive information is leaked or lost. This can be personally identifiable information (PII) or intellectual property (IP). In case of PII, a data leak can result in serious fines.
- **Disruption of ICT** – online services are (temporarily) unavailable as a result of sabotage by internal personnel or (external) cybercriminals, activists, or cyber vandals.
- **External reputational damage** – leaked information results in long-term damage to the institutions reputation, its personnel, or a third-party – such as a supplier or partner institution.
- **Internal reputational damage** – leaked information causes personal damage to employees, who start doubting the integrity of the organization.
- **Transfer of malware** – malware is passed on unknowingly, causing damage to others.
- **Data loss caused by extortion** – data were made inaccessible or sensitive data are not released until a ransom has been payed.
- **Data loss caused by espionage** – an attacker gained access to sensitive information such as intellectual property, causing substantial economic damage.

1.3 Trends

During the research period, a number of trends have been identified within the sector education and research:

- Phishing, spearphishing and whaling* is growing fast .
- The number of ransomware-incidents increases rapidly.
- DDoS-attacks continue steadily and are becoming more advanced.
- The number of vulnerabilities in software is on the increase.
- Responsible disclosure policies are implemented.
- The importance of Supply Chain Security is recognized.

* Specific form of phishing targeted at a high-profile business executive or upper manager, to entice them into divulging sensitive information or transfer a large sum of money for instance.

1.4 This report's purpose is to increase resilience

This report shows which threats in the cyber domain, our digital world, are relevant for educational and research institutions, thus offering the institutions a better handle on increasing their resilience.

1.5 About this edition

For the third time the "Cyber Threat Assessment – education and research sector" has been published (in Dutch, this is the first time an English version is provided). This edition is based on interviews with Security Officers and (IT-) staff from numerous educational and research institutions, in addition to several public sources. It builds on the previous editions and more or less covers the period between October 2015 and October 2016.

1.6 Relationship with SURF-services

Innovation Program Reliable and Safe Environment

The creation of the Cyber Threat Assessment - Education and Research sector is one of the activities that are part of the innovation program "Reliable and Safe Environment" (Betrouwbare en Veilige Omgeving). With this innovation program, SURF aims at a freely accessible and open Internet as the foundation for a reliable and safe living and working environment. The objective of the innovation program is for 90% of SURF's institutions to be competent in the area of Security, Privacy and Trust by the end of 2018.

Information Security Framework for Higher Education

The threats identified in the Cyber Threat Assessment report provide input for maintaining the Information Security Framework for Higher Education (*Normenkader IBHO*). This framework is based on the International Standard ISO/IEC 27002:2013 - *Code of Practice for Information Security Controls*, the most widely used standard for information security. It also contains all of the privacy aspects mentioned in the CPB Guideline *Securing Personal Data (Richtsnoer Beveiliging van Persoonsgegevens)* [5].

SURFaudit

SURFaudit offers institutions the opportunity to assess the status of their information security, for the entire organization or for parts of the organization, based on the Information Security Framework for Higher Education. This allows the institution to map how well it is in control of information security and to determine priorities for improvement.

1.7 Reading guide

In chapter 2 of the Cyber Threats Assessment, you can read which general trends have been observed and which of those are specific to the education, research and management processes of education and research institutions: the threat landscape.

Chapter 3 addresses the threats for each process and shows the actors (those who attack ICT facilities in education and research) for each threat.

Chapter 4 discusses measures that can be taken against the main threats for each process.

2 Threat landscape

2.1 Introduction: general threats

To protect data is complex

As noted in previous versions of this report, the education and research sector is characterized by the openness of its networks and increasing connectivity with other networks. It is an ever more complex challenge to protect the data (and then we mean to protect the information, not the bits and bytes on a computer) that are exchanged. One of the reasons for this is the increasing cooperation between institutions, and with private parties. Another reason is the ever-increasing exchange of data between students and teachers, and between researchers at home and abroad.

Classification of data becomes more important

The reporting requirement for data leakage as of January 1st, 2016 and the EU General Data Protection Regulation (GDPR), which goes into effect on May 25, 2018 [6] [7] makes data classification, more than before, necessary to determine what data protection measures should be taken before exchanging the data.

Based on data classification, appropriate protection measures can be taken and, if need be, anonymization or pseudonymization (**see section Anonymization and Pseudonymization**) can be applied to comply with the regulation. Failure to comply with the current law, or in due course the GDPR, may lead to very high fines. Special attention needs to be paid to data at the University Medical Centers (UMCs), because UMC's handle very sensitive information that cannot fall into the wrong hands under any circumstances. In particular, electronic patient data and interfaces to the outside world must be well protected to prevent unauthorized access.

Anonymization and pseudonymization

According to ISO/TS 25237:2009 'Health informatics — Pseudonymization'* both anonymization and pseudonymization are subcategories of de-identification.

Anonymization is the process that removes the association between the identifying dataset and the data subject and *anonymized data* are data from which the patient cannot be identified by the recipient of information.

Pseudonymization is a particular type of anonymization that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. A *pseudonym* is a personal identifier that is different from the normally used personal identifier.

Unlike pseudonymization, anonymization does not provide for the possibility to link the same person across multiple data records or information systems.

The Privacy Authority (AP, formerly the College for Protection of Privacy Data) set criteria that must be met when applying pseudonymization**:

- 1 Pseudonymization must be applied in a professional manner; the first encryption takes place at the data provider.
- 2 Technical and organizational measures have been taken to prevent traceability of the encryption (replay attack).
- 3 The processed data do not identify indirectly.
- 4 Before processing the data an independent auditor determines if requirements 1-3 are met.
- 5 The pseudonymization solution must be described clearly and fully in a public document so that every stakeholder can check the level of assurance the solution provides.

* <https://www.nen.nl/NEN-Shop/Norm/NPRISOTS-252372009-en.htm>

** https://www.zorgtpp.nl/userfiles/Downloads/Facsheet_pseudonimisatie_algemeen_201307.pdf
(retrieved on September 26th, 2016)

Governance

For introducing data classification, it is important that the governance of the organization is in order. In that case, the organization considers what information is available from a business perspective, who owns or is responsible for that information, and what the consequences are when that information is leaked, manipulated, or viewed by unauthorized persons.

Increase of cloud services

In addition, we see a strong increase in cloud services such as cloud storage and various *as-a-service* solutions. We all know storage services such as SURFdrive, Dropbox, Google Drive and OneDrive, but the use of online services such as Blackboard, OSIRIS, student registration systems and online HR applications, is increasing significantly as well.

Decide on measures for protection in time

Before adopting cloud services, it is becoming increasingly important to determine which data under what conditions may be stored or processed in the cloud, and what protection measures are required. If only to comply with laws, regulations, and legal and information security frameworks by which an institution wants to abide.

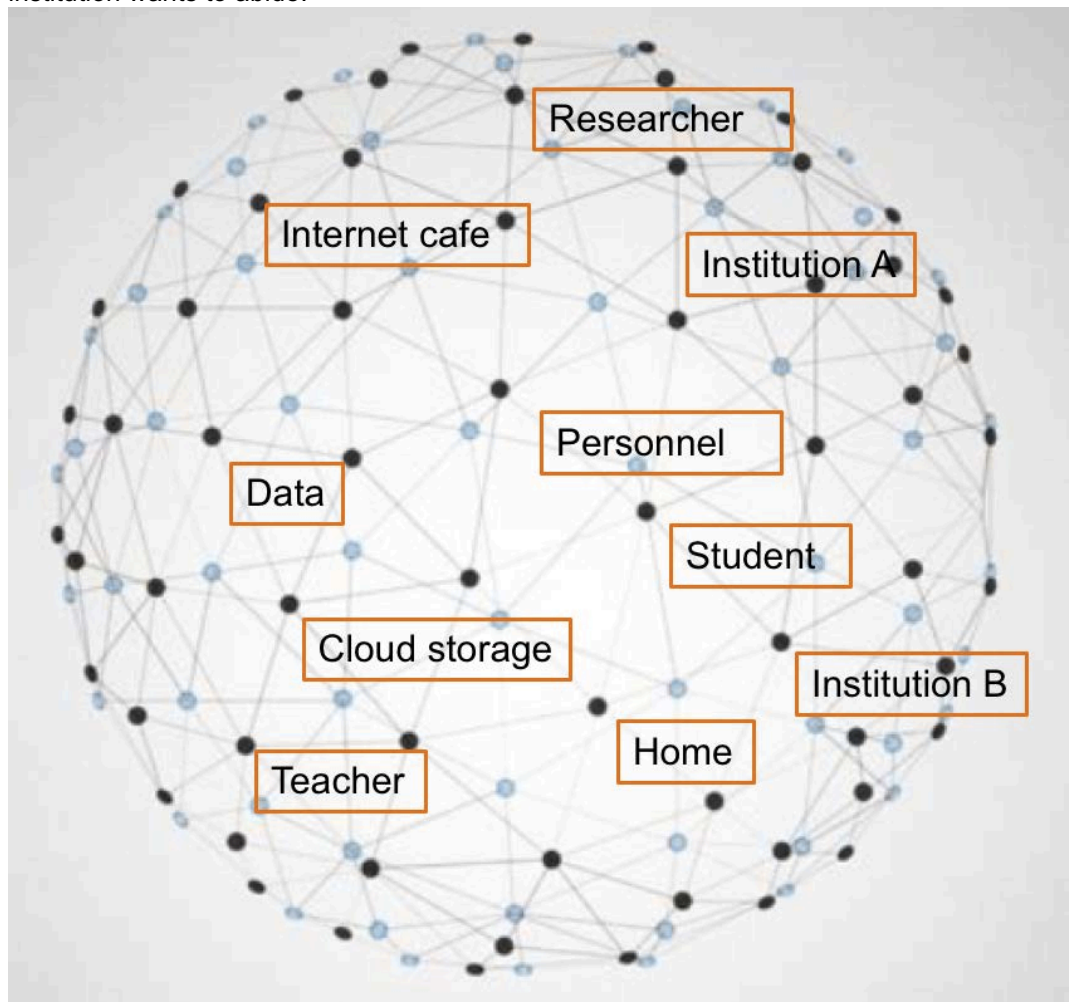


Figure 1: Data and users spread over the globe

Data and users across the entire globe

Data can be spread across different institutions' campuses and other parties' locations, or they can be stored in the cloud, which means that the exact location of the data is unknown.

And not only the data can be everywhere, the users of that data can be located in many places around the world, not necessarily at an educational or research institution's network, but perhaps at home or somewhere on a public Wi-Fi network, networks that are not controlled by the institution.

Many different systems

The diversity of equipment is increasing all the time; in the past, desktops and laptops were used for the most part, now all kinds of devices are online and are used to process educational, research and business data, including tablets, smartphones and wearables. All those devices were novelties not long ago, but have become commonplace now. Many apps are available for email and text messages, and already productivity apps can run on a smartwatch. Many of those collect privacy sensitive data, contact information, and information about browsing behavior [7] without the user's knowledge, and malware to steal data and identity information from the owner is being developed for all those devices and software. In short, working on a wide variety of devices is getting easier, but at the same time more opportunities for attackers to steal or manipulate sensitive data are available.

2.2 Threats for the sector education and research

In this chapter, we discuss the actual threat landscape and the trends of the past year.

2.2.1 Trends

Last year a number of trends can be seen in our sector:

- Phishing, spearphishing and whaling incidents are increasing.
- Strong increase in the number of ransomware incidents.
- DDoS attacks continue and are becoming more advanced.
- Increasing number of software vulnerabilities.
- Responsible disclosure policies are being adopted.
- The importance of supply chain security is recognized.

Phishing, spearphishing and whaling incident increase*

This year the number of phishing and whaling attacks has increased substantially (**see section *Phishing, spear phishing and whaling***).

While phishing emails are fairly easy to recognize by mail and spam filters, whaling emails are much harder to detect because there is not always a link or attachment. An example of whaling is the CEO fraud that has emerged in recent months (mid 2016). The e-mail, which is addressed to a specific person at the finance department, contains a directive to transfer money as quickly as possible, often to overseas. The message has been signed by the addressee's director or manager and it is emphasized that payment must be made as soon as possible. These types of e-mails are becoming more and more intricate; in the business community, several CEO fraud attacks have already been successful [8].

Strong increase in the number of ransomware incidents

In 2015, a substantial number of ransomware incidents have been reported, including the incident at the VU. The number of incidents has seen a steady increase during 2016. Several institutions have suffered ransomware attacks this year, while the ransomware used became more and more difficult to counteract.

* Form of phishing in which the attacker tries to entice a high-ranking staff member to divulge information or transfer a large sum of money.

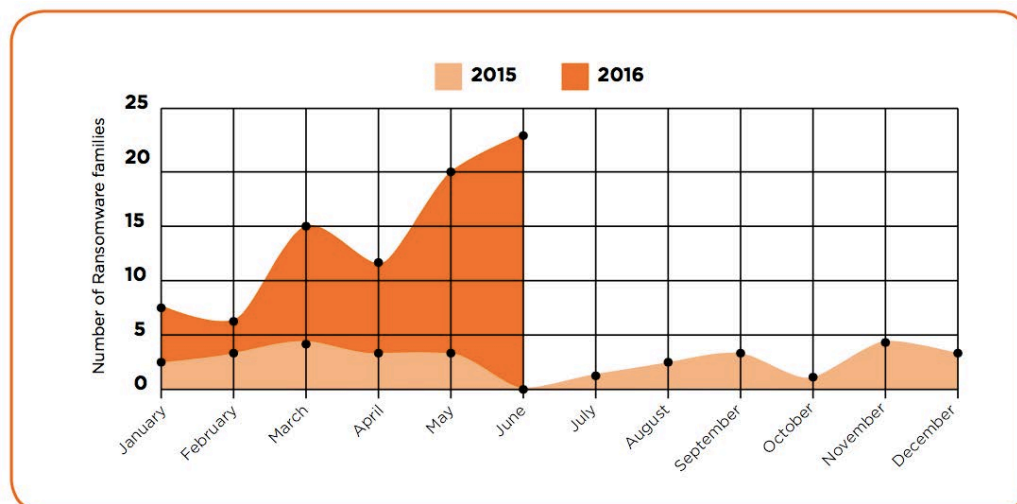


Figure 2: Increase in the number of ransomware families 2015-2016 (source: Trend Micro [9])

Already known were instances where files cannot be decrypted (Cryptolocker). New is the emergence of incidents where files are removed if no ransom is paid (Jigsaw), and incidents where the ransom is continually increased if there is no payment received before the deadline (Surprise) [9].



Figure 3: Increase of ransom if payment is not received in time (source: Fortinet [10])

The most widely used method for distributing ransomware is to send a phishing email with a link that installs the ransomware on the user's system as soon as the victim clicks the link. This method is also seen a lot in the education and research sector.

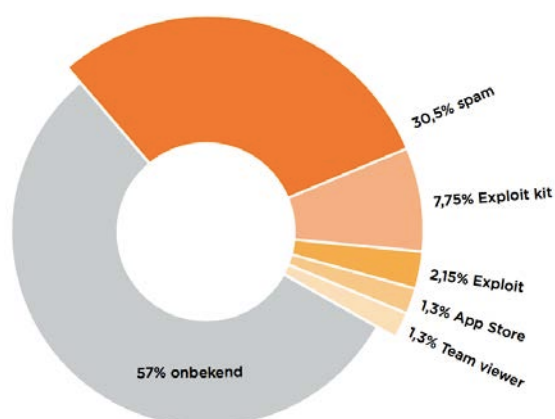
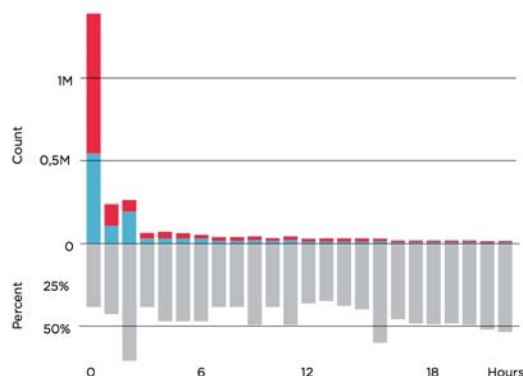


Figure 4: Attack vectors ransomware (source: Trend Micro [11])

Phishing, spear phishing and whaling

Phishing

In a phishing campaign an email is sent to a large group of users for the purpose of retrieving information, such as login credentials, or to stealthily install malware on the user's system. The user is tempted to open a link or attachment in the email. Research from Verizon* reveals that about 30% of recipients open a phishing email and approximately 12% of users click the (malicious) link or attachment:



There are always users who click the link or open the attachment, so when the target group is big enough, the attacker can collect login data or manages to install malicious software on many users' systems. The software can be ransomware, or other malware that, for instance, makes the system part of a botnet.

Spear phishing and whaling

A more targeted form of phishing is spear phishing or whaling. In this case, specific persons are approached. Beforehand, the attacker has investigated who can be approached best. This can be done by e-mail, but also by telephone. One example is the recent CEO fraud campaign**, where the victim is requested to transfer a large amount of money in an email.

* Verizon DBIR 2016 - http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (retrieved on September 26th, 2016)

** <https://www.abnamro.nl/nl/grootzakelijk/over-abnamro/veiligheid/slachtoffer-van-ceo-fraude.html> (retrieved on September 26th, 2016)

In addition, ransomware is widely distributed by all kinds of exploit kits*, which use specific vulnerabilities to deliver their payload. With an exploit kit, anyone can spread malware in a user-friendly way without the need for much knowledge. Well-known and commonly used exploit kits are Angler, Neutrino and Nuclear [9].

A new variant is the DDoS blackmail. The victim receives an e-mail message that threatens with a DDoS attack, unless a ransom is paid (**see section DDoS blackmail**).

DDoS attacks continue and are becoming more advanced

On September 20th, 2016 *KrebsOnSecurity*, researcher and publicist Brian Krebs' web site, came under siege of a denial-of-service [12]. The attack was so intense (a bombardment of more than 600 Gigabits per second) that the ISP took the site offline to protect itself and its (paying) customers. Ultimately, they decided to stop hosting Krebs' web site.

This attack was noteworthy because, as opposed to the ‘normal’ techniques seen with denial-of-service-attacks (**see section DDoS-attack**), the attack originated from many hacked devices, an *Attack of Things* [13]. It was probably executed using a botnet consisting of a great number of Internet of Things-systems, such as home routers and internet modems, cameras and digital videorecorders connected to the internet. These devices tend to have hard-coded passwords, or passwords that can be guessed very easily.

ENISA^{*} [7] also notes a shift from botnets that consist of a number of powerful systems, to botnets that consist of very many simple home systems. Because more and more systems are connected to the Internet, we can look forward to many more of this kind of attacks.

Also, for DDoS attacks, less and less knowledge and skills are needed, which means that for instance students can easily target their schools. Several services (booters or stressers) are available to perform DDoS attacks at low cost [14] [15]. A monthly subscription for a DDoS attack of up to 60 minutes at a time costs 20 to 40 dollars, so an attack with high impact can be performed at very low cost [16]. An estimated 40% of all DDoS-traffic is generated by booters [7].

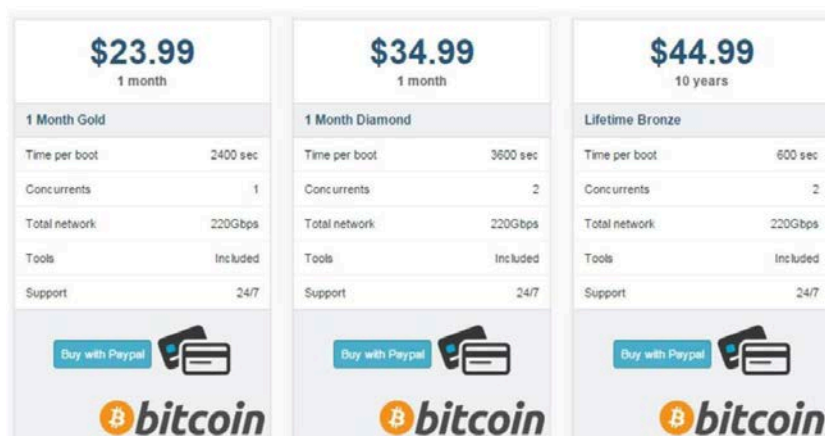


Figure 5: Example of pricing for a booter service (source: Incapsula [16])

In 2015 and 2016 SURFcert received a large number of alarms for denial-of-service-attacks. During vacation periods, the number of alarm decreases significantly, suggesting students perform these attacks.

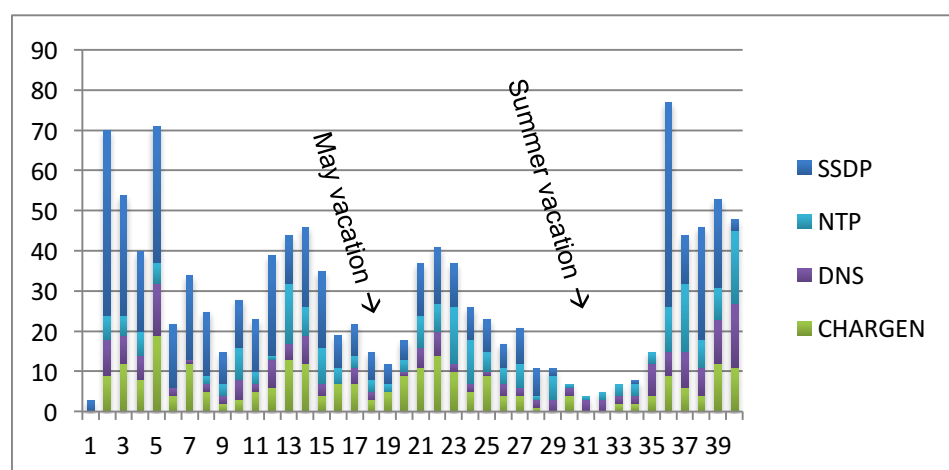


Figure 6: SURFcert – number of alarms per week (Q1-3 2015)

^{*} European Network and Information Security Agency (<https://www.enisa.europa.eu/>)

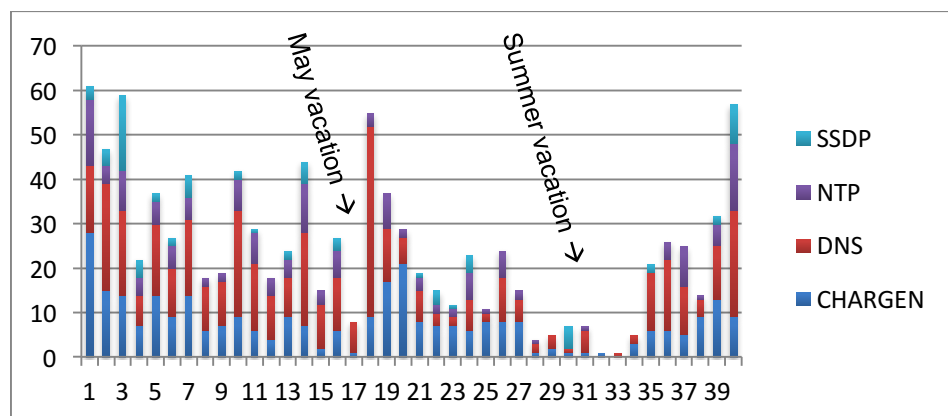


Figure 7: SURFcert – number of alarms per week (Q1-3 2016)

SURFcert has started to implement preventive rate-limiting (**see section Rate-limiting**) filters that counter the most prevalent attacks. The effect appears to be that the average number of alarms is decreasing (see figures 6 & 7), possibly because the attacks have become less effective.

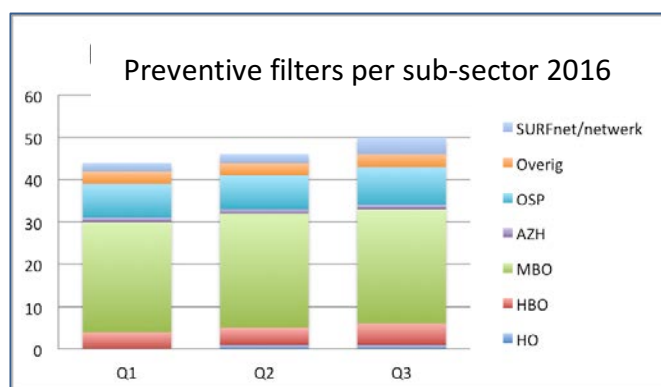


Figure 8: Number of institutions with preventive filters by sub-sector (2016)

Rate-limiting*

With some types of DoS attacks, there's not much you can do to stop the flow of the attack, especially in a distributed DoS (DDoS) attack in which the hacker is spoofing the source addresses and using an unsuspecting company or ISP as the reflector in the attack. Tracing this kind of attack to the hacker can be difficult.

In this situation, the first concern is limiting the impact of the attack on your network, which can be done with rate limiting. Rate limiting enables you to assign a bandwidth restriction to a category of traffic, such as ICMP, UDP, or specific connection types.

Rate limiting is best used on the ISP's router that connects to your network. In other words, if you are experiencing a flood attack that is saturating your Internet link, implementing rate limiting on your perimeter router will not do much good. Instead, work with your ISP to put this in place on the ISP's router.

Also, rate limiting is something you can configure to restrict the amounts of outbound traffic. For instance, if you were a reflector in a Smurf attack, you could use rate limiting as a temporary solution to limit the flood of traffic that you are sending to a victim's network.

* <http://www.ciscopress.com/articles/article.asp?p=345618&seqNum=5>

Increasing number of software vulnerabilities

The number of software vulnerabilities is still on the rise, especially for products from Adobe and Microsoft [17] [18]. Because the time between the publication of a vulnerability and the first available exploitation is between 10 and 100 days (median 30 days), there is not much time to patch systems, especially if you realize that vulnerabilities, before they become publicly known, may have existed and exploited for some time.

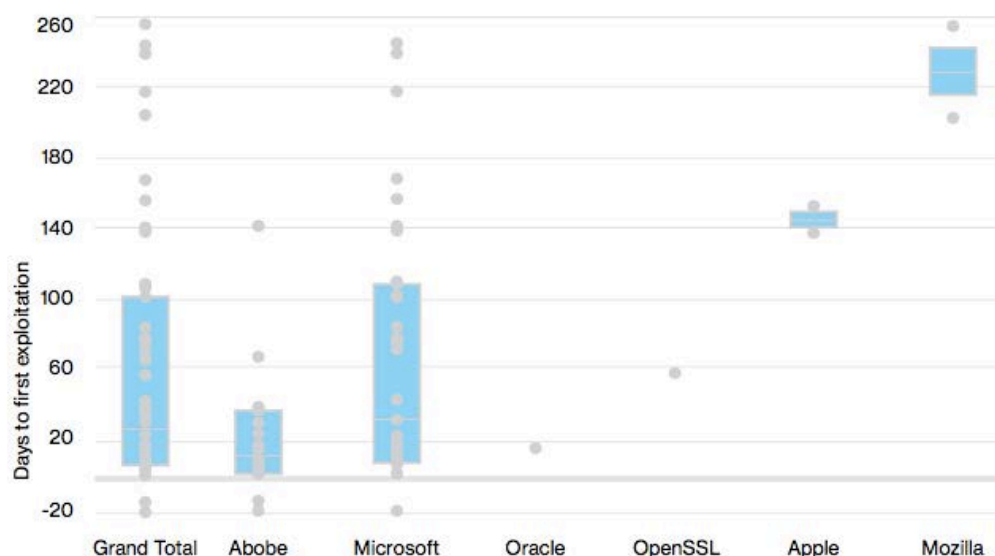


Figure 9: Time to first-known exploitation by vulnerability category (source: Verizon DBIR 2016 [18])

This became evident from the publication of Hacking Team data (July 2015). Hacking Team possessed several zero-day exploits that use (then) unknown vulnerabilities [19].

Responsible disclosure policies are being adopted

Some time ago, SURF provided a model policy and procedures for responsible disclosure to institutions for higher education. Since then SURF and a large number of institutions have implemented them. It allows for third parties to easily report vulnerabilities they found.

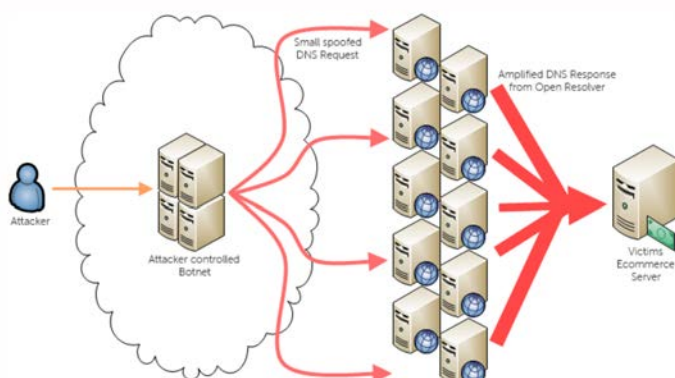
In addition, with approximately 30 other organizations, SURF signed the Coordinated Vulnerability Disclosure Manifesto on May 12, 2016 at the EU High Level Meeting on Cyber Security in Amsterdam.

The importance of Supply Chain Security is recognized

Because applications and storage move to the cloud, supply chain security becomes increasingly important. There are all kinds of risks that must be covered by an organization, other than the institution itself, while the institution itself remains responsible for the ramifications. Many organizations assume that cloud services are trustworthy, even though they have not identified threats to data stored at or processed by a cloud service, and they have not verified whether existing measures are sufficient [7]. However, in many cases it is not clear how information is protected by the cloud service and what the consequences for the institution are if that information becomes available to unauthorized third parties. Fortunately, institutions are becoming more aware of the risks in the supply chain, and measures are adapted accordingly. In addition, SURF encourages the use of the Legal Standards Framework to enforce standards with suppliers (chain partners). And also in other education sectors, there is more attention for chain security: e.g. the privacy convention in the public sector and agreements with publishers in the sector VET.

DDoS attack

In the event of a denial or service attack, a website or an internet connection is inundated with so much traffic that legitimate traffic can no longer reach the site. As a result the website or e-mail server becomes unreachable. A popular variant is the Distributed Denial of Service attack or DDoS attack. For DDoS, different techniques are used, of which reflection and amplification are the very common. In a reflection attack, systems other than those of the attacker are triggered to send network packets to a target. With amplification, the packets sent from the target system are significantly larger than the original packet it received, making the attack much more effective.



Typically, vulnerable protocols such as Network Time Protocol (NTP) and DNS (Domain Name Service) are used.

Many DDoS attacks are performed with so-called booters. A booter is an on-demand DDoS service offered by cyber criminals. They are used a lot by script kiddies, because it enables them to do an advanced DDoS attack at low cost*.

* See <http://www.eweek.com/security/how-do-booters-work-inside-a-ddos-for-hire-attack> (retrieved on September 30th, 2016)

DDoS blackmail*

Example DDoS blackmail message:

From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDoS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday, attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

A well-known example is the 2015 ProtonMail incident, where ProtonMail, a Swiss e-mail service, decided to pay the ransom to avoid a DDoS attack that would hurt other companies using the same ISP as ProtonMail**.

* <https://www.grahamcluley.com/armada-collective-ddos/> (retrieved on November 30th, 2015)

** <http://www.forbes.com/sites/thomasbrewster/2015/11/09/armada-bitcoin-crooks-go-big/#739906c41689> (retrieved on November 30th, 2015)

2.2.2 Increasing complexity

These developments make the threat landscape for the institutions increasingly complex. When making data available, it must be determined how sensitive the data are, who can access them, from which locations, and what access is allowed.

Zero-day attacks

A zero-day attack (zero-day exploit) is an attack that exploits an unknown vulnerability in software or an application. Therefore, the vulnerability is a zero-day vulnerability.

It is not possible to detect a zero-day attack, at least not with traditional means like antivirus software and web site revision databases, simply because the vulnerability is not known yet. Traditional protection software works on the basis of pattern recognition and from a zero-day attack, the pattern is not yet known.

So far, nine zero-day exploits have been discovered in 2016, in 2015 there were thirteen*. According to earlier FireEye research, it takes about 310 days before vulnerabilities discovered by cybercriminals become known**.

These types of vulnerabilities are sold openly for large amounts:

*"Researchers from Trustwave's SpiderLab team have uncovered a zero-day exploit on Russian underground malware forum exploit.in, affecting all versions of Microsoft Windows OS from Windows 2000 all the way up to a fully patched version of Windows 10."****

The price of this vulnerability is \$ 90,000 ...



* <https://www.fireeye.com/current-threats/recent-zero-day-attacks.html> (retrieved on September 30th, 2016)

** <https://www2.fireeye.com/rs/848-DID-242/images/wp-zero-day-danger.pdf> (retrieved on September 30th, 2016)

*** <https://thehackernews.com/2016/06/windows-zero-day-exploit.html> (retrieved on October 7th, 2016)

Datatypes per business process

We make a distinction between data relevant to business, education or research (or a combination):

Information	Description	Education	Research	Operations
Study results	Data indicating whether a study activity has been achieved and its scores. For example, results of exams, assignments and presentations, which determine external accountability and funding.	•		
Research data & Intellectual property	The outcome of research can lead to new technologies, innovations and methods. Intellectual property can also include study materials, methods that are under development, papers and reports.		•	
CBRN+ data	Sensitive Chemical, Biological, Radiological and Nuclear data that is the result from research.		•	
Operational data	Information used for operations, including management information and financial information of the institution.			•
Sensitive personal data	Institutions possess a large amount of sensitive personal information (SPI) of employees, students, test subjects and others.	•	•	•
Commercial & legal data	For instance information about procurement and project plans, but also information about current legal matters.			•
(Research)partner information	Information about partner institutions, subcontractors and other third parties.		•	•
Exam data	Information about the content of the exams, the correct answers and scoring methods.	•		

Table 2: Information and processes

Datatypes by security aspect (availability, integrity, confidentiality and privacy)

The security aspects availability (A), integrity (I), confidentiality (C) and privacy (P) apply as well:

Information	Description	A	I	C	P
Study results	Data indicating whether a study activity has been achieved and its scores. For example, results of exams, assignments and presentations, which determine external accountability and funding.		•	•	•
Research data & Intellectual property	The outcome of research can lead to new technologies, innovations and methods. Intellectual property can also include study materials, methods that are under development, papers and reports.	•	•	•	•
CBRN+ data	Sensitive Chemical, Biological, Radiological and Nuclear data that is the result from research.			•	
Operational data	Information used for operations, including management information and financial information of the institution.	•	•	•	
Sensitive personal data	Institutions possess a large amount of sensitive personal information (SPI) of employees, students, test subjects and others.		•	•	•
Commercial & legal data	For instance information about procurement and project plans, but also information about current legal matters.		•	•	
(Research)partner information	Information about partner institutions, subcontractors and other third parties.			•	•
Exam data	Information about the content of the exams, the correct answers and scoring methods.		•	•	

Table 3: Information and aspects

Risk analysis

To determine which measures are appropriate to protect information adequately, a risk analysis can be performed. Various methods and software packages are in use.

On the other hand, a lot of similarities between institutions for education and research exist, so it is likely that institutions introduce similar measures to cover their risks. To this end, the Information Security Framework for Higher Education (Normenkader IBHO) is a good tool. It contains guidelines for information security and privacy geared towards our sector.

3 Threats for each process

3.1 Introduction

In this chapter, we identify which risks are relevant to educational and research institutions for each process. The risk scale we use is based on the scale introduced in the Cyber Security Assessment Netherlands 2015 [21].

Low	Medium	High
<i>No new trends or phenomena of threats have been observed.</i>	<i>New trends or phenomena of threats have been observed.</i>	<i>There are clear developments which make the threat expedient.</i>
OR	OR	OR
<i>(Sufficient) measures are available to remove the threat.</i>	<i>(Limited) measures are available to remove the threat.</i>	<i>Measures have a limited effect, so the threat remains substantial.</i>
OR	OR	OR
<i>No incidents worth mentioning have occurred during the reporting period.</i>	<i>Incidents have occurred outside of the Netherlands, a few small ones in the Netherlands.</i>	<i>Incidents have occurred in the Netherlands.</i>

Figure 10: Risk scale

For each process the threats with the highest risk rating are mentioned first. For each risk, so-called actors are relevant. We consider actors that attack educational and research institutions. Based on the level of skill and determination various actors can be distinguished:

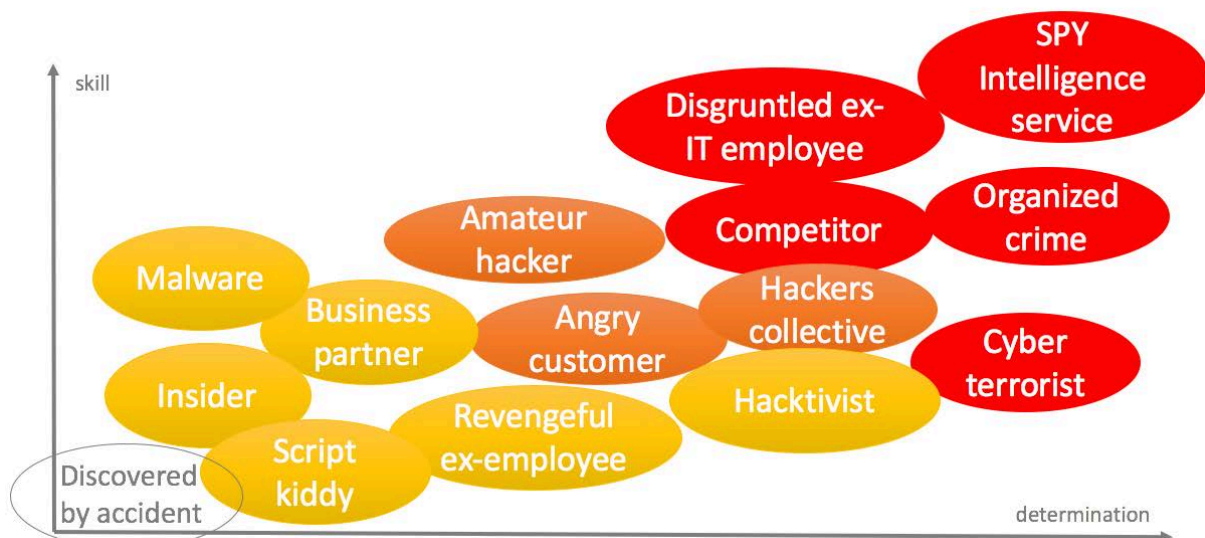


Figure 11: Skill level and determination of attackers

In the sector education and research, we distinguish these actors:

Actor	skill level	Description
Students	Low/ medium	<p>Students benefit from good progress during their study; Manipulation of study results may be interesting to them.</p> <p>They already have access to many systems and networks, and in some cases, they are very skilled.</p> <p>Students are often unaware of cyber threats, making them negligent about sensitive information.</p>
Employees	Low	<p>Employees benefit from good evaluations and achievements. Hence, manipulating HR files may be interesting to them.</p> <p>When dismissal or a reorganization is imminent, employees may inflict damages out of revenge. Some employees may be very skilled and they already have access to systems and networks.</p> <p>Employees are often unaware of cyber threats, making them negligent about sensitive information. In some cases, they are driven more by efficiency and convenience.</p>
Cyber criminals	Medium/high	<p>In general, cyber criminals are driven by financial gain. They sell stolen data or attempt to collect ransom by temporarily making data inaccessible.</p> <p>More and more, cyber criminals are organizing themselves to increase the likelihood of success.</p>
Cyber researchers	High	<p>Cyber researchers are in fact hackers, but with good intentions. If they find problems, generally they will notify the institution (responsible disclosure).</p> <p>They are very skilled and do not always conform to the rules of the institution.</p>
States	Very high	<p>Intelligence agencies and police departments have a lot of knowledge and are highly skilled. A lot of data are collected in the context of anti-terrorism and anti-crime. Foreign intelligence services are driven by business economics (interested in intellectual property and innovative knowledge) and highly skilled.</p>
Commercial companies and partner institutions	Low/ medium	<p>Commercial parties benefit from the early collection of information from competitors. The same applies to rival partner organizations who want each other's research data.</p> <p>They have knowledge and skill, but generally they will not use it against colleagues.</p>
Activists	Low/ medium	<p>Activists have the knowledge and skill to steal data or make systems and networks inaccessible. In addition, the likelihood that they publish data they stole is high.</p>
Cyber vandals	Low	<p>Cyber vandals seek recognition with their peers and like to expose their actions.</p> <p>New are cyber jihadists who try to gather sensitive data to publish for the purpose of propaganda.</p> <p>Their knowledge and skill varies, but is low generally.</p>

Table 4: Actors in education and research

3.2 Education process

Below are the threats that are relevant for the education process.

#	Type of threat	Manifestation of the threat	Risk level
1	Manipulation of digitally stored data	<ul style="list-style-type: none"> Tampering with study results Changing exam questions or answers 	HIGH
2	Identity fraud	<ul style="list-style-type: none"> Student has someone else take his/her exam Student impersonates another student or teacher to obtain exams Student impersonates a teacher or employee to manipulate study results 	HIGH
3	Obtaining and publicizing data	<ul style="list-style-type: none"> Privacy data is leaked and published Fraud by obtaining exam and exercise data 	MEDIUM
4	Disruption of ICT	<ul style="list-style-type: none"> DDoS-attack shuts down IT-infrastructure Exam data is destroyed Educational resources are unusable because of <i>malware</i> (e.g. eLearning or the network) 	MEDIUM
5	Take-over and abuse of ICT	<ul style="list-style-type: none"> Research equipment at the institution is taken over Systems or accounts misused for other purposes (botnet, mining, spam) 	LOW
6	Deliberately inflicting reputational damage	<ul style="list-style-type: none"> WWeb site compromised Social media account hacked 	LOW
7	Espionage	<ul style="list-style-type: none"> Students have access to sensitive information, e.g. during an internship at a company, making the student a target Foreign students controlled by foreign state 	LOW

Table 5: Threats for education

Actor	Level of skill	Threat
Students	Low to Medium	Identity fraud
		Manipulation of data
		Disruption of ICT
		Deliberately inflicting reputational damage
Cyber criminals	Medium to High	Obtaining and publicizing data
Cyber researchers	High	Obtaining and publicizing data
		Disruption of ICT
Activists	Low to Medium	Disruption of ICT
		Deliberately inflicting reputational damage
Cyber vandals	Low	Deliberately inflicting reputational damage

Table 6: Threats per actor for education

3.2.1 Manipulation of digitally stored data

Risk: 

Recording study results is one of the most important processes for an educational institution. If this is not done correctly or if students are able to change the answers of exams and tests afterwards, the results are not reliable. The institution can lose attractiveness and diplomas are not considered valuable anymore. Not only the institution itself but also graduates may suffer. The negative impact can be enormous.

Main actors: students.


3.2.2 Identity fraud

Risk: 

For educational institutes identity fraud is one of the most important problems. Generally, identity fraud is a means for financial gain; in the sector education, it is mostly a way to obtain unauthorized access to systems and applications. When a student impersonates someone at an exam or test, the integrity of all results is at stake. If the student takes a teacher's or an employee's identity, it can be used to view or manipulate data, which can have a large impact on the institutes reputation.

Main actors: students, disgruntled employees or teachers.


3.2.3 Obtaining and publicizing data

 Risk: 

Every educational and research institution collects sensitive data for educational purposes, varying from personally identifiable data to study results. Because in general cyber awareness at the institutions is low (as shown by the results of the SURFaudit benchmark 2015), the likelihood of data leakage is high. Also, technical vulnerabilities, whether zero-day (**see section Zero-day attacks**) or known, can be exploited to gain access to systems and to collect sensitive data. This may result in substantial reputational damage.

Main actors: cyber criminals.

3.2.4 Disruption of ICT

 Risk: 

The availability of networks and systems is crucial, because of the openness of the institutions' networks, the use of online learning resources, intranets and the ever-increasing use of online storage services. SURFcert reports indicate that, although they keep happening every day, most DDoS-attacks can be mitigated effectively. During the research period, a strong increase of ransomware infections has been observed. They can cause files, containing exam results, lesson materials or assignments, to be lost and disrupt the educational process. Damage can be substantial.

Main actors: activists, students and employees.


3.2.5 Take-over and abuse of ICT

 Risk: 

When malicious people get access to systems and the network needed for education, they can be disrupted. However, the likelihood is low.

Main actors: cyber criminals.

3.2.6 Deliberately inflicting reputational damage

 Risk: 

Deliberately inflicting reputational damage usually takes the form of defacing an institutions web site, because in many cases it is easily accessible and reaches many people. However, it can be remediated easily, so damage is limited.

Main actors: students, activists.

3.2.7 Espionage

 Risk: 

Students may have access to intellectual property or sensitive information, for example during an internship at a commercial company or by participating in scientific research, which can be of interest to third parties. The likelihood that student divulge this kind of information is small, but the impact can be significant.

Main actors: students

3.3 Research process

In this section we discuss threats that are relevant to the research process.

#	Type of threat	Manifestation of the threat	Risk level
1	Obtaining and publicizing data	<ul style="list-style-type: none"> Research data is stolen Privacy data is leaked and published Research blueprints fall in the wrong hands 	HIGH
2	Espionage	<ul style="list-style-type: none"> Research data is tapped Intellectual property is stolen through a third party Foreign students controlled by foreign state 	HIGH
3	Identity fraud	<ul style="list-style-type: none"> Activist poses as a researcher 	MEDIUM
4	Disruption of ICT	<ul style="list-style-type: none"> DDoS-attack shuts down IT-infrastructure Critical research data is destroyed Setup of research institutions is sabotaged 	MEDIUM
5	Take-over and abuse of ICT	<ul style="list-style-type: none"> Setup of research institution copied Systems or accounts misused for other purposes (<i>botnet, mining, spam</i>) 	MEDIUM
6	Manipulation of digitally stored data	<ul style="list-style-type: none"> Research data is manipulated 	LOW

Table 7: Threats for research

Actor	Level of skill	Threat
Students	Low to Medium	Disruption of ICT
Personnel	Low	Identity fraud
		Data manipulation
		Disruption of ICT
Cyber criminals	Medium to High	Obtaining and publicizing data
		Take-over and abuse of ICT
		Espionage
Cyber researchers	High	Obtaining and publicizing data
		Disruption of ICT
States	Very High	Obtaining and publicizing data
		Spionage
		Take-over and abuse of ICT
Commercial companies & partner organizations	Low to Medium	Espionage
Activists	Low to Medium	Disruption of ICT
		Deliberately inflicting reputational damage
		Take-over and abuse of ICT
Cyber vandals	Low	Deliberately inflicting reputational damage

Table 8: Threats per actor for research

3.3.1 Obtaining and publicizing data

Risk: 

During research projects, all kind of sensitive information may be processed and stored. This can be knowledge gathered during research or intellectual property, but it can be information about sensitive or controversial research, such as medical research or research on nuclear energy as well. Publication of this type of data can cause social unrest and even lead to liability claims. The SURFaudit benchmark 2015 shows that in general cyber awareness of researchers at our constituency is low and that ease of use and efficiency are considered most important. In this respect, the use of online storage services requires extra attention.

Main actors: cyber criminals, states, activists, researchers

3.3.2 Espionage

Risk: 

Research institutions can possess sensitive information, in which not only criminals, but also states are interested. Because during research projects various institutions collaborate, and sometimes private parties are involved, protection of sensitive research data is an issue. Even when the cybersecurity is in order and sensitive data is stored with due care, information may be stolen, which can lead to claims by third parties. In addition, according to the Dutch Intelligence Services (AIVD), the

top economic sectors, including high tech, chemical industry, energy, water and life sciences & health are a popular target for economic espionage [1]. Also, the AIVD has observed that in digital espionage more complex attacks are used and that detection is becoming much more difficult. Attackers make sure they track their victims remotely, so that they know when their attack has been detected and which measures are taken, giving them the opportunity to take counter-measures in time to maintain their access. Thus, the impact of espionage can be very high, because intellectual property (one of the crown jewel) is stolen, innovative leadership is lost, reputational damage occurs and the incurred cost of (complex) mitigation is high. At the same time, estimating the likelihood of espionage is difficult, as no documented history is available.

Main actors: cyber criminals, states, commercial companies.

3.3.3 Identity fraud

Risk:



Identity fraud is a significant problem for research institutions. While in society in general identity fraud is employed mostly for financial gain, in the research community it is a means to get access to data. For instance, when activists impersonate researchers, they can gain access to sensitive data that are not publicly available. As a result, reputational damage can occur and personally identifiable information can be affected.

Main actors: activists, cyber criminals.

Risk:



3.3.4 Disruption of ICT

Because of the openness of institutional networks and the ever-increasing use of online storage services, the availability of systems and the network is crucial for researchers. SURFcert statistics indicate that although DDoS attacks keep happening [22], they can be averted effectively. In addition, during the reporting period a significant increase of ransomware attacks has been observed. As a result, files, such as research data, may be lost. The damage can be considerable.

Main actors: activists, students and personnel.

Risk:



3.3.5 Take-over and abuse of ICT

A lot of research depends on the availability of systems and network connectivity, for instance when executing calculations. Such systems are an attractive target for third parties who want to use such computing power for their own use, whether illegal or not. First of all, it can affect the capacity that remains for legitimate purposes, but also the institution can be held responsible for illegal activities taking place on its systems and networks. Secondly, activists can try to disturb legitimate processes. In addition, systems at Dutch universities can be used as a springboard for illegal or espionage activities in other countries. This has to do with the high quality of the 'Dutch internet'. Therefore, the impact can be significant.

Main actors: activists, students, cyber criminals, states.

Risk:



3.3.6 Manipulation of digitally stored data

Safe-keeping of research data is increasingly seen as an important task of research institutions to ensure the transparency and accountability of investigations. There have been a number of cases of researchers who seem to have manipulated their research data to show desired results. Also, storage of raw research data is considered a core task of the institutions. However, the chance of manipulation is low.

Main actors: researchers, students

3.4 Operations

Below we discuss threats that are relevant to operations.

#	Type of threat	Manifestation of the threat	Risk level
1	Obtaining and publicizing data	<ul style="list-style-type: none"> Privacy data are leaked and published Other sensitive data (financial) are leaked and published 	MEDIUM
2	Disruption of ICT	<ul style="list-style-type: none"> DDoS-attack shuts down IT-infrastructure Critical research data or exam data is destroyed Educational resources are unusable because of <i>malware</i> (e.g. eLearning or the network) 	MEDIUM
3	Take-over and abuse of ICT	<ul style="list-style-type: none"> Systems or accounts misused for other purposes (botnet, mining, spam) 	Medium
4	Identity fraud	<ul style="list-style-type: none"> Employee accesses employee data. 	LOW
5	Manipulation of digitally stored data	<ul style="list-style-type: none"> Employee manipulates personnel data. 	LOW

Table 9: Threats for operations

Actor	Level of skill	Threat
Students	Low to medium	Disruption of ICT
Cyber criminals	Medium to high	Obtaining and publicizing data
		Identity fraud
Cyber researchers	High	Obtaining and publicizing data
		Disruption of ICT
Activists	Low to medium	Disruption of ICT

Table 10: Threats per actor for operations

3.4.1 Obtaining and publicizing data

Risk: 

In business operations, all kinds of sensitive data are processed and stored, such as personnel data and financial data. Since the introduction of the reporting requirement for data leakage and the forthcoming EU General Data Protection Regulation (GDPR), the protection of personal data is very important. Leaking such data can lead to significant financial and reputational damage.

Main actors: cyber criminals, activists, personnel.

3.4.2 Disruption of ICT

Risk: 

The previously described openness of institutional networks and the increasing use of online applications and storage services, makes availability of systems and the network also important for business operations. The sharp increase in ransomware infections lately has increased the risk of losing files, such as personnel data and financial data. The impact of this can be significant, especially in connection with the reporting requirement of data leakage effective since January 1st, 2016 and any sanctions that may follow.

Main actors: activists, personnel.

3.4.3 Take-over and abuse of ICT

Risk: 

Operations depend on systems and network connectivity, especially due to the increasing application of online applications. As with 'Disruption of ICT', the impact of take-over and abuse can be significant.

Main actors: activists, personnel.

3.4.4 Identity fraud

Risk: 

For operations, identity fraud is not seen as an acute threat. The likelihood that it occurs is very low, although it is conceivable that a dissatisfied employee gains access to, for example, personnel files through identity fraud. This can affect the reputation of the institution, employee privacy, and integrity of dossiers.

Main actors: personnel.

3.4.5 Manipulation of digitally stored data

Risk: 

For providing information and for finance it is important that data integrity is guaranteed. However, these processes are mature already and they are well embedded in the organization. Therefore, the likelihood of manipulation of data is considered very low.

Main actors: personnel.

4 Resilience

4.1 Introduction

As mentioned in chapter 1.6, this report is part of the SURF Innovation Program “Reliable and Safe Environment”. The program’s ambition is that SURF and its affiliated institutions are immune to security incidents and cyberattacks by the end of 2018. Immune means that, although incidents occur, the availability and reliability of high-level information and systems remains guaranteed and recovery and damage costs are low. The result is a quick recovery, which is not at the expense of an open and freely accessible internet.

4.2 Measures



To reach the program’s goal, institutions must take measures to increase their cyber resilience. In the Cyber Threat Assessment 2015 report [22] we observed that the continuing de-perimeterization changes the way we protect data. This translates into other types of measures: the traditional way of protection with firewalls no longer works because often users are not within the perimeter. In addition, data is being processed and stored more and more in the cloud, which also affects the necessary measures. And, as mentioned earlier, data classification is important to determine which measures are adequate to protect data before exchanges between users and users of other institutions or parties take place.

4.2.1 Preparation

Before implementing measures, it is important that the institution's board has a good idea of which threats exist, which are relevant to the organization, what the crown jewels of the organization are and what data is being processed or stored in the cloud.

Furthermore, it is important that the board knows the status of the cyber defenses of its own institution and how it relates to other comparable institutions.

SURFaudit provides for the latter objectives. The self-assessment based on the Information Security Framework for Higher Education (*Normenkader IBHO*) is a good tool for determining how cyber-resistant the institution is. Every two years SURFaudit facilitates a benchmark that allows institutions to compare their cyber resilience to that of other similar institutions.

4.2.2 Measures against the major threats to the educational process

Manipulation of digitally stored data

The approach to this threat includes at a minimum the following measures, which relate mainly to the *integrity* aspect:

- Data classification – A classification system exists, enabling users to determine which data are sensitive and how to deal with them.
- Identity control – There is a system to determine the identity of users. The system distinguishes between the initial identification and verification of the identity at the time access must be granted (be it digital access or physical access).
- Access control – There is an identity and access control system to determine which users can access what data, from which locations, and using which devices.
- Encryption – To protect the integrity and confidentiality of data, data encryption is applied during storage as well as during transport (for example, by email or file transfer).
- Logging – Access to the data is logged, so that how the data are processed, and by whom, can be established (in real-time or afterwards).
- Back-up and restore – There is a procedure to recover data after an incident.

Identity fraud

The approach to this threat includes at a minimum the following measures, which relate mainly to the *integrity* aspect:

- Identity control – There is a system to determine the identity of users. The system distinguishes between the initial identification and verification of the identity at the time access must be granted (be it digital access or physical access).
- Access control – There is a system to determine whether or not access is granted based on the user's identity.
- Awareness – Users must be aware of the techniques attackers use to find out identities, such as (*spear*) *phishing* and *social engineering*, so that they do not become victims.

4.2.3 Measures against the major threats to the research process

Obtaining and publicizing data

The approach to this threat includes at a minimum the following measures, which relate mainly to the *confidentiality* aspect:

- Physical security – There is (for example) a pass system for rooms and locations where systems are housed. A process exists for granting access to the rooms and external locations. For data centers, access is strictly controlled.
- Data classification – A classification system exists, enabling users to determine which data are sensitive and how to deal with them.
- Access control – There is an identity and access control system to determine which users can access what data, from which locations, and using which devices.

- Encryption – To protect the integrity and confidentiality of data, data encryption is applied during storage as well as during transport (for example, by email or file transfer). Encryption protocols and algorithms meet the current state of the art.
- Zoning – For the storage of sensitive data, zoning is applied, for example, using the "Defense-in-depth" principle, so that the data cannot be accessed or publicized after an intrusion occurs.
- Awareness – Users know there is a data classification system and which measures they should apply to protect sensitive data.
- Continuity of information security – When an incident happens, measures must remain effective to ensure the continued protection of sensitive data.

Espionage

The approach to this threat includes at a minimum the following measures, which relate mainly to the *confidentiality* aspect:

- Awareness – Users know there is a data classification system and which measures they should apply to protect sensitive data.
- Access control – There is an identity and access control system to determine which users can access what data, from which locations, and using which devices.
- Encryption – To protect the integrity and confidentiality of data, data encryption is applied during storage as well as during transport (for example, by email or file transfer). Encryption protocols and algorithms meet the current state of the art.
- Zoning – For the storage of sensitive data, zoning is applied, for example, using the "Defense-in-depth" principle, so that the data cannot be accessed or publicized after an intrusion occurs.
- Network monitoring – The internal network and the link to the public network are monitored to discover unusual patterns over a longer period of time.
- Logging – Data on incoming and outgoing traffic is stored for periodic analysis to discover unusual patterns over extended periods. Log files are adequately protected from manipulation.
- System monitoring – Systems are monitored to detect unusual activity that occurs over a longer period of time. Stored monitoring data is adequately protected from manipulation.
- Continuity of information security – Security measures are maintained when an incident occurs and the data cannot be processed in the normal manner.

4.2.4 Measures against threats to operations

Obtaining and publicizing data

The approach to this threat includes at a minimum the following measures, which relate mainly to the *confidentiality* aspect:

- Physical security – There is (for example) a pass system for rooms and locations where systems are housed. A process exists for granting access to the rooms and external locations. For data centers, access is strictly controlled.
- Data classification – A classification system exists, enabling users to determine which data are sensitive and how to deal with them, and to determine who gets access.
- Access control – There is an identity and access control system to determine which users can access what data, from which locations, and using which devices.
- Encryption – To protect the integrity and confidentiality of data, data encryption is applied during storage as well as during transport (for example, by email or file transfer). Encryption protocols and algorithms meet the current state of the art.
- Zoning – For the storage of sensitive data, zoning is applied, for example, using the "Defense-in-depth" principle, so that the data cannot be accessed or publicized after an intrusion occurs.
- Awareness – Users know there is a data classification system and which measures they should apply to protect sensitive data.

- Continuity of information security – When an incident happens, measures must remain effective to ensure the continued protection of sensitive data.

Disruption of ICT

The approach to this threat includes at a minimum the following measures, which relate mainly to the aspects *confidentiality* and *integrity*:

- Antivirus software – Up-to-date antivirus software is installed on all systems to protect against malware infections.
- Network monitoring – The internal network and the link to the public network are monitored to discover unusual patterns over a longer period of time.
- System monitoring – Systems are monitored to detect unusual activity that occurs over a longer period of time. Stored monitoring data is adequately protected from manipulation.
- Logging – Access to the data is logged, so that can be established how the data are processed, and by whom, (in real-time or afterwards). Log files are adequately protected from manipulation.
- Back-up and restore – There is a procedure to recover data after an incident.

Take-over and abuse of ICT

The approach to this threat includes at a minimum the following measures, which relate mainly to the aspects *availability* and *integrity*:

- Physical security – There is (for example) a pass system for rooms and locations where systems are housed. A process exists for granting access to the rooms and external locations. For data centers, access is strictly controlled.
- Access control – There is an identity and access control system to determine which users can access what data, from which locations, and using which devices.
- Network monitoring – The internal network and the link to the public network are monitored to discover unusual patterns.
- System monitoring – Systems are monitored to detect unusual activity that occurs over a longer period of time. Stored monitoring data is adequately protected from manipulation.
- Logging – Data on incoming and outgoing traffic is stored for periodic analysis to discover unusual patterns over extended periods. Log files are adequately protected from manipulation.

5 Bibliography

- [1] AIVD, „Jaarverslag 2015,” Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2015.
- [2] NCSC, „Cyberdreigingsbeeld Nederland,” [Online]. Available: <https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland>. [Geopend 30 september 2016].
- [3] Wetenschappelijke Raad voor het Regeringsbeleid, „De publieke kern van het internet,” Amsterdam University Press, Amsterdam, 2015.
- [4] C. P. Herna Verhagen, „De economische en maatschappelijke noodzaak van meer cybersecurity,” Cyber Security Raad, 2016.
- [5] Autoriteit Persoonsgegevens, „Richtsnoer Beveiliging van Persoonsgegevens,” AP, 2013.
- [6] Autoriteit Persoonsgegevens, „Europese Privacywetgeving,” [Online]. Available: <https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/europese-privacywetgeving>. [Geopend 26 september 2016].
- [7] ENISA, „Enisa Threat Landscape 2015,” ENISA, 2016.
- [8] Fraude Helpdesk, „DUITS BEDRIJF € 40 MILJOEN KWIJT DOOR CEO-FRAUDE,” [Online]. Available: <https://www.fraudehelpdesk.nl/nieuws/duits-bedrijf-e-40-miljoen-kwijt-door-ceo-fraude-2>. [Geopend 6 september 2016].
- [9] Trend Micro, „2016 Midyear Security Roundup,” [Online]. Available: <http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup>. [Geopend 26 september 2016].
- [10] Fortinet, „Take it Easy, and Say Hi to This New Python Ransomware,” [Online]. Available: <https://blog.fortinet.com/2016/09/01/take-it-easy-and-say-hi-to-this-new-python-ransomware>. [Geopend 30 september 2016].
- [11] Trend Micro, „The Reign of Ransomware,” TrendLabs, 2016.
- [12] B. Krebs. [Online]. Available: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>. [Geopend 30 september 2016].
- [13] Flashpoint, „Attack of Things,” [Online]. Available: <https://www.flashpoint-intel.com/attack-of-things/>. [Geopend 30 september 2016].
- [14] Top10booters, „Top 10 Booters - The Booter Ranking Site,” [Online]. Available: <http://top10booters.com>. [Geopend 30 september 2016].
- [15] SafeSkyHacks, „Top 10 DDoser's (Booters/Stressers),” [Online]. Available: <https://www.safeskyhacks.com/Forums/showthread.php?39-Top-10-DDoser-s-%28Booters-Stressers%29>. [Geopend 30 september 2016].
- [16] Incapsula, „DDoS Global Threat Landscape Report Q2-2015,” Incapsula, 2016.
- [17] Verisign, „Verisign iDefense 2016 Cyberthreats and Trends Report,” Verisign, 2016.
- [18] Verizon, „Verizon Data Breach Incident Report 2016,” Verizon, 2016.
- [19] Symantec, „Third Adobe Flash zero-day exploit (CVE-2015-5123) leaked from Hacking Team cache,” [Online]. Available: <http://www.symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache>. [Geopend 30 november 2015].
- [20] GFCE, „Launch manifesto on responsible disclosure,” Global Forum on Cyber Expertise, [Online]. Available: <http://www.thegfce.com/news/news/2016/05/12/launch-manifesto-on-responsible-disclosure>. [Geopend 30 september 2016].
- [21] NCSC, „Cybersecuritybeeld Nederland 2015,” NCSC, 2016.
- [22] SURFcert, „Kwartaalrapportage Q3 security exploitatie & innovatie,” SURFnet, Utrecht, 2016.
- [23] SURFnet, „Cyberdreigingsbeeld 2015,” SURF, Utrecht, 2015.
- [24] Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Wearable_computer. [Geopend 26 september 2016].

6 Contributors

Hans Alfons, Vrije Universiteit Amsterdam
Ronald Boontje, Universiteit van Amsterdam
Ludo Cuijpers, ROC Leeuwenborgh
Margot van Ditmarsch, Leids Universitair Medisch Centrum
Frank Haak, Universiteit van Amsterdam – Hogeschool van Amsterdam
Bart van den Heuvel, Universiteit Maastricht
Karel van Houten, TNO
Xander Jansen, SURFcert
Elma Middel, Hanze Hogeschool
Alf Moens, SURFnet
Menno Nonhebel, KNAW
Wouter Oosterbaan, NCSC
Analist, AIVD
Martijn Plijnaer, Hogeschool Inholland
Anita Polderdijk-Rijntjes, Windesheim
Remco Poortinga-van Wijnen, SURFnet
Jean Popma, Radboud Universiteit
René Ritzen, Universiteit Utrecht
Martin Romijn, Technische Universiteit Eindhoven
Raoul Vernède, Wageningen University & Research

Original report (in Dutch) can be found at: <https://www.surf.nl/cyberdreigingsbeeld>