government led these organizations to feel pressured into following advice, despite the absence of any formal relationship for control or accountability with national government. These organizations have their own forum responsible for governing them and to whom they are accountable.

4.4 Learning from digital incidents

In bringing about any improvement in safety, it is important to investigate what happened, and which factors contributed to the occurrence and consequences of the incident. These insights are key in preventing future incidents, and limiting their consequences, especially in a domain as dynamic as cybersecurity.

In many domains, major incidents and public outcry serve as an incentive to learn, and improve safety. In the Netherlands, investigations have been undertaken for more than one hundred years into accidents and disasters, initially only in the transport sector. Following the firework disaster in Enschede, and the fire in a café in Volendam, the Dutch Safety Board was established in 2005 to meet the need for a permanent investigative body that as well as transport, was also authorized to carry out investigations into occurrences in other domains.[194] In the domain of transport, this research has a long tradition worldwide. For example, an air crash involving a popular football coach in the US in 1931 eventually led to the establishment of the NTSB (the American counterpart to the Dutch Safety Board).[195]

The digital domain is a relatively recent domain, and the tradition of learning from incidents affecting this domain is limited and still under development. In this section we describe:

- how digital incidents are currently reported and investigated;
- which factors influence how lessons are learned from digital incidents. This relates both to choices and assumptions made and held by investigators and the context within which the investigations take place.

4.4.1 Current practice for investigations into digital incidents

There can be several different reasons for investigating an incident. Firstly, based on the individual needs of the organization affected, be it a manufacturer of software or an organization using software, there is an intrinsic need to learn from occurrences so as to prevent recurrences in the future, not only within the organization itself but also for others. There are also a variety of legal obligations that mean that particular occurrences have to be reported to specific bodies (although they are then not always investigated). Parties such as the police and insurers carry out forensic investigations into occurrences. Below, we will discuss our observations on current practice as regards the reporting and investigation of digital occurrences.

[194] https://www.onderzoeksraad.nl/nl/page/12056/geschiedenis

[195] Anderson, R., *Security Engineering*, 2020.

Reporting and investigation on the basis of statutory obligations

Incidents at vital providers

The European Network and Information Security (NIS) Directive[196] contains obligations for providers of essential services in vital sectors and digital service providers.. The Netherlands has implemented the NIS Directive in the Security of Network and Information Systems Act (Wbni). Pursuant to the Wbni, providers of essential services are required to report serious incidents to the NCSC/sectoral CSIRT and their sectoral regulator. For energy and digital infrastructure occurrences, this is the Telecom Agency; for banks and the payment infrastructure the DNB, for transport and drinking water the ILT and for healthcare the IGJ.[197] For the telecom sector there has been a duty of care and notification including supervision by AT since 2012 based on the Telecommunications Act, regardless of whether a party has been designated as vital by the Ministry of Economic Affairs. In addition to this sectoral legislation and regulation, the Wbni includes a duty to report to the NCSC only for the vitally designated telecom parties.

The appropriate specialist department in consultation[198] with JenV then imposes threshold values, above which the incident must be reported. The Wbni specifies that in preventing or managing an incident requiring public awareness, the authority in question is permitted to inform the public about the reported incident. The authority can also call upon the vital provider to inform the public itself.[199]

It is also important for learning that other organizations can easily absorb the lessons from the studies that are relevant to them, and in that way learn from what other organizations have suffered. Occasionally investigations in response to reports are published on the website of the relevant authority or regulator. Examples are the investigations by the Radiocommunications Agency Netherlands (AT), the Inspectorate of Justice and Security (IJenV) and the Health and Youth Care Inspectorate (IGJ) into the failure of the 112 alarm number[200] and the investigation by ILT into cybersecurity at Waternet, in response to signals in the media that there were cybersecurity problems.[201] We were unable to find an overview on the websites of the NCSC, AT or other sectoral regulators of which incidents have been investigated, nor were we able to find an aggregated overview of the number of incidents, the factors that led to those incidents and the various lessons learned from them. On the other hand, it is possible that the lessons from these incidents were implicitly integrated in the recommendations and information provided by these organizations to their target organizations.

[196] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32016L1148&from=EN. Under the Wbni, the following are designated as providers of essential services: entities designated as vital providers that operate in sectors listed in the appendix to the NIS Directive (see Article 2 Bbni). For some categories of other vital providers, separately from this, there is also an obligation to report serious incidents to the NCSC (see Article 3 Bbni), but they are not subject to the other obligations arising from the NIS Directive. In addition: providers of essential services are required under Article 10 Wbni to report serious incidents to the NCSC and the sectoral regulator, but not also (or instead) to a "sectoral CSIRT". Incidentally: the regulator for entities within the health care sector has already been determined (in Article 4 of the Wbni), but within that sector no providers of essential services have yet been designated (to whom the obligations from the NIS Directive would apply).

[197] https://zoek.officielebekendmakingen.nl/stb-2018-387.html

[198] Because of the often dual reporting requirements to both the subject department and JenV (NCSC).

[199] Article 20(4)(b) Wbni https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2020/januari/20/brochure-meldplicht-voor-aanbieders-van-essentiele-diensten/Brochure+Meldplicht+voor+aanbieders+van+essentiële+diensten.pdf

[200] https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112

[201] https://www.ilent.nl/documenten/rapporten/2021/4/2/onderzoeksrapport-stichting-waternet

In practice, inspectorates are currently still working internally on the question of how they can and should interpret their own responsibility. For example, inspectorates write in their first joint inspection report that supervision is still in a constructive phase and that they cannot yet make coherent statements (draw common threads) about how things are going at the moment with regard to cyber security in vital sectors and processes.[202]

Investigation into data leaks

Organizations that have suffered breaches of personal data are legally required to immediately report the occurrence to the Dutch Data Protection Authority (DPA (AP in Dutch)). The term data leaks refers to 'access to or the destruction, rectification or release of personal data from an organization, contrary to the intentions of that organization'.[203] The legal obligation to report data leaks is based on the European General Data Protection Regulation (GDPR) in the EU. Because the GDPR is a Regulation, this European rule of law applies directly across the entire European Union.

The Dutch DPA publishes investigation reports and reports on the imposition of fines in response to reports of data leaks and other signals.[204] The investigations by the Dutch DPA focus on the extent to which organizations have complied with their legal obligations, such as the taking of technical and organizational measures to prevent data leaks and the evaluation of data leaks. If an organization has failed to comply with the statutory measures, the DPA can impose a fine. For this reason, organizations are reluctant to report potential data breaches. However, non-compliance with the legal obligation to report can also lead to additional fines, regardless of the extent of the original data breach. Another limitation is that the reports must involve the leaking of personal data, and that is only the case in some of the incidents. Furthermore, the AP's investigations focus mainly on compliance with legislation and regulations. In order to learn, the underlying question of non-compliance is particularly relevant: what factors may have led to organizations not complying with the obligations and what can be learned from this?

Each year the DPA publishes an annual report. The annual report for 2020 states that the majority of data leaks reported in 2020 were the consequence of the wrong sending or issuing of personal data (66%). The DPA reports that in 5% of the data leaks reported in 2020, a digital incident (hacking, malware, phishing) was the cause of the breach and the proportion is rising. In its report, the DPA discusses in depth the contribution that multi factor authentication (MFA) could have had on preventing and mitigating 249 data leaks, whereby according to estimates, at least 607,846 and at most 2,092,946 people were involved.[205]

At present, the Dutch DPA offers no further insights for organizations that use software. To be able to gain more insights from the reports of data leaks, and in that way to identify potential further lessons for other organizations, in 2020, the Cyber Security Council (CSR) submitted a study proposal to the Minister of Justice and Security. The aim of this study is to show the extent to which the scientific and/or statistic study of data leaks can

[202] ANVS, DNB, IGJ, IJenV, ILT, *Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021,* June 2021.
[203] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
[204] https://autoriteitpersoonsgegevens.nl/nl/onderzoeken
[205] https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

increase the understanding of the effectiveness of safety measures (or the absence of such measures).[206]

Forensic investigations

There are a number of organizations that carry out subsequent investigations into incidents. Some of these organizations are recognized as forensic cyber investigation offices. This recognition means that their reports can be accepted as forensic evidence in a court case. Forensic substantiation is primarily focused on substantiating legal liability, not on learning from the incident to prevent future recurrence. In most cases, these digital forensic investigation firms work on behalf of the affected organization and/or their insurer. The investigations generally remain confidential to the commissioning organizations (unless the organization publishes on its own initiative, see the section below). Other organizations gain no insight into the lessons learned and they make no contribution to an overall picture of factors and the effectiveness of measures. At most, they are shared within the offices of the affected insurer (silos between insurers).

The police (HighTech Crime Team and regional cybercrime teams) and the NFI also carry out forensic investigations. For these organizations, the same applies broadly as for investigative agencies in terms of the ability to learn from their investigations. In the event of a court case, some of this information may be made public via the media and by the court judgement. However, the information cannot be examined by other organizations, as for example is the case in the event of road traffic accidents that are registered in a road traffic accident register, that among others can be used for scientific research (for example by the Institute for Road Safety Research, SWOV) and in support of future policy.

Investigations and publication on individual initiative

A number of organizations have decided to publish the results of forensic or other investigations, in the public interest and as a way of accounting for their activities to their grassroots (individual citizens and students).

[206] https://www.cybersecurityraad.nl/documenten/adviezen/2020/02/11/csr-advies-beschikbaar-stellen-datalekmeldingen-voor-onderzoeksdoeleinden---csr-advies-2020-nr.-1

Investigation into cyber attacks in public

In June 2019, the police informed the municipality of Lochem that the municipality's digital system had been compromised. Since that time, the Mayor of Lochem has seen it as his personal mission to inform municipalities and other government organizations about this risk and to underline the importance of cyber resilience.[207]

On 23 December 2019, Maastricht University became the victim of a cyberattack. The university commissioned an investigation into the occurrence, and kept its staff and students informed of the events. During a symposium on 5 February 2020, the university presented the reports of the investigation, and explained how the accident occurred and explained the lessons learned.[208] The Inspectorate for Education also investigated the accident.[209]

In December 2020, the Municipality Hof van Twente was hacked. As a consequence, the municipality was forced to shut down its services to local residents for a number of weeks (for passports, driver's licences, central register extracts) and for municipal tax, for several months; the municipality was also unable to pay invoices or cooperate securely with other organizations. The municipality was also forced to fully rebuild its digital system. Just like the Maastricht University, the Municipality of Hof van Twente kept its residents informed, with regular updates. They also commissioned an investigation, and published the results for the general public.[210]

In February 2021, the University of Amsterdam and Amsterdam University of Applied Sciences also suffered a cyber-attack. They too commissioned an investigation, and published the results.[211]

The tradition of learning from occurrences is still developing in the digital domain. Occurrences must be reported, but are not systematically investigated. An 'infrastructure' for shared learning by manufacturers, organizations using software and other relevant public and private parties is lacking.

[207] https://ibestuur.nl/magazine/cyberaanval-lochem-gaat-de-hele-overheid-aan

[208] https://www.maastrichtuniversity.nl/nl/updates-cyberaanval

[209] https://www.onderwijsinspectie.nl/documenten/rapporten/2020/06/12/rapport-cyberaanval-universiteit-maastricht

[210] https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/03/artikel/hof-van-twente-cyber-hack-stevige-les-voor-ons-1872

[211] https://www.uva.nl/content/nieuws/nieuwsberichten/2021/07/evaluatie-cyberaanval.html

4.4.2 Barriers to learning from (investigations into) cyber occurrences

In the previous section, we described the various ways in which cyber occurrences are currently reported and investigated. We also discussed the way in which the results of these reports and investigations are used to give organizations a greater insight into what they can do to prevent future recurrence.

Across the board, the current method shows that learning from cyber accidents is hindered by a number of factors.

Reporting and publication

The Municipalities of Lochem and Hof van Twente and the educational institutions Maastricht University and University of Amsterdam/Amsterdam University of Applied Sciences can be seen as exceptions to the rule that says that organizations are unwilling to share in public the fact that they have been the victim of a cyber-occurrence, and the lessons they have learned as a consequence. In the discussions held by the Safety Board with various organizations and the parties representing them, a number of reasons are mentioned, of which three are discussed below.

Firstly, the fear of harm to reputation and loss of confidence from parties with whom the organization cooperates. A cyber occurrence such as a ransomware attack can be seen by the outside world as a sign that information security at the organization is below par. This can lead to a loss of confidence in the organization in question. This effect is difficult to measure. So far, there are no signs that data breaches necessarily lead to a decline in the value of the company. In addition, in other domains such as the food sector, there is evidence that organizations can actually maintain or strengthen trust if they come forward voluntarily with a security problem and address it decisively.[212] Another psychological effect is shame. This effect is greater in the event of cyber occurrences than other incidents such as a car accident. One of the reasons for this sense of shame is that the persons disadvantaged by a cyberattack, like a ransomware attack, feel that they have been cheated, that they have fallen for some trick and have failed. As well as losing their sense of safety, this also leads to a loss of status.[213]

A second obstacle to announcing an occurrence is the potential for legal consequences. If the cyber occurrence is accompanied by the violation of legal rules (for example if data has leaked or a duty of care has not been complied with), then regulators can take steps to enforce the rules. Other parties (consumers, end users, suppliers, shareholders) may also feel that their rights have been negatively affected, and in response sue the organization. One of the software manufacturers we spoke to, for example, learned lessons from the occurrence, took measures and shared a number of lessons and enhancements via hun website. However, it did not actively share those lessons with other manufacturers, parties involved or the public. If the software industry remains mutually and publicly closed about how errors occur, there can be no shared learning.[214]

[212] See for example https://doi.org/10.15728/bbr.2017.14.2.4.

[213] Goffman, E., 1952. On Cooling the Mark Out, *Psychiatry,* 15:4, 451-463, DOI: 10.1080/00332747.1952.11022896

[214] See also E. Tjong Tjin Tai and B. Duties of care and diligence against cybercrime *(NJb)*, 2015.

The third obstacle mentioned is that the organization is afraid of the increasing risk of attacks, as soon as it becomes known that the organization has already been (successfully) attacked before.

The way in which cyber occurrences are investigated

Another obstacle to learning that relates to the barriers outlined above is how the factors that contributed to the occurrences taking place are described in the reports. As outlined above, reputation damage is one reason for not reporting occurrences. Shame (stigma) also plays a role. Evaluations that summarize the mistakes made by an organization without investigating and explaining how the organization found itself in that situation can increase the sense of stigma and do not contribute to the willingness of organizations to share their experiences with the outside world, so that others have an opportunity to learn.

Many of the evaluations are aimed at what the organization in question itself should do, and do not consider the system question that lies behind the question of why it is so difficult for organizations to prevent being attacked, and to successfully resist attacks. In the evaluations, the focus is more on security and less on establishing a safe digital system that is resistant to all kinds of possible threats.

Willingness to understand how things could happen is crucial in all occurrence investigations, including the ones under scrutiny. Therefore, in order to learn from accidents, it is important how the accident investigation is structured: that the accident investigation is aimed at being able to explain the accident. That in turn requires that the investigation goes beyond an assessment based on standards (single loop learning), and that it also reflects on the principles employed (double loop learning). Especially in a domain where learning from occurrences is evolving, it is important to also reflect on how we learn (third loop learning or deutero learning). Most evaluations examined by the Dutch Safety Board were restricted to single loop learning. Those evaluations consisted primarily of observations that the organization in question had failed to implement all the specified or expected basic measures, and that these were factors that had led to the occurrence. Or there were evaluations that, while analyzing the approach and policies, did not reveal what factors contributed to the occurrence of the incident.

The evaluation by the Inspectorate of Education of the ransomware attack on Maastricht University shows that a reflective approach to an incident investigation is both possible and worthwhile. In that investigation, for example, an explanation was sought for the fact that the information security did not satisfy the available standards. One of the explanations was that because of the multi-layered administration of colleges and universities, it is not possible for the governing board to maintain a clear view of the status of information security. This is an essential insight, because a multi-layered administration of this kind is present at all colleges and universities, and may well prevent the governing boards of other educational institutions from obtaining a clear view of the status of information security.

The dissemination of insights to parties that need those insights

In the subsection above, we refer to different types of investigations into occurrences. The information generated by these investigations is only published in a limited number of cases: when, by way of exception, the organization opts to publish, or is required to do so by the regulator. In the previous subsection, we took as examples Maastricht University, the University of Amsterdam/University of Applied Sciences Amsterdam, the Municipality of Lochem and the Municipality Hof van Twente. We also suggested that the majority of investigations into occurrences are not published, or only within a closed circuit. The information is in fact only comprehensible for a limited group of experts, and that makes it appear an abstract, technical event. For that reason it is important when sharing insights from cyber-attacks to demystify them and to underline their human consequences.[215]

Moreover, at present there is no single entity that collects the information from investigations and reports for the purpose of scientific and/or statistical study. In the cyber domain, which enjoys a relatively new tradition in respect of incident investigation, there is a clear need for a platform where knowledge is shared and retained and where organizations can go in search of relevant insights to further improve their information security policy (historic capture). Incidentally, this aligns with the NCSC's mission as the National Cyber Security Center: to understand and interpret what is happening, to connect parties, knowledge and experience with the goal of preventing recurrence. [216]

In current practice, many organizations do not come clean about the fact that they have been attacked. The investigations do not provide the explanations needed to improve the system. Involved organizations do not share the lessons learned from occurrences outside their own organizations or communities.

4.5 Policy and the international context

At the European level, there are various regulations in the field of cybersecurity, as well as a number of initiatives under development. These regulations and initiatives each have a different purpose and target group. The table below lists some of the characteristics of the regulations.

[215] Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat.* 2020 https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm

[216] https://www.ncsc.nl/over-ncsc, accessed on 13 September 2021.