Næringslivets sikkerhetsråd

Norwegian Computer and Data Breach Survey 2018

Information security, privacy and cybercrime

Conducted by Opinion AS for The Norwegian Business and Industry Security Council

Foreword

Norway is one of the most digitised countries in the world, which brings opportunities as well as new vulnerabilities and challenges.
Big investments have been made into innovation and development, but not as much has gone to IT security education and competency. This is a gap that must be filled.

This study is meant to not only chart the security situation and IT security incidents, but also contribute to raising the expertise and assistance in preventive security efforts. We have emphasised preventive activities and measures in the report.

The Unrecorded Statistics Study 2018 is the 11th such study conducted by the Norwegian Business and Industry Security Council. Through it, we collect data regarding the IT security situation in the private and public business communities, and the study holds a central place in our education and information strategy.

The study shows that businesses have a lacking over-view of the costs related to security incidents, costs that are estimated to tens of billions of NOK each year.

Both the Unrecorded Statistics Studies of 2016 and 2018 reveal that IT security incidents are largely discovered by chance. One of the positive findings in this year's study is that the presence of management systems and operation of systematic preventive security efforts make businesses better at discovering incidents. This allows them to more quickly implement cost-reducing measures, while simultaneously contributing to a more robust and conscious digital society.

We therefore hope that this year's study and report will contribute to a greater understanding of security, a stronger ability to discover incidents, and good preventive security efforts.

We would like to thank everyone who has supported the study and given their contribution to the report.

Jack Fischer Eriksen
Director of The Norwegian Business and Industry Security Council


NASJONAL
SIKKERHETSMYNDIGHET


POLITIET
POLITIDIREKTORATET


telenor


Nordea


coop


ONE VOICE


Microsoft


KPMG


VISMA


THOMMESSEN


mnemonic

Contents

Summary

To a large degree, IT operations are organised as they were in 2016. 17 percent of businesses fully and entirely outsource IT operations, 31 percent conduct partial outsourcing while nearly half (48 percent) organise IT operations internally. Furthermore, six out of ten businesses have a management system or framework for information security. This is also at the same level as in 2016. While outsourcing is more common among smaller businesses, having a management system is more common among larger companies.

Virus and malware infection are the security incidents that affect the most businesses. 21 percent of businesses have suffered such incidents in the course of 2017. Compared with 2016, there is a clear rise in the share of businesses exposed to phishing, hacking attempts and actual hacking, DDoS attacks or threats thereof, and fraud.
Of those exposed to security breaches in 2017, 67 percent believe that the incidents were due to chance or bad luck, while 55 percent believe the cause was human error. Businesses with a management system are less likely to see chance and bad luck as a cause for an incident than those without such systems.

When it comes to the reason the security breach was discovered, there is again a difference between companies with and without an information security management system. In total, 40 percent believe the incident was discovered by chance. Among companies without a management system, 50 percent discovered the incident by chance. In businesses with management systems, 37 percent discovered it by chance. Businesses with management systems are more likely to discover incidents through internal routine security monitoring (44 percent). This is mentioned by only 28 percent of businesses without management systems.

Upper management was brought into the case for 61 percent of businesses exposed to security incidents. Another 31 percent went on to report the incident to the board of the company. For 19 percent of businesses with security incidents, the results were financial losses. For 9 percent of the businesses, the incident led to changes to the organisation. Incidents are mostly reported to the administrator of the technical system (72 percent), while 3 percent report to NorCERT and 2 percent to Sector CERTs.

Nearly half (48 percent) of the businesses have made changes or improvements in their privacy and information security efforts as a result of the implementation of the new privacy regulations (GDPR).

Six out of ten business have over the past year completed activities to improve the security awareness of their employees. This is far more common in large businesses than in small ones, and in businesses with information security management systems than those without.

About the study

Background
Opinion has conducted the Unrecorded Statistics Study 2018 on behalf of the Norwegian Business and Industry Security Council. Leading up to the 2016 study, a number of changes were made to the questions and data collection methodology used. Comparisons can therefore not be made with results from before 2016.

Population
The population of this study is Norwegian businesses in the public and the private sector with 5 or more employees. The selection of this study is drawn from Bisnode's database, which collects information from the Central Coordinating Register for Legal Entities. Compared with the previous study in 2016, there has been a conscious effort to interview more major businesses. This means that the selection has a different composition than the previous study, and that our comparisons have controlled for the differences between the selections and interpreted them with care.

1500 interviews have been conducted in this study.

Data collection
Data collected was conducted with the aid of telephone interviews (CATI) in the period from 1 to 19 February 2018.

Error margins
Opinion notes that all surveys entail error margins. The error margins primarily involve statistical uncertainty. There are sampling biases, which prevent the sample from being identical to the universe or to the target population. These differences may relate to certain characteristics or behaviours.

At 1500 respondents or interviews (n=1500), we can claim with 95 percent probability that the exact result is within ± 1.1 and ± 2.5 percentage points, independent of the percentage size. Uncertainty is at its highest at percentage results of 50 percent, and at its lowest with percentage results of 5 percent/95 percent.

Definition of framework for information security

A framework for information security means internal control through established routines, management, clear chains of responsibility and reporting to handle information security, covering the entire value chain of the business.
The framework should be adapted to the business, such as with sectors like healthcare, power and local governance. Hereunder also with regard to best practices, ISO standards, preparedness regulations, the Security Act, privacy legislation (hereunder GDPR) and international regulations and directives such as NIS. See also decisions from the National Security Authority on their website. [1)]

Facts on testing and inspection of the business's security situation

Arranged tests and inspections of the business's security situation may reveal vulnerabilities and result in documentation for implementing essential measures, and should be seen as an annual security hardening effort. For more information, see the website of the National Security Administration.

[1)] The European Parliament and Council's directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the EU.

Characteristics

Survey respondents have the following distribution across the private and public sectors:

Sector	Number (n)	Share Interview
Private	947	63 %
Public	553	37 %
Total	1500	100.0 %

Geography

Below is an overview of the respondents' location by county:

County	Number Interview (n)	Share Interview
Østfold	66	4.4 %
Akershus	130	8.7 %
Oslo	187	12.5 %
Hedmark	71	4.7 %
Oppland	74	4.9 %
Buskerud	82	5.5 %
Vestfold	59	3.9 %
Telemark	64	4.3 %
Aust-Agder	36	2.4 %
Vest-Agder	45	3.0 %
Rogaland	106	7.1 %
Hordaland	148	9.9 %
Sogn og Fjordane	47	3.1 %
Møre og Romsdal	90	6.0 %
Sør-Trøndelag	66	4.4 %
Nord-Trøndelag	45	3.0 %
Nordland	106	7.1 %
Troms	54	3.6 %
Finnmark	24	1.6 %
Total	1500	100 %

Business size

The survey encompasses businesses in the following size groups:

Business size	Number Interview (n)	Share Interview
5 to 19 employees	728	48.5 %
20 to 99 employees	508	33.9 %
100 or more employees	264	17.6 %
Total	1500	100 %

Industry

The survey encompasses businesses in the following industries:

Industry	Number Interview (n)	Share Interview
Primary	15	1.0 %
Industry etc.	170	11.3 %
Construction	97	6.5 %
Retail, etc.	310	20.7 %
Logistics	45	3.0 %
Accommodation/food services	58	3.9 %
Service industries	252	16.8 %
Public administration	81	5.4 %
Education	278	18.5 %
Healthcare and social services	194	12.9 %
Total	1500	100 %

1. Organisation of IT operations

This chapter covers questions pertaining to how the businesses have organised IT operations, as well as management systems or frameworks for information security.

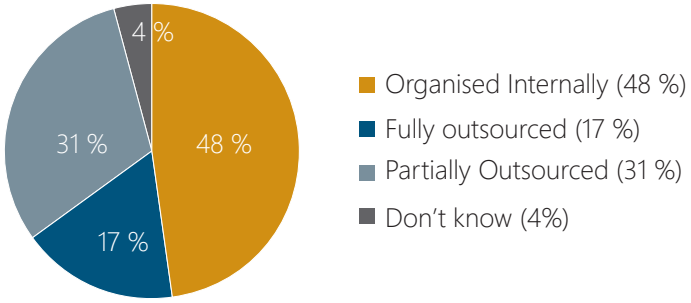
1. Organisation of IT operations

1.1 Outsourcing

17 percent of the businesses have fully outsourced IT operations. 31 percent of the businesses have partially outsourced, while 48 percent have organised IT operations internally.

Question: Are the business's IT operations organised to be fully outsourced, partially outsourced, or are all operations organised internally? (n=1500)

Figure 1



It is more common for businesses with fewer than 100 employees to completely outsource IT operations than for businesses with 100 or more employees to do so. Among businesses with 100 or more employees, 12 percent have fully outsourced these operations. This is in line with the 2016 study, when 13 percent of large businesses reported the same. Among businesses with 5 to 19 employees and 20 to 99 employees, 19 and 18 percent have fully outsourced IT operations, respectively. This too is in line with 2016, when the distribution was 22 and 23 percent, respectively.

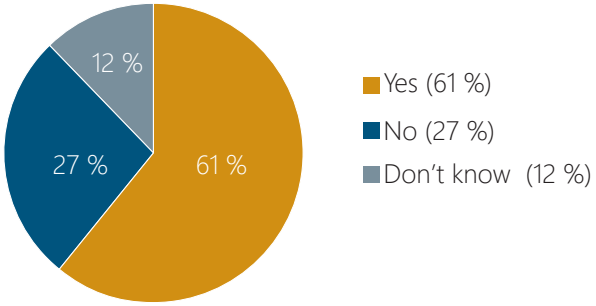
Among those who fully or partially utilise outsourcing, 15 percent use outsourcing services overseas. This is equally common for both larger and smaller businesses. Furthermore, 82 percent of those using outsourcing services overseas are aware of where the data is stored physically, while 18 percent are not.

1.2 Management systems and frameworks

Six out of ten businesses report that they have a framework or management system for information security.

Question: Does the business have a framework and/or management system for information security? (n=1500)

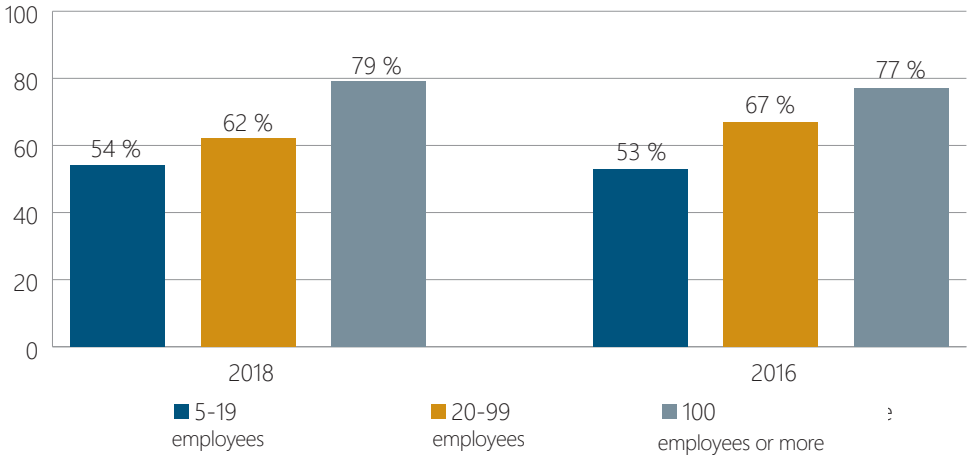
Figure 2



There are vast differences between the smallest and largest businesses on this question. While 54 percent of businesses with 5 to 19 employees have one, 62 percent of those with 20 to 99 employees

and 79 percent of those with 100 or more employees have a framework or management system for information security. The results are on the same level as in 2016. Figure 3 shows the share in each size category that has a framework/management system in 2018 and 2016, respectively.

Figure 3

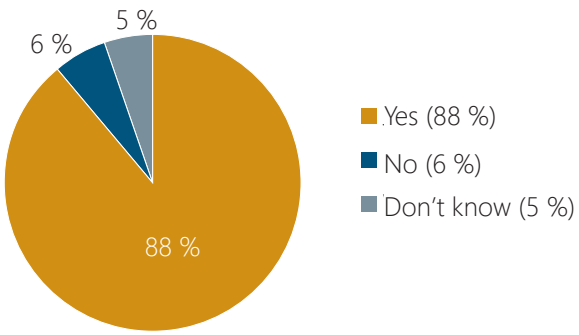


The question does of course leave the respondent with some room for interpretation. It is not unlikely that the definition of what a framework or management system is, how much it encompasses and how well-implemented it is may vary from respondent to respondent. Nonetheless, we observe that businesses reporting that they have a framework or management system are different from businesses that do not in a number of areas. In other words, the case is such that regardless of how the businesses define the terms, there is still a difference between those replying that they have such systems and those reporting that they do not.

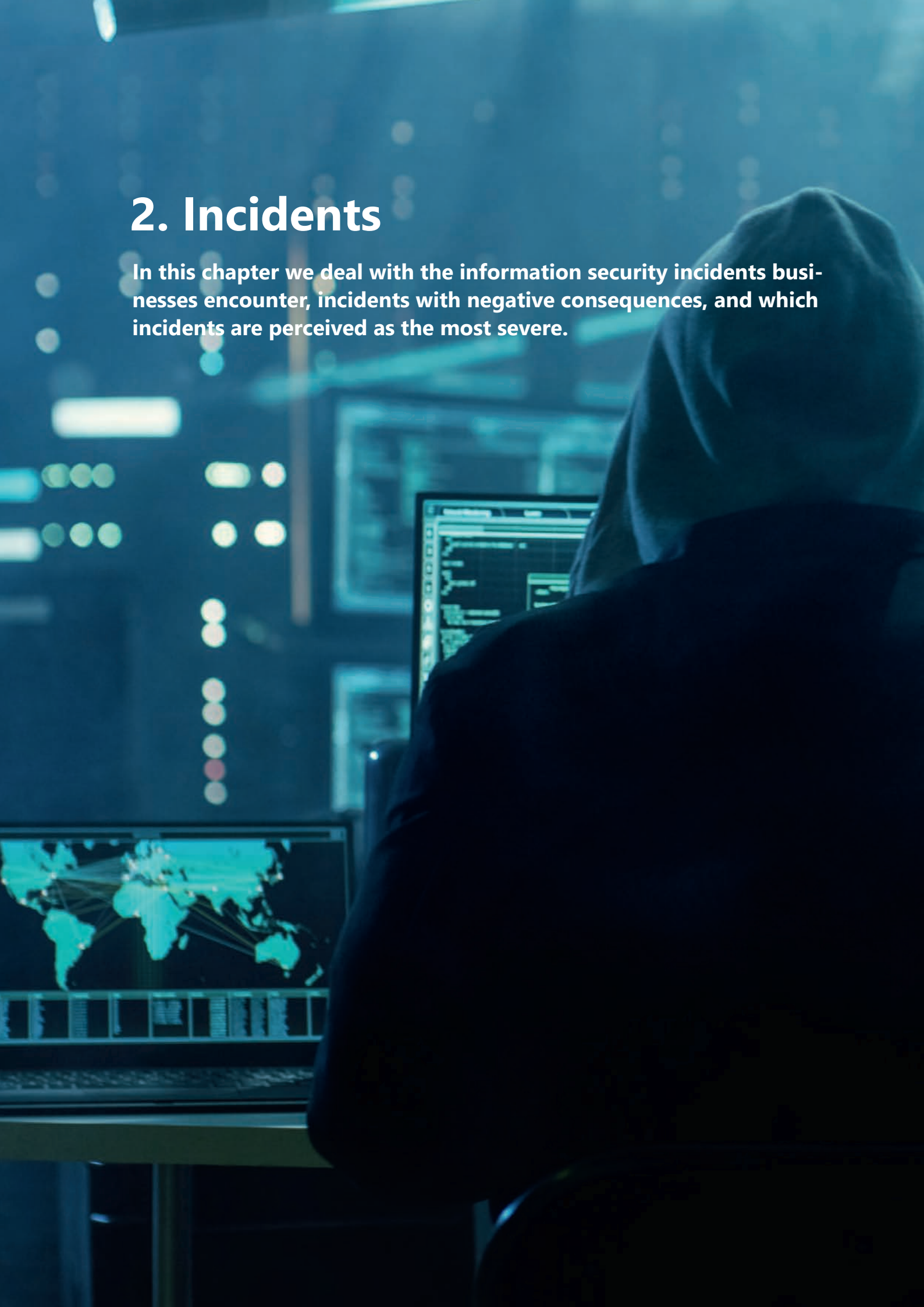
To a large degree, businesses with a framework or management system believe that these are complied with in the organisation. Nearly nine out of ten share this view.

Question: Do you feel the framework/management system for security is adhered to in your organisation? (n=912 – businesses with frameworks/management systems)

Figure 4



Major businesses are less likely than small businesses to feel that their management system is complied with. 12 percent of businesses with 100 or more employees answer no, compared with 4 percent of those with 5 to 19 employees.



2. Incidents

In this chapter we deal with the information security incidents businesses encounter, incidents with negative consequences, and which incidents are perceived as the most severe.

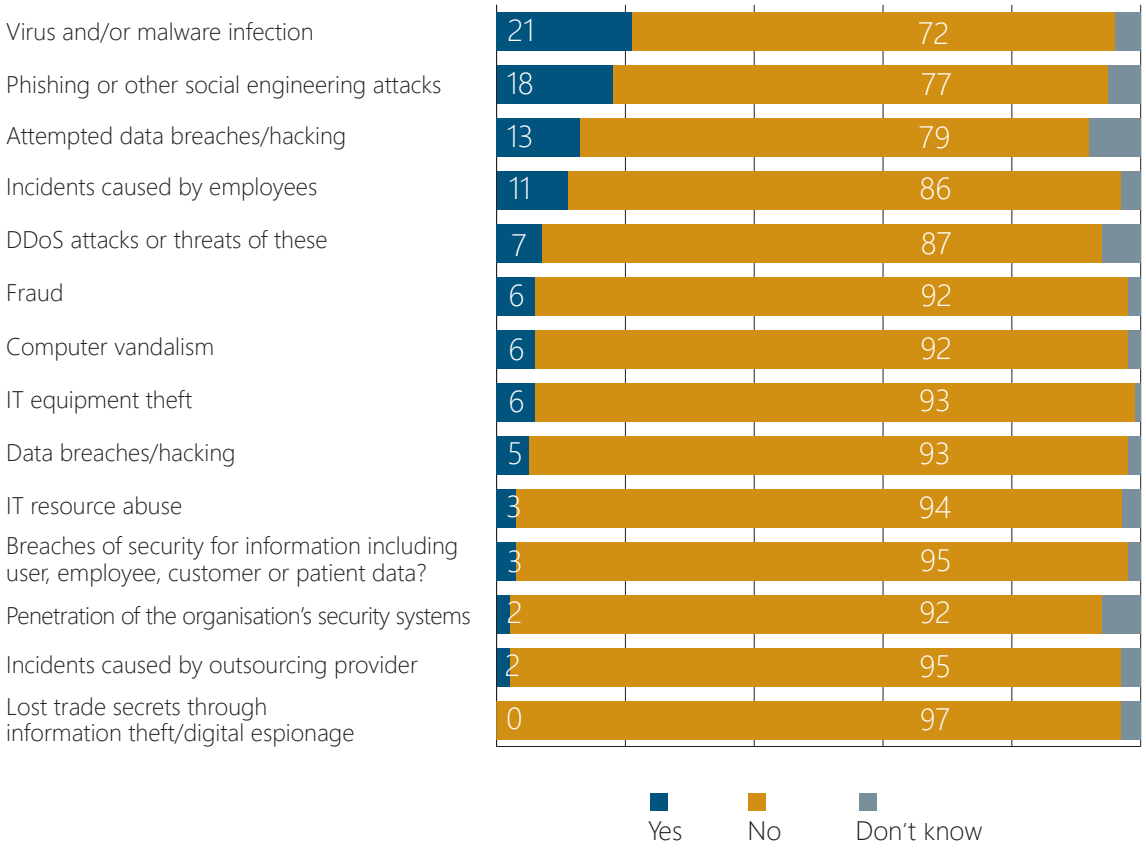
2. Incidents

2.1 Information security incidents

Viruses and/or malware infections as well as phishing or other social engineering attacks are the most common incidents. Respectively, 21 and 18 percent of businesses have encountered these. Furthermore, 13 percent have been affected by data breaching/hacking attempts, and 11 percent of these incidents are caused by employees. Incidents caused by outsourcing suppliers are however far less common, and no businesses report that they have lost trade secrets due to digital espionage.

Question: I will now read out some possible information security incidents and ask you to answer yes or no to whether your business has encountered these in the calendar year 2017. (n=1500)

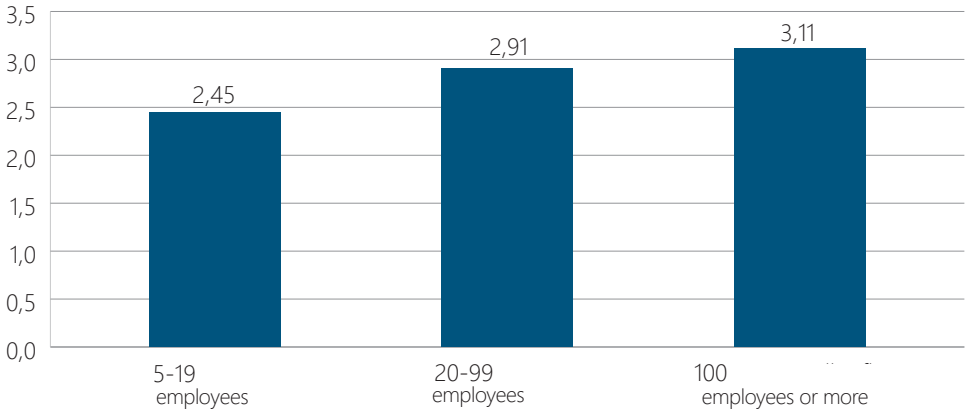
Figure 5



Among those who have experienced incidents, an average of 2.8 such incidents were encountered. As may be expected, incidents become more common the larger the business is. (We are here referring to the number of different types of incidents, not the number of incidents in total.)

Average type of incidents among businesses (n=563 – answered yes on one or more alternatives in the question above)

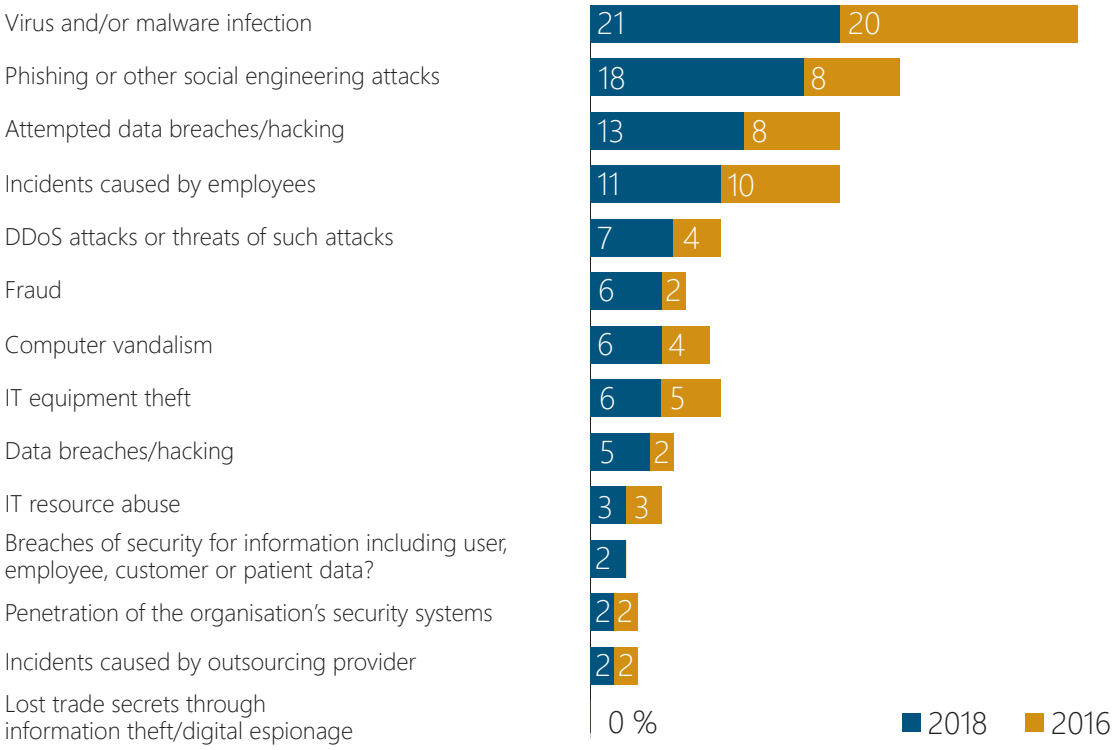
Figure 6



The smallest businesses have an average that is significantly lower than the other two size groups, while there is no significant difference between businesses with 20 to 99 employees and those with 100 or more employees. In other words, large businesses suffer a wider range of incidents.

Compared with 2016, there has been a particular increase in the incidence of phishing, data breaches/ hacking, DDoS attacks or threats of these, as well as fraud.

Figure 7



2. Incidents

2.2 Incidents with negative consequences

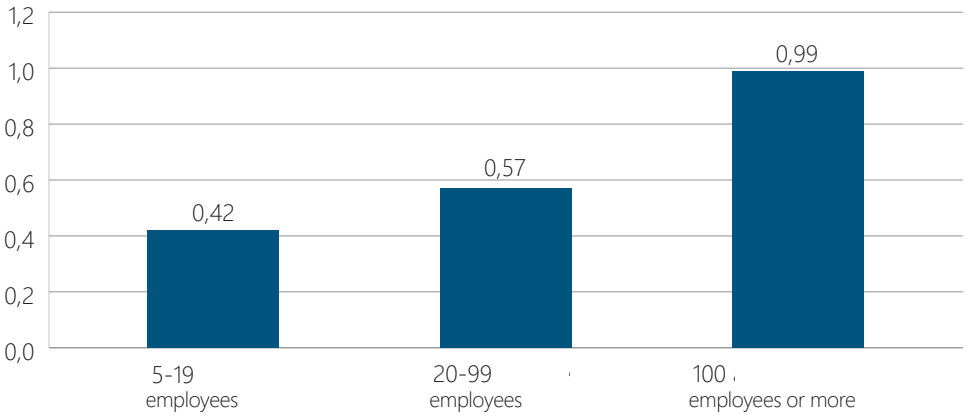
On the question of whether there have been information security incidents that negatively affected the business in terms of financial losses or a weakened market position, 19 percent of the businesses are aware of such incidents and are able to quantify how many.

Among those who have experienced incidents with negative consequences such as financial losses or a weakened market position, the average has been 3 such incidents throughout 2017. The median is 2 incidents, so typically 2 to 3 incidents have been experienced by those who encountered them.

If we assume that the businesses that do not report a number are also not exposed to such incidents, the average in the entire population (businesses with 5 or more employees) is 0.6 incidents with negative consequences throughout 2017. Businesses with 100 or more employees encountered an average of one instance of security incidents with financial losses or a weakened market position. This is significantly higher than businesses with less than 100 employees (0.4 in businesses with 5 to 19 employees and 0.6 in businesses with 20 to 99 employees).

The average number of incidents with negative consequences in the form of financial losses or a weakened market position.

Figure 8



When it comes to what the most severe incident was, regardless of whether the incident resulted in negative consequences or not, viruses, phishing, hacking and DDoS attacks recur the most.

Question: What was the most serious incident in 2017?

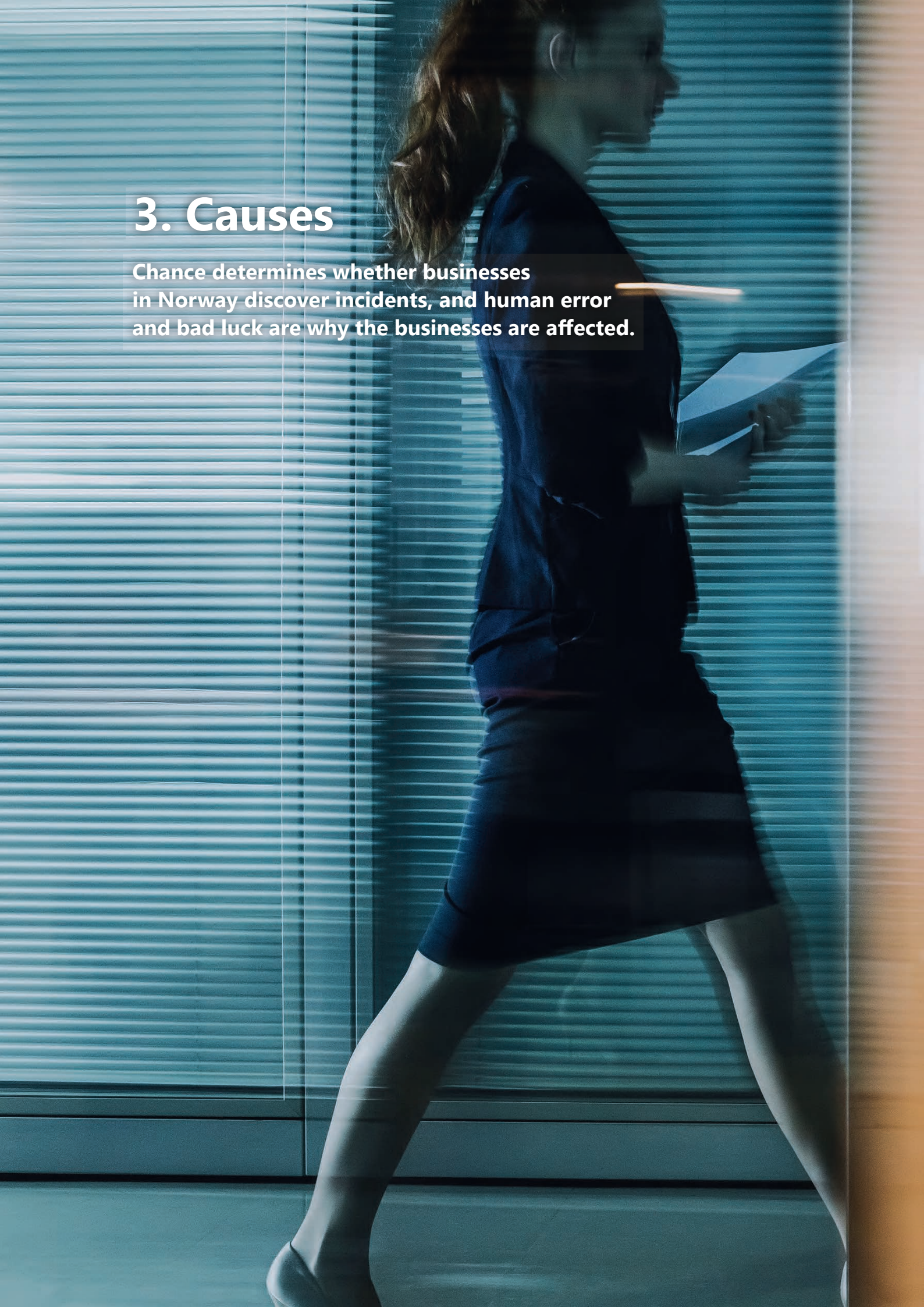
Figure 9

Viruses or malware infections are also the incidents that occur the most often, and a number of the businesses reporting these as the most severe have only encountered virus/malware infections.

If we look only at businesses that have, in total, encountered at least four information security incidents, the picture is a little different, and DDoS attacks become a more dominant presence.

Figure 10

As for why these incidents were perceived to be the most severe, the most commonly reported factors are financial losses, downtime, and a loss of working hours and production.



3. Causes

Chance determines whether businesses in Norway discover incidents, and human error and bad luck are why the businesses are affected.

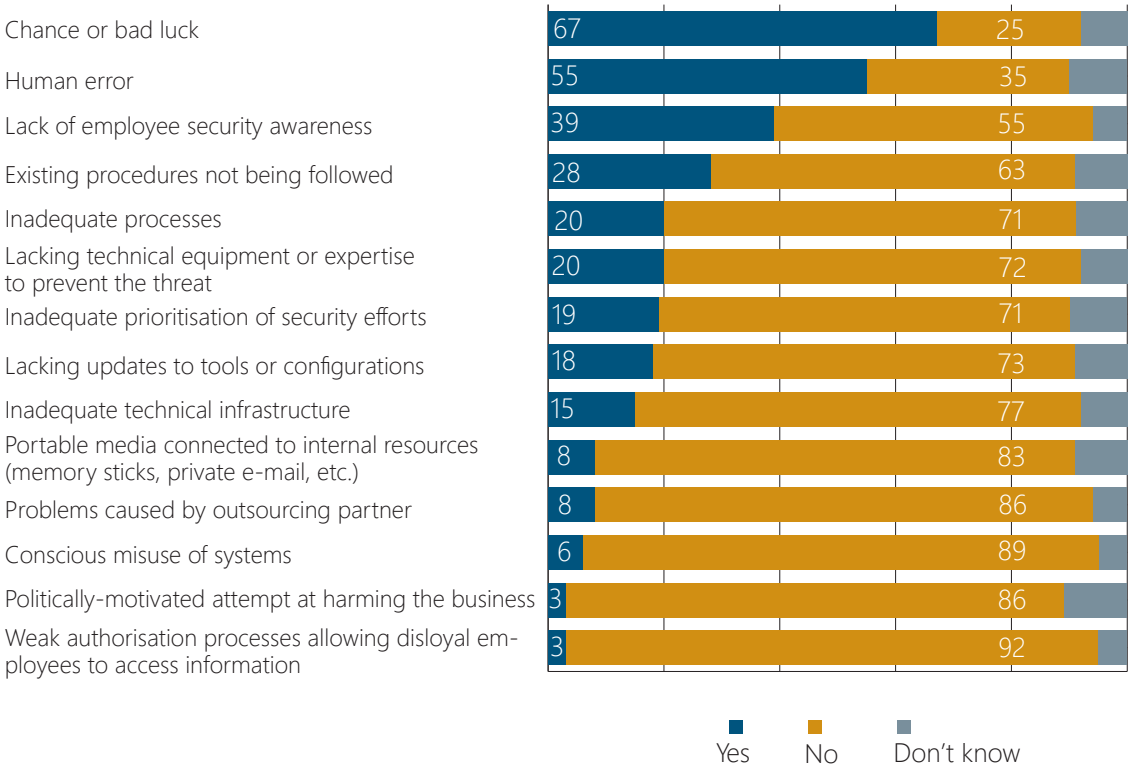
3. Causes

3.1 Why security breaches occurred

Norwegian businesses largely believe that security breaches occurred as a result of chance or bad luck.

Question: Were any of the following factors the reason the security breach occurred? (n=572)

Figure 11



Among those who have experienced incidents, 67 percent believe the cause was chance or bad luck, while over half also attribute the security breach to human error.

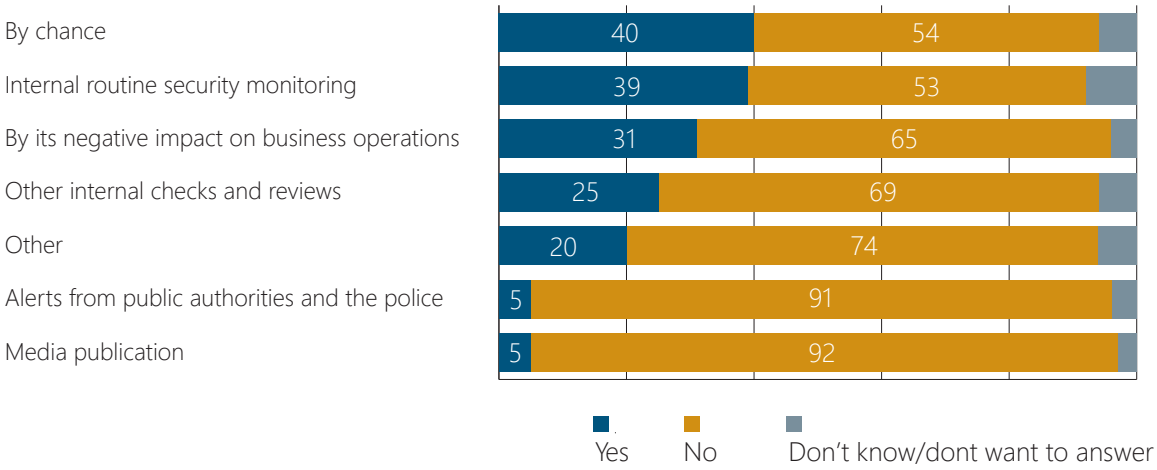
Chance and bad luck are less likely to be given as a cause among those with a framework or management system for information security. 74 percent of businesses that have experienced incidents and do not have a management system believe it is due to chance or bad luck, while 65 percent of those with management systems report the same. Furthermore, those without management systems were more likely to attribute the incident to a lack of technical tools or competency to prevent the threat. While a total of 20 percent report this reason, this breaks down to 25 percent of those without management systems and 17 percent of those with management systems.

3.2 How security breaches were discovered

When it comes to how the security breach was discovered, an equal number report that it was by chance and that it was by internal routine security monitoring

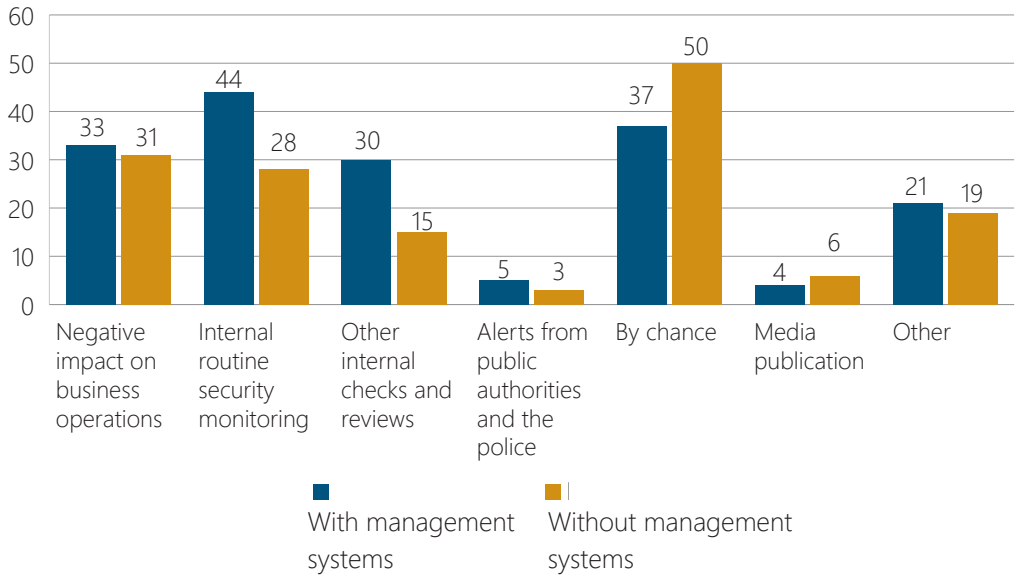
Question: Were any of the following the way the incident was discovered? (n=572)

Figure 12



There is a difference between companies with and without management systems for information security when it comes to how the incident was discovered.

Figure 13



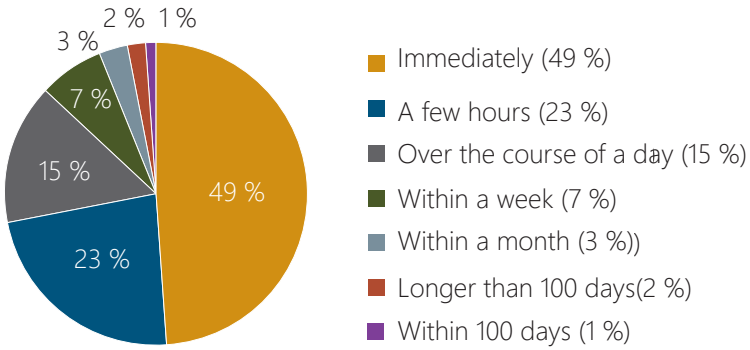
3. Causes

Businesses with a management system are more likely to discover security breaches as a result of internal routine security monitoring and other internal checks and reviews than businesses without management systems. Businesses without management systems, however, are more likely to discover security breaches as a result of chance than businesses with management systems.

Half of the businesses discovered the incident immediately (answering for the last/most severe incident). A further 24 percent discovered it in a matter of hours, and 15 percent in the course of a day. There is no difference between businesses with or without an information security management system, or larger and smaller businesses.

Question: How long did it take from when the incident occurred to when it was discovered?

Figure 14



It may be difficult to protect yourself from dangers you cannot see.

4. Incident consequences and handling

This chapter revolves around conditions such as the consequences of the incident, who it was reported to, organisational consequences and costs.

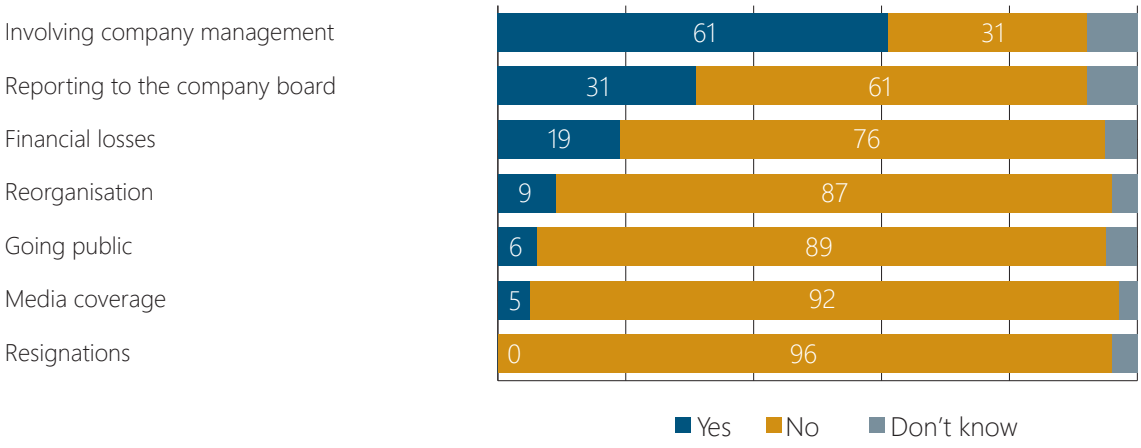
4. Incident consequences and handling

4.1 Incident consequences

In six out of ten businesses that encounter information security incidents, one of the consequences is that the company's upper management gets involved.

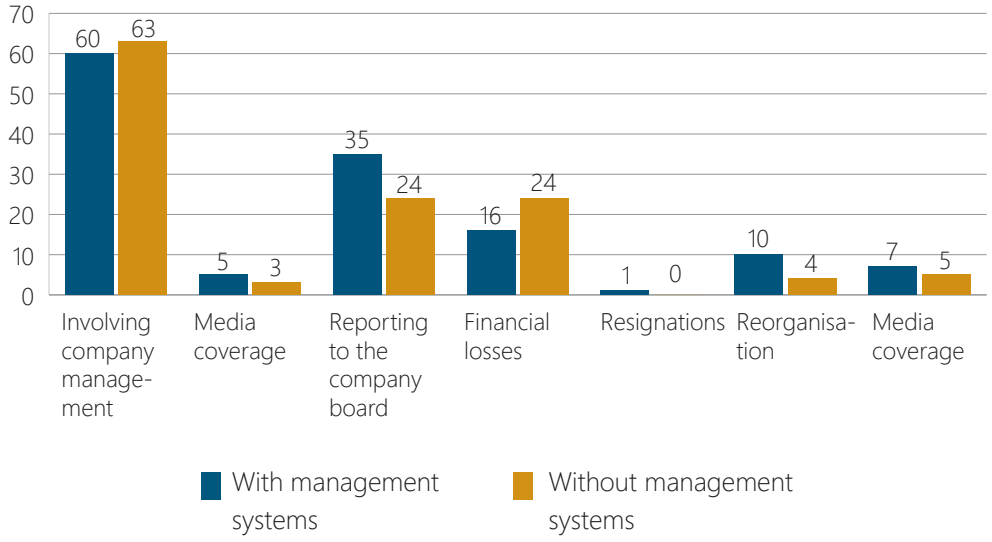
Question: Did this specific incident lead to the following? (n=572)
– respondent answers based on the last incident/most severe incident.

Figure 15



Both the involvement of the company board and the involvement of management are more common in smaller businesses than in large ones, while there is also a difference between businesses that either do or do not have an information security management system. Those with a management system report to the board more often, are more likely to implement organisational changes, and face financial losses to a smaller degree.

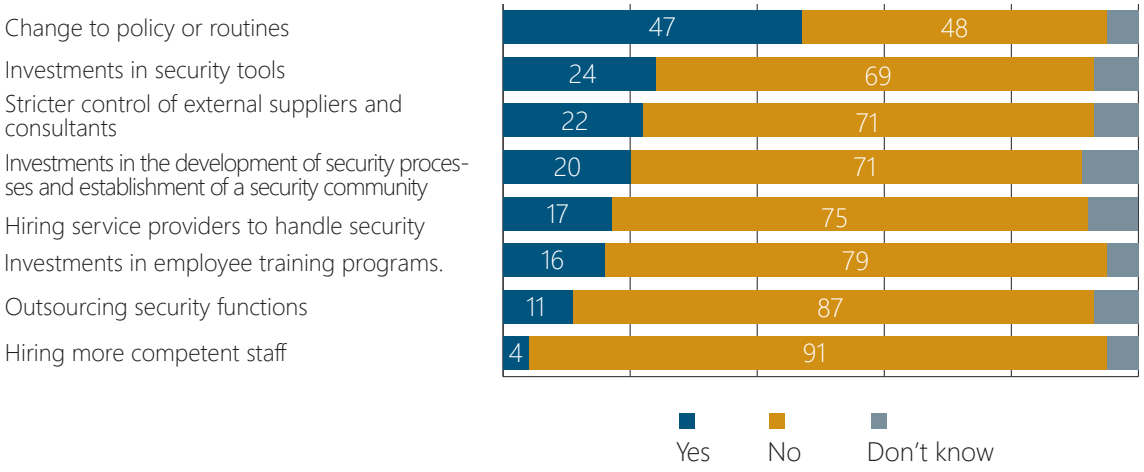
Figure 16



In addition to the consequences mentioned previously, security incidents have also led to changes in a number of the affected organisations, where 47 percent have changed policies and routines.

Question: As a result of the incident, were any of the following changes made in the organisation? (n=572)

Figure 17



Small businesses have made changes by referring to expertise outside their own organisation to a greater degree than larger ones (100 or more employees). While 22 and 14 percent of the smallest businesses have hired a supplier to handle security and have outsourced security functions respectively, 9 and 5 percent of businesses with 100 or more employees have done the same. Smaller businesses have invested in security tools and implemented stricter control of external consultants to a greater degree as well. Larger businesses have, however, invested in training for employees. Businesses with an information security management system have to a greater degree than others invested in the development of security processes and established a security community. While 24 percent of businesses with a management system have done this, 11 percent of those without a management system have done the same.

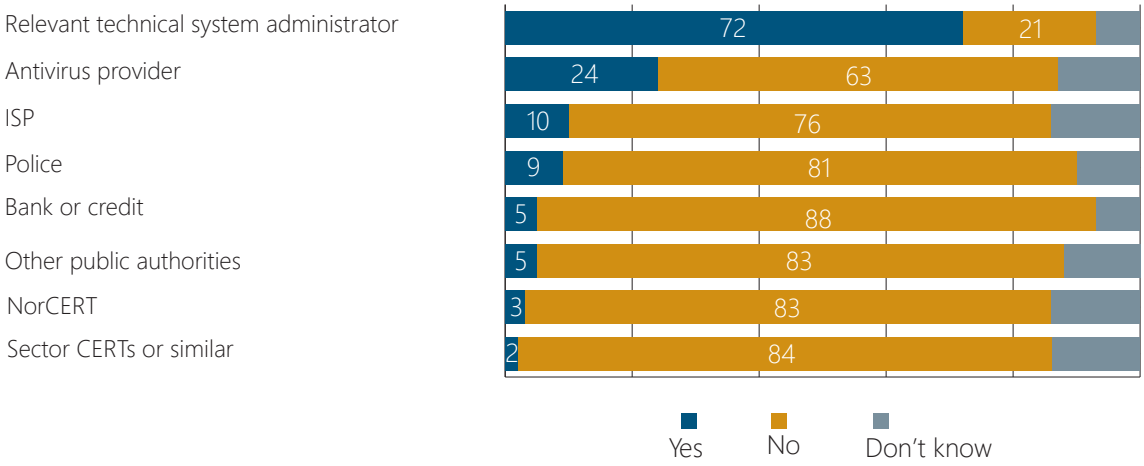
4. Incident consequences and handling

4.2 Reporting

72 percent of businesses that have encountered security incidents have reported the incident to the relevant technical system administrator, while 9 percent have reported the incident to the police. A mere 3 and 2 percent have reported to NorCERT or Sector CERT, respectively.

Question: Was the incident reported to any of the following? (n=572)

Figure 18

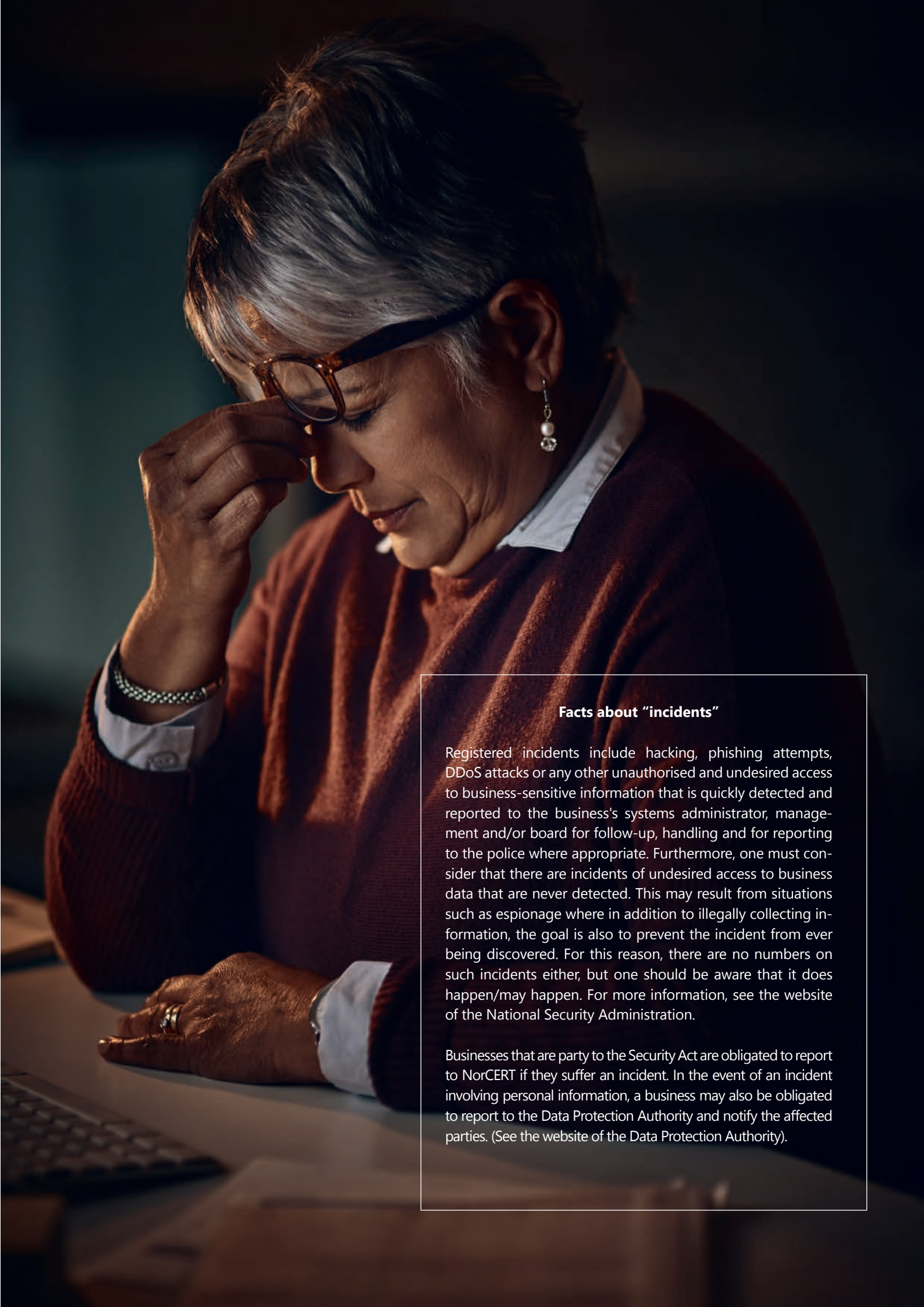


Those with a management system have to a greater degree than others reported to the system administrator and ISP, but the pattern is less clear than it is for certain other questions. It is also worth noting that those with a management system to a greater degree do not know if they have reported the incident to NorCERT or Sector CERT.

Businesses of different sizes follow the same pattern. For example, there is no significant difference between larger and smaller businesses with regard to whether they report to NorCERT or Sector CERT. Reporting to NorCERT varies from 2 to 4 percent in different size groups, while the equivalent for Sector CERT is 1 to 3 percent.

4.3 Costs of incidents

Among those affected by incidents and who are able to quantify the financial cost of the incident, including those who know that there has been no financial cost, the average cost is approximately 54,000 NOK for the most severe incident in 2017. Those most seriously affected estimate a cost of 2 million. There is no significant difference between businesses that have and do not have information security management systems, or between businesses of different size.



Facts about "incidents"

Registered incidents include hacking, phishing attempts, DDoS attacks or any other unauthorised and undesired access to business-sensitive information that is quickly detected and reported to the business's systems administrator, management and/or board for follow-up, handling and for reporting to the police where appropriate. Furthermore, one must consider that there are incidents of undesired access to business data that are never detected. This may result from situations such as espionage where in addition to illegally collecting information, the goal is also to prevent the incident from ever being discovered. For this reason, there are no numbers on such incidents either, but one should be aware that it does happen/may happen. For more information, see the website of the National Security Administration.

Businesses that are party to the Security Act are obligated to report to NorCERT if they suffer an incident. In the event of an incident involving personal information, a business may also be obligated to report to the Data Protection Authority and notify the affected parties. (See the website of the Data Protection Authority).

5. GDPR and security awareness

This chapter examines changes to efforts involving privacy and information security related to the implementation of GDPR and activities to improve security awareness among employees.

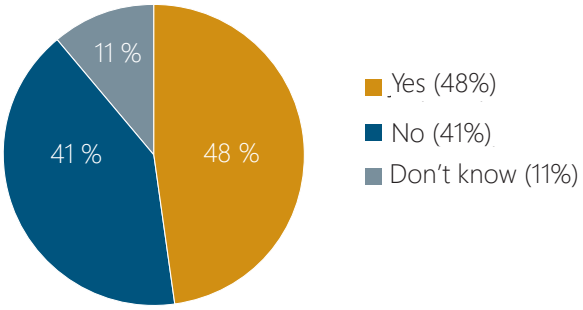
5. GDPR and security awareness

5.1 Changes resulting from GDPR

Approximately half of the businesses have made changes to their privacy and information security efforts as a result of GDPR.

Question: New privacy regulations (GDPR) take effect starting in May 2018. Has this led the organisation to implement changes/improvements to its efforts involving privacy and information security? (n=1500)

Figure 19



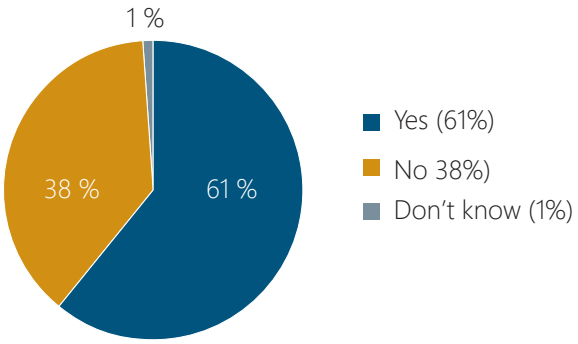
While 66 percent of businesses with 100 or more employees have made changes, 40 percent of those with 5 to 19 employees report the same. Furthermore, 57 percent of those with a management system have made changes, while 31 percent of those without a management system have done so.

5.2 Increased security awareness

61 percent have over the past year completed activities to improve the security awareness of their employees.

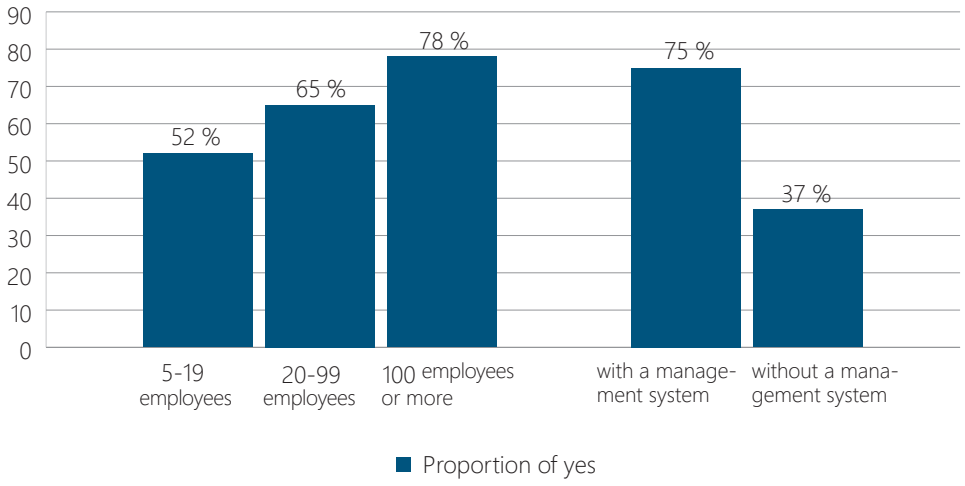
Question: Has the business completed activities to improve the employees' awareness regarding security over the past year? (n=1500)

Figure 20



Large businesses with 100 or more employees and those with information security management systems are also the ones who have completed such activities to the greatest degree. While 52 percent of businesses in the smallest size group have completed activities, 78 percent among the large businesses have done so. 75 percent of businesses with information security management systems have completed activities, while only 37 percent of those without such systems have done so.

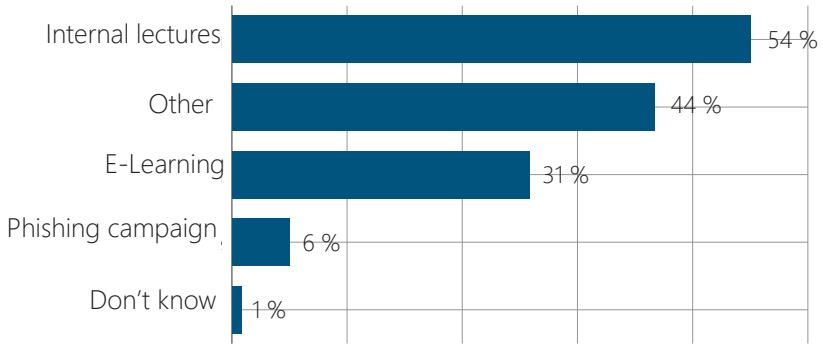
Figure 21



Among those who have completed activities, internal lectures are the most common measure.

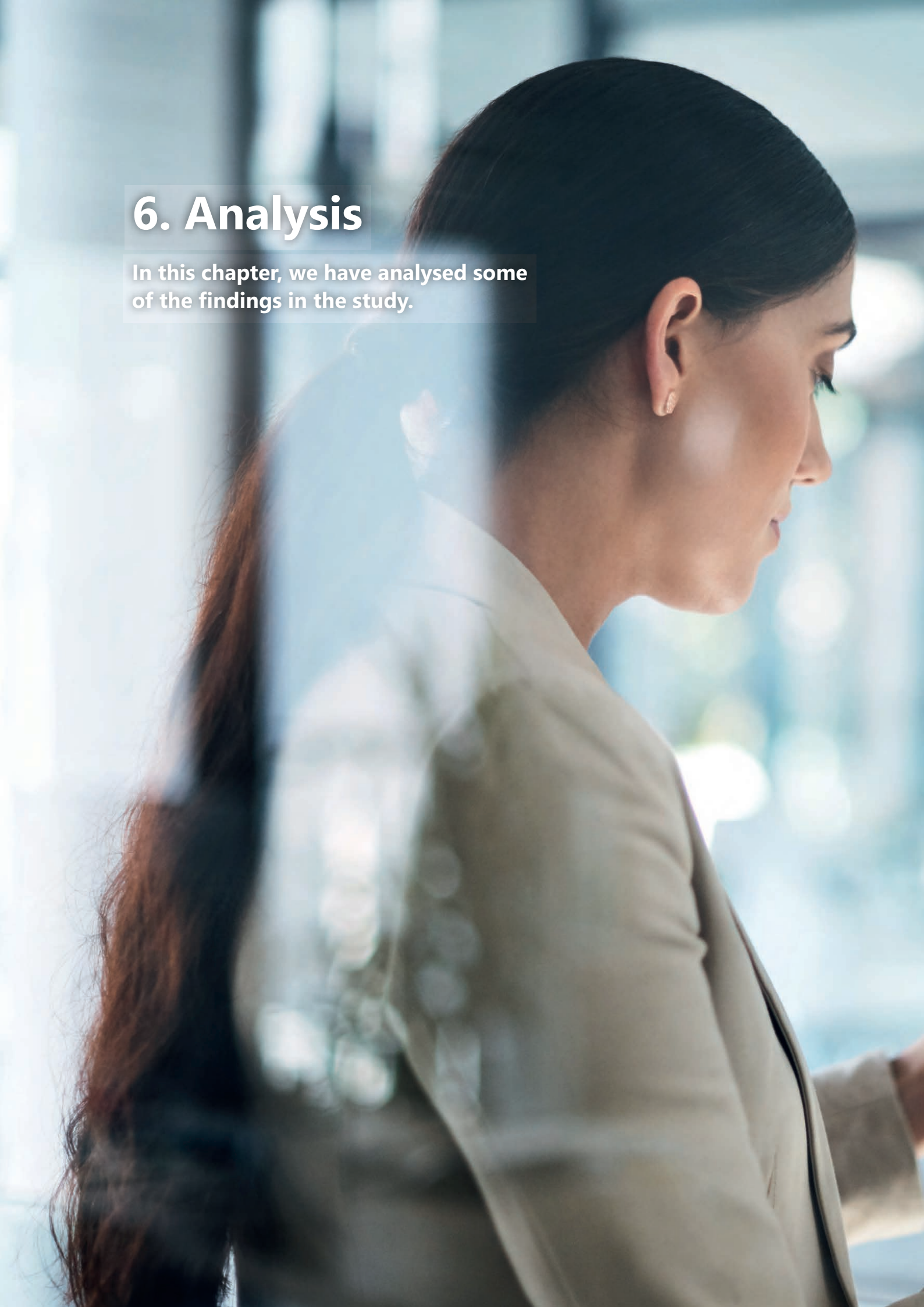
Question: Which types of activities to increase employees' awareness regarding security have been completed over the past year? (n=913)

Figure 22



6. Analysis

In this chapter, we have analysed some of the findings in the study.



6. Analysis

6.1 Key findings in businesses reporting that they have a security framework

6.1.1 In the public sector

A high percentage of public businesses have an information security management system or framework. Out of those reporting that they have a framework for security systems, 82 percent (public administration) to 88 percent (healthcare) of public businesses report that these routines are complied with.

The study also shows that in security breaches, 22 percent of public healthcare businesses report that the breach occurred due to a lack of prioritisation of security efforts.

Another reason for security breaches reported among those who have an information security framework is the inadequacy of their processes.

In public administration, 25 percent of respondents report that lacking security processes led to security breaches. Even more respon-dents, 40 percent in public administration, report that the business has experienced security breaches due to a lack of follow-up in their processes. In the healthcare sector, 33 percent report the same. **This is interesting as a high degree of compliance to security frameworks is reported while lacking processes and routines are named as a significant cause of security breaches.**

The findings indicate that despite large swaths of the public sector having information security management systems and frameworks, and a considerable share reporting that these are complied with in the organisations, the follow-up of these security measures remains inadequate for securing the businesses in question.

Between 33 percent (public administration) and 41 percent (education) in public administration, health and education report that they discovered security breaches by chance. **When over a third of public businesses discover security breaches by chance, one must question how effective compliance with the frameworks for infor-mation security really is in practice, as well as the effect a lack of existing processes or compliance with routines has on security efforts.**

On the other hand, 40-50 percent of the public businesses that have experienced security breaches report that these were discovered immediately.

6.1.2 In the private sector

As expected, there is a greater variation between different fields in the private sector. In construction, service, and industry, under 50 percent report that they have a security framework in place.

Construction generally reports a low degree of readiness in information security. Up to 20 percent of the businesses report that they do not know whether they have a framework for information security.

Among private businesses that have a security framework or management system, a large share also reports that these are complied with. Here the accom--modation and food services as well as retail distinguish themselves with over 90 percent believing that the security frameworks and routines surrounding these are complied with. However, where there have been security breaches, the reports from accommodation and food service businesses indicate that 29 percent believe breaches occurred due to a lack of prioritisation on security efforts. **This does not appear to follow from the sector's perceived compliance with existing security frame-works.**

Overall, businesses in the private sector follow processes for security breaches and similar situations to a greater degree than the public sector.

About a quarter of businesses in the private sector believe security breaches occur due to a lack of compliance with and follow-up of existing processes.

In industry, 30 percent of businesses report that security breaches occurred due to a lack of follow-up of processes and 55 percent report that security breaches were discovered by chance.

In cases of security breaches, industry, accommodation and food service businesses as well as service industries present the lowest degree of readiness in terms of discovery, with less than half discovering breaches immediately after they occur. In other sectors, between 50-70 percent report that they discovered security breaches immediately after they occurred.

6.1.3 In summary

Cyber threats and attacks have become a part of our digital daily life and are something we must all take into account. Therefore, it will become more important to not only invest in security and defence mechanisms, but also to prepare the business for compliance with frame-works and guidelines, as well as follow-up in case of incidents.

The study shows that many outsource IT operations, and few security breaches are reported at third-party suppliers. In spite of this, it remains important to understand the threat in the business's value chain and to ensure continuous follow-up of security measures with business partners as well.

Businesses recognise the importance of cyber security and of protecting themselves against attacks, but this is not reflected well enough in their reported follow-up of security breaches.

GDPR requires organisations to have a plan for breaches of personal data security, but many businesses still have not established a security framework and do not follow policies and routines for following up security breaches.

There is an increasing need to secure data and privacy. This will also be highlighted to a greater degree than before through public discussion, as well as through national and international laws, regulations and directives such as GDPR and NIS.

Many report that the contrast between the business's work, its focus on security frameworks, and its lack of follow-up for security routines and processes in daily activities causes security breaches in the businesses.

6. Analysis

6.2 Reporting and notification of security incidents

The businesses that invest the least into information security likely have an increased chance of being affected by cybercrime. Furthermore, one can be affected over time without being aware of it. It is made evident in the study that businesses without management systems are the most likely to discover incidents by chance. To a greater degree, businesses with a management system discover security breaches as a result of having routines for active information security efforts. This may indicate that many businesses do not invest enough into information security.

There may be a variety of different reasons one may choose not to invest in proper information security, such as the perception that the business is not an attractive target for threat agents. Or one may believe that the probability of being attacked is low considering all the businesses in the world that could be targeted instead. In one report[2)], four out of ten decision-makers in businesses have stated that they would rather pay a ransom to hackers than to invest in data security.

As for the causes of security breaches, many businesses report that the dominating factors are hum-an error, a lack of security awareness among employees and a failure to follow existing processes. This may also indicate that many choose not to invest in information security enough. The whole time, threat agents often use social engineering as a key tool, so increasing awareness and knowledge among employees is an essential information security measure. One can have strong logical and technical system security, but the human factor may still be the weakest link in security.

6.3 GDPR and security awareness

This year, we have received new privacy regulations in Norway. The General Data Protection Regulation (GDPR), which is incorporated into Norwegian privacy legislation, is an EU directive that applies to the entire EU/EEA. The new regulations bring with them a range of new duties for businesses and strengthened rights for citizens.

It is worth noting that privacy legislation in Norway over the past 20 years has included many of the same requirements that are now made clear and concrete in the new directive to contend with the increasing digitisation of society. Compliance with the new legislation will strongly contribute to an increased focus on security and safer systems.

In this year's study, questions were asked regarding whether businesses have made changes/improvements to efforts involving privacy and information security. We see in figure 19 that only 40 percent of the smaller businesses report that they have made changes related to GDPR. This may indicate that many businesses are unaware of the regulations and do not realise they must comply with them. The privacy regulation applies to all businesses that handle personal information - such as the collection, use, communication, transmission, storage and processing of personal information. All the businesses that have responded in the study have at least five employees and must therefore at the very least handle personal information regarding their employees, making them obligated to comply with the regulations in the same manner as businesses that have users, customers, patients, clients, students, etc.

The privacy regulation includes requirements to know where personal information is located. In point 1.1 Outsourcing, we see that the number of businesses that outsource services to overseas is now 15 percent, a clear rise from the previous study, where 8 percent gave this reply. Out of those, nearly a fifth (18 percent) reply that they do not know where their data is physically stored.

2) NTT Security, Risk:Value Report.

If personal information is among the data that is outsourced, and a business does not know where the data is physically stored, it may be located in countries outside of the EU/EEA. In this case, it is likely that there has been no risk assessment of the provider or the country the data is stored in, and that there is no legal basis to store personal information there. If this is the case, this would constitute a breach of the privacy directive and a breach of personal data security.

The privacy directive stipulates that businesses that discover breaches of personal information security must report discrepancies to the Data Protection Authority within 72 hours. Examples of incidents that must be reported to the Data Protection Authority include:

- Documents made available online, where these documents include information that is subject to a duty of confidentiality or which include sensitive or other confidential personal information.
- Information on persons living at a secret address which has been publicised in information services or has been distributed to unauthorised persons.
- Unauthorised persons gaining access to the membership list of a political party or religious congregation.
- Unauthorised persons altering personal information that may harm individuals, e.g. loss of reputation, discrimination, danger to life and health.

The Norwegian Data Protection Authority received 370 discrepancy reports last year, and around the same number halfway through 2018. It can be stated with some certainty that there are major unrecorded statistics here. We see in figure 13 that 50 percent of businesses without a management system discovered incidents by chance. With the 72-hour requirement for reporting, it may be wise not to rely on chance and the unknown causes of incidents. Breaches of the privacy directive may lead to fines of up to 4 percent of gross global revenue, or 20 million Euro, depending on which is higher.

7. Risk profile/trends

In this chapter, we present risk profiles and trends observed by different authorities and private parties.

7. Risk profile/trends

The National Security Authority (NSM)
NSM has the mission of detecting, reporting, and handling incidents pertaining to attacks on critical infrastructure and key resources. Within the scope of its mission, NSM has for several years observed a steady rise in targeted data breaches against Norwegian interests, both public and private. In addition to the increase in targeted attacks, there is a rise in criminally motivated actions in Norwegian cyberspace. A large share of these attacks have become more advanced than before.

The most common method used in targeted attacks is the use of infected e-mails ("Phishing"). In this method, the e-mail contains a malicious attachment or link to a website loaded with malicious code. In most cases, the e-mail is constructed using information relevant to the receiver and is only sent to a limited number of users (spear phishing). Information on the recipient of the e-mail is collected from information available to the attacker, whether it stems from freely available sources or compromised data.

Aside from e-mail, the most popular type of attack used the past year has been scanning followed by exploitation of vulnerable systems. Unlike phishing, this approach is less reliant on human interaction. Scanning for vulnerable versions of software in a network is a popular choice for attackers. If the business is lacking update routines, older versions of software may provide the attacker with a cheap way into the company's network. A lack of network segmentation often allows attackers to move between different parts of the business's ICT solutions. NSM observes that such attacks almost always utilise known vulnerabilities. In exceptional cases, NSM observes that "unknown vulnerabilities" or 0-day vulnerabilities are exploited.

NSM also notes a trend in which outdated web server installations at smaller businesses with limited IT resources are compromised. The compromised servers are then used as middlemen in new attacks on other targets, both domestic and abroad. Vulnerable versions of software are not the only ones to be exploited. NSM observes that attackers to a greater degree exploit vulnerable implementations of systems, which here refers to a function or a program that is vulnerable to being compromised due to weaknesses in the design of a service, or due to misconfiguration. Such systems often suffer attacks exploiting these vulnerabilities in order to leak information that can be used to access the system.

Attacks via the supplier chain is a technique where an agent chooses to attack the value chain in a business instead of using a direct attack. NSM observes that agents are increasingly attacking weak links in value chains.

A severe negative development in cybercrime is mining for cryptocurrency. Illegitimate cryptocurrency mining (also known as "crypto-jacking") is rising sharply and has thus opened for a range of new problems in preventive IT security.

NSM has not observed any attacks conducted by hacktivists that have had major consequences for Norwegian society, but services and websites have suffered extended downtime.

NSM has observed a trend in which attacks are growing more complex, and advanced agents are moving away from phishing and onto other techniques. This may entail that in many cases, it has become more difficult and more demanding to detect data breaches. NSM strongly advises businesses to continue focusing on e-mail security, as phishing remains an attack method that can cause major damage to businesses. Furthermore, businesses must develop a general resistance in order to detect and resist various complex attacks.

Above all else, businesses must maintain control of their entire value chains within their ICT environments, and the NSM Basic Principles are developed to assist in these efforts. This begins with processes regarding the identification and charting of the ICT environment. Protect, preserve and discover are key elements to protect yourself from being compromised, and when things go wrong, there should be well-tested routines for handling and re-establishing your ICT environment. NSM recommends all businesses use the Basic Principles as a minimum in their security efforts.

National resistance and readiness in the digital space must be strengthened. Therefore, the National Cyber Security Centre will be established as a part of NSM in the fall of 2018. The centre will make the digital space safer for Norwegian parties.

Telenor

Towards the end of 2017, ransomware became the most-discussed threat in the computer security world. Fortunately, Norwegian businesses often maintain relatively strong basic security. As a bare minimum, operating system patching is conducted by the vast majority of companies. Pirated copies of Windows are also quite uncommon. This allowed Norway to largely steer clear of the major spread of ransomware and software that erased hard drives in 2017 (WannaCry/NotPetya). This malware spread through local networks by using vulnerabilities in Windows. Microsoft had however already patched the vulnerabilities when the spread began, so fully-patched computers were immune. None of our Norwegian clients were affected by these attacks.

In early 2018, malware extracting crypto-currency took the spotlight. Attacker-s began to scan for vulnerable systems, web servers in particular, and infected them. A number of Norwegian businesses suffered this as well, including several of our clients. For attackers, there are a number of advantages to using this type of malware going forward:

- Victims often do not realise that they are affected and that the resources of their PCs are being abused.
- The resources can therefore be abused over a long period of time.
- The money is made completely automatically, without the victim having to transfer money or do anything actively.
- No communication is needed with the victim.
- Ransomware attacks can cause harm to the victim and therefore lead to heavier penalties or even a bad conscience for the culprits. Stealing computer resources is not destructive to the same degree.

Overall, there are fewer general infections on PCs and servers in Norway now than before. Exploit kits that used to infect computers through browsers have disappeared almost completely. Instead, people are tricked into surrendering user names/passwords through the use of phishing. Web mail is a very popular target, as the company either operates the e-mail service themselves or delegates it to the cloud. Attackers then often trick a few employees before making targeted phishing e-mails from a victim's account. Often, e-mail forwarding is activated for e-mails from compromised accounts, so that the attackers can steal trade secrets or plan further exploitation, such as CEO fraud. We recommend the use of two-factor authentication for all e-mail accounts to limit this type of attack.

CEO fraud has become even more sophisticated and targeted in recent years. Perpetrators are becoming more skilled at charting roles and relationships in businesses before attacking, and can write in proper Norwegian. These attacks can often provide considerable gains to their perpetrators. This is a type of fraud

7. Risk profile/trends

fraud that is difficult to build technical defences against. Here, training employees and maintaining good internal routines is key.

Data breaches from foreign powers against Norwegian targets with the aim of operating espionage and information gathering continues. In the vast majority of cases, e-mail is the way in for the attackers. They often use phishing or Microsoft Office files with malware attachments. Examples of businesses that have recently been affected by this are NUPI and the Southern and Eastern Norway Regional Health Authority. Many Norwegian companies are likely subject to industry espionage without being aware of it.

Businesses continue to face waves of threats of DDoS attacks. Companies are threatened to pay "ransoms" to prevent purported upcoming attacks. The threat is often accompanied by a "test attack". However, major attacks do not come after the test attack quite so often, even if the ransom goes unpaid. The number of DDoS attacks in Telenor's network has dropped somewhat, but the vast majority of victims are private users. We have seen 1806 attacks so far this year. 599 of these attacks were handled and mitigated by TSOC. The biggest attack was as large as 101 Gbps and lasted for an hour. Typically, 4-10 of our paying customers using DDoS filtering are attacked over the course of a month.

The National Criminal Investigation Service (Kripos)

Threat activities against Norwegian businesses continue to consist of known crimes such as CEO fraud, phishing campaigns and denial of service attacks.

Kripos has noted that threat agents
have become more technically competent and are to a greater degree acquiring illegal access (compromising) e-mail accounts, etc. By having access to e-mail accounts, threat agents can believably appear to be a person within the business, and in this manner mislead others to perform the actions they seek. The language in correspondence with victims has also improved in both Norwegian and English. In many cases, the language appears completely spotless, and the threat agent quickly replies to the victim using a proper written tone, leaving the victim unable to take this as a warning. The result of this is that it is more difficult to detect that one is a target of fraud, and this puts businesses' routines and security systems to a bigger test going forward.

The rise of cryptocurrency has entailed that threat agents use illegally acquired computer power to extract gains. There have also been several cases where people have been defrauded by fake cryptocurrency exchangers. As long as cryptocurrency holds a certain value, it is highly likely that certain agents will continue to defraud people and use other people's computer systems to make money by extracting cryptocurrency.

Cryptoviruses make the distinction between state agents and organised criminal groups more complicated. Cryptoviruses may be used both as a tool of sabotage and as a means for demanding ransoms. Threat agents have become better at building on experiences from previous ransomware campaigns, and they continuously update their tools and techniques to penetrate computer systems. More advanced ransomware or cryptovirus campaigns are therefore expected going forward.

New mobile solutions are constantly being developed for payment services and other service offers. From our international partners, several reports have been received regarding malware adapted for individual-based devices including code for attacking foreign banks. Kripos has previously noted persons purchasing malware adapted for individual-based devices with the goal of using them for an

attack on a Norwegian bank. They were arrested before the attack could take place. It is likely that we will see threat agents targeting mobile devices to a greater degree going forward.

Norwegian banks continue to face threat activities, and there have been several attempts at targeted attacks on bank employees and online banking customers. It is highly probable that the development is largely because global threat agents are targeting increasingly large attack surfaces for their activities. Many global threat agents appear advanced or well-organised. It is highly likely that they have access to vast malware development resources and have a large infrastructure of compromised servers at their disposal. We therefore expect the threat to Norwegian banks and bank customers to continue or increase going forward.

mnemonic

In the past few years, we have observed that malware campaigns often occur in a cycle like this: a major campaign is spread widely without being targeted at a specific goal. As a consequence, we see many infections during the period of the campaign. Then it goes quiet again, until the next campaign strikes a few months later. The whole cycle repeats with a few months in-between. We have now waited a long time for the next big campaign, without anything seeming to materialise.

While the world becomes more aware of threats such as ransomware and other malware, criminals continue to seek new and more efficient ways to make money. Observations from our SOC (Security Operations Centre) show a shift in the threat profile from the wide, generic distribution of malware we have seen in the past few years to an increase in several large, targeted attacks. This tendency is most visible in attacks on larger organisations and companies.

The attacks are targeted in that they go after one specific organisation, or organisations with a certain number of end-points, in one specific geographical location or industry. Overall, we observe that the threat agents are placing a bigger emphasis on researching their target prior to attacking. We also see that these threat agents are persistent, and may return with different attack methods and techniques, applying knowledge from earlier attempts. More money and resources are behind these types of attacks than in the generic distribution campaigns. The attacks also use ransomware and other malware in a more targeted fashion than we have seen used previously.

One consequence of this is more and larger security incidents with a potentially more significant influence on the organisation than with more generic attacks. They may also be more difficult to detect, as they are customised for the specific goal the attacker wishes to achieve. Although such heavy, targeted attacks have mainly been observed among larger organisations and companies, we do not rule out that as attack methods become more advanced, they will also be used to go after smaller businesses.

We observe that organisations are slowly but surely changing their mindset from trying to prevent all attacks to accepting that some attacks will be able to get past preventive security controls. As part of this, we see that many organisations are preparing themselves for such situations by improving the way they detect threats, establishing routines for incident handling, and generally having a more balanced approach to preventive and reactive security strategies.

This shift is due to a number of factors. We can speculate that one factor is new regulations, including the GDPR and NIS directives, which require organisations to maintain more control of their data and systems. These force organisations to at least dis-

7. Risk profile/trends

cuss and evaluate different information security situations. Another factor may be that the media reports on new data breaches and leaks almost daily, making the majority of people more aware of IT security. Media coverage, which in many cases includes well-known brands and organisations, as well as several reported data breaches and leaks, may have helped make more people used to the thought that this could happen to themselves as well. It could also be explained by the industry becoming more advanced and developing over time.

Although the change is slow, it is possible to observe it through the collaborations and discussions we have had with the industry, as well as through the inquiries we receive. We believe this is a step in the right direction.

Nordic Financial CERT – NFCERT

NFCERT is a joint project of Norwegian, and eventually Nordic, banks, and has become its own unit - the finance industry's "fire department" against cybercrime in the Nordic countries.

NFCERT offers a closed communication platform between participating financial institutions, allowing them to warn each other about computer and fraud attacks and to share experiences.

In summary, based on observations from operational incidents and other experience-based information from participants, the threat profile is the biggest in the following areas:

- Mobile and online banking fraud
- Denial of service attacks (DDoS)
- Targeted attacks/data breaches
- Fraud by e-mail (incl. phishing and malware)
- Ransomware
- Known vulnerabilities

The banking and finance industry face regular targeted attacks in the areas mentioned above. Attacks come from various international or local groups and vary in strength and frequency. Attacks may slow down or stop completely when, for instance, Europol arrests individuals connected with certain criminal groups, but we then see that activity often starts up again after a break of a few months following such an arrest.

There is a wide range of threat agents - from complete amateurs with a limited ability to carry out attacks, through hacker groups and organised criminals, to state-funded organisations where the latter agent possesses considerable knowledge and a high motivation to carry out different types of attacks.

Major incidents in 2017 show beyond a shadow of a doubt that the finance sector is not immune to this. Stolen credit card information is regularly sold on the "Dark Web", and after it was revealed that the credit reporting agency Equifax suffered a data breach in which the data of up to 146 million customers was compromised, the stock market reacted by sending its stocks down 33 percent.

NFCERT saw a relatively calm end to 2017, although we have seen increased interest and focus from threat agents, particularly with regard to malware on mobile devices. This is a trend that has grown in scope in 2018, and it must be expected that this area will continue to be targeted in the time to come. Financial institutions in the Nordic countries are a target of choice for malicious software and the development of attacks and fraud is on the rise. In the Nordic countries, there have been no new malware-based attacks on bank services for a long time, but more harmful malware has entered the market on the "dark web" for both Android and PC platforms. We believe we will see an increase in malware-based attacks again over the course of the year.

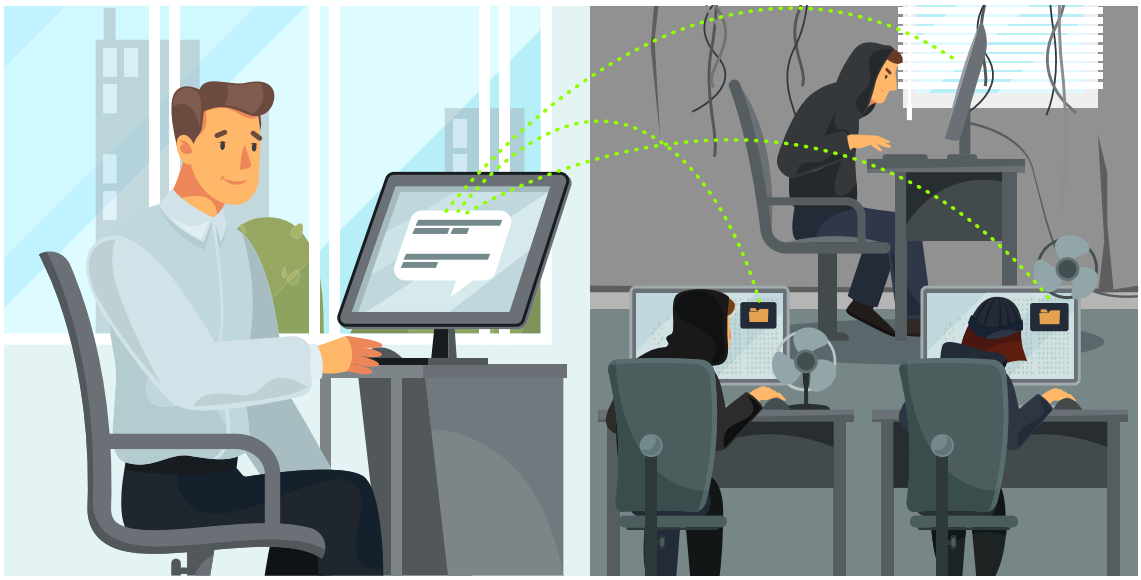
Another concern is the increase in hardware vulnerabilities (cf. Meltdown and Spectre on the most widespread processors) which can be exploited in the

internal systems of companies. Patching or replacing vulnerable equipment usually takes an exceptionally long time and leaves threat agents with plenty of time to develop tools to exploit this type of vulnerability.

In the beginning of 2018, there was more activity targeting bank services than we have seen in a long time. Phishing campaigns have continued, and there are several varieties of malware directly aimed at financial institutions. Advanced agents have also been active in the Nordic countries with targeted attacks on financial institutions by sending spam/e-mail with malicious attachments.

Further into 2018, we now see an increase in CEO fraud again, after the trend decreasing over the past half year.

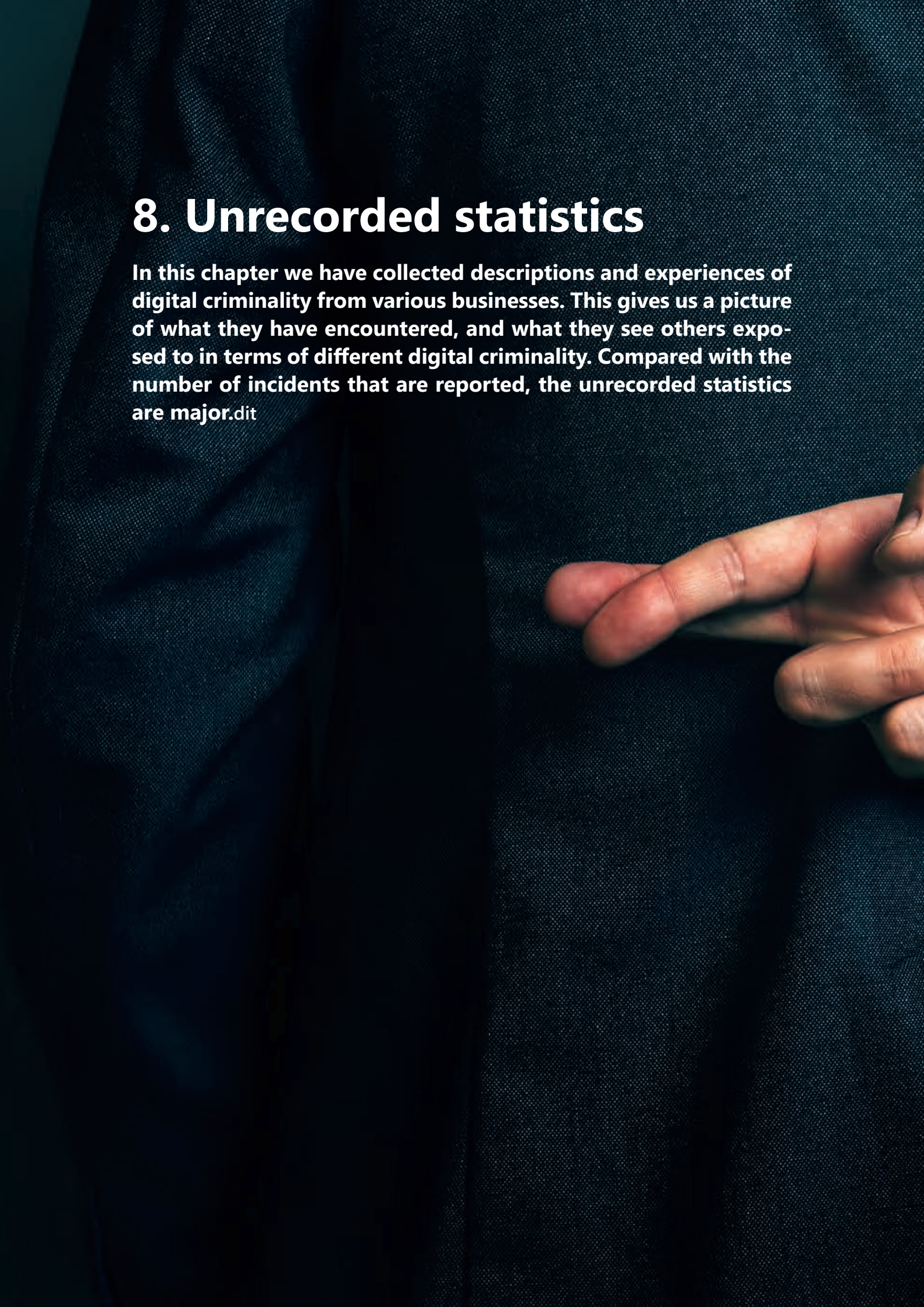
On this positive side, there has been a relatively steep decline in the spreading of ransomware leading into 2018. This means that the global volume of ransomware has decreased by more than 30 percent compared with the previous year. We have observed a considerable reduction in activity from our members with cases involving ransomware, which in practice confirms this declining trend.



Many businesses have limited detection capabilities, and little knowledge regarding the financial losses in an event.

8. Unrecorded statistics

In this chapter we have collected descriptions and experiences of digital criminality from various businesses. This gives us a picture of what they have encountered, and what they see others exposed to in terms of different digital criminality. Compared with the number of incidents that are reported, the unrecorded statistics are major.dit



8. Unrecorded statistics

Experiences from Kripos

The reason so few incidents are reported to police may rest on several factors, both internally in the business and externally. An internal factor may be the awareness of what can be considered a criminal incident that should be reported.

External factors could be the circumstances surrounding the act of submitting a report. The way police reports are received today may appear as cumbersome to some companies, which may lead them to not prioritise reporting incidents. By making reporting available online, it will be possible to reduce the threshold for businesses to report incidents. One could also facilitate the uploading of files that are relevant to the case while filling out the report, so that the case can be clarified as well as possible. From Kripos's side, a guidance form for reporting cybercrime has been developed to simplify the process for both the aggrieved party and the police. This form, as well as information on cybercrime, is available on the police's websites.

There seems to be a perception among a number of businesses that the police do not have the resources to investigate cybercrime, or that making such a report may lead to even more work for the business. In recent years, the police have on several occasions investigated and brought cybercrime cases to trial, achieving good verdicts for several types of cybercrime. The cooperation between the aggrieved business and the police has been completely essential to successfully obtaining a good result. As criminal elements improve their technical expertise, it will benefit the police and the business world to help each other out. It will therefore be beneficial if businesses see additional work that may occur as part of their social responsibility in order to help team up with the police to defeat cybercrime.

In order for businesses to develop strong counter-measures, we depend on knowledge on both the criminals and the technology. Many of the categories in cybercrime generate many incidents that again could have resulted in many reports from the business community. Through strong cooperation and regular dialogue, the police can establish a good overview of the overall scope while putting in resources on matters where there is a higher chance to get results and increase knowledge both on the criminals and the technology involved. This could again foster stronger counter-measures for businesses to implement. Kripos cooperates with several agents that build a stronger connection between the police and the business community, while police districts also have their own business community contacts. A future challenge could be to get better at sharing information between the police and the business community to acquire improved knowledge on cybercrime and achieve more positive results in the justice system.

Cybercrime demands a lot of resources to investigate, and with an increased number of cases, the need for resources also increases. The police take cybercrime seriously and intend to make it a bigger part of the portfolio than before. This can be observed in the establishment of NC3, in addition to each police district now having established its own section for digital police efforts. The police can however stand to improve their own ability to convey to the business community what capacities are available in cyber-crime and what results have been achieved previously. This could be done to increase the business community's motivation to prioritise reporting incidents. It should also be added that the police wish to inform the public on threats and challenges in ICT criminality, most recently in a report published at politi.no in December 2017.

Experiences from Visma

Visma is a supplier of software, outsourcing services, purchasing solutions, debt recovery services, shop data solutions, as well as IT-related development and consulting activities.

Today's attack pattern against our businesses is composite. What Visma sees as "normal background noise" includes the endless search for known vulnerabilities by nation-states, organised crime and similar activity by hacktivists, independent "script kiddies" and other bored parties. These are largely automated scans with varying levels of technical expertise.

The number seen as normal for one of Visma's services (Website/Webshop) is about 800,000 irregularities per month. This could be compared with an "unknown person" testing the door outside your house to see if it's locked or not.

Visma's analyses show that 6-10 of these are advanced or targeted enough to appear as "attempted break-ins", "attempted fraud" or "attempted industrial espionage, or nation-states attempting espionage against Visma or their customers".

Visma provides about 300 different services, so if the attack rates and attempts for different criminal activities were assumed to be equal for all services, this would give a foundation for between 1800 - 3000 police reports per month.

The pattern we see is that there is a large variation in how advanced these attacks are. The best attackers are highly advanced in terms of technique and challenge our ability to "buy security" by continuously investing more and more to protect our services.

For Visma's smallest customers (those operating their own hair salons, street kitchens, workshops, electricians, plumbers, etc.), it is unlikely that they will have the expertise or time to operate security efforts as advanced as those of a major service provider. The estimations Visma has made are based on incidents where Visma is the aggrieved party. If Visma's customers were included, the number would be even higher.

Experiences from Nordea

Nordea's customers are, like the rest of Norway's inhabitants, the subject of various kinds of fraud attempts. The attempts come in waves, sometimes more and sometimes less, and we are well aware that the more people who fall victim to fraud, the higher the risk is of the fraud growing in severity. In our daily efforts, we run into complications involving unrecorded statistics daily. Overall, it affects Nordea in a manner that allows us to fully comprehend how the risk profile looks. We keep statistics of the attacks we know about, both in Norway and in the Nordic countries. However, we do now know how large a portion of our customers actually report fraud attempts, or completed incidents of fraud (which have resulted in losses for private individuals and/or businesses).

We work from what we see, but seek a clearer profile of the reality. In Norway in 2018, we have mostly seen investment fraud, romance scams, and on third place, invoice fraud. This is based on the statistics we have registered without regard to any unrecorded statistics. We have seen twice as many investment fraud incidents as romance scams in 2018, and about twice as many romance scams as incidents of invoice fraud.

CEO fraud, like all types of fraud, carries with it a sense of shame. We know about many attempts and we know about businesses that have lost money, but we also hear about businesses that report neither attempts nor completed incidents of CEO fraud. When a business loses money due to CEO fraud, it says a lot about the business's internal routines, reporting routines and payment tasks, and one may get the impression that employees do not know how to behave in such situations. This gives a presumption that the business does not wish to share its experiences with fraud because they are unsatisfied with how it was handled internally.

8. Unrecorded statistics

If everyone, both private individuals and businesses, set aside this sense of failure, we would be able to learn from each other's mistakes together and form a stronger front against scammers.

Experiences from Coop

Coop experiences, like many other larger agents in retail, that its brand is abused in phishing campaigns. The phishing campaigns come in waves and the vast majority are aimed at customers – regardless of their customer relationship with Coop. The campaigns are conducted via e-mail and SMS, and the goal is always to collect personal information or trick the recipient into conducting bank transactions to the fraud agent's benefit. The way the campaigns are designed consciously exploits the recipient's trust in Coop in order to achieve this goal.

Coop has actively worked to build up expertise among its own employees to handle this type of fraud attempt. A centrally-established security group in Coop has been set up to handle security incidents, as well as to raise awareness of computer security among its employees. This group cooperates with customer support centres to handle referrals from shops and customers. The referrals are logged in their own case system by the customer centres, and the security department follows them up. This makes the security department able to quickly identify, and differentiate between, the various fraud campaigns. Routines for attempting to take down fraudulent pages are established, as well as for reporting fraud campaigns that abuse Coop's brand name to the police. Routines for reporting back to customer centres and information to customers regarding ongoing fraud campaigns help limit the extent of the damage, while helping to engage those affected by fraud attempts to continue to report new fraud attempts.

Coop is working to establish more cooperation with other businesses encountering this issue, so that these can more effectively coordinate and act against the fraud agents. The impression is that fraud agents have for a long time been able to operate without a great risk of being caught. Cooperation and expertise sharing between the police and cooperating businesses may change this. Cybercrime isn't limited by national borders, and individual businesses often have a limited ability to identify and pursue fraud agents based in a foreign country. The police's response to reports and their ability to act against fraud agents will become highly important for their engagement with the businesses.

Experiences from Telenor

The Norwegian Intelligence Service's threat assessment FOKUS 2018 highlights foreign nations' use of digital channels as the biggest intelligence threat to Norway. State agents, contractors, organised criminals and politically motivated hacktivists run operations against, or in, our infrastructure and our services. Telenor Norge sees these threat agents becoming ever more advanced and persistent. This applies to both criminal communities and state agents. Advanced agents with financial gains as their intention have become more focused and have gained access to more advanced tools. Telenor Norge also sees that threat agents wish to exploit agents on the inside to achieve their goals.

Telenor Norge is an attractive target for advanced agents due to our socially critical infrastructure, our national symbolic value, and our customers from all industries and sectors.

9. Preventive activities/measures

Good preventive activities and measures contribute to reduced vulnerability and reduced consequences. We have therefore collected good advice and guidelines from various parties.

9. Preventive activities/measures

9.1 Digital security culture

Society's self-defence capabilities depend on both public and private businesses maintaining sufficient digital security expertise. Society expects individual businesses to be able to protect themselves, and to help protect others. This means that everyone must know what should be done, and what should not be done. This is easier said than done, as complexity is rising and ever more areas are digitised. The government facilitates long-term build-up of digital security expertise through a national competency strategy for ICT security. In this manner, a foundation will be laid for the growing generation to bring ICT security expertise into their continued education and later on in their working life.

In this study, phishing and social engineering are the most common information security incidents, and the number of these has more than doubled since 2016. When asking about the reasons these incidents occur, the four most common reasons received are chance and bad luck, human error, lack of security awareness among employees and a failure to follow existing processes. NorSIS advises that thorough instruction and training in digital security will both prevent such incidents and ensure that the consequences are lower when incidents do occur.

- Ensure that employees are given training in the business's security routines with a special emphasis on resisting social engineering and fraud.
- Strengthen employees' security knowledge, such as through the aid of training packs
- from NorSIS and internal training. National Security Month is held in October each year and can be used to give employees some insight into the threats and how they, by following security procedures, can minimise the risk of undesirable incidents.
- Chart the business's digital security culture to uncover if there is a need to implement measures.
- Financial department staff should be trained on CEO fraud, and businesses should implement routines for larger transfers, making it harder for CEO fraudsters to succeed.

9.2 Use NSM's Basic Principles

Maintain a secure ICT infrastructure

For the business's employees to work effectively and trust work tools, the information systems must be trustworthy. This is done by establishing robust systems and services, configuring and adapting hardware and software and verifying that configurations are correct.

Businesses with few staff may benefit from seeing recommendations at nettvett.no for securing computers, mobile phones and tablets.

Maintain control of ICT infrastructure

Business ICT infrastructures will be exposed to external and internal influences. This may include harmful software that can damage machines and networks, or planned changes resulting from a new accounting system being implemented. Regardless, there will be a number of considerations the business must make in order to ensure that the information systems maintain the desired robustness. In addition to the advice in basic principle 2.4 – "Maintain control of ICT infrastructure", the business should also implement measures to protect against malware, monitoring and analysis of the ICT system and for handling change. To determine if the correct security measures are in place, it will in many cases pay off to conduct tests and drills where you attempt to access resources and data that you should not have access to.

Maintain control of the business's data and services

Businesses must maintain control of their own data and services to ensure that the requirement for confidentiality, integrity and accessibility is preserved. This is done by keeping control of the flow of information in and out of the business's network, including within the network itself. Data and services must be protected both when they are located at the business itself, or with a service provider (see measure 3), and when data is transferred through various information channels. E-mail and web browsers should be particularly emphasised, as many of the threats (malware such as cryptoviruses, phishing attempts, CEO fraud, etc.) from the internet enter through these channels. See also NSM guidelines "Basic measures for securing e-email".

Control access to data and services

Access to the business's data and services must be controlled to keep them from being abused by unauthorised parties. This is done by maintaining control of accounts, controlling the use of administrative privileges, ensuring secure log-ins, such as by using two-factor authentication, and by establishing purposeful logging.

9.3 Security expert recommendations for service outsourcing

Outsourcing ICT services to professional parties may yield greater security as well as more stable and available services. Access to expertise and tools one does not possess oneself can be improved, costs can be made lower and more predictable, and a stronger emphasis can be placed on the business's core activities to a greater extent. At the same time, businesses must be conscious of the risks involved when outsourcing services. Equivalent or higher levels of service quality and ICT security should be the target when outsourcing services.

Outsourcing services places strong requirements on one's own business and requires different expertise than if the service is provided by one's own organisation. Before a strategic decision can be made on the use of service outsourcing, the business should assess whether it is "equipped" to handle each phase of the service outsourcing process. The business must also chart the laws, requirements and rules that apply, both nationally and internationally. For example, both the Security Act and the Personal Data Act stipulate provisions that give guidelines for outsourcing services. Some sectors also have regulations for what opportunities the business has to outsource services.

In order to maintain ICT security when outsourcing services, NSM recommends that the business is conscious of the need for:

- An overview and control of the entire lifespan
- Good purchaser expertise
- Good risk assessments in order to make the right decision
- Appropriate and good requirements for ICT services and to suppliers
- The right decision on the right level

In today's digitised society, the removal of ICT services will most often affect the entire or major parts of the business. If business-critical services are transferred to a third part, it may increase the risk of both intentional and unintentional incidents, such as the loss of services or loss/alterations to data.

The decision to outsource services should not be made exclusively by the business's ICT community. The choice of supplier model and ICT service outsourcing is a key strategic part of business management. The leader of the business should ensure a strongly-anchored process for all affected parties in the business. When a decision regarding service outsourcing is made, it should be based on risk assessments that describe the service outsourcing's effect on the entire, hereunder the ability to deliver, ICT portfolio, finances and need for expertise.

9. Preventive activities/measures

9.4 General data protection regulation (GDPR)

The Data Protection Agency's advice to businesses:

- Chart what personal information you handle, and ensure that the way in which it is handled is legal, such as by documenting purposes, and comply with deletion requirements.

- Establish internal control or management systems to maintain your duties and the rights of those registered (such as by giving information, insight, correcting and deleting information).

- Conduct risk assessments of the personal data you handle and make sure to sufficiently secure the information with both technical and organisational measures. Confidentiality, integrity, availability and robustness must be ensured here. For instance, one must protect oneself against unauthorised persons gaining access to see, alter and destroy data, and against incidents caused by accidents, human error and inadequate routines. Some basic measures include establishing access management, activating two factor authentication wherever possible, encrypting communication channels and individual files, keeping systems and software up to date, and implementing a culture of privacy and information security.

- If you outsource systems or utilise services where a provider handles data, the business will still be responsible for the personal information it handles. Among other things, this entails that one knows where data is physically stored, conduct a risk assessment of the supplier, establish a data handler agreement, and conduct security reviews of the provider.

- Establish routines for tasks such as re-establishing normal operations in the case of incidents, as well as a process for testing, analysing and assessing security measures.

- Establish routines for incident handling, meaning routines for discovering and handling incidents, determining whether personal information is involved in the incident and whether the Norwegian Data Protection Agency should be notified, as well as whether the people affected by the incident must be informed.

Read more about the new privacy regulations, internal control and discrepancy handling at datatilsynet.no.

9.5 Securing websites and e-mail

As the internet becomes an ever more critical part of social infrastructure, it becomes more and more important to ensure that information isn't falsified or doesn't end up in the wrong hands. Behind some cryptic acronyms like DNSSEC, SPF, DKIM and DMARC are some opportunities to secure safer communications online. DNSSEC (DNS Security Extensions) is a security mechanism inserted into the domain name system. With DNSSEC, answers are signed on a domain registry, making it possible to make sure they are coming from the correct source and have not been changed along the way.[3)]

Why is DNSSEC important?

In the modern day, the internet is a key platform for creating value. In 2017, online shops in Norway had a revenue of over twenty billion NOK (source: SSB). Five percent of all Norwegian domain names with a website have a shopping cart feature connected to the site, and for many businesses, the internet is their primary sales channel. The internet is also a primary channel for communication between public authorities and citizens and businesses, such as when reporting tax returns and payroll taxes, and for access to public services. In all these cases, it is essential that the users actually access the site they intended to access.

You can access a website in various ways: By clicking a link, from an app, from results in a se-

[3)] Read more at: https://www.norid.no/no/dns/dette-er-dnssec/

arch engine, or by typing in the URL in a web browser. In all these cases, you are looking up a domain name. The look-up initiates a search of an IP address, which is used to contact the machine that is operating the service the user wishes to access. Initially, the design of the domain name system did not ensure that the reply to a look-up came from the correct source. This means that it is possible for an attacker to falsify a reply and send a user to a different IP address than the one actually connected to the domain. For example, a user could be sent to a website that looks like the web shop she or he intended to access, but which in reality is a website located on a machine controlled by a fraudster.

DNSSEC (DNS Security Extensions) is a security mechanism that offers a solution to this problem. When a domain is secured with DNSSEC, all replies to a domain look-up will be cryptographically signed. This makes it possible to ensure that the reply comes from the correct source and that it has not been altered along the way.[4)]

Technologies for securing e-mail

SPF (Sender Policy Framework) allows you to tell the outside world which machines/systems are permitted to send e-mail from your domain. What this achieves is that the outside world can protect itself from false e-mails appearing to come from your domain. This way, you can help prevent your domain name from being associated with spam. In addition, you contribute to a "cleaner" internet", since others can use the information you publish to protect themselves.

Similarly, your business can use the SPF information published by others to check that an e-mail is coming from the reported sender. Control of SPF is set up at the recipient e-mail host for your domain, and you can use the information to either dismiss e-mail or mark it so that it can, for instance, be sent for a stricter virus inspection.

DKIM (DomainKeys Identified Mail) allows a sender to sign an e-mail cryptographically using public key technology, where the public key is published in the domain name system as DKIM information. The signature is typically done by the business's e-mail host and is therefore "invisible" to users.

The recipient's e-mail host can use the sender's public key to verify that the e-mail is coming from someone with control of the domain name that is being used, and that the contents of the e-mail have not been altered. You should consider implementing this for outgoing e-mail from your domain. As with SPF, you help the outside world avoid false e-mails that appear to have been sent from your domain. Your e-mail office can also be set up to check DKIM information on incoming e-mail, which may help your users detect falsified e-mails.

DMARC (Domain-based Message Authentication) builds on both SPF and DKIM and gives a recommendation on what the recipient's e-mail host should do if a received e-mail has failed one of these two checks. Like SPF and DKIM, DMARC information is published in the DNS linked to the domain name used to send e-mail. If you wish to use SPF, DKIM or DMARC for your domain, you must get in touch with those operating your e-mail host so that they can implement it.

STARTTLS is an expansion of the protocol for transferring e-mails between e-mail servers. It offers encrypted transfers of e-mails between e-mail servers provided both e-mail servers communicating have activated this. It requires no effort from the user sending the e-mail or requirements to the e-mail the client is using. TLS certificates are used for confidentiality protection. Authentication is only received if one uses certificates issued by a trusted third party.

4) Read more and see the animation: How DNS SEC works: https://www.norid.no/no/dns/

DNSSEC also contributes here

SPF, DKIM and DMARC are all based on the recipient looking up information linked to a domain name in DNS. It is however possible for scammers to falsify these replies and thus trick a recipient into receiving a fake e-mail.

When a domain is secured with DNSSEC, all replies to domain look-ups will be signed cryptographically. This makes it possible to ensure that the reply comes from the correct source and that it has not been altered along the way. Signing the domain name will therefore be useful even if the domain is only used for e-mails.

Signing the domain name is free, but the information must also be registered by Norid. The signing and contact with Norid will be handled by the business's domain reseller.

Preventive activities and measures help reduce the consequences of incidents.

10. Afterword

In this year's study, one of the most positive and important findings is that maintaining management systems and operating preventive security efforts is what gives businesses a better ability to detect incidents. Furthermore, it gives room to implement appropriate and consequence-limiting measures. This is valuable knowledge for a digital society that must continuously work together against a threat profile that is growing ever more advanced and comprehensive, and which affects us all regardless of industry.

At the same time, this year's study reveals that knowledge is important for preventive efforts. Knowledge all businesses, regardless of size, should have access to, independent of their geographical location. Many need help to turn knowledge into actual measures within their own businesses. We therefore still need arenas for sharing updated knowledge and experiences that together will contribute to a more robust digital society. We need updated and relevant guidelines, advice and capabilities for support from relevant authorities in handling cyber incidents.

Experiences and knowledge are also important for an improved understanding of risk. The more conscious our country's businesses are of the risk profile today and how they must manage their resources in relation to it, the better equipped we will be to handle the modern threat profile both now and in the future. These are important foundations for an increased understanding of security and for a collective digital security culture we must all participate in.

We therefore hope that this year's study can be used as an active tool in ongoing security efforts that involve both businesses and public authorities, while simultaneously promoting more cooperation in digital security.

Contributors to the study and report, aside from the committee

The Norwegian Business and Industry Security Council has multiple collaborative projects ongoing at all times, but which involve security in different ways. This grants us a wider understanding, as well as access to knowledge and resources that contribute to the high quality of our products. In connection with analyses related to the Unrecorded Statistics Study 2018, we therefore wish to thank the following contributors:

Birgitte Førsund – Senior Manager, KPMG
Ingunn Kolberg Vedeld– Associate, KPMG
Magdalena Agata Szwiec – Associate, KPMG
Espen Johansen – Operations & Security Manager, Visma Software International
Isabel Quiroga Arkvik – Fraud management, Nordea.
Hege Ossletten – Deputy chairperson, UNINETT Norid AS

Information security committee

Tønnes Ingebrigtsen, CEO and founder of mnemonic. (Committee leader)
Tønnes has been the leader of the IT and information security company mnemonic since the company was founded in spring 2000. He sits on the board of NTNU's Centre for Cyber and Information Security (CCIS) and is the committee leader in NSR's expert committee, the Information Security Committee. He has a master's in informatics from NTNU.

Johnny Mathisen, senior advisor, Telenor Group
Johnny has a master's degree in telematics from NTH in Trondheim and one in information security from the University College of Gjøvik. He has worked at Telenor for over 30 years, the last 25 of which have been in information security, and he has been a member of NSR's Information Security Committee since 2010.

Christophe Birkeland, administrative director at Symantec (Norway) AS
Before going over to the private sector in 2011, he held various management positions in the public sector (the Intelligence Service and the National Security Authority). Birkeland has a doctorate from NTNU in 1997, and also attended the Norwegian Defence University College in 2005.

Vidar Østmo, Security architect/CISO, Verdipapirsentralen ASA
Vidar is CISSP and GCIH- certified and has many years of experience in work involving information security in both Telecoms and Finance. He has experience from both technical and non-technical sides of security efforts.

Martha Eike, technical director at the Norwegian Data Protection Authority
Martha is an educated computer engineer with a background in software development in the private sector. She has worked at the Norwegian Data Protection Agency since 2012 and has experience with built-in privacy, DPIA, cloud services, the digitisation of the public sector, the training sector and Big Data. Martha coordinates exter-nal efforts in information security.

Peggy Heie, administrative director for NorSIS
Peggy is an educated civil economist with a specialisation in information leadership. She is also CISA and CRISC-certified by ISACA. Since 1998, Peggy has worked with various tasks in risk-management, business development, IT auditing, financial auditing and information security.

Bente Hoff, acting section director of the National Cyber-security Centre, National Security Authority
Bente has more than twenty years of experience in digitisation and cyber-security in both the private and the public sector. He is a civil engineer from NTH and has a master's degree in technology leadership.

John Arild A. Johansen, Chief Information Security Officer (CISO) and Data Protection Officer (DPO), Gjensidige Bank
John Arild has over 25 years of experience in the field from both the public and the private sector, has been the Chairperson and member of the board of the Norwegian Information Security Forum (www.isf.no), Norm for Information Security in the Health and Welfare Services (Normen.no) and currently works as the security director and data protection officer at Gjensidige Bank.

Ole Tom Seierstad,
National Security Officer,
Microsoft Norge
Ole Tom has worked at Microsoft since 1990 and has held several different roles. In the last couple of years, he has focused on security and issues surrounding this. His areas of responsibility include most Microsoft products and contact with various segments that use Microsoft software, whether they are consumers or larger organisations.

Anders R Hovdum,
technical director for public safety in the Directorate of Public Roads in the Norwegian Public Roads Administration.
Anders is responsible for following public safety in the Norwegian Public Roads Administration, including information security and readiness. Anders has had a long run in the security field, including the Ministry of Transport and Communications and the Norwegian Directorate for Civil Protection.

Soner Sevin,
CISO, COOP
Soner Sevin has had a long run in the information security field, and has served as a CISO in various public and private businesses. Over the years, he has worked on an operational, tactical and strategic level. His involvement and contributions to the security field have inspired many in the industry. Over the past five years, Soner has worked as the chief of security at the Coop conglomerate, where among other things, he has helped uncover various types of online fraud campaigns in addition to establishing an operative CSIRT unit at Coop.

Bjørn R. Watne,
CISO, Storebrand ASA
Watne has worked with information security since the turn of the millennium, and has served as the Chief Information Security Officer at the Storebrand conglomerate since 2014. He sits on the board of ISACA Norway – a special interest group for professionals in IT auditing and security, and is also involved in expert groups with The Norwegian Computer Society, The Norwegian Information Security Forum and the Cloud Security Alliance. For education, he is an engineer in Computer Science, and has an MBA from ESCP in Paris.

Rune Rudi,
Police superintendent, cybercrime section, Kripos
Rune works with cybercrime at Kripos and has a lot of experience as an investigator, but in recent years, he has worked on cyber-intelligence. He has an earlier background in the Norwegian Armed Forces and the private security industry.

Arne Røed Simonsen,
senior advisor in The Norwegian Business and Industry Security Council
(committee secretary)
Arne has been an employee of NSR since 2004 and has a background In both the Norwegian Armed Forces and the police. He belonged to the investigation section of Kripos prior to his employment at NSR.

www.nsr-org.no

Næringslivets sikkerhetsråd

Against crime - for business and society