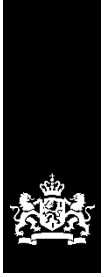

Inspectie van het Onderwijs
Ministerie van Onderwijs, Cultuur en Wetenschap

CYBER ATTACK ON MAASTRICHT UNIVERSITY

MAASTRICHT UNIVERSITY (BRIN: 21PJ)

Utrecht, May 2020

CONTENTS

Summary

On 23 December 2019, Maastricht University (UM) was hit by a cyber attack. Due to the scale of the attack – and thus the potential risks to the continuance of education and research – the Inspectorate of Education (hereinafter: the Inspectorate) conducted an inquiry in the period February – March 2020. The main question was: *Did Maastricht University take appropriate measures before, during and after the attack to ensure the proper continuance of education?* The inquiry was incidental, conducted in accordance with the Education Inspection Act (*Wet op het onderwijstoezicht*, WOT), Article 12a, paragraph 3.

We answer the main question on the basis of three sub-questions:

1. *Prevention: How was UM prepared for a cyber attack and had UM taken preventive measures to ensure proper continuance in the event of a possible attack (cyber resilience)?*

In recent years, data security has increasingly been the subject of discussion and awareness campaigns. However, the topic has particularly centred on GDPR and not on the possibility of a cyber attack. UM was affiliated with SURFcert and participated in SURF cyber exercises. The most recent of these focused on a cyber attack. UM has its own Computer Emergency Response Team (CERT) and Chief Information Security Officer (CISO). Systems to monitor the implementation of IT policy internally and to follow up on agreements were limited. Cyber threat was not at the top of the risk list. Malicious activities, such as ransomware, were not included in the plans for a major incident. Prior to the cyber attack, there was no overall view or oversight of the IT organisation and therefore only a limited view of the cyber resilience of the university as a whole. It should be said that UM is not alone in this: other academic universities (*universiteiten*) and universities of applied sciences (*hogescholen*) also have multi-layered administrative structures and are therefore potentially vulnerable. The challenge is to establish information security policy and its implementation and monitoring given the decentralised structure of the university as a whole.

We note that there was attention for information security at UM prior to the cyber attack, but that before the discovery of the ransomware attack on 23 December 2019, appropriate measures were not always taken. As a result, it was not noticed that third parties had gained access to the network, and the impact of the attack was more far-reaching than necessary.

2. *Response: What action did UM take in response to the cyber attack to restore the continuance of education as quickly as possible?*

Fox-IT has determined that after the opening of a phishing email, insufficient detection, monitoring and follow-up activity took place, which enabled hackers to carry out a ransomware attack on part of the UM network on 23 December 2019. The Executive Board dealt with the cyber attack in close coordination with the Crisis Management Team, the Supervisory Board, the representative bodies and other sections within the university. The continuance of education and research was paramount. Communication to staff and students was an essential parallel process. In addition, the Executive Board and Supervisory Board decided to share as much information as possible with other higher education institutions. The university saw it necessary to obtain the decryption key by making a ransom payment. It first

investigated whether an alternative was feasible. Had no payment been made, recovery and reconstruction could have taken months and there was no assurance of a full recovery, which would have seriously compromised the continuance of education and research. In addition, the cost of self-recovery would have been many times greater than the ransom amount.

We note that the crisis management was adequate: the Inspectorate found no indications that UM could have taken any other more appropriate measures after discovering the ransomware attack. Moreover, by organising a symposium, UM has demonstrated openness in order to warn other organisations and has thus contributed to the learning capacity of the higher education system.

3. *Learning capacity: What provisions has UM made to prevent the occurrence of similar incidents in future, with a view to the proper continuance of education?*

During the management of the cyber incident, work was carried out on tightening cyber security (so-called 'increased dike monitoring'), for example through the continuous (24/7) monitoring of the IT systems by externally contracted parties. In addition, a survey was made of the entire central and decentralised IT infrastructure, and there was a clear awareness of the preventive measures that needed to be tightened. UM needs more cooperation with other educational institutions, more knowledge sharing with regard to cyber threats, and clear government support. UM staff indicate that a discussion about cyber security should take place, and that now is the time for further measures to be taken. Attention should be paid to the dilemma between investment in the primary process of education and research on the one hand and cyber resilience on the other. The level of support for information security measures within UM will only become apparent in the coming period.

UM implemented appropriate measures by introducing 'increased dike monitoring' in the initial period after the crisis had been resolved. It is not yet possible to determine whether in the long term appropriate measures are in place at UM to prevent the occurrence of incidents of a similar magnitude.

Conclusion

We conclude that due to adequate intervention during the cyber attack, the extent to which it endangered the proper continuance of education and research was limited. Only for a short period of time was there a continuity problem for education and research. UM's Executive Board took informed decisions which it shared and implemented within the organisation in order to ensure the proper continuance of the planned educational activities after the holiday period. Although UM failed to take sufficient appropriate measures in a preventive sense, the response and initial lessons learned were adequate.

Follow-up supervision

The Inspectorate finds that Maastricht University acted adequately in dealing with the cyber attack and has confidence in the follow-up investigation that has already been instituted. The Inspectorate will not therefore prescribe additional points for improvement at UM. Other universities and colleges may also be vulnerable to cyber risks. In early 2020, the Inspectorate therefore decided to institute a two-part inquiry, firstly regarding the university and secondly regarding the higher education system. In relation to this second part of the inquiry, the Inspectorate requests UM to inform it of the results of the follow-up investigation which UM has instituted.

1 Background and Context

The Inspectorate of Education (hereinafter: the Inspectorate) conducted an inquiry at Maastricht University (UM) in the period February - March 2020. The inquiry was prompted by the cyber attack that affected Maastricht University on 23 December 2019 and considered the actions of Maastricht University before, during and after the attack. The inquiry was incidental, conducted in accordance with the Education Inspection Act (*Wet op het onderwijstoezicht*, WOT), Article 12a, paragraph 3.

On 26 December 2019, the Vice-President of UM (who also chaired the Crisis Management Team) informed the Inspectorate of the cyber attack on the university. Since the evening of 23 December 2019, some of UM's systems and data had become inaccessible due to encryption. A ransom was being demanded for a key that could be used to 'disinfect' the systems and decrypt the data files. The Vice-President also indicated how UM was working on restoring the university's IT environment with the assistance of the company Fox-IT. After this initial contact, UM provided the Inspectorate with new information where relevant.

Due to the scale of the cyber attack – and thus the potential risks to the continuance of education and research – the Inspectorate decided to institute a two-part inquiry. The first part was to be an inquiry at institutional level centred on UM. The second part was to be thematic: at the level of the higher education system, the Inspectorate was to consider what lessons from the cyber attack at UM are widely applicable to other universities. On 13 January 2020, the Inspectorate informed the Executive Board by telephone of the decision to institute an inquiry. The decision was also confirmed in writing to UM in a letter dated 30 January 2020.

1.1 Reading guide

The background to the problem will be discussed in the remainder of this section. Chapter 2 discusses the form of the inquiry. Chapter 3 contains the conclusions, followed in Chapter 4 by the findings on which they are based. Chapter 5 relates to the follow-up supervision.

1.2 Digital threats and higher education

Digital threats are increasingly common both nationally and internationally. In 2018, for example, there were 1.2 million individual victims of digital crime, such as property crime or identity fraud (CBS, 2018[1]). Digital crime is increasingly common not only among individuals, but also among companies and organisations. Higher education institutions can be attractive to digital criminals in a variety of areas. For example, it recently became evident that state hackers from Iran were trying to obtain educational material and login data for scientific literature at various Dutch higher education institutions.[2] Attempts are also being made, as recently occurred at Maastricht University, to encrypt university networks in exchange for a ransom payment. Research and education at higher education institutions depends almost entirely on digital networks, making them an attractive target.

[1] Statistics Netherlands (Centraal Bureau voor de Statistiek, CBS) 2019. *Digitale Veiligheid & Criminaliteit 2018.* https://www.cbs.nl/nl- nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

[2] https://www.nrc.nl/nieuws/2020/02/14/nederlandse-onderwijsinstellingen-doelwit-van-iraanse-hackers-a3990472 (consulted on 10 March 2020)

Securing the ICT network at a higher education institution is a challenge due to the nature of the organisation. Such institutions are open learning environments with many different users, including students, researchers, lecturers, staff and guest users, and hence there are many different needs and wishes with regard to ICT facilities. The ICT network therefore requires custom-made security. Universities also have a multi-layered administrative structure with various administrative bodies: at central level, a university is managed by the Executive Board, and at decentralised level, the organisation consists of deans at faculty level, education and research directors at educational level, and professors and lecturers at research level. ICT policy and security occurs at these various levels and extra attention is therefore needed to ensure that it is effective.

1.2.1 Responsibility for digital security in higher education

The government has defined a vital infrastructure consisting of processes that are so essential to Dutch society that failure or interruption would lead to serious social disruption and would pose a threat to national security (NCTV, 2020[3]). Examples of these vital processes are electricity, internet access, drinking water and payment transactions.
Since the Security of Network and Information Systems Act (*Wet beveiliging netwerk- en informatiesystemen, Wbni*) came into effect, a so-called duty of care has applied to some vital infrastructure providers: they have an obligation to take adequate measures for the security of their network and information systems.

Organisations and companies in the Netherlands that are not part of the vital infrastructure have no established guidelines for their digital information security. This is also the case for higher education institutions. The responsibility for adequate business operations lies with the institution itself. This also applies to the integrated security policy of which digital information security is a part. In higher education, institutions have been working together on ICT infrastructure for a long time. This collaboration can be seen in SURF, a cooperative association of Dutch educational and research institutions in which members jointly purchase or develop digital services. As members, the educational institutions are also owners of SURF. SURF annually publishes a cyber threat assessment detailing trends in threats to education and research.[4] The organisation provides information and coordinates the implementation of information security, such as digital security audits and support in relation to security incidents. This takes the form of participation by universities in SURFcert, a team that supports them in dealing with security incidents. All government-funded academic universities (*universiteiten*) and university medical centres are affiliated with SURF and SURFcert. All government-funded universities of applied sciences (*hogescholen*) are affiliated with SURF, of which 94% are also affiliated with SURFcert.

[3] https://www.nctv.nl/onderwerpen/vitale-infrastructuur (consulted on 6 March 2020)
[4] see: SURF, 2018. *Cyberdreigingsbeeld*. https://www.surf.nl/files/2019-03/surf_cyberdreiging_2018_web.pdf
[5] This is stipulated in the regulation for the designation of computer crisis teams, *Staatscourant* (Government Gazette) 2020, 4410.

Since 24 January 2020, SURFcert has been designated by the Minister of Justice and Security as one of the information hubs for non-vital sectors that is in close contact with the National Cyber Security Centre (NCSC).[5] The NCSC distributes information among the various information hubs when there are threats or vulnerabilities. The hubs are then responsible for informing and assisting their target groups.

1.2.2 *Standards for digital information security*

Various standards and methods for securing digital information have been developed worldwide. The International Organization for Standardization (ISO) has set out international information security standards in ISO 27001. These globally recognised standards describe the entire information security process. ISO 27002 provides additional standards, containing advice on how to implement the security measures referred to in ISO 27001. These international standards form the basis for other digital security standards worldwide. The Dutch national government has implemented ISO 27001 and 27002 in the Information Security Baseline for Government Bodies (*Baseline Informatiebeveiliging Overheid, BIO*). This framework of standards for information security indicates the basic level of information security that all government parties must meet.[6] Government institutions are recommended to comply with the BIO standard, but compliance has not yet been established in law.

SURF has also developed a standards and assessment framework that is based on the ISO standard and which also complies with the Data Protection Authority's Personal Data Security Guideline. SURF has selected measures from the ISO standard that must at minimum be established at an educational institution. These measures are classified in the following clusters: 1) policy and organisation, 2) staff, students and guests, 3) rooms and equipment, 4) continuity, 5) confidentiality and integrity and 6) control and logging. This standards and assessment framework forms the basis of the SURFaudit. Universities of applied sciences or academic universities can use it to assess the information security of their institution. This can be done for the institution as a whole or for individual departments. Every two years SURF carries out the SURFaudit benchmarks, showing how universities of applied sciences and academic universities are performing. The benchmark provides the individual higher education institution with insight into its own scores compared to those of others. Institutions affiliated to SURF can voluntarily test their own information security by conducting internal audits based on self-assessment. In addition, peer reviews of the self-assessment can be conducted by professionals from similar organisations, or external audits can be conducted.

1.2.3 *Prevention, incident response and risk management*

Among the aims of the design of information security is the prevention of possible incidents. Elements of prevention include incident management, alterations to the network, access rights, configurations and patches. Organisations' ICT departments are responsible for the implementation of measures related to these elements. In addition to establishing preventive measures, it is necessary according to the information security standards to create a Computer Security Incident Response Team (CSIRT) within the organisation, also known as a Computer Emergency Response Team (CERT). This team is responsible for dealing with network security incidents and is generally led by the Chief Information Security Officer (CISO).

[6] The Information Security Baseline for Government Bodies (BIO) is not yet based on legislation. It is, however, based on international standards: ISO 27001 and 27002. These are included as mandatory standards on the 'apply or explain' list of the Dutch Standardisation Forum, see: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit. The Ministry of the Interior and Kingdom Relations is working on the establishment of the BIO in law.

In higher education, SURFnet supports the establishment of these CSIRT teams. Ultimately, it is important that risk management should take place within all layers of the organisation for the purposes of information security. Having reflected on different standards, the organisation or its executive board in non-vital infrastructure can ensure the effective management of risks related to information security. The Dutch national government framework of standards, the BIO, describes seven useful standards that administrators can apply to the organisation's information security policy. These seven standards are: 1. increasing awareness, 2. safe and open culture, 3. establishing a risk team, 4. assuring risk management, 5. attention for supply chain cooperation, 6. monitoring and evaluation, and 7. investing in information security. We have used these standards in our inquiry. This will be discussed further in the next chapter.

2 Form of the Inquiry

2.1 Purpose and scope of the inquiry

The purpose of this inquiry was to determine whether there was any question of maladministration with regard to Maastricht University's actions before, during and after the cyber attack. By maladministration we mean serious negligence on the part of the executive or supervisors to take measures that were necessary to ensure the proper continuance of education at the university (Higher Education and Research Act [*Wet op het hoger onderwijs en wetenschappelijk onderzoek*, WHW], Article 9.9a). The inquiry is limited to the proper continuance of the bachelor's, master's and doctoral programmes. In higher education, the Inspectorate itself does not investigate the quality of education; this task (by means of accreditation) is the responsibility of the Accreditation Organisation of the Netherlands and Flanders (Nederlands Vlaamse Accreditatie Organisatie, NVAO). If the Inspectorate sees signs that quality is not as it should be, it informs the NVAO. There were no signs before or during this inquiry that the quality of education was at stake.

The main question this inquiry sets out to answer is:

Did Maastricht University take appropriate measures before, during and after the attack to ensure the proper continuance of education?

This main question is divided into the following three sub-questions:

- *Prevention: How was UM prepared for a cyber attack and had UM taken preventive measures to ensure proper continuance in the event of a possible attack (cyber resilience)?*
- *Response: What action did UM take in response to the cyber attack to restore the continuance of education as quickly as possible?*
- *Learning capacity: What provisions has UM made to prevent the occurrence of similar incidents in future, with a view to the proper continuance of education?*

The inquiry relates to the situation as of 18 February 2020 (date of the on-site investigation).

2.2 Assessment framework

The Inspectorate conducts investigations into compliance with the statutory regulations and financial legality at higher education institutions on the basis of Article 12a, first paragraph, of the Education Inspection Act (WOT).

This investigation focuses on whether or to what extent maladministration has occurred. The Higher Education and Research Act describes maladministration as follows: *serious negligence on the part of administrators or supervisors to take measures that are necessary to guarantee the quality and proper continuance of education at the institution* (Article 9.9a, second paragraph, under b, of the Higher Education and Research Act).
Serious negligence can be said to have occurred when:

- A failure or incident occurs because no (effective) action is taken while objectively this was possible and necessary; and/or
- No (effective) action is take at the time of and subsequent to the occurrence of the failure while objectively this is possible and necessary; and/or
- No action is taken to prevent comparable incidents from occurring in future and no appropriate organisational measures are taken.

Serious negligence results in the unnecessary continuation of a problem situation and/or the occurrence of additional and serious problems. It therefore concerns neglect attributable to the Executive Board or the Supervisory Board.[7]

The Higher Education and Research Act (WHW) does not contain a standard framework for the assessment the structure of ICT systems at higher education institutions. However, the act does contain regulations for the administration and organisation of academic universities (Chapter 9 WHW) and universities of applied sciences (Chapter 10 WHW). The relevant provisions for this investigation are included in Appendix 1.

In the current inquiry, we use the BIO standards for administrators (see Section 1.2.3) as a framework to answer our questions. For each question, we will determine which measures have been taken before, during and after the incident regarding each of the seven standards. The relevant standards arise from the ISO standards 27001 and 27002 and are therefore applicable to any organisation that aims to implement the ISO standards, including Maastricht University. As previously mentioned, institutions are not legally obliged to comply with these standards; they serve only as guidelines for the design and implementation of information security. The seven standards that administrators can use are described in the BIO as follows:

1. *Increasing awareness*: During meetings, executives should regularly place the importance of information security on the agenda. Awareness-raising measures should be in place among students, researchers, lecturers and staff who are regularly deployed.
2. *Safe and open culture*: Information security is essentially risk management that starts with identification. The executive should promote an open and safe culture in which employees feel free proactively to report actual or potential risks to the appropriate person.
3. *Establishing a risk team*: Make use of the knowledge and responsibilities of process and system owners. There should be cooperation within a risk team on the part of the Chief Information Security Officer (CISO), Data Protection Officer (DPO) and Controller. These system owners should also function as independent advisors to the board.
4. *Assuring risk management:* Risk management is a cyclical, iterative and recurring process: threats, environment and legislation change. These changes should be taken into account so that measures are effective and efficient.
5. *Attention for supply chain cooperation:* Partners and suppliers are able to demonstrate independently that they meet the applicable requirements.
6. *Monitoring and evaluation:* Regular monitoring and evaluation are important to gain proper insight into the extent to which information security policy and risk management are embedded in the organisation (e.g. regularity, reporting).
7. *Investing in information security:* Sufficient funds should be made available to deal with the identified risks adequately.

[7] 33475, no. 15, Quality Assurance in Higher Education Act (*Wet versterking kwaliteitswaarborgen hoger onderwijs*)
[8] M. Dijkstra & M. van Dantzig (2020) *Spoed Ondersteuning Project Fontana*. Support with ransomware attack. (project no. 190346) version 3.0. public version including response from Maastricht University made available via the university's site on 05-02-2020.

2.3 Institutional visit and document analysis

For this inquiry, the Inspectorate made use of the report prepared by Fox-IT on the cyber attack.[8] The report describes the results of Fox-IT's forensic investigation and discusses the results of the root-cause analysis[9] to the ransomware[10] attack of 23 December 2019 and whether data was accessed or stolen. In addition to the Fox-IT report, the Inspectorate consulted documentation by Maastricht University (see Appendix 2) and held discussions with various sections of the organisation (see Appendix 3). These discussions took place on 17 and 18 February and 9 March 2020.

2.4 Report

After the visit, a draft report was prepared and submitted to the university on 14 April 2020.

The draft report was discussed by telephone with a representative of the Executive Board on 23 April 2020. The university gave its written response to the report on 24 April 2020. The report was adjusted where necessary. The report was approved on 12 May 2020 and sent to the university.

[9] Root Cause Analysis is a systematic approach to the identification of the underlying causes of a problem. The analysis also focuses on finding measures to eliminate these causes.

[10] Ransomware is a type of malicious software with which access to files and/or systems can be blocked until a ransom is paid (Fox-IT, glossary).

3 Conclusions

3.1 Main question

The investigation was prompted by the cyber attack that affected Maastricht University (UM) at the end of 2019. The Inspectorate considered the following main question: *Did Maastricht University take appropriate measures before, during and after the attack to ensure the proper continuance of education?*

In summary, we note that UM did not always take appropriate measures prior to the cyber attack and as a result its impact was a more far-reaching than necessary. During the first phase of the incident, the measures also proved to be inappropriate, with the result that it was not noticed that third parties had gained access to the network. The crisis management itself, on the other hand, was adequate: in this second phase of the incident, which began after the discovery of the ransomware attack, the Inspectorate found no indications that UM could have taken any other more appropriate measures. Appropriate measures in the form of tightened cyber security ('increased dike monitoring') were also taken for the first period after the crisis has been resolved. Moreover, by organising a symposium, UM has demonstrated openness in order to warn other organisations and has thus contributed to the learning capacity of the higher education system. It is not yet possible to determine whether in the long term appropriate measures are in place at UM to prevent the occurrence of incidents of a similar magnitude.

We conclude that due to adequate intervention during the cyber attack, the extent to which it endangered the proper continuance of education and research was limited. In the period from 24 December 2019 to 2 January 2020, staff and students had no access to the UM systems. This means that there was only a continuity problem for education and research for this short period. UM took every effort to ensure that educational activities were able to continue as planned after the holiday period. UM's Executive Board took informed decisions which it shared and implemented within the organisation. Consequently, all planned educational activities were able to continue from 6 January 2020. UM therefore restored the continuance of education and research in a timely manner, so it was not endangered in the long term. Although UM failed to take all appropriate measures in a preventive sense, no serious negligence or maladministration occurred: attention was already being paid to cyber resilience before the attack, the response to the incident was decisive, and UM is adequately implementing the first lessons learned.

3.2 Answers to sub-questions

The conclusion from Section 3.1 is further substantiated in this section in the answers to the three underlying sub-questions. We use the BIO standards which can be applied by administrators (see Chapter 2.2) as a framework. Where a standard is applicable to a conclusion, it is mentioned in italics.

Sub-question 1 - 2. Prevention: How was UM prepared for a cyber attack and had UM taken preventive measures to ensure proper continuance in the event of a possible attack (cyber resilience)?

UM is an internationally oriented institution and historically has a highly decentralised organisational form. This decentralised structure and management also applies to the university's IT. This is a deliberate choice primarily for the benefit of research: the decentralised structure means that researchers have great freedom in determining the systems that are desirable for their studies (*standard 2: safe and open culture*). As a consequence of the organisational structure, prior to the cyber attack, there was no total overview of the ICT structure of UM as an organisation and therefore only a limited view of the cyber resilience of the university as a whole (*standard 2: safe and open culture*). The faculties are responsible for the security of their own ICT facilities within the framework of central ICT policy. Little or no restriction is imposed by the central ICT Services (ICTS) department on the faculties and services of the UM; its primary function is to provide services to the faculties. Due to the customer-oriented relationship between the faculties and ICTS, in addition to providing services, it chiefly has an advisory role. In recent years, data security has increasingly been the subject of discussion, and awareness campaigns have been mounted within UM. However, these focused on personal actions – such as safe data storage and the use of strong passwords – and less on the chance that third parties might gain access to the UM network by means of undesirable activities *(standard 1: increasing awareness)*. Since 1994 UM has had a Computer Emergency Response Team (CERT) and since 2003 a Chief Information Security Officer (CISO) and a plan for major incidents (including ICT), but this did not include ransomware attacks *(standard 3: establishing a crisis team).* Barely any internal control is established on implementing ICT policy and following up on agreements; external control is process-based and only focuses on the financial and HR package of UM's central IT *(standard 6: monitoring and evaluation)*. The UM-CERT is affiliated with SURFcert and thus exchanged information with other partners in the chain about information security, and UM took part in the SURF cyber exercises *(standard 5: supply chain cooperation).* UM was redesigning its IT organisation *(standard 7: investment/measures)*; however, the Executive Board and the organisation as a whole did not prioritise cyber risks as one of the most important risks in relation to ensuring the smooth continuance of education and research *(standard 4: assuring risk management)*. UM makes use of the annual cyber threat assessments produced by SURF. Here too, a cyber attack was not among the risks that were assigned the highest priority. In addition, the incorporation of cyber security into risk management is made more difficult because these risks come on top of the existing considerations regarding expenditure, and a deeper knowledge of the subject is needed in order to discuss the issue *(standard 4: assuring risk management)*. The choice of a decentralised organisational form, such as that of UM, can make an organisation vulnerable. Other universities and colleges also have a multi-layered administrative structure and are therefore potentially vulnerable. The challenge lies in the combination of ICT policy, the implementation of digital information security throughout the organisation, and monitoring given the organisational form.

Sub-question 2 - Response: What action did UM take in response to the cyber attack to restore the continuance of education as quickly as possible?

On 15 October 2019, a phishing email was opened. Fox-IT has determined that, due to insufficient detection, monitoring and follow-up, hackers were able to carry out a ransomware attack on part of the UM network on 23 December 2019 *(standard 1: increasing awareness)*. In the period after the ransomware attack was initiated, the Executive Board dealt with it in close coordination with the university's Crisis

Management Team, Supervisory Board, representative bodies and other sections within the university *(standard 3: establishing a crisis team; standard 2: open and safe culture)*. Communication to staff and students was also of paramount importance and took place by means of daily updates via the UM website *(standard 3: establishing a crisis team; standard 2: open and safe culture).* In addition to broad coordination, an informed decision was made on how education and research could resume after the Christmas period *(standard 4: assuring risk management)*. To ensure the continuity of the organisation, the university saw it necessary to make a ransom payment in order to obtain the decryption key. Had the payment not been made, it was expected that repair and reconstruction would take several months, which would have seriously jeopardised the proper continuance of education and research. In addition, there was no assurance that without the decryption key, the IT infrastructure and data could be fully restored. A broad consideration was made of different scenarios. At the request of the Supervisory Board, a cost estimate was also made of the alternative of the university restoring the IT infrastructure itself. The cost was estimated to be many times that of the scenario of making a ransom payment *(standard 4: assuring risk management; standard 7: investment/measures)*. During the management of the incident, the Executive Board and Supervisory Board decided to be open where possible, so that other higher education institutions could draw lessons from the cyber attack at Maastricht University *(standard 5: supply chain cooperation; standard 2: open and safe culture)*.

Sub-question 3 - Learning capacity: What provisions has UM made to prevent the occurrence of similar incidents in future, with a view to the proper continuance of education?

Since this inquiry took place in the two months after the ransomware attack, the Inspectorate focused only on UM's initial lessons learned. In addition to the chiefly technically oriented vulnerabilities that Fox-IT exposed, the Inspectorate believes that the university also faces multiple organisational challenges in order to increase its cyber resilience. The university indicates a need for knowledge-sharing regarding cyber threats and clear support from government *(standard 5: supply chain cooperation)*. During the management of the cyber incident, work was carried out on 'increased dike monitoring'. By means of external contracting the IT systems were continuously monitored in this phase. In addition, a survey was made of the entire central and decentralised IT infrastructure *(standard 4: assuring risk management; standard 6: monitoring and evaluation).* There was a clear awareness of the preventive measures that needed to be tightened. In the long term, UM wishes to introduce continuous (24/7) network monitoring in cooperation with other educational institutions *(standard 5: supply chain cooperation; standard 6: monitoring and evaluation)*. The entire UM organisation has indicated that cyber security needs to be discussed *(standard 1: increasing awareness)*. Because the systems in everyday use have been restored, some people are under the impression that the cyber attack has been fully resolved, and parts of the organisation are returning to normal *(standard 1: increasing awareness).* ICT staff indicate that now is the time to take further measures, for example by increasing attention to detail, maintaining a permanent overview of all existing and new IT systems, improving the organisation of the audit, and conducting a periodic test to identify weaknesses in the infrastructure *(standard 4: assuring risk management; standard 6: monitoring and evaluation)*. In the coming period it will become apparent how much support there is for such measures within UM when budget discussions deal with the dilemma of choosing between investing in the primary process of education and research on the one hand and cyber resilience on the other *(standard 2: safe and open culture)*.

4 Findings

We base the conclusions in Chapter 3 on our institutional visit and document analysis. In this chapter, we describe our factual findings for each sub-question that led to these conclusions. The findings are arranged according to the aspects of the BIO guidelines that may be used by administrators. In Section 4.1 we first describe the chronology of the cyber attack at Maastricht University (UM). In the subsequent sections, we discuss the findings in the areas of prevention, response and learning capacity.

4.1 Timeline of the cyber attack

Figure 1: Timeline of the cyber attack at Maastricht University

In the timeline (see Figure 1) we identify five phases. The first phase (the first block in the figure, on the left) relates to the period prior to the opening of the phishing email which ultimately led to the cyber attack. On 15 October 2019, a document was opened via a link in a phishing email. This gave the hackers initial access to the UM network. This phase is discussed in Section 4.2.

The second phase relates to the period from the time that the hackers explored the network after the phishing email had been opened until the ransomware attack was initiated on the evening of 23 December 2019 (second block in the figure). After the attack was noticed because UM no longer had access to parts of the IT systems, UM started crisis management. In this third phase, the decision-making took place which ultimately led to the payment of a ransom to the hackers in order to obtain the key with which to restore the IT infrastructure (third block in the figure). The second and third phases together are central to Section 4.3.

On 12 February 2020, UM scaled down the crisis management to tightened cyber security, or 'increased dike monitoring' (fourth block in the figure). At the start of this phase, most of the IT infrastructure had been restored. UM realised an increased level of vigilance by continuing to use external monitoring. Crisis management also continued, including a leniency scheme for students and additional research into the cyber attack itself. At the time of writing this report, it is not yet known when UM will switch from 'increased dike monitoring' to a new regime of regular cyber security. Section 4.4 focuses on the lessons that UM has already learned for the future (the last two phases in blue in the figure).

4.2 Findings for sub-question 1: Prevention - Prior to the cyber attack

The findings below relate to the first sub-question: *how was UM prepared for a cyber attack and had UM taken preventive measures to ensure proper continuance in the event of a possible attack (cyber resilience)?*
The findings in this section relate to the period prior to the cyber attack – the period up to 15 October 2019.

Increasing awareness

- With regard to awareness, UM has mounted various campaigns in recent years. An important catalyst was changing privacy legislation (GDPR). The emphasis in campaigns was therefore on privacy protection, such as: 'treat your password as if it's your underwear'. This was aimed at raising awareness: not sharing passwords with other people, changing them regularly and not treating them carelessly. Presentations about the General Data Protection Regulation (GDPR) were also given in various sections of the university. Because at that time the Chief Information Security Officer (CISO) also fulfilled the function of Data Protection Officer (DPO), cyber security topics were also included in these presentations. However, during interviews with the Inspectorate, staff and students did not mention campaigns aimed at the dangers of malware. During these conversations, the representative bodies said that they did not know what level of awareness there was within UM. Those who were interviewed said they assumed that they did not click on phishing emails themselves, but they did not know whether this was definitely the case. On the other hand, staff of the central ICTS organisation has devoted attention to research by UM staff on malware, as they set up a protected network for it.
- The GDPR privacy legislation also prompted some units to critically examine the use of external data storage using Dropbox. Within each faculty, for example, staff were not only made aware of an alternative, but the switch was 'guided'; the information manager ensured on his own initiative that SURFdrive[11] was made available to individual researchers within the faculty.
- A tightening of password policy, to use stronger passwords, was initially introduced only for staff. According to various sections of the university, discussions about introducing it for students had been ongoing in the pre-attack phase for a long time. After the cyber attack, a measure whereby students switched to stronger passwords was quickly implemented. There was no incidence of the problems that constantly blocked the introduction of this measure prior to the attack.
- While the issue of cyber threats was discussed within the university, it was not prioritised as one of the highest risks, according to various interviewees, including members of the Executive Board.
- In early October 2019, at the request of the Supervisory Board, a training session was organised for the Supervisory Board on IT security and privacy, in the context of lifelong learning. This training was provided by various parties at UM: the Chief Information Security Officer (CISO) and two UM professors from the UM European Centre on Privacy and Cybersecurity (ECPC). The importance of increasing awareness was one of the lessons in this training session.

Safe and open culture

As with other universities, UM has widely varying degrees of freedom in its organisation. This is reflected in the UM Administration and Management Regulations, and also applies to IT. The IT structure therefore differs for each faculty. This situation has arisen historically, as a result of differing wishes depending on the education and research within units in the organisation. Faculties and services themselves determine what services they will obtain from ICTS and what will take place within their own network management. The central ICTS organisation is regarded by everyone within the UM as a service provider. The client, including decentralised organisational units, determines the desired IT structure, which therefore differs locally. This also means that there are many and varying exceptions to more central principles.

[11] SURFdrive is a file storage service similar to Dropbox, but hosted by SURF and made available via ICTS.

- The central organisation at UM, including ICTS and the CISO, has a limited overall view of IT within the university as a whole. Due to the structural differences between the university's organisational units, signals from IT systems partly arrive at different locations in the organisation, and prior to the cyber attack they were not all forwarded to one central point. Although a lot of log files are already collected at a central location, and attacks are detected, some matters were hidden from view. Members of the UM-CERT indicated during the interviews with the Inspectorate that in this sense monitoring was inadequate: because malicious activity (including malware) looks increasingly 'normal', it is difficult to identify immediately. Only when a connection can be made between multiple reports do you start to recognise the nature of such activity, interviewees indicated.
- Signals about ICT can also come from staff and students, who can make a report to the service desk. However, conversations with staff and students show that if they are suspicious, they sometimes also choose to perform a virus check themselves and not report it to the service desk. UM's Information Security Policy makes clear that each organisational unit is responsible for identifying and reporting incidents and breaches of information security.
- Each faculty has an information manager (IM) who is the contact point for the CISO and the Data Protection Officer (DPO), from the perspective of security and GDPR respectively. The IMs also hold meetings for knowledge sharing and discussion.
- Various sections report that there is openness to discussion within UM, but it is hard to arrive at operational agreements. Many subjects related to structural issues often go undiscussed for long periods.

Establishing a crisis team

- UM has had a Computer Emergency Response Team (CERT) since November 1994, chaired by the CISO. The UM-CERT has 11 members, almost all of them staff of the central ICTS department. CERT members are available on call on a voluntary basis, also outside office hours.
- UM has a general plan for major incidents, which includes determining the composition of the crisis team and the involvement of the executive and the communications department. The plan provides no specific framework for a ransomware attack of the magnitude faced in December 2019.
- If a limited cyber incident occurs, it is normally dealt with by two to four people. A problem is never solved by one person alone, but at minimum by two.
- UM participates in exercises related to digital security run by SURF. Exercises also take place locally at UM. The exercises do not only involve technicians, members of the CERT; a conscious choice has been made also to involve management and communication.

Assuring risk management

- Prior to the attack, the risk of external cyber threats was not the highest priority for UM. Risks for education and research at UM related to the political and social discussion concerning language and internationalisation were higher on the agenda. In discussions between the Executive Board and the representative bodies, the topic of workload also played an important role, a situation which is not unique to UM. UM makes use of the annual cyber threat assessments for higher education produced by SURF. Here too, a cyber attack was not among the highest prioritised risks.

- According to the Executive Board, establishing infrastructure for the university, such as cyber security and accommodation, always involves taking difficult decisions about the budgets to be spent, which are then not available for the primary process: education or research. These are subjects which can only be considered by the Executive Board and its discussion partners (representative bodies and the Supervisory Board) after careful study.
- Every two years the central organisation participates in the SURFaudit. In 2019, UM's score was 2.5; the average score of participating universities of applied sciences and academic universities in that year was 2.3.[12] The most recent audit was performed by one person, partly based on the audit information relating to the annual financial statements. The audit has so far focused on central IT, not on the variety of IT facilities in the various UM organisational units. Few of the UM staff with whom the Inspectorate spoke were aware of the SURFaudit and its results. There was wider awareness of questions asked by the external auditor as part of the financial audit about business-sensitive IT systems, including the HR system.
- At the training session in the autumn of 2019, the Supervisory Board became aware of the partnership within SURF and the audit standards that are applied in the SURFaudit.
- Various discussions dealt with the fact that in the field of information security, in the Deming circle (plan-do-check-act, PDCA), UM often omits the steps 'check' and 'act'. We will return to this subject under the topic 'monitoring and evaluation' later in this section.

Supply chain cooperation

- In the field of cybersecurity, CERTs from academic universities, universities of applied sciences and a few vocational education and training (MBO) institutions exchange information. They do so in the SURFnet Community of Incident Response Teams (SCIRT) and with SURFcert. The UM-CERT is affiliated with SURFcert. Within SURFcert discussions have previously been held on the dependence on external companies to deal with cyber crises and on a joint effort to monitor external threats. Until the attack on UM, this did not result in any concrete agreements. However, SURFcert does conduct a large-scale cyber exercise every two years. Such a national exercise took place in 2016 and 2018, in both of which UM participated.
- Given that in UM's organisational units, within the framework of central policy, it is possible to determine how IT is structured, there is also supply chain cooperation within the UM organisation. Network administrators indicate that different configurations are in use within UM for each system type or system. The central network manager knows which variants are available within the central structure. However, in some organisational units, differing configurations may occur. The central ICTS department lacks insight into the various options that are in use within UM. This means that the 'apply or explain' principle is not fully observed within the UM organisation.
-

[12] See: B. Bosma (2020) *SURFaudit benchmark 2019 – rapport*. Version 1.0. https://wiki.surfnet.nl/pages/viewpage.action?pageId=31103911

Monitoring and evaluation

- As indicated under the topic of risk management, the 'control' function at UM with regard to information security is limited. UM has an internal central auditing service that has not played a role in investigations into the risks of ICT systems. Risks to IT systems are part of the annual audits by the external auditors. In the context of their assignment, the audit of the financial statements, the external auditors limit their annual investigations, and thus also the cyber risks to their client's financial and HRM systems. These systems were not the target of the hacking attack, according to UM.
- In the past five years, external auditors have reported very generally on the risks associated with cyber crime and cyber security. Possible forms of cyber risks specific to UM are not mentioned here. The auditors have not received any additional instructions from UM for a specific investigation into cyber risks. However, the auditors have discussed ICT risks un general terms, and have determined that it has regularly been included in spending assessments made by the UM administration. These considerations always had to be made within the financial frameworks (available funding and resources) and the rapidly and dynamically developing technical complexity of ICT.
- Staff responsible for the management of business-sensitive information systems within UM indicate that they have answered questions for the external auditor. They note that these questions have been aimed at a process-based check, while at security level it is precisely the details that are of great importance. They consider that a process-oriented audit is not a sufficient test of information security.
- With regard to monitoring information security, the Supervisory Board indicates that developments in this field are moving so fast that board members increasingly require regular information from experts.
- In the field of data protection, the DPO also has a monitoring (supervisory) task within UM. In the field of information security, the CISO has so far mainly played an advisory role within UM. The CISO advises on the infrastructure by indicating areas in which risks may or may not be taken. There are no checks on the actual implementation of the IT system. An example from the interviews provides an illustration: in one of the faculties, grant applications always have to go to a policy officer and budget controller. Depending on which policy staff consider the application, an IM will be called in at the point that changes are requested in systems on the basis of grant funds.
- Another faculty has chosen to have as much as possible hosted centrally by ICTS. This faculty manages less and less internally and almost all staff use a Virtual Desktop Infrastructure (VDI) workstation. If desired, staff can deviate from this. As a result, advice from the IM about the workstation and software wishes of individual staff is less common in this faculty.

Investment/measures

- Investing in IT infrastructure for UM always involves a trade-off between expenditure on ICT or expenditure on primary processes: education and research. This is an issue that is not unique to UM but applies to all higher education.
- In 2017, UM formulated the UM-I Strategy 2018-2021, which set the current IT course. This strategy includes the use of IT for the benefit of education and research, as well as data protection and compliance with security and privacy regulations. The first period that preceded the introduction of this IT course concentrated on establishing the organisation, including recruiting a new Chief Information Officer (CIO).
- After all positions were filled, the wishes for the establishment of a Security Operations Centre (SOC)/Security Information and Event Management (SIEM)

team were indicated. Members of this team focus entirely on security vulnerabilities. This is not the case for CERT members, who stop their normal activities in the event of a crisis in order to focus on the crisis. An SOC provides capacity for monitoring the IT infrastructure. A few years ago, in the context of SURF, UM participated in a study into whether the organisation of specialist team for monitoring by universities could be taken on by SURF. This was because UM did not expect to be able to set up a 24/7 facility using its own resources. At the time, the proposal was rejected. UM had planned to start its own SOC by January 2020.

- Staff can report software wishes to the IM of their own faculty or service. The wishes vary widely, partly due to cooperation with institutions from other countries. To accommodate new wishes, IMs from different faculties and services coordinate with each other to determine whether it would be possible to acquire a university-wide licence.
- The choice of workstation design differs for each organisational unit at UM: there are units in which a VDI workstation is assumed as a standard, and those in which the employee is free to choose. These freedoms depend in part on the preferences of deans and may therefore differ from one period to another.
- In some cases a group within a faculty may have funding from a research project and will thus purchase its own devices which it wishes to have incorporated into the network. In general, the purchase of the devices is included in the funding, but often the additional cost of arranging information security is not included. Due to the variety of devices, a large number of Windows versions or other operating systems are in use. In some cases these are old operating systems that are no longer supported by the manufacturer.
- UM operates a variety of rights structures for workstations. Regularly, more than standard user rights are granted. During the interviews with the Inspectorate, an ICT staff member indicated that he had administrator rights on the laptop, but that this was unnecessary for 99% of his work. The same will also apply to researchers; a variety of their activities, such as answering e-mails, searching for information on the internet or writing, no extensive rights are necessary. It is not customary to discuss when such extensive rights are used.
- Staff members indicate that the procedure for issuing a new workstation is simple: you simply pick up the device and start work. No specific instructions are given on what you can and cannot do, or on the risks the user should be aware of. Students can also start work immediately after logging in for the first time.

4.3 Findings for sub-question 2: Response – cyber attack and crisis management

The following findings relate to the second sub-question: *What action did UM take in response to the cyber attack to restore the continuance of education as quickly as possible?*

We consider the period from 15 October 2019 to the point that UM crisis management switched to 'increased dike monitoring' on 12 February 2020. The Inspectorate focuses on the actions of the organisation, not on the technical details of the attack. The Fox-IT report provides additional insight into these details.

Access to the network by means of malware (increasing awareness)

- On 15 October 2019, a UM staff member opened an Excel document via a link from a received email. The forensic investigation conducted by Fox-IT revealed that this Excel document contained malware that gave the hackers initial access to the UM network. On 16 October, a second employee opened a similar Excel document via a link from a phishing email. The hackers were then able to map the UM network.
- In October 2019, a number of phishing emails were received within the UM domain, which a few other staff members also reported to the ICT service desk. The response to these reports, as appears from the Fox-IT report, was not always adequate.
- Various tests at universities of applied sciences and academic universities show that there are always people who respond to such phishing emails. For example, in April 2017, 31% of the staff of HAN University of Applied Sciences entered their details in an email about the abolition of staff Christmas gifts,[13] and 9% of staff at Erasmus University responded to a satisfaction survey[14] that did not originate from their own organisation. Shortly after the cyber attack at UM, in February 2020, staff at Avans University of Applied Sciences filled in personal details to send a Valentine's message.[15]

Propagation within the UM network not prevented (safe and open culture)

- A number of weaknesses in the IT infrastructure and organisation at UM contributed to the magnitude of the eventual ransomware attack, as shown by the root-cause analysis conducted by Fox-IT. The latest security updates had not been performed on a number of servers in the network and there was limited segmentation within the UM network. In addition, monitoring was inadequate, so no response was given to the reports of a virus scanner that was ultimately manually disabled by the hackers. Among the consequences was the failure to detect the malware. The complexity of UM's IT infrastructure, the lack of an overview of the structure of the infrastructure as a whole, and the lack of a central location to receive all reports from the various systems in the UM network have already been discussed in section 4.2.
- The limited segmentation, according to the Fox-IT report, relates both to the network architecture and the user rights. The Fox-IT report observes that the hackers first obtained administrator rights on a number of insufficiently updated servers in order to obtain full administrator rights to the UM network on 21 November 2019. This was possible because there was too little segmentation between the admin domains. As indicated in Section 4.2, UM staff can easily obtain more user rights in various organisational units within the UM organisation. Examples from the interviews showed that there is rarely any discussion of a more careful use of extended rights.

[13] See: https://www.businessinsider.nl/hogeschool-han-doet-een-test-met-phishingmails-en-31-van-het-personeel-trapt-erin/ (consulted on 7-03-2020)
[14] See: https://www.ad.nl/rotterdam/erasmus-universiteit-test-medewerkers-een-op-de-elf-trapt-in-val-phishingmail~a6883d30/ (consulted on 7-03-2020)
[15] See: https://punt.avans.nl/2020/02/geen-valentijnsactie-bij-avans-maar-phishingtest/ (consulted on 7-03-2020)

Starting the crisis organisation (establishing a crisis team)

- On the evening of 23 December 2019, it became clear that a major cyber security incident was taking place. The director of the central ICTS department was therefore called by a UM-CERT member. UM-CERT members could not log in as an administrator from home. Some of them came to Maastricht. The Vice-President of the Executive Board was also informed. It was decided to isolate the entire UM network by taking the systems offline and closing the university buildings. The upscaling to board level was in line with the plan of action that had been practised in the last national SURF exercise, OZON.
- UM-CERT members have the contact information for SURFcert and Fox-IT. Both organisations were contacted and asked for assistance during the night of 23 to 24 December 2019. It became clear during the night that the incident was more serious than a regular cybersecurity problem. In accordance with regular UM protocols, crisis management subsequently came into effect.
- The Crisis Management Team (CMT) met for the first time on the morning of 24 December 2019. The team consisted of the Vice-President of the Executive Board, the Director of ICTS, the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Managing Director of Legal Affairs (also Secretary to the Executive Board), the Deputy Director of Legal Affairs, three varying representatives of marketing and communication, and staff of Fox-IT.
- The focus for the CMT changed over the course of the cyber crisis. After identifying and securing systems, priority was given to the proper continuance of education and research, with the ultimate consequence that forensic data could have been lost as a result. Later, after obtaining the key from the hackers, the priority shifted to the recovery of the entire IT infrastructure by UM and the securing of forensic data by Fox-IT in order to investigate both the root causes (circumstances, cause and scope) and the hackers' access to data (including viewing, stealing or otherwise processing). Fox-IT was present on site in Maastricht from the afternoon of 24 December 2019, and besides conducting an investigation, it advised on mitigation and recovery measures.

Communication after the ransomware attack (establishing a crisis team)

- As a consequence of taking all systems offline, communication via UM email addresses was not possible. Through SURF, UM obtained a number of temporary email addresses (such as info@m-u.nl) so that students and staff could ask questions. A staff member indicated that an email[16] was received about the cyber attack. Because this person had no access to their own UM email account, they checked with a colleague to find out whether this message was true.
- In addition to formal communication, there was a desire for contact among staff and students. Various WhatsApp groups were therefore created within UM.
- Because the UM website was not infected, it remained online and the CMT used it as a communication channel. Updates were published daily, with the main focus on providing information to the internal organisation, staff and students. However, this information was also available to external parties.
- Faculties and student associations helped to share this information through their social media channels. Information desks were set up once the buildings had reopened. In the interviews with the Inspectorate, staff and students indicated that the updates that appeared on the website a few days after the cyber attack created understanding and alleviated concerns. On the basis of this, information you knew what was working and what was not.

[16] This was an email sent to a private email address, as no email could be received via UM email addresses.

- In the week after Christmas, in consultation with the Supervisory Board, the Executive Board decided to be open about what had happened and to share the lessons in a symposium. UM sees this as its duty to society.

Considerations in combating the cyber attack (assuring risk management)

- The ransomware installation on the evening of 23 December 2019 took place during a relatively quiet period for the university. Staff and students were not present in large numbers due to the holidays. The course period was to resume from 6 January 2020. This gave the Executive Board and the crisis organisation more time than would have been available during a regular course period to assess the impact of the attack and investigate scenarios to restore the IT infrastructure. The scale of the cyber attack turned out to be considerably larger than that simulated in the SURF-OZON and UM-NOZON exercises. Considerations that the board faced had never featured in the cyber exercises.
- The Executive Board and the CMT were faced with the task of choosing which primary processes were to be restored first. This was done in coordination with all deans and directors. Education was given priority over research. The continuance of the planned teaching and exams from 6 January 2020 was given the highest priority. Coordinated by the CMT, working back from 6 January, it was decided what needed to be done to be ready on that date in order to restart the teaching process.
- The Executive Board's options to deal with the crisis consisted of three scenarios:
  1. Build a decryptor to remove the encryption;
  2. Completely reconstruct the IT infrastructure and then restore backups to return to the pre-attack situation; or
  3. Meet the hackers' ransom demands.
- Fox-IT's investigation of the encryption revealed that the first of these options was not realistic. If successful, the continuance of education and research would be disrupted for more than three months. The second option, rebuilding the IT infrastructure, was estimated at two to three months. This would mean that an entire course period would be lost both for degree programmes and research. Moreover, with this option it was not clear whether all data could be recovered. The fact that UM's backups were mainly online rather than offline made this option more difficult. UM mainly made backups online because this has the advantage of enabling staff and students to access educational and research data again relatively quickly in the event of disruption. However, in principle online backups can also be infected by malware, making them unusable.
- In view of the course period that was due to start within two weeks, the Executive Board started orienting itself towards meeting the demands of the hackers. During the decision-making process about the scenarios, the Executive Board had close contact with the Supervisory Board, the deans, the council of directors and the chairperson of the central representative body. External legal advice was also sought with regard to the scenario in which UM would make contact with the hackers. In addition to informing the sections of the university internally, the Executive Board also informed the Ministry of Education, Culture and Science, the Inspectorate and the Police (High Tech Crime Team) about the conclusion of the decision-making process. There was also contact with the Dutch Data Protection Authority in connection with the data breach because third parties had gained unauthorised access to the UM network.

Contact with hackers and ransom payment (assuring risk management)

- The general line of central government is that it advises against transactions with criminal organisations. This is a view which UM fully endorses. In practice, however, such a general line has proved to be complex. For the Executive Board, these considerations of public interest could not prevail over the interest of the university, which was to get 'back in business' as soon as possible so that it could fulfil its obligations to students and staff.
- Before meeting the hackers' demands, UM attempted to realise a number of safeguards. These consisted of:
    - Sending a small number of encrypted files to the hackers – containing no personal information – for decryption
    - Making a trial payment in bitcoins to the hackers, after which the hackers were asked to indicate the amount they had received
- These safeguards were aimed at gaining a degree of certainty that UM was in contact with the right people and an idea of the reliability of their organisation. For the same reasons, some technical questions were put to the hackers. In addition, the email address obtained from the hackers was information that could be of use in tracing the criminals.
- As part of this inquiry, the Inspectorate considered whether the payment of approximately €0.2 million (in bitcoins) to the hackers falls within the limits of the effective use of government funding. During the cyber attack, UM considered the cost of repairing the hack itself. The conclusion was that due to the size and complexity of the IT system, it would have taken at least a few weeks to three months to restore all systems safely and to make old files accessible. In addition, the use of external specialists would have been necessary. The long duration and the high costs of deploying internal staff and hiring external specialists, as well as the increasing liability towards students, would have been many times the amount of the payment to the hackers behind the cyber attack.
- To make the payment in bitcoins, UM selected an external company that was able to pay in this currency. To cover the payment, in 2020 UM will draw on dividend payments from its subsidiary Maastricht University Holding BV, which recently sold a start-up subsidiary and therefore has more than enough liquidity to pay a dividend that is well above the amount paid to the hackers. Because UM has never distinguished between public and private equity, this payment will be made from public equity.

Sharing 'Indicators of Compromise' and assistance (supply chain cooperation)

- In the forensic investigation, Fox-IT identified Indicators of Compromise (IoCs). IoCs can indicate malicious activities in a digital environment. On 24 December 2019, UM shared the IoCs with other affiliated universities and colleges via SURF-CERT. Other higher education institutions can use the IoCs to check whether suspicious activity is taking place on their networks. The Executive Board and Supervisory Board see sharing the IoCs as their obligation as a university that receives public funds.
- On the other hand, UM indicates that universities cannot necessarily expect to receive IoCs from other institutions. They concern information both from within the Netherlands and from abroad – after all, cybercrime is not only a Dutch matter. For example, UM was not aware that the University of Antwerp had recently been subjected to a ransomware attack, in October 2019. This incident was not mentioned on the warning list regarding cyber attacks that SURF regularly provides to universities. SURF was not aware of this attack either. The attack in Antwerp took place at the stage when access to the UM network had already been obtained.

- As previously indicated, UM does not have a specific protocol for handling a cyber attack, and the crisis organisation was set up on the basis of the UM protocol for major incidents. In the field of IT, this focuses on major disruptions without malicious intent. On 24 December 2019, UM contacted the National Cyber Security Centre (NCSC) to ask if a protocol was available. This was not the case. UM had contact with the NCSC a number of times that day and provided information that enabled the centre to inform the healthcare CERT so that they could take precautions. The NCSC provided UM with the contact details of the police High Tech Crime Team and also indicated that for legal reasons information could only be shared via SURFcert, not provided directly to UM. The NCSC is the body for vital sectors and central government.

Restoration of business operations (supply chain cooperation)

- During the course of the crisis, the CMT's focus switched to restoring business operations. For education, coordination took place with the Education Executive Agency (*Dienst Uitvoering Onderwijs,* DUO) regarding the closing deadline for enrolment for degree programmes with intake restrictions (*numerus fixus* programmes). It was agreed with DUO that enrolment via Studielink could take place as normal, but that prospective students could supply the necessary documentation for the selection procedure at a later date.
- Researchers have to meet deadlines with regard to research grant applications. UM contacted the Netherlands Organisation for Scientific Research (NWO) and the EU in connection with this. Because most researchers store their important data, including grant applications, in multiple locations, it was possible to agree with NWO that applications would be submitted by the deadlines, but that UM researchers would be granted a postponement for the mandatory appendices to their applications (e.g. data held on UM systems). The EU did not grant any postponement. The Executive Board has received no indications that researchers were unable to submit their proposals.
- It should be noted that the storage of data (e.g. Dropbox) by staff in some cases contravenes UM information security policy. Under normal circumstances, prior to the cyber attack, this was a vulnerability for users with regard to information security (see Section 4.2). However, at the time of the cyber attack, it proved to be of benefit, thus incorrectly confirming staff members' impression that it is good to store data elsewhere.

Monitoring and evaluating

- As mentioned earlier in this section, the network monitoring at the start of the incident was not sufficient to counter the propagation between 15 October and 23 December 2019. After the ransomware attack had been initiated, Fox-IT, in consultation with UM, installed a number of network sensors and the Carbon Black monitoring tool on Windows Servers and workstations. Using these tools it is possible to detect centrally whether there are irregularities on systems and in the network.
- As indicated in Section 4.2, UM planned to set up a Security Operations Centre (SOC) in January 2020, but the choice of monitoring tool still had to be made. As a consequence of the cyber attack, a tool was chosen, namely Carbon Black. The tool was initially deployed on the hacked servers for the forensic investigation conducted by Fox-IT. It was then rolled out to the rest of the Windows Servers and finally to the Windows workstations, both physical workstations and VDI systems. The tool was installed on Windows Servers before they became available again within the network. From the go-live (2 January 2020), UM introduced 24/7 monitoring in collaboration with Fox-IT.

- The Supervisory Board indicates that the Executive Board provided it with a great deal of information in relation to its supervisory task, such that it was aware of the most important facts. The Supervisory Board approved the approach chosen by the Executive Board and requested a specification of the financial consequences of the alternative of the university repairing the IT infrastructure itself. In addition, the Supervisory Board requested that communication both internally and externally about the cyber attack and the lessons to be learned from it should be as transparent as possible.
- Fox-IT investigated the attacker's activities on a number of critical data systems, 'the crown jewels'. The investigation was limited to two UM systems on the basis of known IoCs. As a result of this survey, Fox-IT indicated that no traces had been found other than the ransomware. Fox-IT does note, however, that these findings cannot yet exclude the possibility that data was viewed, stolen or processed by the hackers. Fox-IT recommends that the UM follow-up investigation should be conducted in order to be able to make a statement with greater certainty.
- The attackers' activities were discussed in the interviews with the representative bodies, and with staff and students. Students indicated that there was certainly a fear among graduating students that raw or processed data had been lost. People would like to know who exactly has been 'in the building'. In addition, they said they wished to know which systems had *not* been affected, about which there was therefore no cause for concern. In this sense, the current results are not yet satisfactory.

Investment/measures

- During the restoration of the IT infrastructure, various measures were taken to improve digital security at UM. In addition to network monitoring by the sensors and the Carbon Black software, the following measures were taken to improve monitoring and evaluation:
    - Password reset and strong password policy for everyone: all staff and students were required to create a new password when they first logged into the UM network after 2 January 2020. The new strong password policy, which already applied to UM staff, also became applicable to students. The password policy was mentioned as an example of issues that had previously been dealt with slowly but which were now being implemented rapidly, and which met with understanding.
    - Minimum requirements for operating systems on workstations and servers: older operating systems that are no longer supported by the manufacturer are not permitted on the UM network.
    - Additional restrictions on the network segmentation within the UM network: this increases the overview of the entire network, which also benefits monitoring.
    - Offline backups to be made before a system can go live.
- Regarding the combination of measures already taken, ICT staff indicated that it is important that monitoring should remain at a high level, because infections will always occur, as they cannot be prevented. In order to prevent attackers from penetrating more deeply, it is important to protect 'endpoints' optimally (good server management).

- Another measure was to introduce a leniency scheme for students who have been disadvantaged or suffered damage as a result of the cyber attack. The scheme was established in coordination with parties including the boards of examiners. By mid-February 2020, only seven reports had been received. These were processed and resolved individually, for example by means of financial compensation (e.g. one month's tuition fees because graduation had to be delayed by a month).

4.4 Findings for sub-question 3: learning capacity – prevention of future incidents

The findings in this section relate to the third sub-question, on the learning capacity of the organisation: *What provisions has UM made to prevent the occurrence of similar incidents in future, with a view to the proper continuance of education?*
In this section we consider the period from 12 February 2020 onwards. From that point, UM's crisis organisation was no longer convened, and the cyber attack would now be dealt with on the basis of tightened cyber security, or 'increased dike monitoring', for example by hiring Fox-IT to realise 24/7 monitoring. In this section, the Inspectorate discusses the lessons that UM has learned to achieve a new level of cyber resilience for the university.

Increasing awareness

- Fox-IT recommends that periodic attention is required to maintain security awareness. This should take place not only by mounting campaigns, but also, for example, by conducting phishing tests within the organisation. In addition, the representative bodies have indicated that UM has drawn up digital hygiene rules. These rules have not been communicated to staff and students in the setting of a formal meeting. They are not aware whether such meetings are planned.
- Both the CMT and the ICT staff indicate that there is a danger that the UM community will backslide and fail to learn the appropriate lessons. People are no longer even aware that hard work is still being carried out to complete the recovery and maintain information security at a high level. From a number of interviews it was apparent that sections of the UM community were under the impression that the organisation is now functioning as before, because the university went live very quickly. This was noticeable, for example, when it became possible to print again in UM buildings.
- In addition, staff members' old behaviour of storing data in Dropbox, for example, has been reinforced, because it was this that enabled the university to continue working while the system was 'locked'. Staff must be made aware that this is not wise, ICT staff say.
- The Executive Board notes that the cyber attack at UM and the Citrix problems that occurred shortly afterwards have sparked a nationwide debate. The representative bodies indicate that it is important to them that the Executive Board as a whole should carry the load.

Safe and open culture

- Fox-IT also recommends ensuring that users more frequently report incidents, whether deliberate or unintentional, and that the reports should subsequently be followed up and adequately addressed. Fox-IT indicates that the existing open culture of communication can be used to increase the willingness to report.
- The need to improve incident reporting and follow-up action was raised in a number of interviews. For example, it was indicated that while it is possible to make a report digitally, the reporter does not always receive feedback.

- The challenges facing ICT staff – given that UM's IT infrastructure is so multifaceted and diverse – have already been discussed in section 4.2. Although on many systems logging does takes place, the data is not all compiled in a single location. The Executive Board sees this as an important area for improvement. This has also been indicated by Fox-IT as a recommended measure (monitor log files for anomalies) to increase the chance of detection. During 'increased dike monitoring', the monitoring has been partially outsourced so it can take place day and night.
- The attack has illustrated to the representative bodies the importance of cyber security. As far as they are concerned, the discussion with the Executive Board on this topic is still ongoing and will also continue when the new representative bodies convene. The Executive Board is open to discussion about considerations and obstacles, the representative bodies say, but naturally there are differences in affinity with the subject of cyber security.
- The Supervisory Board indicates that there are many people with relevant specialist knowledge at the university itself. The organisation can draw on this for future cyber resilience.
- The various participants in interviews said they were proud of the organisation and the way the cyber attack had been resolved. Loyalty and commitment was displayed, also during the Christmas holidays. The Executive Board is aware that there are also critical voices, as shown by student reactions to the payment of a ransom. However, the predominant response of students and staff was appreciative.
- ICT staff are also pleased with the way in which the crisis was tackled. However, as previously mentioned, they also express concerns about the danger that insufficient lessons are learned.

Establishing a crisis team

- As previously mentioned in Sections 4.2 and 4.3, UM does not have a specific framework or protocol on how to deal with a ransomware attack of this magnitude. Fox-IT recommends that an incident response plan should be drawn up for this type of emergency. UM has indicated that it followed the general UM procedures for crisis management, which the CMT describes as a workable approach. In consultation with the Executive Board, the CMT called in specific expertise, for example in relation to Bitcoin payments.
- As part of its reporting, the ICTS has assessed the functioning of the crisis organisation, in relation both to its organisation and to its key activities.
- UM-CERT worked on the incident outside of office hours with an on-call list on a voluntary basis. The voluntary aspect of this approach is currently being reconsidered. This also depends on the structure of the SOC and the possibilities for collaboration with other higher education institutions.

Assuring risk management

- It is hard to assess whether UM is vulnerable to the return of these or other hackers. The Executive Board indicates that the Fox-IT investigation mentions a group that has carried out 150 successful cyber attacks since February 2019. So far there are no indications that the same group is returning, and this seems to have been a one-off ransom demand. On the other hand, the Executive Board notes that criminological research shows that if you have been a victim once, the chances of recurrence increase. The Executive Board is of the opinion that in any case they should be better prepared.
- The Supervisory Board states that such a situation, with the possibility of tens of thousands of students not knowing for months whether their degree programmes will continue, whether they can take exams or whether they have passed, must not be allowed to recur. The Board indicates that the

ransom payment, although morally objectionable, offered a solution for exams to go ahead as scheduled.
- ICT staff indicate that more attention needs to be paid to cyber security, also at national level. They hope that this will result in a movement. On the other hand, they also say that now is the time for action, otherwise the crisis will have been in vain. They cite examples such as the destruction by fire of a server room at the University of Twente a few years ago. This temporarily resulted in increased attention, but this subsequently subsided.
- ICT staff also say that 'UM can never become Fox-IT', meaning that detecting abnormal activities within the IT environment is the core business of Fox-IT, but not of a university. The ICT staff and the CMT indicate that more attention should be paid to details in the field of cyber security within UM.
- The incident has made it clear to the representative bodies that cyber security issues should be critically discussed, considering not only the cost of taking measures but also the disadvantages of not doing so. This discussion has been taking place since the attack and should be continued.
- Other staff and students qualified this view and indicated that current efforts regarding increased vigilance should not come at the expense of other existing ambitions regarding ICT, which include in the short-term the planned replacement of Blackboard by Canvas (digital learning environment).

Supply chain cooperation
- The Executive Board indicates that it sought help from external parties in handling the incident. SURFcert assisted in the analysis of the malware. UM was also dependent on Fox-IT. The Executive Board also indicates that universities will be dependent on companies such as Fox-IT in the future. UM itself is not able to acquire the specialist knowledge internally that this company can provide. The Executive Board indicates that in addition to Fox-IT, SURF is also available to share information, but data security is not SURF's only activity.
- UM wishes to discuss cooperation with other universities for the purpose of monitoring and detecting unwanted activities such as malware. Continuous monitoring for a single institution is not financially feasible.
- The Executive Board indicates that in its view more information sharing is necessary regarding risks. The Supervisory Board sees this exchange as concerning data security risks in a broad sense, including the risk not only of an attack aimed at obtaining a ransom, but also of activities aimed at acquiring sensitive research data or other sensitive information. The Supervisory Board indicates that the government should also be transparent about where the risks lie.
- Various interviewees said they were aware of a demand for knowledge sharing, as they had received questions from other educational institutions in the Netherlands and abroad, from research institutes and also from the business community. The symposium which UM held on 5 February 2020 was also viewed online by a variety of educational institutions and other parties.

Monitoring and evaluation
- Fox-IT conducted a limited investigation of attacker activities, as mentioned in Section 4.3. Fox-IT recommended that a broader study be conducted in order to be able draw conclusions on data extraction with greater certainty. The Executive Board has decided to conduct an additional investigation. For scholars it is important to also be able to state in discussions with partners that data is reliable. With additional research, the degree of certainty will increase, but 100% assurance is not possible.

- Interviewees at UM indicate that both internal and external control of the IT infrastructure should be broadened. In various conversations it was indicated that self-assessment alone is insufficient. A vacancy for an IT auditor has been advertised online since mid-February 2020. The privacy and security audits should work collaboratively. According to the CISO, the audit can then develop into a regular (annual) self-assessment, a regular audit with peer review, and periodic external audits. The contours of this system are included in UM's new draft information security policy.
- ICT staff and also the Supervisory Board say that a process audit is not sufficient and that the infrastructure should be tested periodically for weaknesses.

Investment/measures

- Fox-IT made several recommendations in the report of measures that can contribute to increasing the security level at UM. In response to the Fox-IT report, the Executive Board indicates that it will take these recommendations into account in its own internal follow-up study, in which UM aims to test its security policy and determine which existing plans should be modified and/or expanded. In addition to the measures mentioned previously in this section, Fox-IT recommends:
    - Avoidance of administration work using domain administrator accounts: the report recommends that administration work be performed as much as possible from the principle of 'least privilege'. This is in line with the examples cited by ICT staff who indicate that staff do not need the most extensive rights for a large proportion of their work.
    - Fox-IT advises that the use of (unsigned) macros should not be permitted, a protected users group should be used, especially for accounts with higher privileges, and operating systems should be kept up to date.
    - With regard to response after an incident, it is also recommended that a data recovery plan should be drawn up and practised.
    - The restoration of the IT infrastructure after the cyber attack has also increased the visibility of the systems within the network. Fox-IT recommends improving the response by creating a centrally managed Configuration Management Database.
- The representative bodies note that sufficient resources must be made available to take the necessary security measures and to gain control.
- During the incident, UM decided to use the software Carbon Black for monitoring purposes. In the interviews, ICT staff raised the issue that they were not aware whether the installation of Carbon Black on new systems throughout UM has been arranged and checked. The installation of Carbon Black related to the restoration of the existing systems in the network. The interviewees were not aware whether at the time of the interview the same high coverage of Carbon Black was till applicable.
- With regard to the future level of cyber resilience, the Executive Board indicates that the SOC is now being established, for which either new staff are being recruited or existing staff are being relieved of present duties.

5 Follow-up supervision

The Inspectorate finds that Maastricht University acted adequately in dealing with the cyber attack and has confidence in the university's follow-up investigation that has already been instituted. The Inspectorate will not therefore prescribe additional points for improvement at UM. However, the Inspectorate requests UM to inform it of the results of the follow-up investigation, partly in relation to the inquiry at education system level that the Inspectorate is to conduct. The challenge for UM is to maintain the momentum to build support for the implementation of effective measures throughout the organisation by making use of the increased focus on information security, even though it is now subject to another external threat, the coronavirus crisis. The cyber attack on UM was a wake-up call for the whole of higher education. Given the nature of their organisations, other universities are also potentially vulnerable. They must also consider on a daily basis where money and time is to be spent. Directors, representative bodies and internal supervisors are faced with the challenge of continuing to discuss the policy and its implementation, and of monitoring the implementation in a way that is appropriate to the organisational form and the digital and non-digital threats.

In early 2020, the Inspectorate decided to conduct a two-part inquiry: into Maastricht University as an institution and into the higher education system. The present report relates to the UM inquiry. Since the Inspectorate's decision to institute an inquiry, the Minister of Education sent a letter to the House of Representatives on 14 February 2020 regarding cyber security in educational institutions.[17] On 20 March 2020, the Minister of Justice and Security sent the House of Representatives a government response[18] to the report published by The Netherlands Scientific Council for Government Policy (WRR) on 'Digital Disruption'.[19] The government response stated that the Inspection Council is to be requested to put forward a proposal on how best to achieve broad cooperation and coordination between the national inspectorate and cyber security supervisors. The present report, the ongoing follow-up investigation by UM, the aforementioned parliamentary letters and the assignment to the Inspection Council are all relevant to the inquiry at education system level by the Inspectorate.

In addition to the digital threat that has become more apparent due to the attack on UM, Dutch universities of applied sciences and academic universities now face a second major challenge, given the pandemic caused by the coronavirus. As a result of government measures, since 12 March 2020 the universities have provided teaching only online, doctoral hearings have been postponed, and it has not been clear how examinations can take place. Again, this is an external threat that may jeopardise the continuance of education and research. In the approach to the coronavirus crisis, the digital infrastructure and online education facilities that universities have developed in the past decade are not an obstacle, but rather part of the solution to be able to maintain the proper continuance of education and research. This also illustrates the importance of digital infrastructure for the continuity of primary processes such as education and research.

[17] House of Representatives, year of session 2019–2020, 31 288, no. 832.
[18] House of Representatives, year of session 2019-2020, 26 643, no. 673.
[19] The Netherlands Scientific Council for Government Policy (Wetenschappelijke Raad voor het Regeringsbeleid, WRR) (2019) *Voorbereiden op digitale ontwrichting*, WRR-Rapport 101, The Hague: WRR.

Appendix 1: Legal framework

For each of its investigations, the Inspectorate of Education determines the applicable statutory provisions according to which the situation in question can be assessed. On this basis, for this inquiry, the points of interest below were selected.

In Section 2.2 it is explained that the inquiry focuses on serious negligence as referred to in the Higher Education and Research Act (WHW) Article 9.9a, second paragraph, under b. This article reads:

> serious negligence, in any event in violation of Article 1.18, to take measures necessary to guarantee the quality and proper continuance of education at the institution and to prevent the quality of the system of academic education from being jeopardised;

Other provisions of the Higher Education and Research Act relevant to this inquiry are:

Article	
2.9, par. 1:	Before 1 July of each year, the executive board of the institution must submit a report to Our Minister. The report shall consist of the annual financial statements with accompanying budget, the management report and other financial information, as well as justification for any deviation from the sector code of governance, insofar as such a code in accordance with Article 2.14 has been established. The report is required to demonstrate the extent to which the activities for which government funding has been granted have been properly conducted and are an effective use of government funding, also in the light of the institutional plan. Government funding is not deemed to have been used effectively in any event insofar as amounts are used to conduct the procedure for recognition of prior learning or to compensate internal or external students in any way for tuition fees, examination fees, course fees or for the contribution under Article 7.50, second paragraph, except in the case of financial support as referred to in Articles 7.50, third paragraph, or 7.51 to 7.51k.
2.10	The auditor charged by Our Minister with the examination of the ministerial annual accounts shall have access to each institution for the purpose of carrying out this examination. The auditor may also be charged by Our Minister with an investigation into the effectiveness of the governance of the institution. The auditor shall be provided with all information that he/she deems necessary for the performance of his/her duties.
9.2, par. 1:	The executive board is charged with the administration of the university as a whole and with its management, without prejudice to the powers of the supervisory board in accordance with this chapter.
9.4:	The executive board shall draw up administrative and management regulations to regulate the administration, management and organisation of the university.
9.5:	The executive board may adopt guidelines with a view to organising and coordinating the exercise of the powers referred to in Articles 9.14, third paragraph, and 9.15, first paragraph.

9.6:	The executive board is accountable to the supervisory board. The executive board shall provide the supervisory board with requested information regarding its decisions and other actions. The executive board shall provide Our Minister with requested information about the university.
9.8, par. 1:	With a view to the tasks of the university as referred to in Article 1.3, first paragraph, the supervisory board shall supervise the performance of activities and the exercise of powers by the executive board and shall support this board with advice. The supervisory board is charged in any event with: a. […] b. approving the administrative and management regulations; c. approving the budget, the financial statements, the management report and the institutional plan; d. […] e. assuring the compliance by the executive board with legal obligations and the observance of the sector code referred to in Article 2.9; f. […] g. […] h. […] i. reporting annually on the performance of the duties and the exercise of powers referred to under a to h by means of the university's management report.
9.12:	1. The provision of education and the pursuit of scholarship and science shall take place in the faculty. The faculty is headed by the dean of the faculty. 2. Contrary to the first paragraph, the administrative and management regulations may stipulate that the faculty is headed by a board consisting of the dean of the faculty, who is also the chair of the board, and one or more other members. If the first sentence has been applied, in this title and in Title 2, with the exception of Article 9.13, fourth and sixth paragraph, the dean also means the faculty board. If the faculty is headed by a board with more than one member, a student of the relevant faculty shall be given the opportunity to attend the meetings of this board, in which meetings this student shall have an advisory vote. The administrative and management regulations shall determine how the student referred to in the previous sentence is designated.
9.14:	1. The dean is responsible for the general management of the faculty. The dean is also responsible for the management and organisation of the faculty for education and science. 2. The dean shall contribute to the management of the university by, among other things, consulting the executive board with regard to the preparation of the institutional plan and the budget. 3. Without prejudice to Article 9.5, the dean shall draw up faculty regulations further to regulate the management and organisation of the faculty. 4. The faculty regulations require the approval of the executive board. Approval may only be withheld where regulations violate the law or run counter to the common good. 5. If the faculty regulations are not established or are not fully established within a period to be determined by the executive board, the executive board shall establish the regulations or the missing part thereof.

In addition to the Higher Education and Research Act (WHW), the universities endorse the Code for Good Governance of the Association of Universities in the Netherlands (VSNU). At the time of the opening of the first phishing email (15 October 2019) and later at the time of the ransomware attack (23 December 2019), the 2017 version was in effect. Since 1 January 2020 there has been a new version of the Code for Good Governance. This industry code is based on self-regulation. Relevant articles from the codes are as follows:

VSNU Code of Good Governance (2017 version) (apply or explain) *[English translation by VSNU]*

Article 2.1.4 The executive board will ensure that the activities of the university are appropriately arranged administratively, legally, organisationally and financially, are transparent and can be accounted for.

VSNU Code of Good Governance (2020 version) *[English translation by VSNU]*

9. The university has professional internal risk management and control systems in place. WHW ss 2.10 and 9.8 apply to the elaboration of this principle. 9.1. The executive board is responsible for identifying and managing risks associated with the strategy and implementation of the university's activities. 9.2. The executive board is responsible for the presence and functioning of internal risk management and control systems. The components of this system in any event include: i. a description of the key risks associated with strategy implementation or risks that could affect the continuity of the university; ii. determining the willingness to take risks regarding key strategic themes and activities (risk appetite), and reporting on this in the annual report; iii. the systematic management of the risks in all investment and innovation projects. Decision-making, including the advice used, is recorded; iv. properly designed processes and business systems designed to manage risks associated with the university's activities. 9.3. The executive board monitors the functioning of the internal risk management and control systems and systematically assesses the design and operation of the systems at least once a year. The executive board reports in the annual report on the establishment, functioning and key results of the internal risk management and control systems, and on any modifications thereto. 9.4. The executive board is responsible for the internal audit function. The internal audit function assesses the design and effectiveness of the internal risk management and control systems. The supervisory board monitors the internal audit function and maintains regular contact with the internal auditor. If there is no internal audit function in place, the supervisory board assesses each year whether effective alternative measures have been put in place. 9.5. The executive board discusses the effectiveness of the design and operation of the internal risk management and control systems with the supervisory board in any event once a year. In addition, the supervisory board discusses the long-term forecasts in any event once a year and assesses whether the financial continuity of the organisation is safeguarded in those forecasts.

Appendix 2: Overview of UM documentation

At the Inspectorate's request, the following documentation has been made available:

- The UM administrative and management regulations as applicable on 10/1/2019 and beyond
- Faculty regulations, from one of the UM faculties (as an example)
- UM information security policy as applicable on 10/1/2019 and beyond
- GDPR data protection policy, GDPR protocol as applicable on 10/1/2019 and beyond
- UM policy regarding Bring-Your-Own-Device as applicable on 10/1/2019 and beyond
- Management letters for the financial years 2015 to 2019
- Auditor's reports from 2015 to 2018
- Assignment, task description and organisation of the CERT team
- Results of the last two UM Audits performed in the context of the SURF-IT Audit
- Protocol/working process with regard to maintenance and updates of the UM network as applicable on 10/1/2019 and beyond
- Protocol/working process with regard to backup facilities as applicable on 01-10-2019 and beyond
- Instructions issued to staff and students regarding UM workstations and virtual workstations (on first use)
- Protocol/working method with regard to the digital working environment for students, staff, and in particular IT officials
- Example of recent incident reporting to management regarding digital security
- Protocol/procedure for incident reporting by staff (particularly in relation to digital security)
- Protocol/procedure for dealing with incidents by the service desk, ICT and network management
- The most recent awareness campaign on digital security for staff and students prior to 23 December 2019
- An account of the facts regarding the cyber attack, contact with the ransomware attacker, IT measures, administrative and legal matters, and communications both internally at UM and externally.
- Documentation regarding action for improvements currently formulated by UM as a result of the cyber attack.

Maastricht University has also provided additional documentation that gives insight into the institution's cyber resilience. This documentation is as follows:

- Documentation of the implementation policy of two faculties with regard to information security and privacy
- Communications on awareness
- Improvement measures and innovations, including the Security Operations Centre (SOC), Identity and Access Management (IAM), improvements in network facilities, and two-factor authentication
- Risk management documentation that includes attention for cyber security and privacy as part of risk management
- Documentation on I-strategy and I-board
- GDPR awareness
- Additional documentation related to the cyber attack itself

Appendix 3: Overview of interviews

On 17 and 18 February 2020, interviews were held with:

- the entire Executive Board
- representatives of the Crisis Management Team (CMT) that was concerned with handling the cyber attack
- representatives of UM's Cyber Emergency Response Team (UM-CERT)
- UM's Chief Information Security Officer (CISO)
- representatives of ICT/network administrators from UM's central organisation and from two faculties
- representatives of staff and students from the participative bodies of the central University Council and a number of UM faculties and services
- students and staff from various UM programmes, faculties and services, in a group discussion
- three members of the Supervisory Board

On 9 March 2020, interviews were held with:

- the financial director and director of ICT at UM
- the external auditors of the past five financial years

List of abbreviations

BIO	*Baseline Informatiebeveiliging Overheid* Information Security Baseline for Government Bodies
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMT	Crisis Management Team
DPO	Data Protection Officer
DUO	*Dienst Uitvoering Onderwijs* Education Executive Agency
GDPR	General Data Protection Regulation
IoCs	Indicators of Compromise
ISO	International Organization for Standardization
NCSC	National Cyber Security Centre
NVAO	*Nederlands Vlaamse Accreditatie Organisatie* Accreditation Organisation of the Netherlands and Flanders
NWO	*Nederlandse Organisatie voor Wetenschap* Netherlands Organisation for Scientific Research
SCIRT	SURFnet Community of Incident Response Teams
SOC	Security Operations Centre
UM	*Universiteit Maastricht* Maastricht University
VDI	Virtual Desktop Infrastructure
VSNU	*Vereniging van Universiteiten* Association of Universities in the Netherlands
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek Higher Education and Research Act,
WOT	*Wet op het onderwijstoezicht* Education Inspection Act
WRR	*Wetenschappelijke Raad voor het Regeringsbeleid* The Netherlands Scientific Council for Government Policy

Inspectorate of Education | Inspectie van het Onderwijs
PO Box 2730 | 3500 GS Utrecht
www.onderwijsinspectie.nl

A copy of this publication in Dutch can be downloaded from the website of the Inspectorate of Education: www.onderwijsinspectie.nl.

English translation by Maastricht University