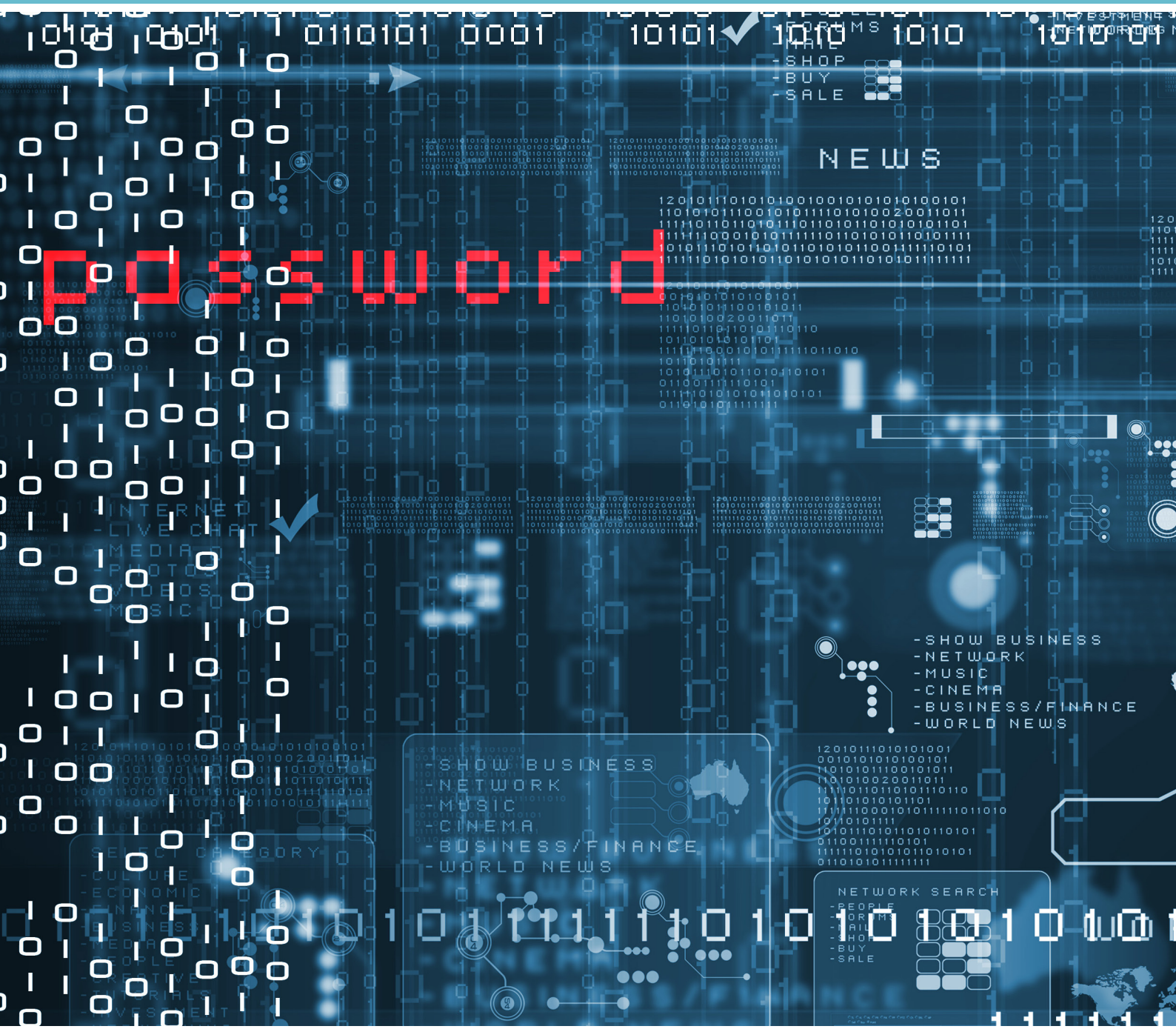
NORWEGIAN COMPUTER CRIME AND DATA BREACH SURVEY 2016

MØRKETALLUNDERSØKELSEN 2016

- Information security, privacy and cybercrime



NSR NÆRINGSLIVETS SIKKERHETSRÅD

The Norwegian Business an Industry Security Council

CONTENTS

Published:
September 2016

Printed by:
NHO Servicepartner

Layout and illustration:
The Norwegian Business and Industry Security Council

Photos:
Adobe Stock

Contact:
E-mail: nsr@nsr-org.no

Address:
Middelthuns gate 27, Majorstuen

1 INTRODUCTION

Key message

More than one quarter of Norwegian businesses - 412 out of 1500, or 27% - have experienced undesirable security incidents in the past year. The businesses report that this leads to a loss of productivity in 4 out of 10 cases (in the form of lost work hours), but only 2 out of 10 report that there have been costs incurred by these incidents. This indicates that businesses lack a full view of the costs incurred by such security incidents, or that they are underestimating the costs. Only 9% of businesses exposed to attacks bring the matter to the police. This implies that considerable statistics remain unrecorded, and that the criminal enterprises carrying out these attacks against Norwegian businesses are effectively immune from prosecution.

Source of data

For the 2016 Unrecorded Statistics Study, the 10th such study carried out by NSR, Opinion AS interviewed a total of 1500 businesses by phone during a period ranging from May 18th to June 9th, 2016. Opinion contacted a random set of businesses with five or more employees collected from the Norwegian Company Register, which meant that our respondents reflected the overall industrial structure in Norway to a greater extent than before. There was an emphasis on smaller businesses, and the proportion of larger businesses was considerably lower than in previous studies. New collection methodologies renders it more difficult to compare historical data, and as such, this year's findings will not be compared with prior studies. This year's study draws inspiration from a study performed in Great Britain[1] , and the emphasis is on incident detection and handling, using the worst case as a starting point.

1 http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

The information security committee consisted of:

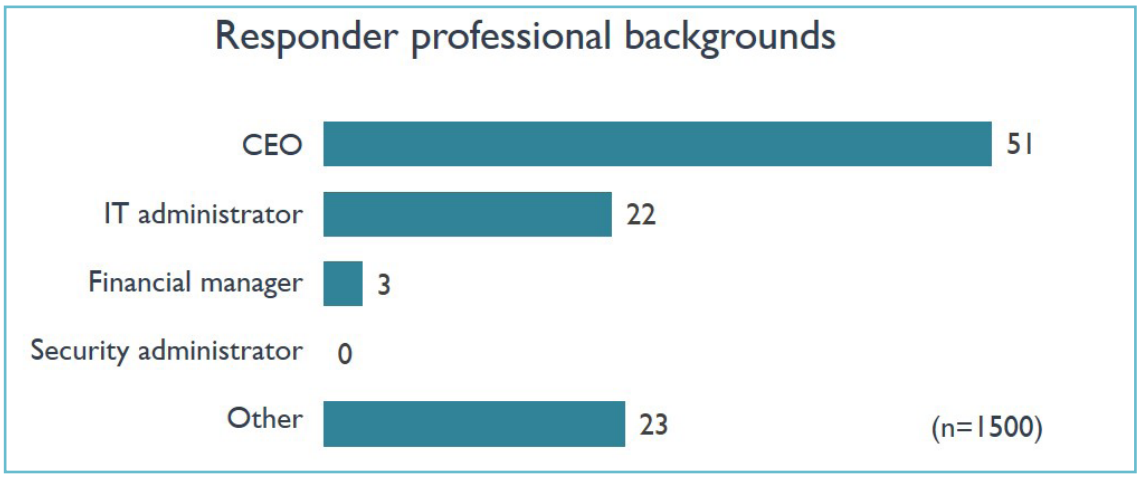
- Tønnes Ingebrigtsen (mnemonic, CEO)
- Janne Hagen (Norwegian Water Resources and Energy Directorate)
- Vidar Østmo (Verdipapirsentralen ASA)
- Johnny Mathisen (Telenor)
- Ole Tom Seierstad (Microsoft)
- Christophe Birkeland (Blue Coat Norway)
- Eiliv Ofigsbø (National Criminal Investigation Service)
- Martha Eike (The Norwegian Data Protection Authority)
- Bente Hoff (National Security Authority)
- Roger Johnsen (The Norwegian Centre for Information Security)
- John Arild A. Johansen (Directorate of Health)
- Arne Røed Simonsen (NSR)

- Fredrik Walløe (mnemonic, contributor)

2 REGARDING THE STUDY

Who responded?

More than half of the respondents were general managers, while another 22% had backgrounds as system administrators. Note that in many smaller and medium-sized businesses, system administrators also serve as security administrators. The remaining 27% had other (various) backgrounds.



The businesses that replied to the study had an average of 39 employees. There are only 89 businesses with more than 100 employees among the 1500 in our data set.

The majority of the businesses belong to the following industries:

- Retail and vehicle repair 21%
- Education 18%
- Health and social services 18%

It is worth noting that only the introductory questions yielded 1500 respondents. For the remaining questions, where we asked about the worst incident, data is limited to the 412 respondents who have experienced undesirable incidents.

Organisation of IT operations

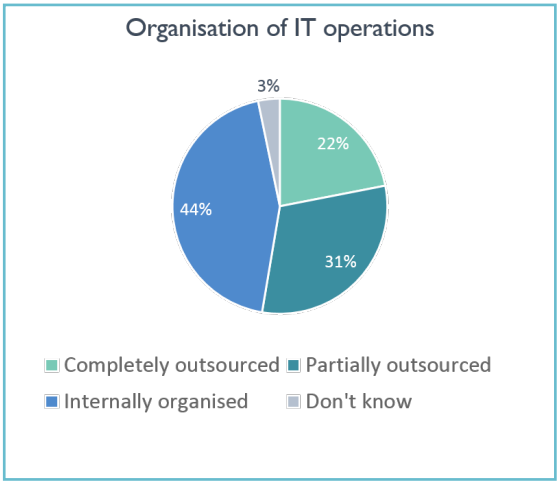
Out of the 1500 businesses that answered the question on the topic of how their IT operations are organised, 44% stated that they operate their own systems, 22% completely outsource their operations and 31% use a compromise between the two.

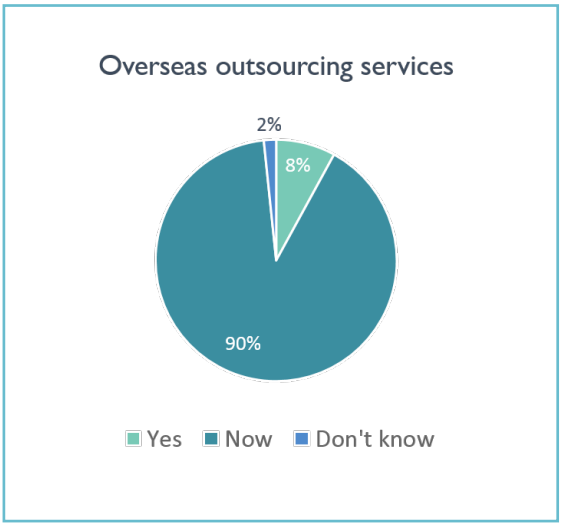
Out of the 790 companies that responded to the question of whether they utilise overseas outsourcing services, only 8% replied that they do.

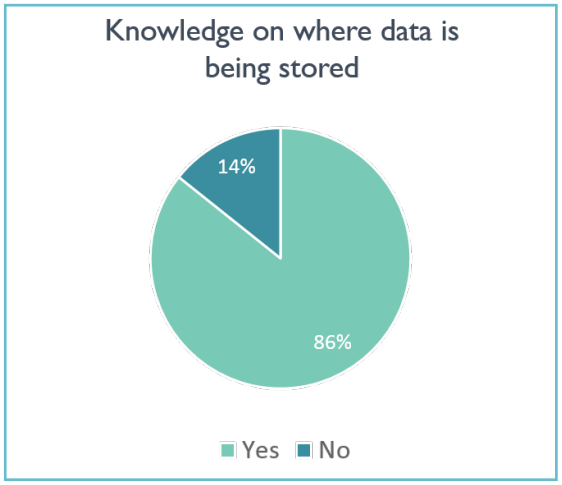
86% stated that they know where their data is stored, while 14% are uncertain.

Information security framework and/or control system

Out of 1500, 60% stated that they have an information security management system.


Organisation of IT operations
3%
22%
44%
31%
Completely outsourced
Partially outsourced
Internally organised
Don't know


Overseas outsourcing services
2%
8%
90%
Yes
Now
Don't know


Knowledge on where data is being stored
14%
86%
Yes
No


-INTERNET
-LIVE CHAT
-MEDIA
-PHOTOS
-VIDEOS
-PEOPLE
-FORUMS
-MAIL
-SHOP

3 RISK PROFILE

NSM Risk Profile

NSM NorCERT has the mission of detecting, notifying of, and handling incidents pertaining to attacks on critical infrastructure and key resources. Within the bounds of this mission, NSM NorCERT has observed a clear and steady rise in the number of targeted cyber attacks on Norwegian interests, both public and private. In addition to the increasing number of targeted attacks there is a steadily growing extent of various politically and criminally motivated actions in Norwegian cyberspace.

Severe targeted attacks

In 2015, NSM NorCERT noted a break in the trend, and the number of severe attacks detected against critical infrastructure and key resources was lower than in 2014. There is no easy explanation to this fact, but NSM NorCERT claims this is due to the increasingly advanced nature of some of the attacks. Based on the NSM NorCERT statistics, no definite conclusion can be drawn whether the actual number of targeted attacks and threat agents is increasing, or if existing agents have simply performed more attacks than before. The attacks remain constant, however, indicating that threat agents have the resources to sustain methodical activity in the long term.

One commonality in all of the successful attacks is that the primary vector in targeted attacks was that e-mail sent to users at the targeted organisation. The e-mail contained a malicious attachment or a link to a website containing 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 about the recipient of the e-mail is collected from information available to the attacker, whether it stems from freely available sources or compromised data.

Unfortunately, NSM NorCERT has also observed that attacks using older vulnerabilities remain successful. It is the exception that "unknown vulnerabilities", so-called 0-day vulnerabilities, are used. Over the past year, NSM NorCERT has been involved with several cases in which obsolete web server installations were compromised at smaller companies with limited IT resources, The compromised servers were then used as middlemen in new attacks on other targets, both domestic and abroad.

Hacktivism in Norway

Hacktivism is an activity primarily using computers and networks in order to promote a point of view or a political agenda. Social media such as Twitter are often used to drive a campaign where boycotts of, or attacks on, one or more businesses are encouraged. The employed method of attack and its consequences vary greatly.

DDoS is frequently used around the world, as its consequences are highly visible and gain media recognition of the "hacker brought down service X"-variety. DDoS is also cheap and easy to perform.

Another method of attack is to alter the contents of the target's website. It has also become increasingly common to publish sensitive materials online, which can again harm the company's reputation.

Although hacktivism remains a small scale problem in Norway, NSM NorCERT has observed a growing tendency the past few years. In 2015 and 2016, Anonymous ran a campaign against whaling, putting Norway, Iceland and Japan on their hit list. Using hashtags like #OPSEAWORLD, #OPKILLINGBAY and #OPWHALES on Twitter, they encouraged a boycott of Norway. The campaign peaked in early 2016 when several Norwegian websites were partially taken down. The attacks forced hosting services to block foreign traffic in order to keep the sites operational.

It can be difficult to determine whether a DDoS attack is related to hacktivism, extortion or a targeted attack, as it may not be easy to connect a DDoS attack to any specific hacktivist campaign. NSM NorCERT has observed 13 DDoS attacks so far in 2016, compared to 10 in 2015. 40% have ties to hacktivism.

NSM NorCERT hasn't observed any attacks performed by hacktivists that have had major consequences for Norwegian society, but services and websites have suffered extended downtime. This may changing, however. The theft and publication of sensitive information may be one of the larger risk factors that Norwegian businesses should take into account, along with DDoS attacks.

Going forward it will be important not to underestimate hacktivist groups and their ability to carry out attacks of scale.

Cybercrime in Norway

The past year has seen a sharp rise in ransomware spread by e-mail. NSM NorCERT and other sector CERTs have cooperated in several cases where waves of attacks were reported. Although various national and international security communities are working hard to take down the infrastructure used by the attackers, many - both individuals and businesses - are being affected. Warnings sent by NSM NorCERT in 2015 focused on the importance of maintaining strong secure backup routines. There are many concrete examples of ransomware attacks that have left it extremely difficult to recover the files once they were encrypted. Part of the reason the attacks have been successful in Norway is due to the contents of the e-mails, in which the attacker claims to be a part of Norway Post, or another Norwegian business. Being written in proper Norwegian also contributed to their efficacy at fooling people. NSM NorCERT has recommended against paying ransoms. This is because there is no guarantee that a working decryption key will be provided, and because it will encourage the attacker to continue to perform extortion campaigns.

NSM NorCERT has observed that new encryption viruses are constantly being put on the market, and so-called ransomware-as-a-service has made it very easy to send such e-mails. As long as people choose to pay, we can expect that this activity will continue to grow. NSM NorCERT receives daily reports from its partners regarding Norwegian websites that redirect to websites infested with malware (Exploit Kits). This has been a common vector for the distribution of not only ransomware, but other malware as well.

At the end of 2015, the groups DD4BC (DDoS for bitcoins) and Armada Collective were at the centre of attention. These groups specialised in extorting businesses with threats of major DDoS attacks if they failed to pay a sum of Bitcoins. The group had a relatively high success rate as the amounts they demanded were low enough that major companies decided it would be easier to just pay. After major international police action, several DD4BC members were arrested, to great effect. In the aftermath, NSM NorCERT observed a number of copycats attempting the same strategy, but in lieu of any actual DDoS capacity, they remained unsuccessful.

CEO Fraud

Phishing and fake invoices are nothing new, but one new trend in 2016 is called CEO fraud, also known as whaling. The essence of these attacks is a thorough investigation into the targeted company. Attackers map out financial executives and employees with transaction responsibilities. The attack often begins with an e-mail using a spoofed sender. This can be done by exploiting weaknesses in the way senders are displayed in e-mail clients, or through typosquatting (for example, @company.com versus @compan.com), where the attacker registers a domain that can be confused with the target's domain. The e-mails are often written in proper Norwegian, and the target is asked to make an urgent payment that must be kept secret. The e-mail correspondence often begins with an e-mail saying "Hi, are you at the office? Best regards, Boss". Afterwards, a fake invoice is sent with contents appropriate to the company's business. Social engineering of this type has proven to be highly effective, and NSM NorCERT has data on several Norwegian businesses sending relatively large amounts overseas. NSM NorCERT has a good partnership with FinansCERT and the banks, who summarily blacklist bank accounts and initiate further investigation. NSM NorCERT sent several warnings in collaboration with The Norwegian HealthCERT, whereby we wished to direct more attention to these e-mails. During the period from June to August, 2016, NSM NorCERT was notified of 45 businesses that had suffered CEO fraud. Several of these appear to have suffered attacks from multiple different agents. Based on the infrastructure observed in these attacks, the number of companies that notify NorCERT regarding these incidents is minimal, and significant statistics have therefore gone unrecorded.

In 2016, the trend has continued through other types of generic fraud making use of known brand names such as Netflix, Amazon and PayPal. "Microsoft Call Centre Fraud", where an attacker calls the target and tells them the computer is infected, remains a problem. Some cases have been observed where scammers claim to work for the National Security Authority. The media wrote about this a lot in 2016, which contributed to heightened and essential awareness.

Mnemonic threat assessment

Introduction

mnemonic's customers are made up of all types of businesses - in both public and private sectors. mnemonic's security monitoring services cover several hundreds of thousands of employees, most of which are located in Norway. Since their threat assessment for the Unrecorded Statistics Study 2014, mnemonic has warned their customers of over 35,000 security incidents. A total of 9 out of 10 have been compromised by malicious code.

The IT and information security challenges faced by Norwegian interests have never been bigger. mnemonic believes it is essential that the security industry confronts its unnecessary secrecy. The grading of threat and attack information must be balanced with the need to share. Their hypothesis is that if the Norwegian IT security community knew what the entire community as a whole knew, far more attacks could have been prevented. Major strides have been made in this area the past two years, but we still have a long way to go.

In their 2016 threat assessment, mnemonic wishes to focus on three primary threat agents; organised crime, activism and intelligence.

Organised crime

On the 18th of April, 2016, VG wrote about what is likely the biggest theft in Norwegian history. Under the guise of being the head of an international company, thieves won the confidence of employees at a Norwegian company. Within a few days, half a billion NOK had gone astray. The fraud was discovered, transactions were stopped and accounts were frozen. Even so, the culprits got away with approximately 100 million NOK. By comparison, the NOKAS robbers got away with about half as much. And yet not much can be heard about the surprise heist in the media. Some may claim that it was less serious because nobody was injured or killed. Unlike traditional heists, they didn't use any weapons, masks or getaway cars. This robbery happened online.

Between October 2013 to February 2016, federal agents in the United States registered 17,642 victims of so-called CEO fraud, with combined losses of 2,3 billion US dollars. Statistics in Norway are lacking, but mnemonic is aware of several Norwegian businesses having been affected to varying extents. The list of victims is growing, but the unrecorded statistics are considerable, and for various reasons, many hesitate to report the incidents.

The most significant development observed by mnemonic the past few years is the use of extortion. Such attacks have hitherto been opportunistic; unsuspecting users opening contents in e-mails from unknown senders - such as collection notices from Norway Post, or they browse websites that distribute malicious code. Many have been forced to pay a ransom to unlock encrypted data they cannot afford to lose.

Meanwhile, mnemonic is more worried about data breaches where the victims aren't selected at random. It is likely only a matter of time until we witness targeted attacks holding information assets of critical operations hostage. It gets even worse when businesses, for various reasons, cannot afford to withhold payment. In the USA, hospitals have been an example of companies giving in to this type of extortion. The criminal networks developing and proliferating malware get all the advantages, while Norwegian businesses in both the public and private sectors, as well as individuals, defend themselves with a blindfold and a hand tied behind their back.

Unfortunately, there are no simple solutions to the security challenges brought by Norway's digitalisation. What we do know, however, is that both consumers and authorities have much to gain by setting security standards on the solutions they choose to use. Furthermore, it is about time to bury the taboo around getting "hacked". A heightened awareness of what the cybercriminals of today are capable of may in and of itself be preventative. If more companies could have stepped forward like Telenor, Ulstein Group and the Norwegian State Educational Loan Fund have, other breaches may have been avoided.

The authorities have started taking on the challenges, the Lysne Committee's report, the findings of the Office of the Auditor General of Norway from recent years, advice from the National Security Authority and the Justice Department's (JD) "Cyber Crime Strategy" contains all the concrete measures needed to improve security, defeat cybercrime and strengthen privacy. Time will tell if these measures can be implemented.

Hacktivism

Over the past decade, we have gotten to know a new variety of political activism. Hacktivism, a portmanteau of "hacking" and "activism", describes the exploitation of IT systems to influence public opinion, as well as to spread ideological and political propaganda.

Norwegian hacktivist communities appear fragmented. Their membership numbers are estimated to be low, and the leadership vacuum makes it hard to coordinate with allies.

However, such communities can prove to be a moderate threat. In the summer of 2014, a teenager performed denial of service attacks of a greater scale against several of the largest businesses in Norway, and in 2016, both the Green Party (MDG) and the Socialist Left Party (SV) suffered breaches that among other things led membership lists to be manipulated and exposed. Although the attacks were performed by individuals, they contain an important message; the knowledge and resources needed to perform attacks is steadily growing more accessible, and the tools are getting easier to use. This development will likely lower the barrier to participate, strengthening their recruitment opportunities. In conjuncture with the lack of a leadership structure in hacktivist communities, this provides some cause for concern. The average hacktivist is a young man, who will most likely be influenced by his more experienced "colleagues". Thus it is possible that groups with more resources and different motives could exploit hacktivists to achieve their goals.

Intelligence

Intelligence can be defined in several different ways, but can roughly be described as activities, processes and products that reduce uncertainty and contribute to creating operational or competitive advantages.

Technological developments in society, particularly the use of the internet, continue to make us more vulnerable, and the threat to Norwegian interests varies among businesses. The intelligence operations of foreign states will also be different depending on what they wish to achieve.

The Norwegian Intelligence Service's annual unclassified evaluation of relevant security challenges - FOKUS 2016 - names both Russia and China as foreign states that have performed "persistent activities targeting Norwegian authorities and businesses". It is worth noting that Norway is one of few western countries willing to point out the intelligence activities of specific foreign states in official and unclassified reports.

The Intelligence Service divides threats in the digital space into three categories: intelligence, sabotage and influencing, which mnemonic also finds to be suitable. The commonality between these categories is the threat agent's need to avoid identification. In most cases, the intelligence services of foreign states will benefit from not being held responsible for attacks or breaches. They will in many cases also go to great lengths to deny their involvement, or sow doubt regarding the causes of the incident. The resources at the command of such services make it highly challenging to protect oneself, even for mature organisations with solid defence mechanisms and a security focus.

Espionage

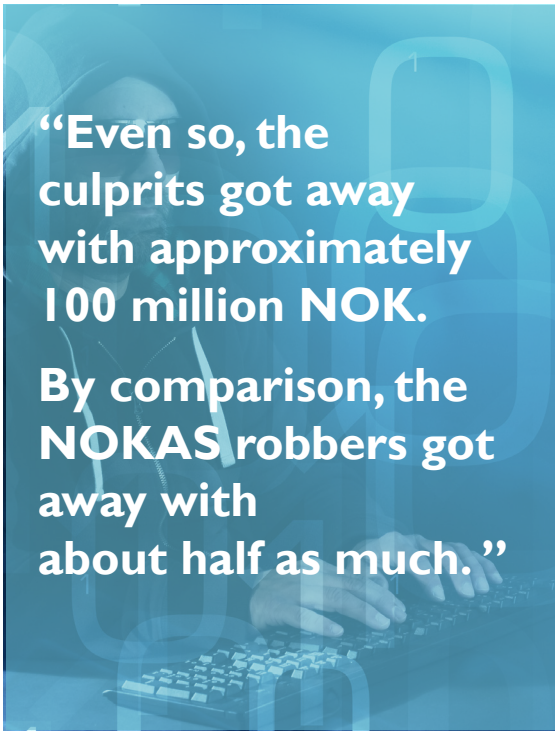
Over the course of more recent years, mnemonic has investigated several serious incidents where threat agents have used vulnerabilities at third party suppliers as a major step in attacks on their ultimate goal. As the use of cloud storage and cloud services proliferates, resource-heavy agents will have less of a need to directly break into the business in question. Outsourcing services can bring many benefits, including security benefits, but these must be evaluated alongside the need for security.

Sabotage

Sabotage as a direct, intentional result of a data breach first gained recognition when the Stuxnet worm was discovered in 2010. The attack on the Iranian nuclear programme reopened the debate on vulnerabilities in critical infrastructure, and many expected that we would see more such attacks. With the exception of an attack on a German industrial plant in 2014, it could seem like the doomsday prophecies have yet to come to fruition. During Christmas in 2015, this changed. A coordinated attack on the power grid in the Ivano-Frankivsk region of Ukraine caused hundreds of thousands of homes to lose power. Publicly-available analyses show that the attacker, having locked operators out of the system, turned off fuses, causing nearly 30 substations to go off the grid. They also struck two main substations and sabotaged emergency power solutions, causing both power allocation and troubleshooting to take longer than estimated. The incident illustrates that even the central pillar of digitalised society, power access, is vulnerable to be sabotaged by resource-heavy agents. For Norwegian businesses, this development means that to a much greater extent than before, traditional readiness measures may not always be reliable, placing very high demands on redundancy and resistance.

Influencing

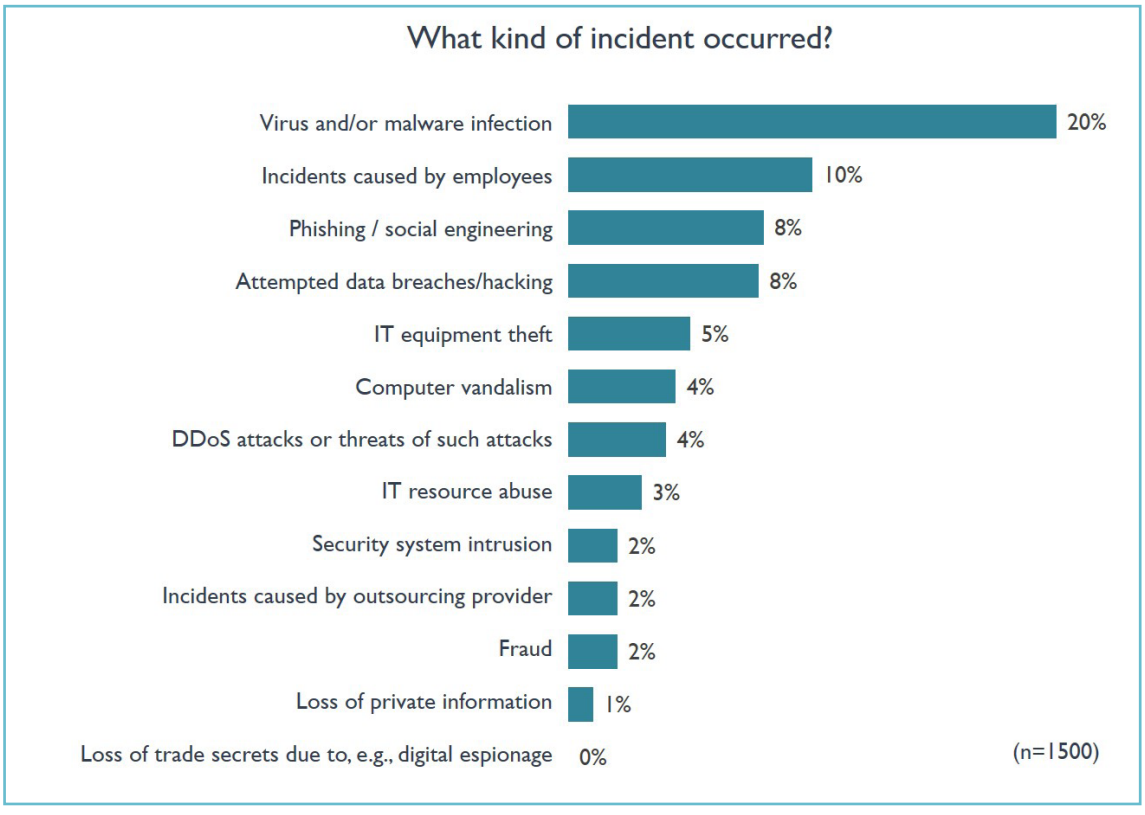
Influencing involves the misuse of news sources and social media with the intention of manipulating the information receiver's perception of reality. Unsurprisingly, few successful attacks of this variety ever become known. However, in 2016 there was a leak of sensitive information from the American Democratic Party. At the moment it is uncertain who is behind the attack, but many experts are pointing at Russia. If this is the case, the incident represents a major change, a foreign state may have performed a data breach with the intention of influencing the American presidential election. From a Norwegian perspective, one can imagine a great number of economic and political topics where multiple agents will likely attempt to exert their influence; the United Kingdom's decision to leave the EU, increased immigration as a result of trouble in the Middle East, and an increasingly cold security political climate due to Russia's superpower ambitions. On the 11th of September, 2017, Norway will hold its general elections. It is not unlikely that foreign states will be interested in influencing public opinion.



4 DATA BREACHES AND SECURITY INCIDENTS

Viruses and malware struck at least one out of five businesses in 2015. This wide category includes everything from malware that excessively consumes resources in order to annoy, to severe infestations that can cause extensive data loss, intellectual property theft and halted operations. Out of the 1500 business that answered the question regarding security incidents, 10% also reported incidents caused by their own employees. This is followed by social engineering and data breach attempts, both at 8%.

Only 4% of the 1500 businesses experienced distributed denial of service attacks (DDoS) There was no significant difference between the branches these companies belonged to, but small businesses were far less likely to suffer such attacks than large ones. In the 5-19 employee category, 3% reported a DDoS, the 20-99 employee category reported 4%, while in the major business category (100 employees or more), 12% have experienced a DDoS attack.



Incidents uncovered by Telenor

DDoS

Telenor has tools within their own core network to detect and filter DDoS attacks, as well as a service for business customers that allows them to actively filter attacks once discovered.

Over the past year, there have been an average of 750 attacks each month on Telenor's network and customers in Norway, Sweden and Denmark. This number has remained fairly even the past year. However, in the past half year, there have been two months that stood out with single attacks of record size. These occurred in April and June with 163Gbps and 277Gbps respectively. Solid infrastructure is needed to resist this kind of attack.

As for attacks on Telenor's business customers, we see that a typical attack lasts 30 minutes and reaches 6Gbps. Over the course of a month, these customers are exposed from 5 up to 20 attacks.

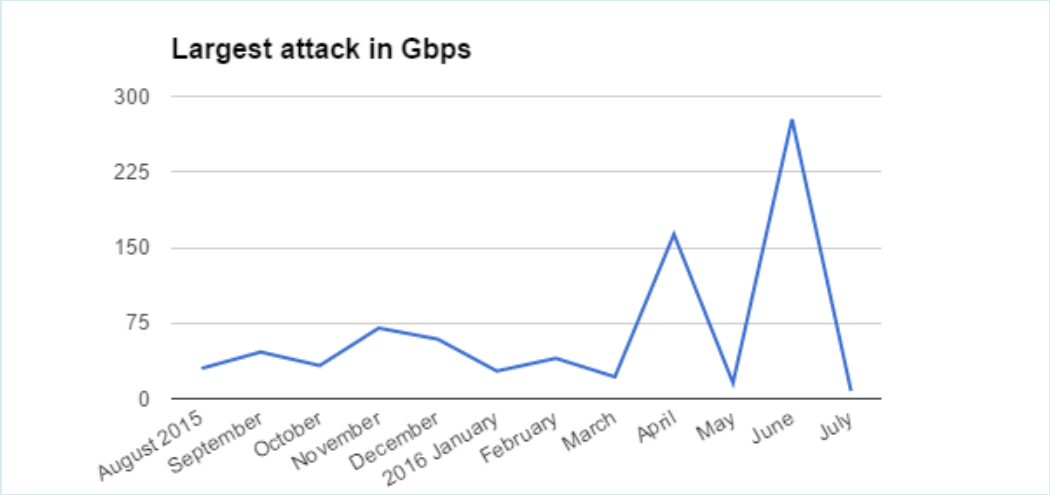
The attacks still mainly consist of reflected packets. The attacker sends a large volume of spoofed packets (packets with a fake sender address) to thousands of misconfigured servers on the internet. These servers send their replies to the victim. This means that attackers with relatively few packets, the attack can be amplified tens of times. Often, servers running NTP (Network Time Protocol), DNS (Domain Name System) and CHARGEN are the ones being exploited.

Over the past months, Telenor has also seen a rise in direct attacks using large volumes of SYN packets. SYN packets are used to establish an internet connection. These packets can't be amplified through the use of a reflection attack, so they are sent directly from compromised servers with a wide bandwidth or from botnets to overwhelm the server.

Most DDoS attacks are quickly filtered, defeating the attackers in a few minutes. Telenor has seen examples of more sophisticated attacks, where the attackers have clearly made preparations. In some cases it is also clear that attackers are paying attention to the response time of service they are attacking, and will change their methods if they see the attack is unsuccessful or prevented. Telenor has also seen attacks where one customer is attacked in multiple places at once, e.g. attacks on services from various data centres. This is not a random kind of attack, and is often performed by a competitor or an extortionist.

Security monitoring

Telenor Security Operation Centre (TSOC) has a network security monitoring service for customer networks. A sensor is placed in the customer's network to monitor traffic for unwanted traffic and infected devices. Over the past three years, Telenor has seen a reduction in the number of severe unwanted incidents suffered by their customers. Even so, more than 85% of TSOC customers have suffered a severe unwanted incident in the past two years.



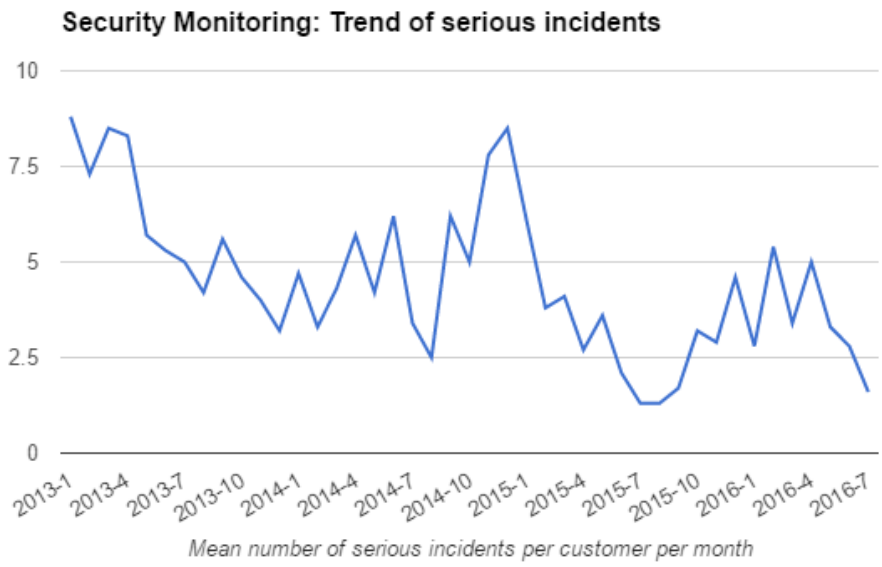
A few years ago, many devices were compromised through the use of "drive-by exploits", whereby devices are infected by malware merely by the user visiting a website. The vulnerabilities exploited in these attacks were often found in third-party browser plugins, e.g. Java, Silverlight and Flash. In response, many browsers began to block vulnerable plugins. Browsers started receiving automatic, and more frequent updates. This has reduced the number of easily-exploitable vulnerabilities on most company PCs.

Lately, the trend towards the use of social engineering has continued, with users being tricked into installing malware themselves, or to give away sensitive information, a phenomenon known as phishing. The entry point of these attacks is often e-mail attachments that pique the user's curiosity, frightening/threatening ads on the internet, or malware being covertly installed alongside otherwise familiar software installed by the user.

Before the summer of 2016, there was a major wave of ransomware attacks on Norwegian businesses, many of which suffered encrypted devices and file servers. The malware was often spread as an e-mail attachment. Telenor is of the impression that many companies now use better filtering for e-mail attachment, which has recently contributed to limiting infection. In the USA, there have also been instances of targeted ransomware attacks, particularly hospitals. Attackers breach the network, encrypt multiple critical servers simultaneously and demand large ransoms. Telenor hasn't seen much of this in Norway yet.

In 2016 there has also been a sharp increase in the amount of CEO fraud. This scam consists of sending falsified e-mails to employees who can transfer money overseas. The e-mails often appear to be sent by the company's CEO. This is a type of scam that may be difficult to stop through technical security measures. Here it is essential to maintain good routines with regard to payment, as well as employee training.

Several devices are also exposed to installations of programs at the very limits of what could be considered desirable and legal, so-called "potentially unwanted programs". These programs are often installed alongside other software installed by the user. These hidden programs can serve up ads, alter DNS settings, click ads in the background, upload browser history and device information, etc. Sometimes, pure malware can be installed as well. It is becoming more and more difficult to define what malware is and is not.



5 INCIDENTS AND UNRECORDED STATISTICS

The rest of the report is based on responses from 412 of the 1500 businesses. They have gone on to talk about the most severe security incident they experienced during that period and its consequences.

Viruses and malware are the cause of the worst incidents for Norwegian businesses. The study revealed that 132 businesses (32%) were affected by unspecified viruses or other malware. The severity of such malware varies. Ransomware was the worst incident for 58 businesses (14%), and several of these companies lost files, while 40 businesses (10%) listed spam as their most severe security incident.

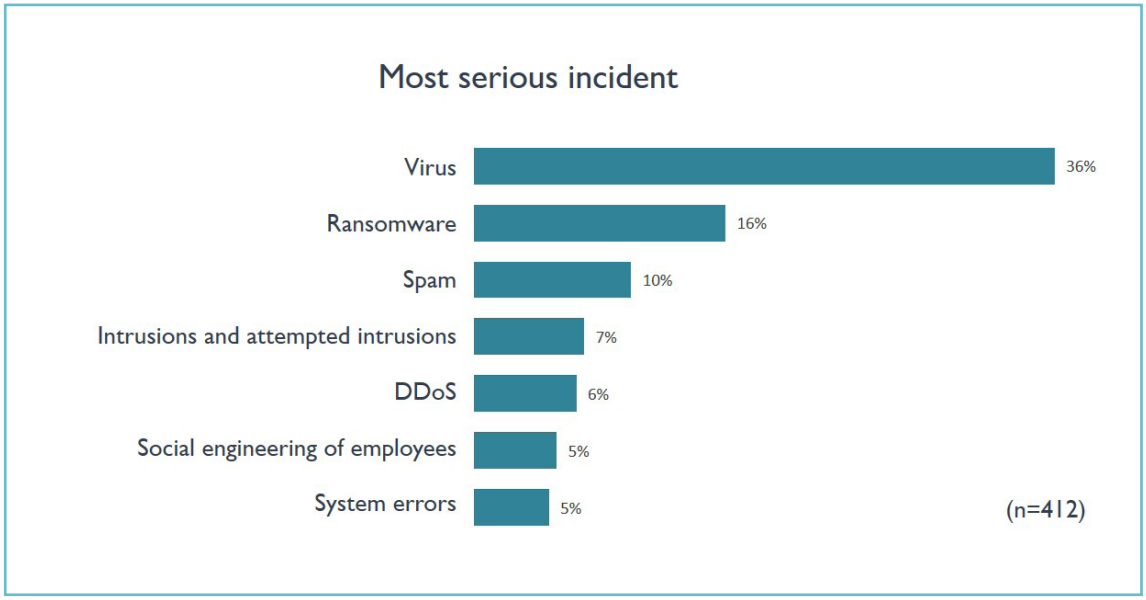
The most wide-ranging consequence was reported to be extra work in the form of work hours (41%), followed by lost or stolen data (16%). Only 12% report direct financial losses. 53 businesses (13%) have no idea of the consequences of the incident. What is clear, however, is that the incidents had some form of consequence for many of the responding businesses. Putting in work to handle an incident naturally also comprises a financial loss. Statements like *"This affected daily operations, requests that came in couldn't be answered, and this could lead to financial consequences", "Everything was destroyed and it took immense resources to search through other systems to put it back together again" and "The most serious aspect was that this was before the summer season. We couldn't see which customers had made a booking or who was coming to the hotel. Everything was deleted, and we couldn't book new guests either, since we had no overview of the customers that had already booked"* illustrate the difficulties experienced by various *businesses*.

The study shows that breaches into computer systems, system errors and viruses primarily led to lost work hours. With ransomware, however, lost data is clearly the biggest consequence, followed by work hours. The consequences are more complex when the business is the target of spam and social engineering. Here the consequences can be divided into data loss, direct financial consequences, work hours and unknown consequences.

Over 50 businesses didn't have any idea how much the incident cost them, and there is a tendency to underestimate these costs. A business that had files on its servers encrypted reported that the incident didn't cost them anything, despite the fact that it must have taken some time to recover the files. Another company reported that a ransomware attack had cost them 100 NOK, which also appears to be an unrealistic figure. Meanwhile, certain companies reported considerable expenses related to their worst security incident. For a company with 27 employees, phishing led to an expense of 600,000 NOK, while an educational business with 15 employees that partially outsourced its IT operations saw its partner suffer a data breach causing the theft of personal information and enormous expenses.

Inadequate secure backups seems to be a problem for many smaller businesses, leading to unavoidable losses when security incidents occur. One business lost two months of accounting information when a device stopped working, forcing them to re-enter this information, and another company lost files due to ransomware to an estimated cost of 1,000,000 NOK. Meanwhile, the fear of ransomware spreading led to some dramatic decisions. One business "shut the whole network down", preventing 1200 users from doing their work. Another temporarily shut down a file server, with consequences for five different municipalities. The study shows that businesses with good secure backups report considerably smaller consequences as a result of ransomware infections. The gap between a few lost work hours to a loss of several hundreds of thousands is enormous, and is an example of the importance of good security routines.

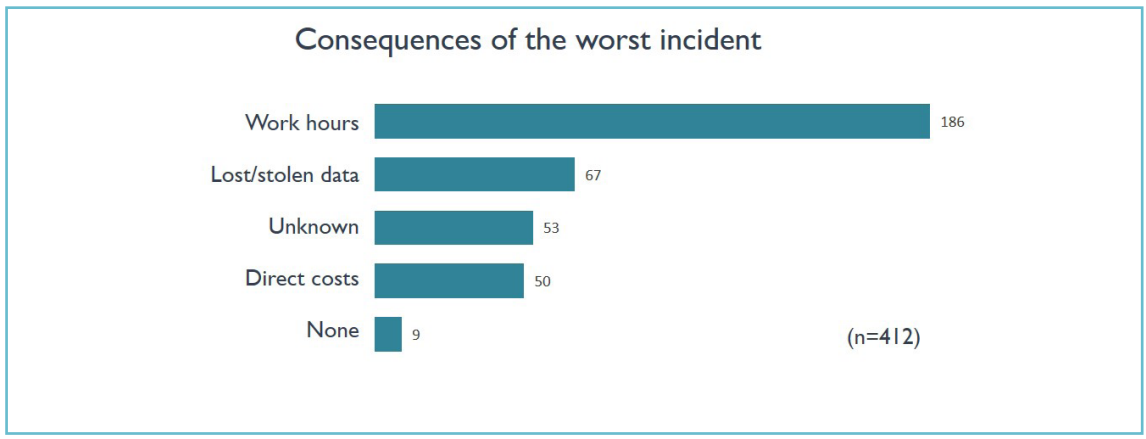
21 businesses, or 5%, discovered attempts at social engineering against their employees during 2015. The consequences of such attacks can be severe, as employees can be used to circumvent security routines, or can be fooled into sharing seemingly harmless information that can be used in future attacks. In its threat assessment, NSM warns of CEO fraud, which has affected several Norwegian businesses this year. In these attacks, the scammer impersonates an executive in a business and attempts to fool a financial department employee to pay an invoice or transfer money to an account, which is often overseas. The ability to perform these attacks varies, and Norwegian businesses must be prepared for everything from automatically-translated e-mails to fake invoices sent from the compromised e-mail account of an executive, as well as scammers with detailed knowledge about the company calling specific financial department employees. Thoroughly-considered routines regarding the payment of invoices and employee training can reduce the probability of such attacks being successful, and ensure that they can be discovered quickly.



Ransomware affects Norwegian companies

A company with 8 employees and a revenue of approximately six million NOK ended with costs estimated at 200,000 NOK after an e-mail containing ransomware led to a server being encrypted.

"Everything was destroyed and immense resources were needed to seek out the files in other systems". That is a considerable expense for a single security incident that could easily have been prevented with regular secure backups.



Fooled into transferring 500 million NOK

In January, the Norwegian subsidiary of a global conglomerate was contacted by a man claiming to be one of the top executives of the parent company. The man asked the subsidiary to transfer millions to several accounts in Asia. The Oslo office spent the following days transferring about 500 million NOK.

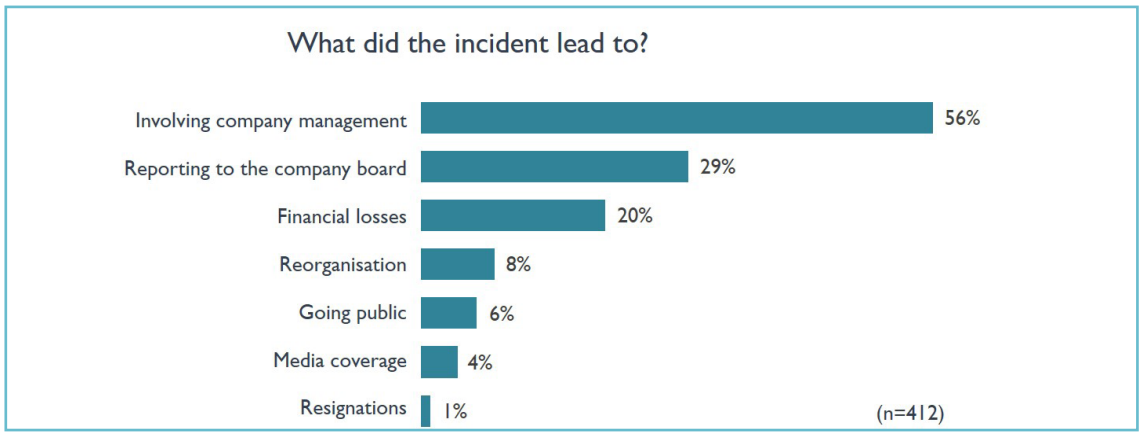
From there, the money travelled around and across various borders.

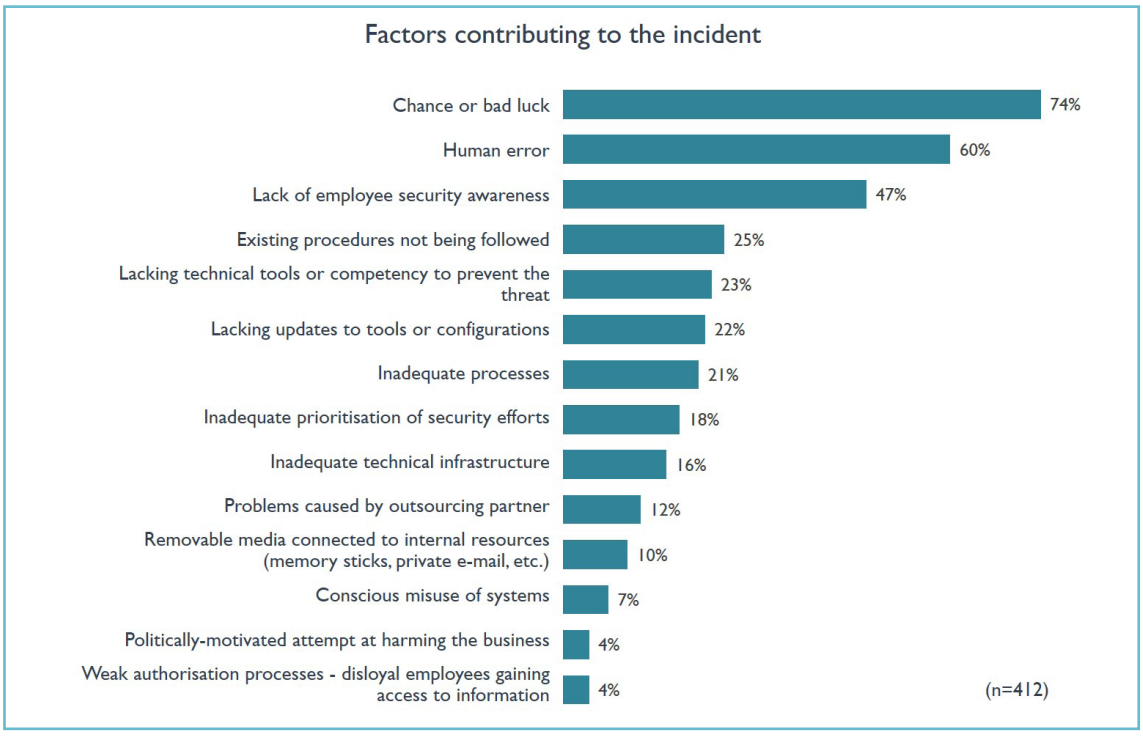
The attack was quickly discovered, and the police were able to stop most of the transfers, but about 100 million NOK remains missing.

What did the incident lead to?

The quality of the descriptions of the worst security incident at the 412 businesses who answered the question varies. The fact that they have answered this question does not mean the incident was catastrophic. It may just as well have been a nuisance. Over half of the businesses (56%) contacted upper management, while nearly a third (29%) chose to inform the board. It is therefore somewhat surprising that only 20% of the businesses reported that the incident led to financial losses. Note that this number is lower than the portion that reported extra work as a result of the incident (41%). There are financial losses which are hidden here; time spent handling an incident could otherwise have been spent on tasks that would generate revenue. The figure below shows a comparison of what the businesses reported as the results of the incident. Only 6% of the incidents were made public, and as a result, the unrecorded statistics are major.

The businesses report that the worst security incident occurred as a result of chance or bad luck in 74% of the 412 incidents, indicating that the businesses mostly do not perceive the attacks as being targeted at themselves. It is also reported that in 60% of the cases, employees made mistakes that contributed to the security incident, and a lack of security expertise was a factor in 47% of the cases. A lack of investment in, and prioritisation of, security efforts is behind a considerable amount of incidents: insufficient technical infrastructure (16%), processes (21%), a lack of sowftware updates or configurations (22%), a lack of technical mechanisms or competency (23%), breach of procedure (25%) and a lack of employee security awareness (47%).



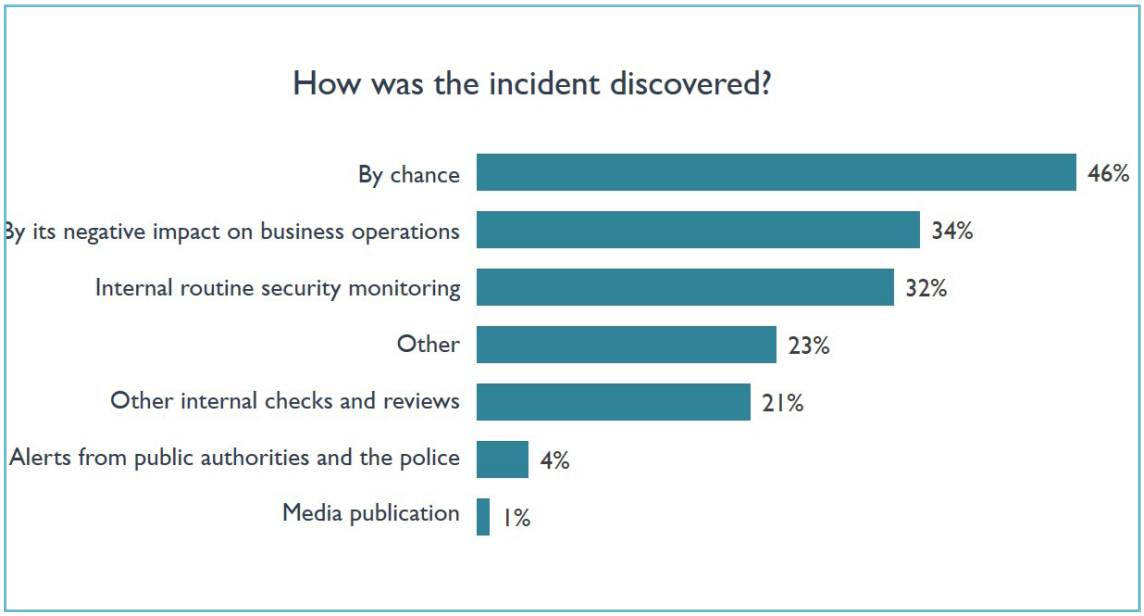


Ransomware

The hour is 08:56 when an alarm goes off at mnemonic's 24-hour Security Operations Centre (SOC). They discover traffic from a customer going to a domain known to distribute malware. The security analysts examine the incident, and conclude that one of the customer's clients has most likely been infected by the ransomware program TorrentLocker, which is primarily spread by spam, and has been encrypting files at businesses worldwide since 2014. At the end of 2015, several malicious e-mails claiming to be from Norway Post were observed. The receiver was notified of an attempted package delivery, and were told that they had to follow a link in the e-mail to receive a collection notice so that they could pick up the package at their nearest post office. The e-mail was written in Norwegian and used the Norway Post logo. If a user is tricked into opening the link, they reach a page that appears to be the ordinary Norway Post site, where they are asked to complete a captcha. Having done this, they will download a file bearing the standard Adobe PDF icon, but which actually is an executable file that will begin to encrypt files as soon as the victim attempts to open it. In this case, the receiver was expecting a package, and the e-mail thus appeared to be trustworthy, so she clicked onward. The traffic was not prevented by her firewall, and her antivirus didn't detect the malicious software that had entered the client. Ransomware can also encrypt networked areas, giving it a considerable potential to cause harm. Once the files have been encrypted, they are typically lost, unless there is a secure backup or the ransom is paid. The latter is not recommended, as paying the ransom contributes to the of financing criminal networks, motivating new attacks. It is therefore essential to discover these attacks quickly. In this case, the customer was notified within a few minutes, and was able to take the client offline and reinstall it before the infection could spread. Unfortunately, we also have cases where customers lose several weeks of work because no secure backups of the infected client's files existed.

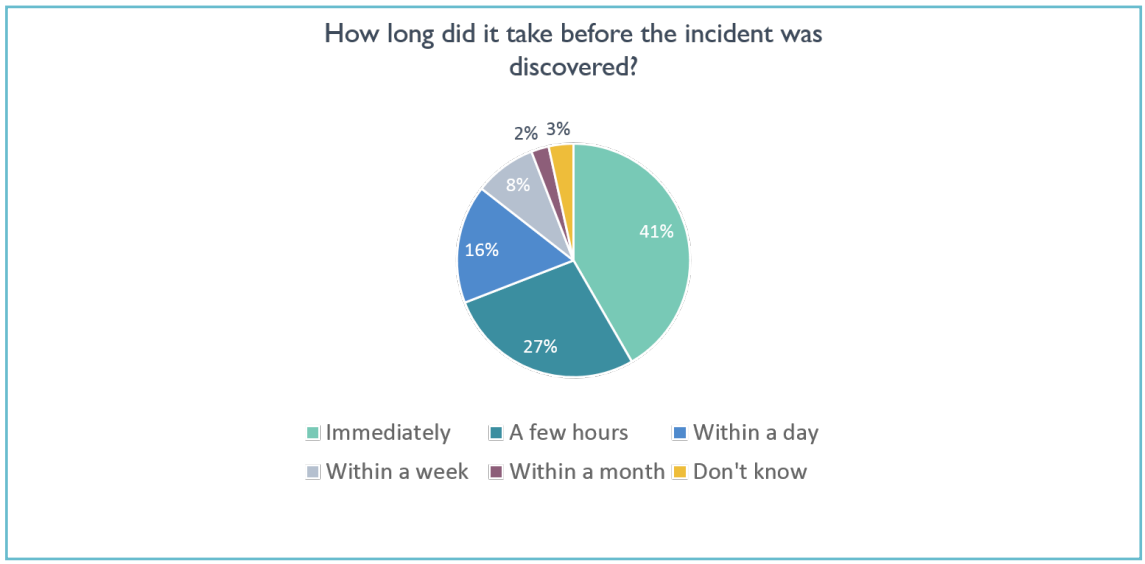
How was the incident discovered?

According to the responses, 46% discovered the incident by chance, 34% due to a negative impact on operations and 32% during routine security monitoring.



How long did it take before the incident was discovered?

The study shows that most incidents were discovered quickly. A total of 84% of the incidents were discovered the same day. None of the 412 businesses have responded that it took longer than 100 days, but 3% were uncertain of when the incident struck. At the first glance, it seems positive that 90% of the incidents were discovered within a week. But when 80% of incidents are discovered by chance or due to their direct impact on operations, this indicates that most businesses lack the necessary mechanisms to detect security incidents. Many businesses may well be compromised without being aware of it, as indicated by other international reports and studies.



Trade secrets gone astray:

A few days before the Easter holidays, an IT employee at the Ulstein Group discovered something unexpected; a Microsoft Exchange Server was about to be filled with files for the second time in a short period. The first time this happened, the IT department cleaned the server, but now the traffic was getting suspicious. They discovered several encrypted archives with unknown contents stored on the server, and the files were being sent out of the company. An alarm was raised and all systems were shut down.

Employees planning on working from their cabins were told there was an IT problem, consultants were called in and the National Security Authority (NSM) assisted in the investigation of what would turn out to be a severe security incident. They couldn't tell employees anything the first week, as it was still unclear if the attacker was an unfaithful servant or an external threat agent.

Before the extent of the attack became known, they also couldn't use any of the company's potentially compromised systems, including e-mail. Those involved in handling the incident kept in touch through SMS until they were certain the intruder had been banished from the system.

Ulstein believes the intruder had been inside the system for over a week, and had had access to several file servers. NSM was able to decrypt a compressed file that had not been sent. It contained files related to the company's innovation projects. About 500 gigabytes were stolen, and trade secrets may have gone astray.

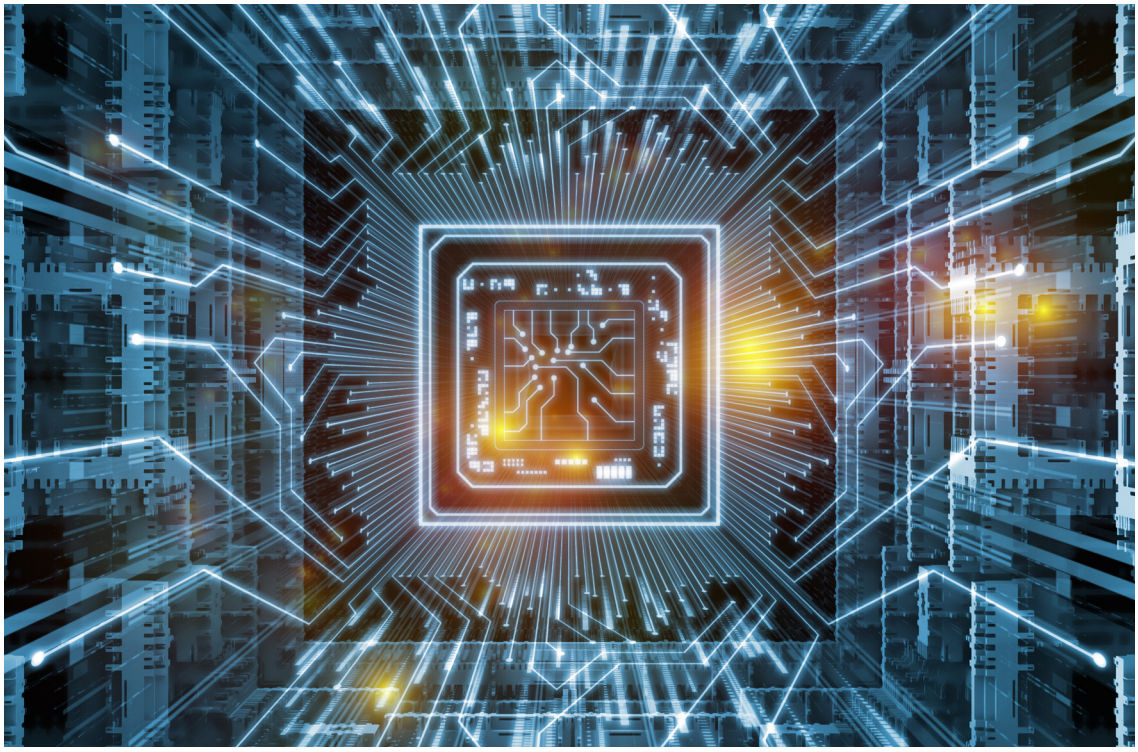
The investigation revealed Chinese characters, and NSM concluded that the computer power used and the complexity of the attack indicated that this had been an attack by an advanced threat agent.

Under guidance of the Norwegian Police Security Service (PST), who became involved when suspicions of an attack by a foreign state arose, Ulstein decided to report the incident and contact the media. The case was dropped after a year, but Ulstein was praised for its openness about the attack, and the group is glad they chose to step forward.

The attack was a wakeup call for the business and they have since taken several steps to make it harder for attackers to navigate the system without being discovered, so that similar attacks may be discovered sooner. They have mapped out their assets as well. But the business has had to acknowledge that technical solutions are only part of the solution. When each user is a possible entry point to the company's assets, the human element is central.

Since the incident, some of the biggest players in the maritime cluster at Sunnmøre have formed an IT security network that regularly meets to share experiences and knowledge.

6 UNRECORDED STATISTICS AND AFTERMATH



How was the incident reported?

The majority, 80%, reported the event to the administrator of the technical system in question. This was followed by their antivirus provider at 24%, ISP at 11% and the police at 9%. Very few made any report to their CERT or any other authority. The fact that the businesses primarily choose to handle incidents internally without notifying others may be related to the study focusing on smaller businesses.

Causes of the incident going unreported

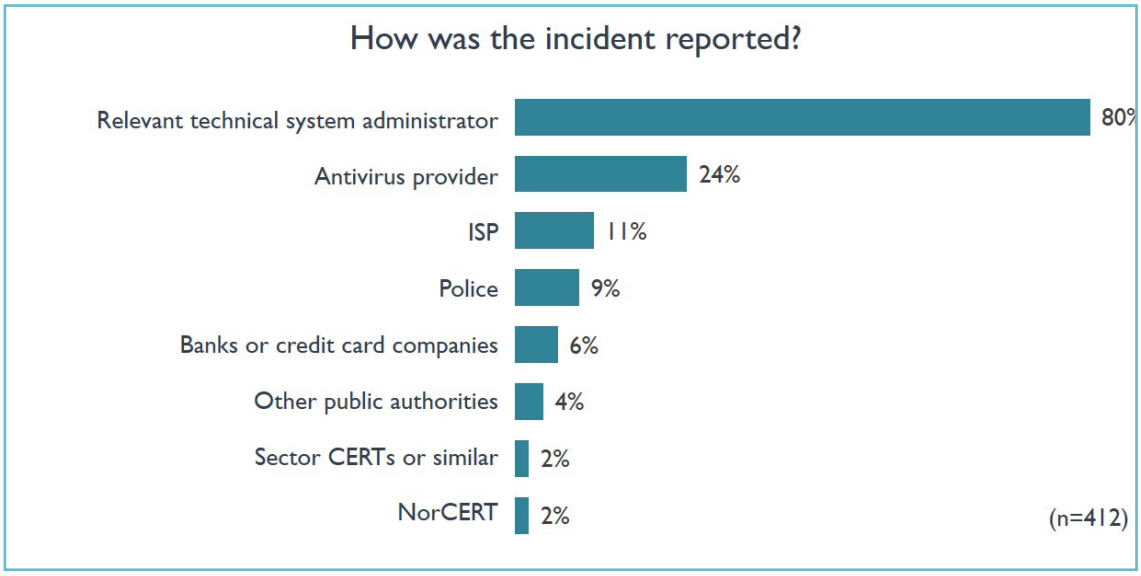
This year's questionnaire does not examine why so few businesses reported incidents, but in the Unrecorded Statistics Study 2014 it was discovered that the majority did not believe it would be possible to find the culprits, while others lacked faith in the competency of the police.

The police received 51 reports of data breaches in 2015, but because so few report attacks, it's natural to assume that the actual number of data breaches is higher. It is a challenge for the police to track criminals online. An attacker situated in France can use tools in China to attack a Norwegian business while making it look like the attack came from Australia. The complexity of the cases often lead to the case being dropped, but businesses under attack should still consider making a report. If the number of unrecorded incidents could be reduced, the police would receive a clearer picture of the current situation, which could lead to work on such crime being prioritised, increasing the expertise of the police.

22% responded to the question regarding the perpetrator of the most serious incident, and a minority of this group knew who was behind it. The answers ranged from their own employees to school students, customers, Russian servers, China, IT providers and people known to the police. The fact that so few were able to answer who the perpetrator was may indicate that these incidents only receive a limited investigation from the side of the business.

Changes to the organisation resulting from the incident

Nearly half of the businesses, 44%, performed policy or routine changes in the wake of the most serious incident, while 25% invested in security tools. Another 20% developed security processes and established a security community, and an equivalent number hired a service provider to handle security matters. 13% outsourced their security functions, while only 3% hired more people with security expertise. The low number may be due to the study's emphasis on smaller businesses.



Discrepancy reports for the Norwegian Data Protection Authority

Today, you are obligated by the Personal Data Act to notify the Data Protection Authority if confidential private information has been leaked. As of May, 2018, new privacy regulations (EU regulations) will take effect, bringing stricter rules for handling security breaches. [2] The regulations place requirements on when to notify, what the notification must contain and who is to be notified. In short, you have to report more quickly and more often than you do today.

2. Read more about the Norwegian Data Protection Authority's discrepancy reports and regulations here:

https://www.datatilsynet.no/Sikkerhet-internkontroll/Avviksmeldinger-til-Datatilsynet/

https://www.datatilsynet.no/forordning

7 RECOMMENDED SECURITY MEASURES

Secure backups

Ransomware is a growing problem, and many businesses reported that this type of malware led to a loss of data and work hours. Therefore, secure backups and swift recovery routines are growing ever more important.

- Implement regular secure backups of your business's data.
- Maintain routines for data recovery, and test them to ensure that they work.

Employee security awareness

Employee mistakes and a lack of competency contributed to the occurrence of security incidents in hundreds of the businesses interviewed in this study.

- Ensure that employees are familiar with the business's security routines and understand why the routines must be kept.
- Improve your employees' security awareness, possibly by using NorSIS training packages and internal training. National Security Month is held every October, 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.
- Financial department staff should be trained for social engineering, and businesses should implement routines for larger transfers, making it harder for CEO fraud to succeed.

Detection

Nearly 70% of the businesses discovered their worst security incident either by chance or because it negatively impacted operations. Norwegian businesses must improve their ability to detect and handle security incidents. The attack on the Ulstein Group also exemplifies the importance of detecting suspicious traffic within the system.

Improve your ability to detect attacks:

- Maintain monitoring systems to detect incidents (Intrusion Detection System)
- Ensure that antivirus systems are operational and that logs are being kept
- Maintain routines to follow up alerts and logs

Fundamental measures for smaller businesses

The study shows that Norwegian businesses still suffer financial losses from security incidents that could have been prevented with some fundamental measures. NSM's four anti-cyberattack measures[3] could stop a large number of the attacks suffered by smaller businesses:

- Upgrade your software and hardware
- Be quick to install security updates
- Do not give end users administrator access
- Block any unauthorised software from running

Systematic security efforts

For medium-sized and large businesses, it is important to systematise security efforts. Information security control systems - such as ISO 27001 or ISO 9001 - are useful to this end. DIFI's guidelines for information security, which are based on ISO 27001, is a good place to start. Here you can find free templates and other tools for direct application in your business. There are also industry-specific control systems, such as the Norms for the Health and Care Services sector.[4]

3. Read more at: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/system-teknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf

4. See: http://internkontroll.infosikkerhet.difi.no

http://normen.no/

Unrecorded statistics

Norwegian businesses must confront their unnecessary secrecy and strive to reduce the unrecorded statistics. Reporting security incidents to the police is the long game; reducing unrecorded statistics gives the police the documentation they need to prioritise improvements to their expertise, and resources, pertaining to this type of crime. Similarly, media coverage can contribute to heightened knowledge on the threats faced by Norwegian businesses: it can give other businesses time to implement measures to face new attack methods, such as CEO fraud.

- Report the incident to your local police office
- Considering contacting the media.

With support from

POLITIET
POLITIDIREKTORATET

BDO

Finans Norge

mnemonic
- securing your business

telenor

Norges vassdrags- og energidirektorat
NVE

NSM