Nordea

Cybersecurity

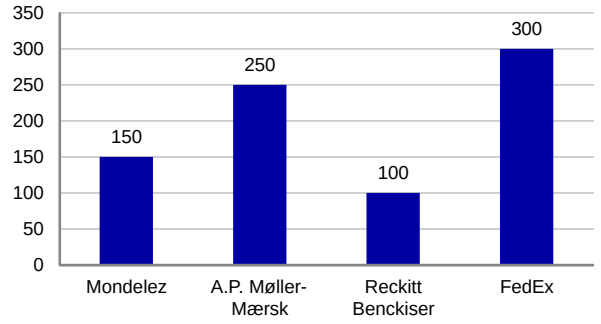
Nordea On Your Mind

Nordea Corporate & Investment Banking 03/2018

IMPORTANT INFORMATION AND DISCLOSURES AT THE END OF THIS REPORT

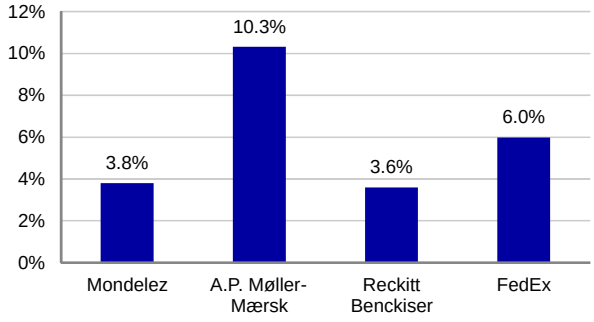
Cybersecurity in numbers

2017 CYBERATTACK COSTS, USDm



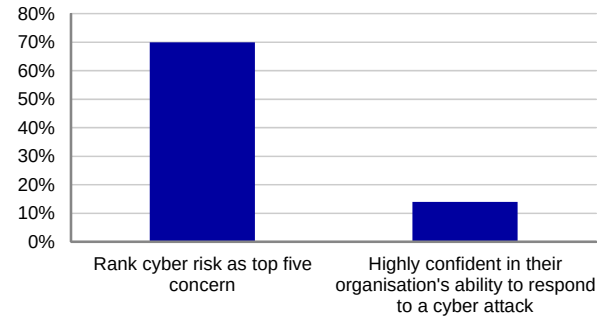
Source: Company data and Nordea Markets

2017 CYBERATTACK COSTS, % OF EBIT



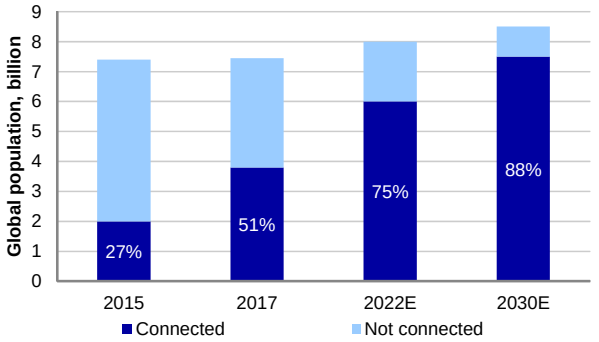
Source: Company data and Nordea Markets

SURVEY OF BOARD MEMBERS, 2017



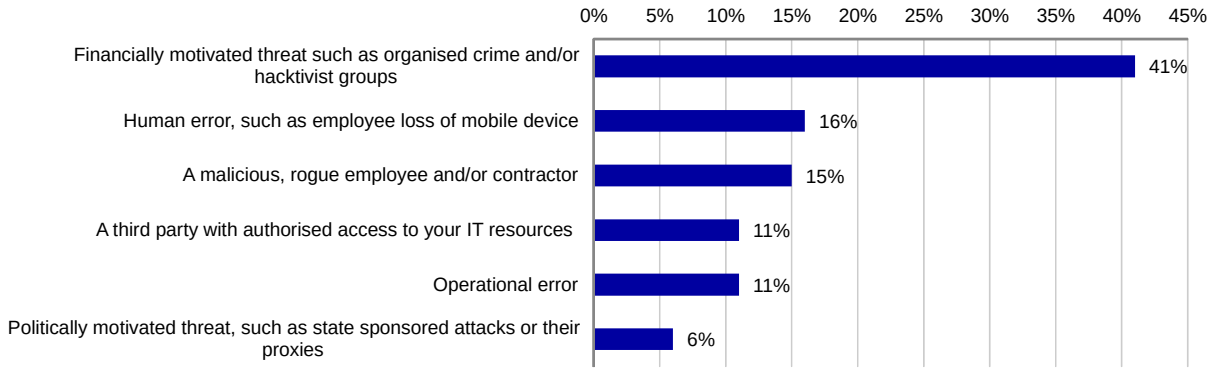
Source: Marsh and Microsoft Cyber perception survey

WORLD INTERNET USERS – GROWING ATTACK SURFACE



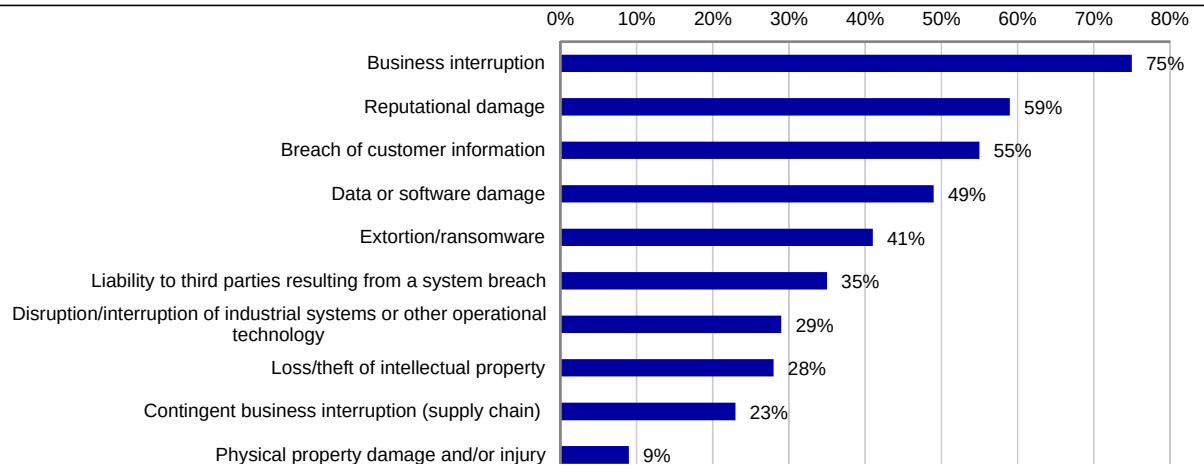
Source: Marsh and Microsoft Cyber perception survey

WHICH CYBERSECURITY THREAT IS THE BIGGEST CAUSE FOR CONCERN?



Source: Marsh and Microsoft Cyber perception survey

WHICH CYBER LOSS SCENARIO PRESENTS THE GREATEST POTENTIAL IMPACT?



Source: Marsh and Microsoft Cyber perception survey

Nordea

The Authors

Johan Trocmé

Johan is responsible for the Thematics unit in Nordea Research at Nordea Markets, having spent the five years prior to that developing thematic research in Nordea Corporate & Investment Banking. His involvement with large corporate customers comes after 20 years as a Nordic and European Capital Goods analyst in equity research at investment banks in Stockholm and London, including Goldman Sachs, UBS, Deutsche Bank and Alfred Berg.

Contact Johan:
johan.trocme@nordea.com

Ellen Benktander

Ellen is an analyst in Nordea Research's Thematics unit. She joined Nordea Markets after graduating with an MSc in Banking & Finance from Stockholm University and a BSc in Business Administration from the University of Gothenburg. She has previous work experience from JP Morgan Chase & Co, Swedbank, Skandia, Lindorff and the Swedish-American Chamber of Commerce in San Diego, US.

Contact Ellen:
ellen.benktander@nordea.com

Cybersecurity: A corporate priority

Cybercrime: Growing along with human connectivity

Humans are increasingly interacting and transacting online, with the share of internet users set to grow from 50% of the total global population last year up to 90% by 2030. Crime will continue to migrate online, targeting a potential 7.5 billion internet users. Perpetrators of cybercrime include organised crime (aiming to make money), hacktivists (who typically have an ideological agenda) and state-sponsored players (aiming for intelligence, sabotage or money). There are industry estimates that total global cybercrime damage costs could double to *USD 6 trillion* by 2021.

Corporates in crosshairs: A look at the big cyberattacks of 2017

Cyber threats now faced by corporates include Distributed Denial of Service (DDS) attacks that overwhelm websites to make them crash, ransomware (malware that encrypts the target's data and demands a ransom payment to release it) and sabotage. An example of sabotage was the NotPetya malware released in the Ukraine during June 2017, which destroyed targets' data, making global corporates such as A.P. Møller-Mærsk, Mondelez, FedEx and Renckitt Benckiser suffer collateral damage and associated costs of USD 100-300m; ie 4-10% of EBIT. The WannaCry ransomware attack in May 2017 affected over 230,000 computers, disrupted the UK National Health Service and led to estimated global costs of up to USD 4bn. The hack and individually targeted data theft from US consumer credit reporting agency Equifax in July 2017 has so far led to the departure of its CEO, costs of USD 439m (~40% of EBIT), a share price drop of 30% at the lowest point and pending civil and criminal litigation against the company.

Corporates now consider cybercrime a key concern

According to a 2017 global survey by Marsh and Microsoft, large corporates now consider cybercrime a key risk. Around 70% of board members surveyed said it was top-five risk, double the share seen in a similar survey from 2016. Tellingly, only 14% of board members are highly confident in their company's ability to respond to a cyberattack.

Cybersecurity: Emergence of a USD 100bn industry

The rising corporate sense of urgency is set to drive ~40% growth in global cybersecurity spending, up to USD 100bn by 2020. Of the top 50 listed players in the industry, two-thirds are from the US, three are Nordic (F-Secure in Finland, Fingerprint Cards and Precise Biometrics in Sweden) and four are European (Gemalto and INSIDE Secure in France; Sophos and NCC in the UK).

Interviews with a corporate victim and cybercrime defenders

In addition to an introduction by Nordea's Global Co-Head of Corporate & Investment Banking **Mathias Leijon**, we interview A.P. Møller-Mærsk's VP and Head of Risk Management **Lars Henneberg**; F-Secure's CEO **Samu Konttinen**; Nordea's Group Chief Information Security Officer, **Tapio Saarelainen**; Nordea's Head of Technology Information Security **Stefan Jäschke**; and **Benjamin Särkkä**, Head of NITSIRT (Nordea IT Security Incident Response Team) at Nordea's Cyber Defence Centre.

Nordea

Cybercrime: A potential existential threat for corporates

Nordea Global Co-Head of Corporate & Investment Banking Mathias Leijon reflects on the severity of the threat from cyberattacks, how well-prepared large corporates are to face cyber threats, and if Nordea has a role to play in helping to manage these risks.

Nordea

Crimes have evolved from being isolated incidents to potentially having a major impact on the whole company

JT: We saw news reports of major cyberattacks causing serious financial damage to large corporates last year. Would you say cybercrime has become a critical issue for corporates and is it a growing problem?

ML: The number of cyberattacks has increased exponentially over the last ten years and the degree of sophistication has moved from hobby hackers to organised crime. To put things in perspective, let's look at the banking business. Not very long ago one of the most typical crimes we faced was robbers coming into a local bank branch to steal money. That kind of incident was of course a traumatic and shocking experience for the employees, but incidents were rather isolated and infrequent. What happens today is that cybercriminals attack Equifax, Tesco and other large corporates, and steal very sensitive private data on thousands of individuals. These crimes are lucrative and very difficult to solve, and with huge costs for those affected. If a company is a victim of a severe cyberattack, even the CEO and the board might get replaced. The company could even potentially face bankruptcy.

We are also seeing an increased number of attempts at forgery, where cybercriminals hack a CEO's email. The CEO then allegedly sends an email to a local controller and asks this person to send money to a lawyer who is helping the company with a sensitive acquisition. The local controller is also informed that he/she is put on an insider list and is not allowed to talk to anyone about this. We, and other banks, have an increased responsibility to pre-empt these types of crime.

Generally, however, the vast majority of all attempts fail and hence it is easy to get overly worried. But the fact is that when they succeed, the consequences are often very, very detrimental to an individual, family, corporate or an entire society. This creates an asymmetry, which warrants spending huge sums on ensuring it doesn't happen.

I also think that one very important distinction to make is that even if nations, corporates or criminals have access to potentially very damaging malware, this doesn't mean that they all have the incentive to use it. Just because you can, doesn't mean you will. And even if state-sponsored players have deployed malware in a critical IT system used in society, which we should arguably assume has already been done, it doesn't automatically mean that they will use it. Should they choose to do so, it could - in a manner of speaking – trigger World War III, and I think most such players with those capabilities would go to almost any lengths to avoid that. The main worry is rather a "mad-men" scenario where logic and rationality don't prevail.

JT: How well-equipped and prepared do you think Nordic large corporates are for dealing with threats from cybercrime? Have incidents in 2017 related to companies such as Mondelez, FedEx, Reckitt Benckiser and A. P. Møller-Mærsk been a wake-up call?

ML: I think that we are not as prepared as we should be. I had a very eye-opening experience during a seminar with one very bright hacker working for Nordea. He asked the audience if anyone dared him to try penetrating their system. One brave company volunteered and he hacked their system live on stage – it literally took him a few minutes!

An IT system is only as strong as its weakest link

That seminar made it clear to me that an IT system is never stronger than its weakest link. From time to time, the weak link can be human individuals. Just ask yourself, how often do you change your passwords? To hack someone's password is not very hard. I think that everyone, myself included, needs to actually realise how important cybersecurity is. How to you protect yourself when outside firms are used to design marketing campaigns and other events that might open up a door into your own system is something that is becoming increasingly important.

We at Nordea have actually come very far in this respect and over time I believe this is a service we could also offer our clients.

JT: What is Nordea doing to manage risks from cybercrime – and is there anything we can do to help our corporate and institutional customers?

Corporates reach out to us for help protecting their systems and recovering from cyber-incidents

ML: I think that we are actually starting to build up competence and a great capability to protect ourselves. We have a lot of super-talented people working with cybersecurity, and this is highly prioritised, because the data we possess is so sensitive and so important to protect - both for us and for society as a whole. Going forward, and to some extent already today, corporates are asking us for help with protecting their systems and recovering from cyber-incidents, and we only too happy to be able to support them in this field in addition to all the banking services we provide. I would not be surprised if we do even more of this in the future, on the back of the capabilities we are building.

Cybercrime: Profit, ideology and politics

As we humans are rapidly migrating online (90% of the global population is expected to be internet users in 2030), crime is unfortunately following us there. With more and more people and devices having an online presence, there is greater potential prey for criminals, including organised crime, hacktivists and state-sponsored players. Global costs for cybercrime damages are set to double to USD 6tn by 2021, with global cybersecurity spending growing 10-15% annually towards a USD 100bn industry over the same time horizon.

Crime has followed society online

Cybercrime has gained widespread attention after big global cyberattacks in the past few years

Crime has been around for as long as humans have had an organised society, and cybercrime – crimes committed on or via the internet – has been around for more or less as long as a significant number of people have been using the web. Something seems to have happened in recent years though, with the more shady internet activity getting picked up by the media or even by consumers or citizens experiencing disruption or fallout from large-scale initiatives or attacks that affect the services we are using.

Historical theft, robbery or extortion have typically been via human interaction. The astonishing growth in human connectivity in the past ten years, further powered by the introduction of smartphones, has led to an explosion in human social and commercial activity on the internet. And as we are conducting more business there, criminals have increasingly migrated there as well, and can now reach victims across the globe. As we expect to be able to transact and interact online, individuals and businesses alike are exposed to crime in these digital channels. In the past we have perhaps feared being robbed late at night in some dark alley. Now we can be targeted via the internet from anywhere in the world, and we will most likely have no idea who is committing a crime against us. Any person or business with some form of presence online is in theory exposed. Growth in cybercrime may seem greater than it really is, as increased attention is also an effect of companies having become much more adept at discovering cyberthreats.

Any person or business with an online presence is exposed

Most of us have been subject to attempts at phishing – fake messages aiming to make us give out data or give access to our system

So what is it we have seen so much of in recent years? Most of us are used to a steady stream of spam, essentially advertising, in our inbox and as messages to our smartphones. We are now having to get used to more volumes of a more sinister form of spam: phishing. This is essentially fake emails and messages, often disguised as coming from credible senders such as banks or telecom operators, containing requests to lure us into providing confidential information or to unknowingly download software (malware) that attempts to steal data or take control of our devices. This writer's private email inbox has a rich daily flow of such phishing attempts, ranging from steamy fake adult dating ad invites ("I have seen you in the neighbourhood – click here so we can connect!") to requests for payments to tax authorities. They are all looking for that payment, credit card or bank account details, or just the click to let malware into the computer.

The clearest threat to large corporates is from big cyberattacks

More notably, however, we have seen big incidents, cyberattacks with effects on a global scale, which have been well planned and organised, with a specific purpose in mind. Examples of such of attacks include:

- **Distributed denial of service attacks (DDoS)**: Typically flooding and overwhelming a high-profile website with botnets (networks with large numbers of hijacked computers); with so many simultaneous requests, the site does not have the capacity to cope, and goes down.
- **Ransomware**: Malware and viruses that gain access to a system or network, find data and encrypt it to make it unavailable to the original owner. The perpetrator then asks for an anonymous payment (typically in cryptocurrency) to unlock the data.
- **Cybersabotage**: Malware that does not aim to take money from victims, but to damage or destroy IT systems or even physical assets and infrastructure.

Nordea

Ransomware encrypts the target's data and demands a ransom payment to unlock it

Ransomware is the method of choice for cybercriminals to try to extract money from corporate targets. Elaborate schemes to take control of a specific company's data, as with a human kidnapping, are more unusual. For cybercriminals, the optimal setup is typically to automate systematic probing for security weaknesses in selected target groups, trying to exploit those found by installing ransomware. The process is standardised, and aimed at making it as tempting as possible for the victims to pay the ransom to have their data released, instead of blankly refusing or making a maximum effort to identify and pursue the criminal, with the aid of law enforcement. The less human, hands-on-keyboard effort needed per victim to make the profit, the better.

DDoS attacks temporarily overwhelm websites, causing them to crash

DDoS attacks can be combined with demands for ransom payments, but tend not to do permanent damage to infrastructure or data. They effectively put a website out of business for a limited time. This is most effective against sites representing entities that rely on a high level of public trust. A government, police, media outlet or cloud service website cannot afford to be offline for too long. But the nature of this attack, with its public and strong symbolic value, makes it more commonly used by players without a profit agenda: those who wish to make a point.

Cybersabotage comes in the form of attacks intending to weaken or destroy an adversary's data or infrastructure

Cybersabotage is all about weakening or destroying adversaries. One of the first examples to become publicly known was the Stuxnet worm in 2010, which sabotaged Iran's nuclear programme by causing centrifuges for uranium enrichment to malfunction. It is widely believed to have been deployed by US and Israeli intelligence agencies, with the clear intent to delay Iran's ability to produce nuclear weapons.

A fresh example of cybersabotage is the NotPetya malware spread through an automatic update of Ukrainian tax accounting software in June 2017. It appeared to be ransomware, showing a screen demanding payment to release locked and encrypted data, but it actually destroyed data irrespective of any response. It caused severe disruptions to Ukrainian infrastructure, including airports, railways, power utilities and banks. But it also affected more than 1,500 companies, including major multinationals such as A.P. Møller-Mærsk (see our interview with VP and Head of Risk Management Lars Henneberg in this report), Mondelez, FedEx, COFCO, Saint-Gobain, WPP, DLA Piper, Merck & Co, Renckitt Benckiser and Nuance Communications. We highlight the costs incurred by some of these corporates in a separate snapshot later in this report. They got caught up in the cyberattack and suffered substantial collateral damage.

Ransomware and cybersabotage sometimes, but not always, depend on successful phishing to be able to deploy. The most sophisticated attacks might be able to use an alternative way into a target network, but the bulk of them need someone to reveal a password or click a fake link that downloads the malware.

Cybercrime players: Meet the good, the bad and the ugly

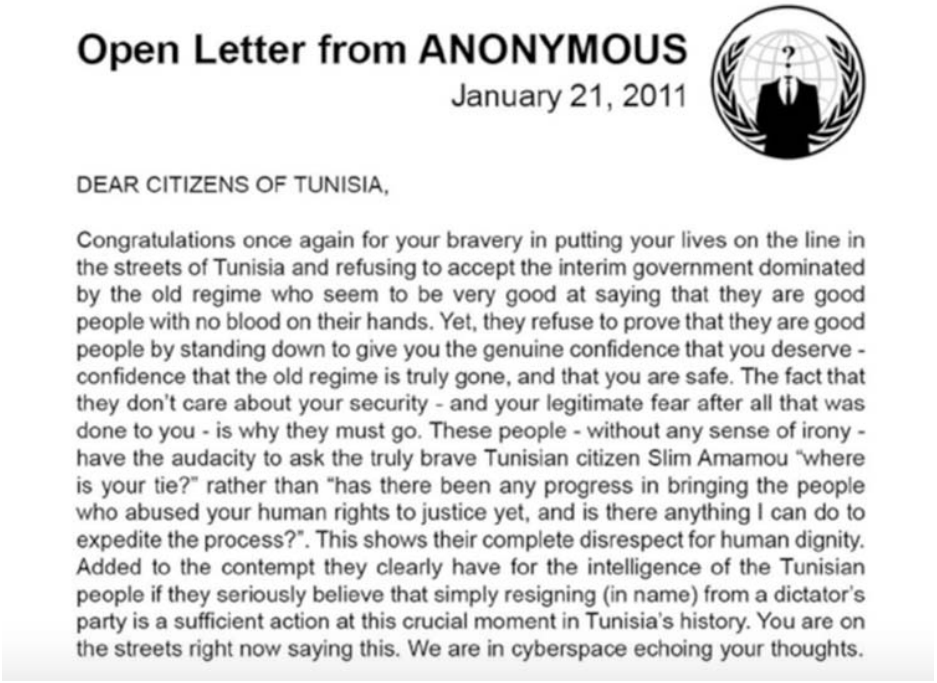
Simply put, we would divide the main players in cybercrime, cyberterrorism and cyberwarfare into three key categories:

- Hacktivists
- Organised crime
- State-sponsored players.

Hacktivists have an ideological agenda; they are not in it for the money

Hacktivists, both individuals and networks, are driven by ideology or principles. Their agenda is not about making profits or pursuing national or geopolitical goals. Their profiles vary, but typical values they promote include transparency, the right to anonymity, human rights and equality. When they engage in cyberattacks, it is often about engaging the public by gaining attention for a critical cause by confronting and humiliating a high-profile adversary who is seen to be violating those values.

OPEN LETTER FROM HACKTIVIST GROUP ANONYMOUS DURING ARAB SPRING IN TUNISIA



Open Letter from ANONYMOUS

January 21, 2011

DEAR CITIZENS OF TUNISIA,

Congratulations once again for your bravery in putting your lives on the line in the streets of Tunisia and refusing to accept the interim government dominated by the old regime who seem to be very good at saying that they are good people with no blood on their hands. Yet, they refuse to prove that they are good people by standing down to give you the genuine confidence that you deserve - confidence that the old regime is truly gone, and that you are safe. The fact that they don't care about your security - and your legitimate fear after all that was done to you - is why they must go. These people - without any sense of irony - have the audacity to ask the truly brave Tunisian citizen Slim Amamou "where is your tie?" rather than "has there been any progress in bringing the people who abused your human rights to justice yet, and is there anything I can do to expedite the process?". This shows their complete disrespect for human dignity. Added to the contempt they clearly have for the intelligence of the Tunisian people if they seriously believe that simply resigning (in name) from a dictator's party is a sufficient action at this crucial moment in Tunisia's history. You are on the streets right now saying this. We are in cyberspace echoing your thoughts.

Source: Screencap

Hacktivist network Anonymous attacked payment service provider websites when they stopped taking donation payment to Wikileaks in 2010

One of the most well-known examples of a hacktivist network is Anonymous, which has championed many causes since 2003. In 2010, when Wikileaks started releasing hundreds of thousands of leaked US diplomatic cables, it faced legal threats from the US government, and was consequently kicked off Amazon's servers and cut off from service (for those who wanted to donate to it) from payment service providers PayPal, MasterCard and Visa. Sympathetic to Wikileaks, Anonymous launched DDoS attacks on websites that brought down PayPal, disrupted MasterCard and Visa, and crashed the website of US senator and Vice President Joe Lieberman, who supported the push to cut services. Anonymous even took on Amazon's website, but with an unsuccessful attack.

Organised crime is seeking maximum profit

Organised crime is represented by individuals or networks who have developed a professional expertise in cybercrime. They are in it for the money, and tend to act like any profit-maximising enterprise, although without any moral or ethical constraints. They will focus on what gives the greatest risk/reward outcome with the tools available. Cybercriminals can become involved in other agendas, offering their expertise for hire in covert, illegitimate forums. They either use their skills to run their own show, or make them available to others for a price.

State-sponsored entities pursue an intelligence or sabotage agenda on behalf of the government they serve

State-sponsored players act, directly or indirectly as proxies, for national governments, typically military intelligence. They can be a directorate or a department of an intelligence agency or even affiliated hacker networks. Their agenda is a function of the geopolitical agenda of their host nation. Russia has been blamed for the NotPetya malware aiming to cripple the Ukrainian financial system and infrastructure in 2017, as well as for influencing the US presidential election in 2016. North Korea has been pointed out as the originator of the 2017 WannaCry ransomware attack, which affected more than 200,000 computers across 150 countries (estimated costs for damages range from a few hundred million up to USD 4bn). The US and Israel are widely believed to be responsible for the Stuxnet worm which sabotaged uranium enrichment facilities in Iran's nuclear programme in 2010.

Cybercrime has become big – costs are soaring

Global cybercrime damage costs likely to double to USD 6tn by 2021

The magnitude of the cybercrime challenge faced by society is highlighted in the *2017 Cybercrime Report*, sponsored by managed security services provider Herjavec Group and produced by think tank Cybersecurity Ventures. Predictions in the report include:

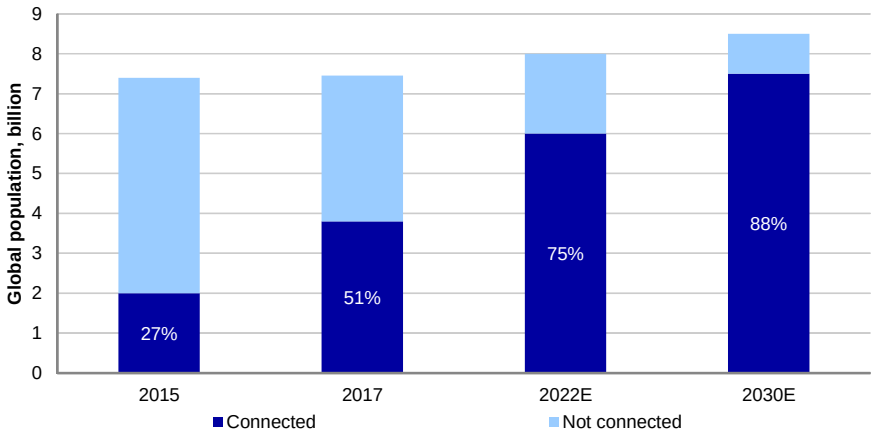
- Global cybercrime damage costs will double from USD 3tn in 2015 to USD 6tn by 2021.
- Aggregate spending on cybersecurity will exceed USD 100bn in 2017-21 (at 12-15% annual growth), which can be compared with Gartner Group's estimate of global information security spending of USD 86.4bn in 2017.
- The human attack surface for cybercrime will reach six billion people (75% of the world's population aged six and over) by 2022 – up from 3.8 billion (51%) in 2017.
- Global ransomware damage costs will exceed USD 5bn in 2017, up 1,500% from USD 325m in 2015.

Soaring cybercrime impact driven by rapid further growth in human connectivity

These predictions are largely based on continued growth in human connectivity, citing among other things Microsoft's prediction that data volumes online will be 50x greater in 2020 than in 2016, Intel's estimate of the Internet of Things expanding from two billion smart devices wirelessly connected to the internet in 2006 to 200 billion by 2020, and the world's digital content growing from four billion zettabytes in 2016 to 96 billion zettabytes by 2020. And in case you were wondering, one zettabyte is 10^{21} bytes, or one trillion gigabytes. The entire internet, the World Wide Web, was estimated to contain 0.5 zettabytes of data in 2009.

According to Cybersecurity Ventures, 111 billion lines of new software code are produced each year, which gives a constantly growing number of new vulnerabilities that can be exploited, leading to a total number of passwords in use worldwide growing to 300 billion by 2020. Specifically, Fortune 500 company employees will own an average of 90 business and personal accounts requiring log-in IDs and passwords, meaning this group alone will manage ~5.4 billion passwords. Interestingly, roughly two-thirds of the 300 billion passwords are expected to be used by machines, Internet of Things devices.

GROWING ATTACK SURFACE FOR CYBERCRIME: INTERNET USERS IN GLOBAL POPULATION



Source: Cybersecurity Ventures

Cybersecurity becoming a USD 100bn industry

Global cyber security spending poised to grow ~40% to USD 100bn by 2020

Exact definitions of cyber-, IT and information security vary, but in addition to the Gartner Group study and the Cybersecurity Ventures projections mentioned above, research from IDC (International Data Corporation) in 2016 pointed to annual spending on cybersecurity growing 38% from USD 74bn to USD 102bn in 2020. And this was before last year's WannaCry and NotPetya cyberattacks.

So who are the corporate players in the cybersecurity industry? To give an idea of what the arena looks like, we provide a list with a summary of those that are, according to Cybersecurity Ventures, the top 50 listed cybersecurity companies globally.

TOP 50 CYBERSECURITY COMPANIES WORLDWIDE

Company name	Market cap, USDm	Revenue, USDm	Headquarters	Description
Level 3	19451	8172	Broomfield, USA	Network & Managed Security Services
Check Point Software	17592	1730	Tel Aviv, Israel	Unified Threat Management
Palo Alto Networks	17314	1762	Santa Clara, USA	Threat Detection & Prevention
Symantec	17310	4019	Mountain View, USA	Endpoint, Cloud & Mobile Security
Splunk	15166	950	San Francisco, USA	Big Data Security
ZixCorp	11699	1165	Dallas, USA	Email Encryption & Data Protection
Fortinet	9147	1495	Sunnyvale, USA	Enterprise Security Solutions
F5	9121	2090	Seattle, USA	Cloud & Data Center Security
Juniper Networks	9085	5027	Sunnyvale, USA	Threat Intelligence & Network Security
Varonis	7818	1131	New York City, USA	Data Security & Analytics
Qihoo 360	7812	1805	Beijing, China	Internet & Mobile Security
BlackBerry	6908	1297	Waterloo, Canada	Mobile & Data Security
Proofpoint	6007	515	Sunnyvale, USA	Security-as-a-Service
Gemalto	5519	3350	Meudon Cedex, France	Digital Identity Management
FireEye	3445	751	Milpitas, USA	Advanced Threat Protection
Sophos	3440	508	Abingdon, UK	Anti-Virus & Malware Protection
Qualys	3030	231	Redwood City, USA	Cloud Security & Compliance
VeriSign	2628	1062	Reston, USA	Internet Security Solutions
LifeLock	2259	587	Tempe, USA	Identity Theft Detection
Mimecast	2236	187	Watertown, USA	Email Security
CyberArk	1771	217	Petach-Tikva, Israel	Cyber Threat Protection
VASCO Data Security	1639	217	Marlborough, USA	Authentication & e-Signature Solutions
Ixia	1635	485	Calabasas, USA	Network Visibility, Security & Testing
Imperva	1619	322	Redwood Shores, USA	Data & Applications Security
Barracuda Networks	1478	353	Campbell, USA	Email & Web Security Appliances
Infoblox	1471	358	Santa Clara, USA	Automated Network Control & Security
Gigamon	1437	311	Milpitas, USA	Data Center & Cloud Security
Rapid7	1256	157	Boston, USA	Security Data & Analytics Solution
Radware	932	195	Tel Aviv Israel	Application Security & Delivery
NCC Group	807	316	Manchester, UK	Information Assurance Services
AhnLab	755	118	Gyeonggi-do, South Korea	Internet Security Solutions
F-Secure	717	167	Helsinki, Finland	Internet Security for All Devices
Verint	528	192	Melville, USA	Security Intelligence & Compliance
Digital Arts	521	45	Tokyo, Japan	Web & Email Filtering Software
Imprivata	493	119	Lexington, USA	Security for Healthcare Providers
A10 Networks	467	230	San Jose, USA	DDoS Cyber Attack Protection
MobileIron	466	164	Mountain View, USA	Mobile Device & App Security
KEYW	386	288	Hanover, USA	Cyber Defense & Digital Forensics
Fingerprint Cards AB	376	731	Gothenburg, Sweden	Fingerprint Biometrics
Mitek	295	45	San Diego, USA	Mobile Identity Verification
FFRI, Inc.	274	13	Tokyo, Japan	Cybersecurity R&D
Guidance Software	236	111	Pasadena, USA	Endpoint Data Security
Absolute	209	93	Austin, USA	Endpoint Visibility & Control
INSIDE Secure	146	48	Aix-en-Provence, France	Smartphone & Mobile Device Security
SecureWorks	109	430	Atlanta, USA	Managed Security Services
CYREN	107	31	McLean, USA	Web, Email & Mobile Security
SSH Communications	103	19	Helsinki, Finland	Privileged Access Control
Finjan Holdings	86	18	East Palo Alto, USA	Cybersecurity IP Licensing
Globalscape	76	33	San Antonio, USA	Secure File Transfer
Precise Biometrics AB	61	11	Lund, Sweden	Mobile Identity Authentication

Source: Cybersecurity Ventures and Thomson Reuters

Nordea

The definition of a cybersecurity company can be debated; we simply use the top 50 list from Cybersecurity Ventures as is, although among the bigger market cap companies we might be reluctant to consider Juniper Networks or Blackberry, for example, as belonging to this category.

The only Nordic players in the global listed cybersecurity top 50 by market cap are F-Secure, Fingerprint Cards and Precise Biometrics

Making instead some general observations on this universe of companies, we note the following:

- Two-thirds of the companies are from the US.
- The industry is still quite new, and fragmented; the top ten players by market cap come from different origins and have different specialities.
- Most companies have their roots in a more mature business (internet network operator, such as Level 3; network infrastructure, such as Juniper; or mobile device maker, for example, BlackBerry).
- There are only three Nordic players in the top 50: F-Secure in Finland, and Fingerprint Cards and Precise Biometrics in Sweden.
- There are only four other European players in the top 50: Gemalto and INSIDE Secure in France, and Sophos and NCC in the UK.
- Israel is over-represented in the cybersecurity industry, with three companies in the global top 50, including the global no. 2, and with several of the US companies in the top 20 having Israeli founders.

Interview: Income streams have become highly dependent on digital data

We interview **Lars Henneberg**, Vice President and Head of Risk Management at global shipping and logistics group A.P. Møller-Mærsk, on how disruption and damage from the NotPetya cyberattack in 2017 has cost the group up to USD 300m, what has been learned from the incident, and how it will approach cybersecurity going forward.

Lars Henneberg

EB: You were victims of the NotPetya cyberattack last year. Could you tell us what happened? How was your business affected?

LH: We had an attack on what we call our MaerskNet, which covers our transportation and logistics business. The malware that attacked us spread quickly across our network. We were infected with the NotPetya malware via an application called MeDoc, which we use to file tax returns to the Ukrainian authorities. From there it spread aggressively around MaerskNet.

It was clear early on that this was collateral damage, and we were not targeted in any way. There were several companies worldwide affected by NotPetya, some as severely as we were.

The biggest hit was to our container liner business, our ports and terminals business and our freight forwarding business. The crisis was global, affecting operations across the world.

It was the administrative IT in our business that was infected, meaning that our vessels could still sail safely. But the breakdown of our administrative IT systems quickly affected operations. For the vessels to know where to drop the containers off and for crane operators to know which container to pick, you need to be connected to the administrative IT system. Even if a vessel came in and managed to drop off the containers, ports were not able to communicate and issue a notice of arrival to customers.

49,000 computers needed to be re-imaged

For us, the incident meant that 49,000 computers had to be re-imaged. Not all had shown signs of infection, but the malware had an inbuilt delay, meaning that determining whether a computer was infected was not a straightforward task. If you reconnected one infected computer to the network, you needed to start all over again.

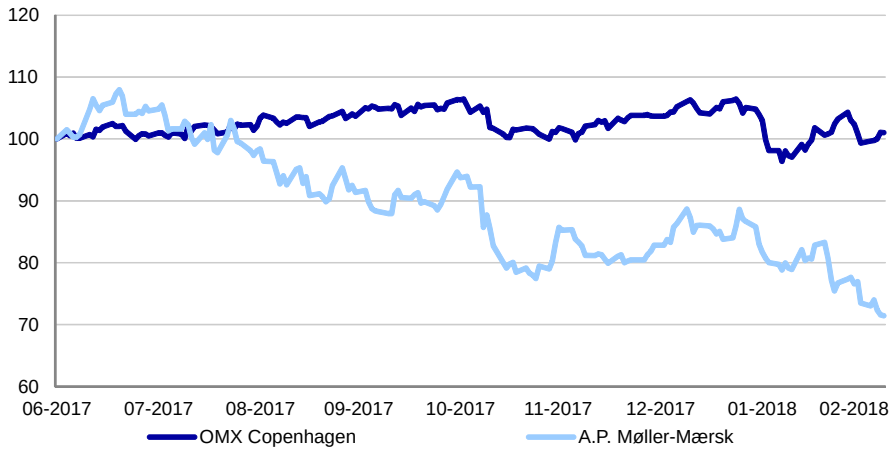
We were also affected from a commercial perspective, since our global customer service systems were not accessible, and for a time we were unable to receive orders or issue invoices. Our email systems were down as well, so we were unable to communicate normally with our customers.

On the administrative side, we had to find alternative ways of making payments to suppliers and paying salaries to employees.

Critical business functions needed to be operated manually for two weeks

We had to manually operate the critical functions of our business for around two weeks, but it took around three months for us to get everything up and running again. This attack demonstrated to us how important it is to be resilient.

A.P. MØLLER-MÆRSK'S SHARE PRICE AND OMXC25, INDEXED 30 JUNE 2017 = 100



Source: Thomson Reuters

EB: What did you learn from the attack?

LH: The attack demonstrated that our income streams are becoming increasingly dependent on digital data rather than solely on physical assets. The way that you manage risks has to follow that transformation.

I also think that to understand how IT and business are linked together, you need to look at IT from a business perspective to see what critical information assets you have that need more protection. They also need to be prioritised for recovery, if it comes to that.

IT and business are interdependent and cannot run in silos

We have learnt that it is critical that the IT organisation understands how it supports the business, and that the business management understands how they depend on IT to run the business. As a general statement, those two cannot run in silos.

We have set five strategic priorities for 2018, and one of them is to strengthen the IT backbone and increase cyber-resilience. The purpose is to be able to support a business that is becoming increasingly digital, in accordance with our ambitions.

On a positive note, one thing we have learnt is the way we can work together as an organisation when under pressure. It was really an amazing thing to see that we arguably completed six months' work in three weeks! The way that we were able to make decisions, to build trust between us, to delegate responsibility and to take swift action without formalities or bureaucracy. That was an experience that we can learn from and take with us in the way that we work together.

EB: **Given A.P. Møller - Mærsk A/S's importance for global trade, and hence for the world economy, did you have interest or involvement from authorities or governments during the malware incident?**

With A.P. Møller - Mærsk facilitating 15% of global trade, many authorities wanted to be briefed during the incident

LH: There were two aspects to it. In some countries, authorities and even ministers requested briefings, and our communications organisation had to brief our local managers to be able to give insights into what was going on. In some areas, police authorities' cyber departments considered the malware a criminal act and wanted to investigate the crime. These things added complications to managing a crisis like this, because all these separate requests needed to be met in an organised and consistent manner. This kind of stakeholder management is, of course, very important.

EB: Who was behind the attack?

LH: We only know that it originated from the MeDoc tax accounting software in Ukraine, and we do not want to speculate on its ultimate origin or creator.

EB: How did you repair the damages caused by the attack?

Creativity and improvisation kept business running

LH: What really matters is how we worked in terms of managing the crisis so that we could continue to serve our customers. We mobilised our cyberincident response team, who were prepared and ready to handle the situation. We also mobilised our crisis management team as this was an incident with repercussions beyond IT, and we quickly needed to perform crisis management in manual mode as we had no access to our email system. We ended up creating some WhatsApp groups for alternative communication. We had to be creative at that stage.

We soon realised that reversing the encryption on our systems was not going to happen and that we would have to recover the systems manually, which could take a long time. We started to recover everything, getting the applications and the systems up and running again.

We were aware that we were in for quite a long period of pain and the business continuity management came into focus: how do we run the business in the meantime? Obviously we could not afford to be out of business for one month, or however long it would take to get everything back up and running. The decision was made to reach out to the different business units to activate their business continuity plans and unleash their creativity, encouraging them to do whatever they could to find solutions for our customers and manage the operational challenges in terms of getting containers in and out of ports.

I think that it is important that businesses are aware what their critical systems and applications are and where to start the disaster recovery, because there will be many people wanting their units to be prioritised. Then what businesses also need to understand is how the various systems and applications are interlinked, how they are dependent on each other and so on.

EB: Have you reviewed your strategy for dealing with any future cyber threats?

Strategic priority to strengthen the IT backbone with robust IT security required by increasingly digitised business

LH: I think that if you go through an incident like this, there are two possible cultural approaches afterwards. You can choose the approach to say that "it wasn't me and we have done everything right". We have instead chosen to view this as an opportunity to learn, and we feel an obligation to learn and to grow in order to become better. We have conducted a number of internal incident investigations, with some external people looking at our maturity level. We have established a short-term plan to deal with the tactical issues and the continuous improvements of the security that we need. Then we have a longer-term plan to strengthen the IT backbone and make sure that there is a really robust IT system around operations to support an increasingly digitalised business model.

EB: Your CEO recently quantified the cyberattack as impacting the results by USD 200-300m due to business interruption. Have you seen any other effects of the attack such as reputational damage, breach of customer information, etc?

LH: We did not at any point in time find indications that we had lost data or that data had been leaked. As I mentioned earlier, this was not a targeted attack and we were collateral damage. Has it meant anything for our reputation? We have actually received much praise for being open about the way that we have handled the attack. We have spent a lot of time meeting our customers to reassure them that our security level is where it should be.

EB: What tools are available for dealing with cyber threats for large corporates? Software systems? Security protocols? Insurance? Others?

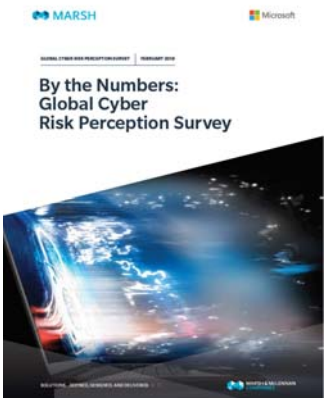
Software tasked to monitor, detect and prevent needs a framework of rules and policies for security controls

LH: To monitor, to detect and to prevent, is largely done with technology, software systems. You need to have a framework of rules and policies that describe the security controls that must be installed. This is also based on your risk appetite, and this needs to be defined. The governance should be shaped around that. You also need to have incident management and crisis management ready. You need to make sure that you have disaster recovery plans in place in a prioritised way, and you also need to make sure that the business can run, even in the case of an IT outage.

These incidents often have a major financial impact. The insurance industry has now also started to get its head around it and has realised that here is also something that would need to be insured. I think that over the past year or two, adequate insurance alternatives have evolved. You can cover restoration costs due to a cyberattack, you can cover liability for data breaches, and you can also cover the business interruption that you may have as a result of a cyberattack, irrespective of there being no physical damage. It is very important to do an analysis of what kind of coverage you need and to tailor your coverage around that. It is not an off-the-shelf product.

Snapshot: Cyber risk perception survey

As an illustration of the current corporate perception of cyber risk, we show selected highlights from Marsh and Microsoft's February 2018 global survey of 1,300 executives. Cyber risk is clearly a top concern at board level, but boards are not typically well-briefed on this, or confident in their company's ability to withstand a cyberattack. The greatest perceived threat is business disruption by financially driven cybercriminals, rather than the alleged state-sponsored players behind the big global WannaCry and NotPetya cyberattacks in 2017.



A broad, global survey of cyber risk perception among senior executives

The rapid growth in human connectivity, paired with fast technological innovation, has led the global population to conduct more of its social and business activity online. This development is widely expected to continue in the coming years, meaning the world's companies need to respond by ensuring they have business models that are compatible with the new, more digital, reality. Having an online presence means being exposed to the risk of cybercrime, with public awareness of such risks and how they could cause major financial damage for large corporates increasing dramatically after the big WannaCry and NotPetya cyberattacks in 2017. As an illustrative gauge of large corporate sentiment and attitudes towards cyber risk, we show a few selected highlights from the February 2018 survey by Marsh and Microsoft.

Listed US software giant Microsoft is the supplier of the Windows operating system. Marsh is the insurance broking and risk management subsidiary of listed US professional services group Marsh & McLennan Companies, which also houses Guy Carpenter, Mercer and Oliver Wyman.

Survey based on responses from 1,300 executives globally

The survey is based on responses from 1,300 risk professionals and other senior executives globally, from corporates of different sizes in 26 industry sectors. Respondents include CEOs, CFOs, chief technology officers, chief risk officers, corporate directors and others, with over half of respondents working at C-suite or board level.

Cyber risk is now a top concern at board level

70% of board members rank cyber risk as a top-five concern

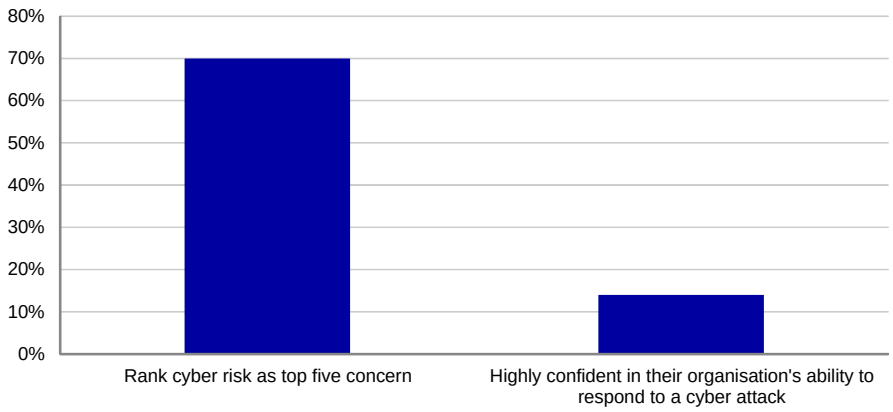
It is very evident from the survey that corporates now view cyber risk as a major challenge. Stripping out just the board member responses from the survey – hence addressing only the top decision makers – 70% of them rank cyber risk as a top-five concern for their companies. This chimes well with the World Economic Forum's 2018 Global Risks Report, in which two technological risks – cyberattacks and massive data fraud – were for the first time in the top five. This percentage is also roughly twice as high as in response to a similar question in a Marsh survey from 2016.

Only 14% of board members are confident in their company's ability to respond

There is a striking divergence between the perceived risk threat and companies' perceived ability to respond, with only 14% board members being highly confident in their organisation's ability to respond and recover from a cyberattack.

Nordea

SURVEY OF BOARD MEMBERS, 2017



Source: Marsh and Microsoft Cyber perception survey

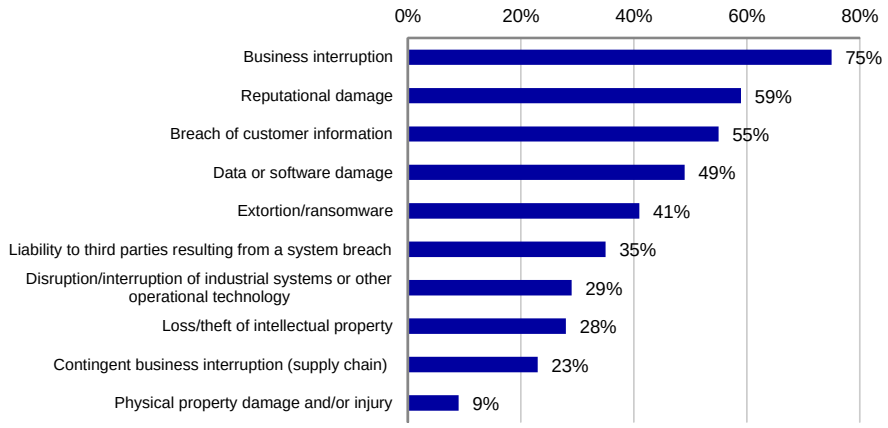
28% of the biggest corporates see maximum potential losses from a cyber incident of more than USD 100m

The fact that major global corporates like Mondelez, A.P. Møller-Mærsk, Reckitt Benckiser and FedEx have all publicly revealed that they suffered costs of between USD 100m and USD 300m in 2017 from the NotPetya cyberattack in the Ukraine seems to have left a mark on corporate executives' perceptions of monetary risk associated with cybercrime. Of the biggest companies – those with revenue of USD 1bn or more – in the survey, 28% see maximum potential losses from a cyber incident in excess of USD 100m, 42% see maximum potential losses of USD 10-100m, while 28% see maximum damage of USD 10m or less.

Corporates see the biggest risk from business interruption caused by financially driven cybercriminals

The experiences from the NotPetya attack also seem to be reflected in the types of damage companies now expect they could suffer from cyber-incidents. Head and shoulders above the rest is "business interruption", which 75% cite as a potential source of costs or losses. This is followed by reputational damage ("do customers want to use us if they see that we are vulnerable to disruption from cyber incidents?") and data loss or damage. Interestingly, actual loss of intellectual property or physical property damage or human injury is at the bottom of the list. Corporates seem less concerned about being raided or individually targeted for blackmail than being caught up in sabotage or crude, standardised and automated mass-volume cyberattack.

WHICH CYBER LOSS SCENARIO PRESENTS THE GREATEST POTENTIAL IMPACT?



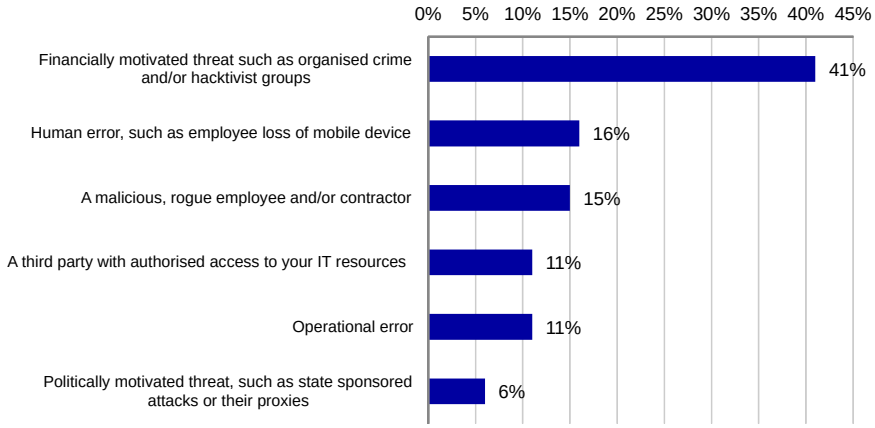
Source: Marsh and Microsoft Cyber perception survey

The two big global cyberattacks in 2017 were allegedly by state-sponsored players – ie the threat less feared by corporates

We note with great interest that the clearly dominant type of cyber threat which concerns corporates is financially driven threats like organised crime. This is a very good reflection of the fact that the bulk of cybercrime taking place on the internet today is represented by high-volume routine probing for weaknesses by organised criminals. It is natural for corporates to see themselves as potentially juicy targets for such criminals. But the fact remains that according to publicly expressed views of major governments or their agencies (see our snapshot on the WannaCry and NotPetya cyberattacks in 2017), the high-profile WannaCry and NotPetya attacks, which both caused massive financial damage for corporates, were both initiated by

state-sponsored players with political (and in the case of WannaCry, also financial) agendas. This represents a sharp contrast to only 6% of corporate respondents in the survey considering such politically motivated attacks the greatest cyber threat.

WHICH CYBER SECURITY THREAT IS THE BIGGEST CAUSE FOR CONCERN?



Source: Marsh and Microsoft Cyber perception survey

Executives pass cyber information to boards – who is not receiving it?

One-third of boards are briefed on cyber issues and events

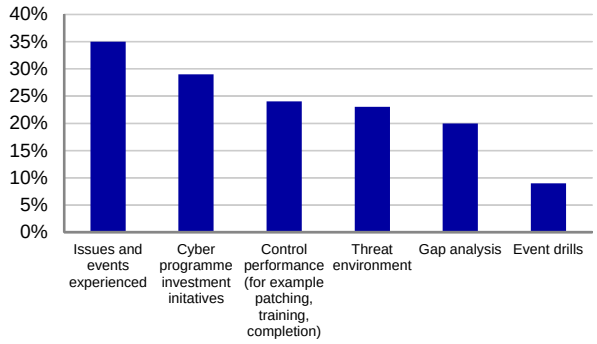
Another interesting observation from the survey is what input the boards of directors of companies receive regarding cyber threats. The general picture is that this flow seems quite filtered and selective. Roughly one-third of boards have issues and events explained. Our spontaneous reaction to this is one of surprise – should this number not be 100%? Who would not want to be informed of actual cyber incidents?

Other types of inputs are even more rarely sent to the board. Fewer than 30% are briefed on cyber programme investments and fewer than 25% on control performance, like patching and completion of security training.

45% of risk and tech executives send info to boards, but only 18% of directors say they receive it

Even more strikingly, there seems to be major disconnect between what risk and tech executives perceive that they feed to boards, and what board directors say that they actually receive. 45% of these executives state that they send information on cyber investment initiatives to board members, while only 18% of board members say that they receive such information. Either there is some miscommunication, or information gets lost on its way to the board room.

INFORMATION RECEIVED BY BOARD DIRECTORS



Source: Marsh and Microsoft Cyber perception survey

THERE IS A DISCONNECT

Risk and tech executives who said they send information on cyber investment initiatives to board members	45%
Directors who said they receive such information	18%

Source: Marsh and Microsoft Cyber perception survey

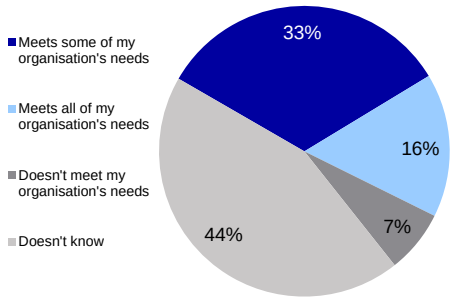
Nordea

34% of corporates have cyber insurance and 22% plan to get it in the next 12 months

Cyber insurance become more common and available

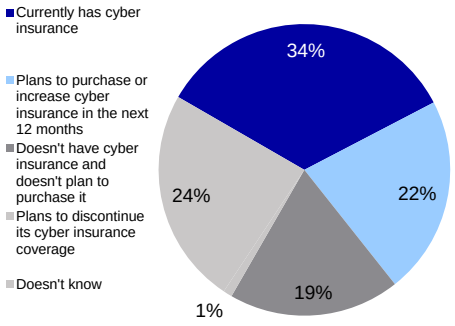
The survey also shows that the insurance industry is starting to respond to the growing need for protection against financial risk from cyber incidents. Looking at the availability of cyber risk insurance solutions, nearly 50% of respondents reply that some or all of their needs are being met. Looking at who is actually using cyber risk insurance today, 34% have insurance cover and another 22% plan to get it within the next 12 months.

CYBER INSURANCE AVAILABLE TODAY



Source: Marsh and Microsoft Cyber perception survey

ORGANISATIONS' CYBER INSURANCE STATUS



Source: Marsh and Microsoft Cyber perception survey

Interview: There is no such thing as 100% protection, so you need detection

We interview **Samu Konttinen**, CEO of listed Finnish cyber security group F-Secure, about the most common cyberattacks today, about how F-Secure works with companies to help them better withstand cyberattacks and about the biggest threats to corporates and society from cybercrime.

Samu Konttinen

By far the most common type of attack is ransomware attacks

JT: Most of us come across attempts to access our private online data, eg through email phishing, and last year saw many large corporates suffer damage from large-scale cyberattacks like WannaCry and NotPetya. How has cybercrime evolved over the past ten years? How much has it grown and how widespread is it today?

SK: During the last ten years, cybercrime has grown massively. On an average day, we are handling around 500,000 new malware samples – the volumes are huge!

The second thing that has changed is that hackers have become much more professional. Around ten years ago, we would still see "hobby hackers" who simply wanted to test their skills in a rather innocent way. Their purpose was not to make money. I would say that today activity is more in the hands of organised criminals.

Cybercrime is also very multi-faceted; online criminals target pretty much anybody. If they manage to hack into tens of thousands of computers, they do not care if these computers are owned by consumers, small companies or global enterprises – they are after whatever money they can make, wherever they can make it. Hence, this problem is not limited to big organisations – everyone is a target.

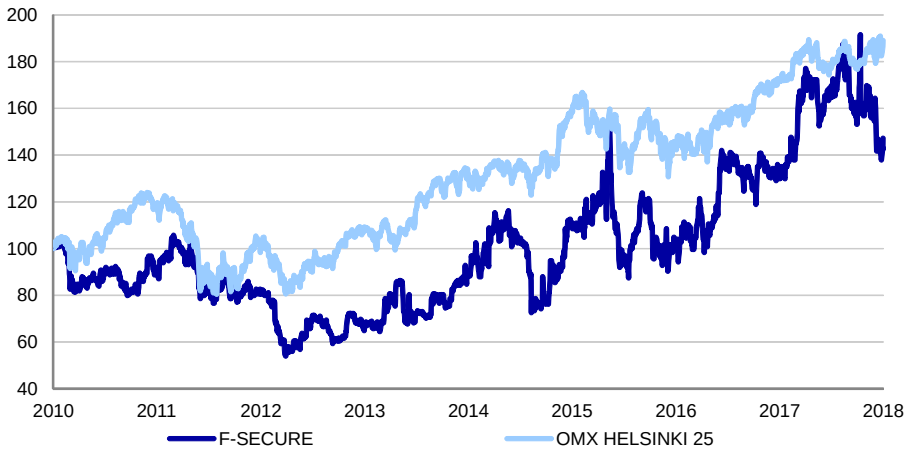
JT: Which are the most common types of cyberattacks today?

SK: By far the most common type is ransomware attacks: A malware that accesses your computer and encrypts your data files with such strong encryption that there is no other option but to pay for a decryption key to get your files back.

There are also other phishing techniques via email. These attempts need to be very convincing, you need to write an email that makes the recipient feel like they have to open it. Once the email is opened, some malware is delivered to your computer. It can be ransomware or a key logger, which accesses different accounts on your device after your username and passwords are recorded and stolen. This information is used to gain access to bank accounts or other sensitive information that can be sold.

The social engineering behind these e-mails is often rather brilliant. I think it is a constant reminder of how big a role human behaviour and psychology plays in crimes like this. We recently encountered one example that is super simple, but has fooled many victims. This specific phishing email looks like a newsletter from a pornographic website, and the email reads something like *"...you are receiving this because you have recently subscribed to our newsletter, if you want to unsubscribe click here..."*. If you click on the link, malware is downloaded to your computer. Many people naturally try to unsubscribe, because they don't want such emails showing up in their inbox, where they could perhaps be seen by a spouse or employer. In this specific example I think it really doesn't matter if you receive it as a corporate employee or on your private PC, as you will likely feel the same urge to unsubscribe immediately. Today we are very aware of phishing emails, but still they are sometimes able to fool us due to excellent social engineering skills.

F-SECURE AND OMXH25, INDEXED 2010



Source: Thomson Reuters

Phishing e-mails can fool us sometimes due to criminals' social engineering skills

Phishing emails can be sent out to thousands of addresses with minimal effort and even if 99.99% of the recipients reject them, criminals can still make a lot of money from the significant number who do not.

JT: What is driving cybercrime? What are the criminals after?

SK: Cyber criminals are driven by a desire to make money. For state-sponsored players there are two drivers; first, *intelligence* to gain access to other governments' data and second, lately we have seen that more of these players are actually sometimes also after money. Taking the WannaCry ransomware cyberattack as an example, North Korea has been pointed out as the force behind it. They did not aim for intelligence or sabotage, they simply wanted money to prop up the sanctioned and embargoed North Korean economy. This was the first time that we saw a state-sponsored player acting like an ordinary criminal. Even though 150 countries were affected by WannaCry, the malware was not financially successful. One reason for this was surely the poor design of the interface for receiving ransom payments.

Malware can really cripple large organisations

When thousands of corporates end up with encrypted files, however, the damage to the global economy is substantial. As an example, the NotPetya cyberattack cost A.P. Møller-Mærsk around USD 300m. Malware can really cripple large organisations.

JT: Who are the most significant players in cybercrime? Lone hackers, networks with a political agenda, organised crime or state-sponsored players?

SK: The attackers are either online cyber criminals who are motivated by financial gains or groups with an ideological agenda – so called "hacktivists" who have a cause justifying their attacks. As an example, they may believe that nuclear power is bad for the world, and would then start to target nuclear power plants to sabotage them. A third category is state-sponsored players, who are generally not driven by money or a cause, but instead by a political agenda or simply modern espionage.

The vast majority of hackers are online criminals

The vast majority are online criminals who are motivated by money. In this group, you have both lone wolves and networks of hackers. It is often hard to determine whether someone is acting alone or not. Targeted attacks against specific organisations make up a minority of the attacks, but they too are constantly increasing.

JT: How well prepared are large corporates to withstand cyberattacks?

The most vulnerable targets are probably companies that were historically "offline industries"

SK: It varies tremendously from company to company. Some companies and industries are far better equipped to face cyber threats. One example of such is the financial industry, whose major players are typically well prepared. The most vulnerable industries are probably those companies that traditionally were in "offline industries". As the world is digitalising, companies realise that they need to adapt and have an online presence. When those companies are introduced to a digital reality, they typically do not have a lot of understanding of the risks online. They are often immature in their cyber resilience, making them easy targets for hackers.

JT: How can large corporates protect themselves from cyberattacks?

The biggest issue today is that the capability to detect an attack is actually lacking in a majority of large corporates

SK: I think today cyberattacks are becoming more and more sophisticated and with the volumes continuously growing, people start to understand that there is no such thing as 100% protection. You cannot with 100% certainty protect your company. This means that you cannot be entirely sure that you will be able to stop an attack. If the attackers are capable and persistent enough, they will find a way to get in. If you cannot stop them, you need to have the capability to detect an attack. The biggest issue today is that the majority of large corporates lack this capability.

As an example, let's say that you have a room with a very expensive painting that you want to protect. Then you probably have a very secure door and lock for the room. If you translate this to the IT business, you could say that the door represents the firewall and the lock is the anti-virus software. Criminals will eventually figure out how to get through your door and will find out what kind of lock you have and how thick your door is. With enough practise, they will get into the room where the painting is. However, if you are clever, you also have an alarm system in place. The alarm system will not prevent them from entering the room, but it will recognise and notify you that there is an intruder. In the past, companies have relied mostly on the door and lock, but today they are starting to understand that it is no longer enough. They need the capability to detect an intrusion as well, because if they only rely on trying to keep hackers out and they eventually get in, the consequences could be devastating. You need to be prepared for the worst. This is our biggest investment area right now at F-secure, and we are seeing a growing trend of our customers subscribing to our Rapid Detection Service which is designed to detect stealth mode attacks that our customers could not prevent.

Once you have detected that you have an intruder it is important to know how to respond to the attack

Once you have detected that you have an intruder, it is important to know how to respond to the attack. Companies today invest a lot of money in managing a proper response and in cyberattack processes.

One service that we offer at F-secure provides companies with "red teamings" which are targeted attack simulations – our customers basically ask us to hack them. The purpose of this service is to test their cyber resilience to see just how protected they are. We do several of these every year at many of the world's largest companies and so far we have had a 100% success rate. There has not been a single case where we did not manage to penetrate a company. That is actually quite scary and the customers often have no idea that they have been hacked. After the red teaming exercise is over, we usually sit down with the company's senior management. When we tell them that the exercise is over they usually respond by saying "...great, so nothing happened?" And we then have to tell them that the situation is actually quite the opposite. Their biggest problem is that they do not know that we hacked them. We tell them how we got into their system so they can make changes and improve security. This is a real eye-opening experience for many companies.

When we get a red teaming assignment, we act like cyber criminals targeting the specific company

When we get these assignments, we act like cyber criminals targeting the specific company. There is no general weakness that applies to most companies, like obsolete systems or defences. There is a myriad of explanations behind a successful hack on a company. Sometimes it is hard to penetrate the business online, so in that case we also try to penetrate the company physically. If you get physical access to computers, hacking into them becomes much more easy. For example, one thing we can do is to install radios in the reception area which copy information from the wireless key cards that employees use. When we have this information, we gain access to the facilities, and then it is very easy to get in and eventually find a computer or server room.

JT: What are the biggest cybercrime threats to corporates and society today?

SK: One thing that I find very worrisome is when attacking tools are being developed by nation state actors such as the NSA, who have access to massive resources. The tools that nations are developing for themselves are ending up in the hands of criminals, which makes the criminals far more competent than they should have been. As we saw last year, code developed by the NSA was leaked, and was eventually used in the WannaCry ransomware attack.

The flipside of digitalisation is that everything online is potentially accessible to cyber criminals

For corporates and societies, I would say that with digitalisation there are huge opportunities but also big threats. The world is becoming much more vulnerable and the impact of cyberattacks can be devastating. The flipside with digitalisation is that everything online is potentially accessible to cyber criminals.

Snapshot: WannaCry and NotPetya

The most headline-grabbing cyber attacks of 2017 which brought cybercrime firmly into the eyes of the general public were 1) the WannaCry ransomware, which disrupted business globally, caused major disturbances for the UK National Health Service and could incur total costs of up to USD 4bn; and 2) the NotPetya malware, which destroyed data for Ukrainian government functions, infrastructure and companies, causing collateral damage worth 4-10% of EBIT for global corporates like Mondelez, FedEx and A.P. Møller-Mærsk with operations in the Ukraine.

WannaCry was a ransomware cyberattack, encrypting data and asking for a ransom payment to release it

WannaCry: North Koreans looking for cash?

The malware WannaCry started to spread across the world in May 2017. It is a ransomware, which means that after infecting a computer it encrypts its files, making them impossible to access for the user, and demands a ransom payment in Bitcoin in order to decrypt the files. The ransom payments demanded were USD 300 per user within three days or USD 600 within seven days.

SCREENSHOT OF WANNACRY RANSOM DEMAND ON INFECTED COMPUTER

Source: Wikipedia

The Windows vulnerability used in WannaCry was discovered by the US NSA, leaked and sold on the black market

The virus exploited a vulnerability in Windows implementation of the Server Message Block protocol which is a program that helps various nodes on a network to communicate. Microsoft itself had discovered the vulnerability a month prior to the attacks and had released a patch, but many systems were not updated and the vulnerability remained in place.

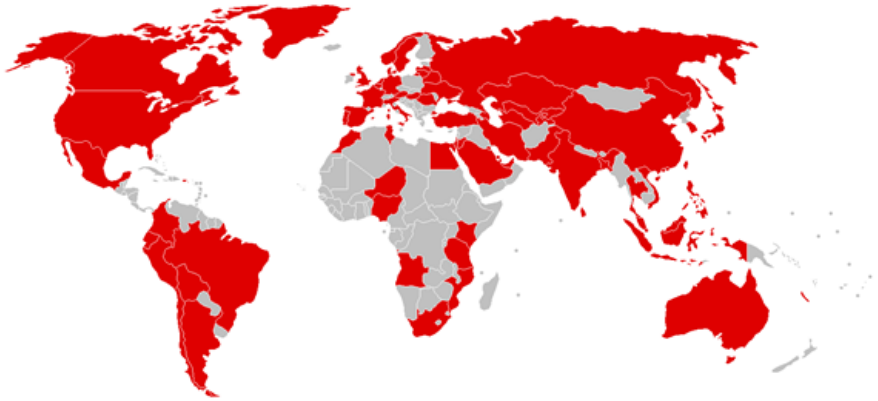
The US National Security Agency (NSA) also discovered this vulnerability, but instead of reporting it, it developed code to exploit it, EternalBlue and EternalRomance. This code was later leaked by hacker group Shadow Brokers, sold on the black market (the dark web) and subsequently used in the WannaCry malware.

Nordea

WannaCry caused massive disruption, including to the UK National Health Service

WannaCry infected over 230,000 computers in 150 countries, the four most affected countries being Russia, Ukraine, India and Taiwan, according to cybersecurity firm Kaspersky Lab. It affected many national important high-profile systems such as the UK's National Health Service (in turn affecting up to 70,000 devices, including MRI scanners, blood storage refrigerators, and theatre equipment) and Russia's railway system. Car maker Renault-Nissan and Spanish telecom operator Telefónica were among the large corporates affected. Total economic losses from the WannaCry attack are estimated to range from a few hundred million USD to USD 4bn globally.

COUNTRIES INITIALLY AFFECTED BY WANNACRY



Source: Wikipedia

Spread of the malware was stopped by security patches

The spread of the malware was essentially stopped after four days through distribution of emergency security patches from Microsoft and certain other defence initiatives.

North Korea has been held responsible by several major governments but denies any involvement

The virus has been linked by the cybersecurity firms Symantec and Kaspersky Lab to the Lazarus Group, which is a hacker outfit connected to the North Korean government, believed to be responsible for the cyberattack on Sony Pictures in 2014 and an attempted fraudulent withdrawal of USD 1bn from the central bank of Bangladesh in 2016. The governments of the US, UK, Canada, New Zealand, Australia and Japan have publicly named North Korea as responsible for the WannaCry cyberattack, while North Korea denies any involvement.

NotPetya: Pretending to want cash but only out to wreak havoc

NotPetya malware released in the Ukraine through an accounting software program update

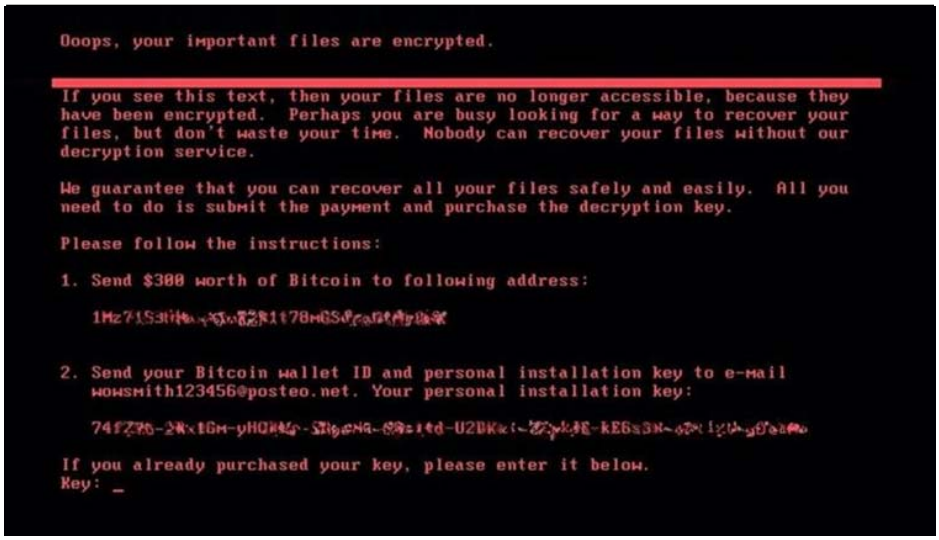
In June 2017, another major cyberattack hit the Ukraine and rapidly spread worldwide. The malware, originally thought to be one known as Petya and similar to the WannaCry ransomware released a month before, originated from an update of a Ukrainian tax accounting package called MeDoc, which is the main accounting option for Ukrainian businesses, used by 90% of domestic firms. MeDoc provides periodic program updates through an update server – this was hacked and instead delivered malware to target computers.

NotPetya asked for ransom payments but destroyed data or kept it encrypted – intended to cause damage rather than make money

Just like with the WannaCry cyberattack, infected computers showed onscreen messages asking for ransom payments to be paid in Bitcoin in order to retrieve encrypted data. But this malware never released any data, instead keeping encryption in place, destroying data and spreading the malware to additional connected computers. The malware was hence renamed NotPetya, to highlight the distinction from Petya, which was actual ransomware.

Nordea

SCREENSHOT OF NOTPETYA MALWARE WITH APPEARANCE OF RANSOMWARE



Source: Wikipedia

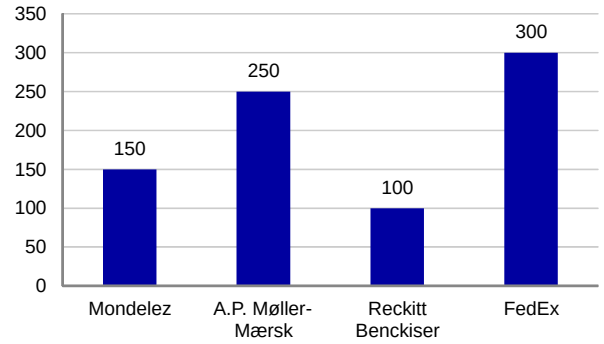
Major disruption for Ukrainian government functions and critical infrastructure

The NotPetya malware was released on the eve of Ukraine's Constitution Day, a public holiday celebrating the approval of the Ukraine's constitution on 28 June 1996, when most government offices would be empty. It affected several government ministries, banks, metro systems, TV channels, utilities, infrastructure like Kyiv and Borispol airports, Ukrtelecom and the other telecom operators, the postal service, and Ukrainian Railways, in addition to bringing the radiation monitoring system at the Chernobyl nuclear plant offline. Ukraine's electricity company went offline but was able to continue generating electricity.

Ukraine, CIA and UK MoD blame Russia, which denies any involvement

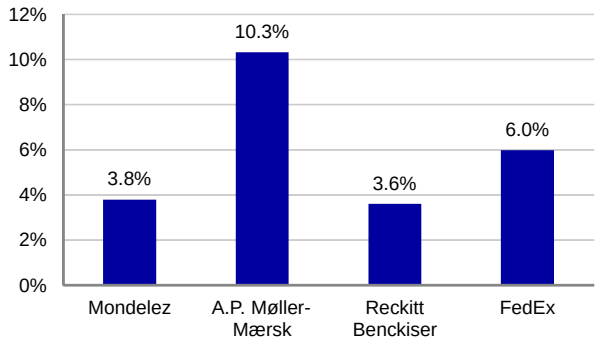
The Ukrainian government stated after a day that the attack had been halted, and on the day after, the Security Service of the Ukraine (SBU) claimed that the cyberattack had been launched by the same perpetrators who in December 2016 attacked the Ukrainian financial system as well as transport and energy infrastructure, implying that Russian special services were behind it. The US Central Intelligence Agency and the UK Ministry of Defence have declared Russia responsible for the NotPetya attack, while Russia has denied any involvement, pointing out that Russian systems were also impacted by the attack.

2017 CYBER ATTACK COSTS, USDm



Source: Companies data and Nordea Markets

2017 CYBER ATTACK COSTS, % OF EBIT



Source: Companies data and Nordea Markets

Global corporates suffered collateral damage worth USD 100-300m, ie 4-10% of EBIT

Over 80% of companies affected by NotPetya were from the Ukraine, but global companies were also affected by the attack through their operations in the Ukraine, for many of them with sharply negative financial consequences. Global corporates hit by data losses and disruption include Mondelez, A.P. Møller-Mærsk, Reckitt Benckiser, COFCO Group, Saint-Gobain, WPP, DLA Piper, Merck & Co, Nuance Communications and FedEx. Some have specified the financial damage they suffered, which we illustrate in the graphs above. Damages range between USD 100m and USD 300m, corresponding to 4-10% of annual EBIT.

Interview: Cyber criminals are stepping up their game. How about you?

We interview two Nordea top IT security profiles, **Tapio Saarelainen**, Group Chief Information Security Officer, and **Stefan Jäschke**, Head of Technology Information Security, on what specific cyber threats banks face, if banks are more exposed than other corporates, how banks can be protected, and what banks can do to protect themselves and their customers.

Tapio Saarelainen

Stefan Jäschke

Nordea

Hacktivists aim to "cyber-punish" organisations with differing ideological values

JT: We hear a lot in the news about cyberattacks against corporates these days. How big an issue has this become, and how has it evolved compared with five or ten years ago?

TS: In recent years, we have seen a rapid increase in cyberattacks targeting corporates. CEOs now view cybersecurity as a serious threat against their companies – for many large companies, this is the no. 1 threat they face.

We also see that attacks are getting more sophisticated; cybercriminals are getting more competent and organised. This means that they now use more advanced, complex attacks to infiltrate systems. Corporates, including banks, and organisations are under constant probing and attempted cyberattacks, and the real challenge is to identify which of those attacks that can actually harm the organisation.

SJ: In fact, ten or even five years ago is completely incomparable to the situation today – companies and societies are more aware of cyber-related threats, which has led to improved security measures. But at the same time IT environments have become more complex and more critical for the success of companies and organisations. That makes them more vulnerable – especially to the more aggressive and sophisticated attacks we saw recently.

An example of this was last year's DDoS attacks. Since then the capacity of these attacks has doubled in just one year, and the sheer force behind these attacks is continuously increasing.

And we see the general trend of using cyberattacks against critical infrastructure, which has become a geopolitical issue. The shockwaves from such attacks can seriously hurt businesses as collateral damage.

JT: What are the typical cyberthreats faced by large corporates today? Which kinds of attacks or crimes can they expect?

SJ: All kinds of attacks, basically whatever you can think of, could potentially happen. If we look at it from a more systematic approach, we have state-sponsored players, and we have organised criminals. Both have the capabilities and resources, and conduct increasingly sophisticated and complex attacks mainly motivated by financial gains.

We also expect a further increase in activity from the groups of people that are called hacktivists. There is a trend that when companies publicly declare viewpoints, some people with differing values will "cyber-punish" such an organisation. The motivation behind the attack is then to harm the reputation of the targeted organisation. The hacktivists are very ambitious and their behaviour is harder to predict.

Another trend is threats from insiders. By that I mean that people with legitimate rights to act within the computer systems of a company can be exploited or blackmailed to harm their employer. The better security controls put in place by the company, the more attractive it becomes to try to infiltrate a company via its employees. This is done by information gathering on employees to take advantage of their accesses and privileges with the aim of stealing money or confidential information. In such a situation, some employees may succumb to those threatening them. It is also a threat that I foresee will grow.

TS: However, many hackers are also helping companies to find vulnerabilities, but the problem is that hacktivists, organised criminals, cyberterrorists and the state-sponsored players are, taken together, outnumbering these.

JT: Are there specific cyberthreats for banks?

TS: There are two typical main objectives when attacking a bank – to destroy its reputation and/or to steal money. We have seen several incidents where criminals have attacked weaknesses in banks' SWIFT connections. They have not been able to breach the SWIFT global intra-bank payment system itself, but have exploited the vulnerability in its interface with that particular bank to steal money.

Most of a banks interface is highly standardised, which is a specific threat and vulnerability for banks

SJ: Most of a bank's interfaces with the outside world, including with other banks, are highly standardised. SWIFT is just one example. These interfaces are a specific threat for banks, since they can be used by cybercriminals to steal money. This setup is very unique for the financial sector. I don't know many other industries that have this kind of standardised communication across the entire industry. *But banks can't just decide to stop using these interfaces, so they need to be able to manage this risk and implement adequate security measures to protect their communication and data exchange infrastructure.*

Banks are an attractive target also for those players who want to act as cyberterrorists and cause chaos in society

I also think that people underestimate how critical banks are in terms of infrastructure. Just imagine if a major bank like Nordea were offline for 24 hours: people would not be able to receive payments, to use their cards, or to transfer money. That is an infrastructure problem, and therefore banks are an attractive target for those players who want to act as cyberterrorists and create havoc in society.

JT: How protected and prepared do you think Nordic large corporates are for the cyberthreats we see today?

Large Nordic corporates are generally in good shape because they are usually very disciplined in how they run their operations

TS: For most financial companies like Nordea, cybersecurity is a top priority and will continue to be so. I would say that the Nordic large corporates are in good shape, because they are typically very disciplined in how they run their operations. They have the basic security in good shape. However all corporates are in a competition with the criminals. Corporates constantly have to improve their systems, and taking care of the defence against cybercriminals requires quite significant activities and investments, in order for the company to remain in good shape.

That said, we should not forget that one-third of cyberattacks start with phishing emails with malicious links or attachments, and this is a real problem for many Nordic large corporates. There is a high level of trust in people in the Nordic societies, and many cybercriminals use this trust to take advantage of the Nordic corporates through social engineering.

When an attack happens, it is important that you are able to detect it in order to control the damage

SJ: I recently moved to Denmark from Germany, and I have also positively noted the high level of trust. Trust creates a great work environment, which I appreciate and enjoy. But we need to balance between trustful and open-minded cooperation with others and a healthy risk awareness, especially when it comes to protecting our IT systems, data and customers against cybercriminals.

JT: Are banks worse or better protected than corporates in general? Are banks potentially juicier targets for criminals?

I think it is fair to say that many other industries are not at the same maturity level in cybersecurity as banks

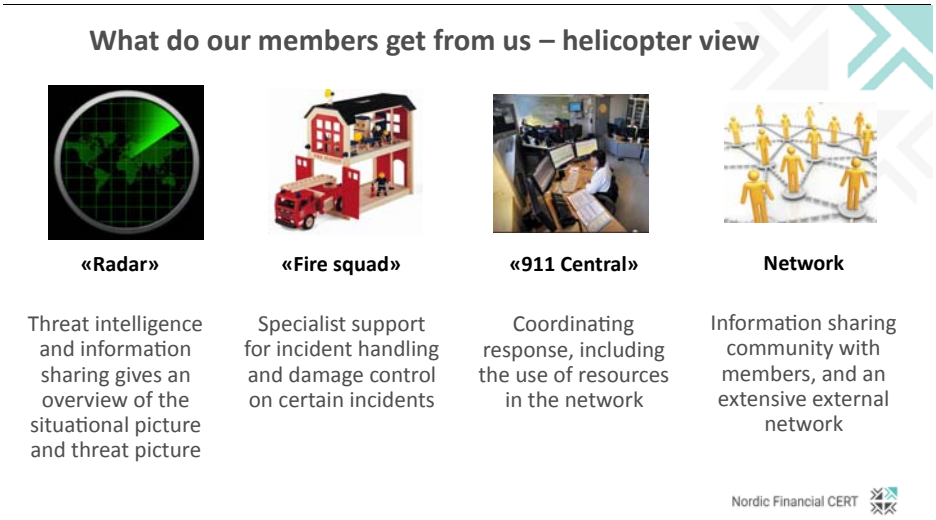
SJ: I would say so. But because of the fact that banks have been attractive targets for cybercriminals for some years now, banks have increased their protection, their detection methodologies and their cybersecurity tools. So I think it's fair to say that not all industries are at the same maturity level in cybersecurity as banks.

It is also worth mentioning that the Nordic banking industry last year established a new collaboration forum for Nordic banks, the Nordic Financial CERT, and Nordea was one of the founders. In this forum, information about cyberattacks is shared, and security incidents affecting more than one bank are coordinated. One of the main reasons for creating this organisation is that when joining forces, banks are a lot better prepared to fight cybercrime and protect customer assets. This is also a good way to help smaller banks to get more knowledge and a way for us in Nordea to contribute to a greater good for society.

Nordea

Nordic Financial CERT

NORDIC FINANCIAL CERT MEMBER BENEFITS SUMMARY



Source: Nordea

JT: What are the typical players behind cybercrime? Individuals, ideologically driven networks, organised crime, or state-sponsored players? What is driving them – what do they want?

TS: We see all of them. The drivers behind the ideologically driven networks' motivation are about ruining the reputation of the targeted company, because it does not align with their ideology. Organised criminals seek financial gains. State-sponsored players aim for espionage, sabotage, access to intelligence about individuals or in some cases just money.

Intelligence gathering is often done by state-sponsored players to gather information about their own citizens. In those cases, hackers attack companies to gain this information, but they don't cause any direct harm to the company itself. However, it is certainly not very nice for an individual to be subject to surveillance.

JT: What level of cyberattacks is Nordea facing on a daily basis? How has this evolved in recent years?

Nordea is constantly probed and attempted attacks are coming from players all around the world

SJ: Nordea is constantly being probed, and attempted attacks are coming from players all around the world. We handle these and continuously develop our capabilities to identify and stop these attacks.

But it is a tough game for two reasons. First, there are about four new severe software vulnerabilities published every day. When security patches are released, it is a race between patching exposed systems and the hackers trying to exploit these vulnerabilities in an attack. It is important to understand that cybersecurity is not a steady state that can be achieved - it is a constant race between having core protection measures in place to eliminate white noise, having a radar for new vulnerabilities, and continuing to patch and close them.

Cyberattacks against critical infrastructure can create shockwaves that seriously hurt businesses and infrastructure; such attacks can lead to companies suffering collateral damage.

The second reason is that in the midst of all this "white noise", there are sometimes severe sophisticated and complex attacks that must be detected. I like to compare cybersecurity and bank robbery. With cybersecurity it is as if somebody is trying to break into a branch office's entrance door constantly. In the beginning they use a hammer, but the hammer does not work so they go back and bring better tools. You can see them from the inside but there is little that you can do about it. If it was a real robbery attempt, you would call the police, but that is not possible when it comes to cybercrime. This situation limits the possibilities to act and challenges you to find other solutions. This is a challenge that many companies have, and I predict that the cooperation on cybersecurity between companies and governments will become much stronger in future.

JT: What can Nordea do to protect itself and our customers from cyberthreats? Is it more about software and systems, or processes, protocols and people?

We recommend bringing the cybersecurity and innovation teams together to make cybersecurity a part of the DNA of the company

SJ: Our approach to this in Nordea is that first of all, you need to have the basic security in order – especially when it comes to maintenance of the systems. It is shocking how often companies forget about these simple things. Secondly you should train your people, make them aware of the threats and get them to understand that security is not part of the problem but a part of the solution. I would also recommend bringing the cybersecurity and innovation teams together, to make cyber security a part of the DNA of the company. Last but not least, you need to have a team of real specialists in order to be on top of everything. You need to have great talents who are able to fight and defeat the most sophisticated attacks. And then you need to be prepared to step up your game all the time, because that is what the criminals do.

Snapshot: Equifax

In September 2017, one of the "Big Three" US consumer credit reporting agencies, Equifax, went public about getting hacked and suffering what could become the biggest data breach in history, with theft of sensitive personal information on 146 million US and 15 million UK citizens. So far, the incident has cost the company USD 439m (39% of EBIT) and cost the CEO, CIO and CIFO their jobs. It has led to as much as a 30% share price drop at the lowest point and hearings by US authorities as well as criminal and civil lawsuits have been filed against the company.

Equifax sells consumer credit and insurance reports to businesses

Equifax is one of the "Big Three" consumer credit reporting agencies in the US, along with Experian and TransUnion. It is a venerable institution, based in Atlanta, Georgia, and founded in 1899. It has over USD 3bn in annual revenue, over 9,000 staff in 14 countries, and is listed on the NYSE. It operates in the business-to-business sector, selling consumer credit and insurance reports and related analytics to businesses within, for example, retail, insurance, healthcare providers, utilities, government agencies and banking. Credit reports include detailed information on personal credit and payment history of individuals.

It was warned of vulnerability in March 2017, but security patch was not implemented

In 2017, Equifax suffered a massive data breach which could become the most expensive breach in history. The US Department of Homeland Security (DHS) alerted the company in March 2017 that it need to patch a software vulnerability in the application called Apache Struts, which Equifax used in a website that let consumers challenge entries in their credit reports. Equifax distributed the warning from DHS internally, requiring the patch to be implemented within 48 hours, but the patch was not applied. Later in March, computer scans done by Equifax's information security department failed to detect the vulnerability.

Hackers got into Equifax's system in May 2017, with massive data theft in July

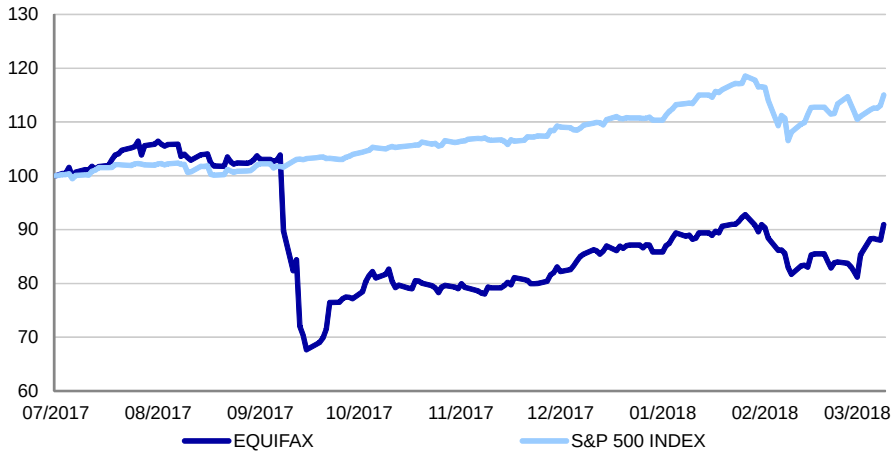
Word of Equifax's system vulnerability spread within hacking communities in March and April, and on 13 May, hackers gained first access to Equifax systems (according to what forensic analysis has shown so far), which also suffered from a lack of segmentation in the network design, potentially inadequate encryption of personally identifiable information and ineffective breach detection mechanisms. On 29 July, the company discovered a breach affecting sensitive personal information, including the social security numbers of 143 million US citizens. The hackers also had access to credit card numbers for some 209,000 US consumers.

After investigating the incident, Equifax reported in October that the total number of US citizens affected was nearly 146 million, along with over 15 million UK citizens.

Breach announced 7 September, followed by share price fall of 30% at low point

Equifax CEO Richard Smith was informed of the cyberattack on 31 July, briefed his senior leadership 17 August, and briefed the full board of directors 24-25 August, following which the company started to develop its response. The company publicly disclosed the data breach on 7 September, triggering a share price fall of up to 30% in the following months.

EQUIFAX SHARE PRICE AND S&P 500 INDEX, REBASED TO 1 JULY 2017 = 100



Source: Thomson Reuters

Estimated costs of USD 439m to date (39% of EBIT) could reach USD 600m

At the time of writing, Equifax's own guidance for total costs resulting from the breach is USD 439m (39% of 2017 EBIT), of which it expects USD 125m to be covered by insurance. Larry Ponemon of the research group Ponemon Institute, which tracks the cost of cyberattacks, has said total costs for Equifax could end up well over USD 600m, after taking into account the impact from government investigations and civil lawsuits against the company. This includes a US Justice Department investigation into possible insider trading, following three Equifax executives (including its CFO) selling nearly USD 1.8m of personal holdings of company share days after discovery of the breach, but more than a month before it was publicly disclosed.

The Equifax data breach is sadly a striking example of how a massive cybersecurity incident can have severe consequences for a company. Here are some of them so far:

CEO, CIO and CIFO resigned, and multiple investigations and lawsuits have been initiated

- Equifax Chief Information Officer, David Webb, and Chief Information Security Officer, Susan Mauldin, resigned 15 September
- Equifax CEO, Richard Smith, resigned 26 September, without receiving any bonus for 2017
- The Senate commerce committee has demanded an investigation
- The Senate finance committee has demanded an investigation
- The Federal Trade Commission has launched an investigation
- The US attorney in Atlanta has announced a criminal investigation of Equifax
- The Massachusetts attorney general has sued Equifax for financial penalties and profits disgorgement for "a shocking betrayal of public trust"
- Ex-CEO, Richard Smith, called to testify before the House energy and commerce subcommittee on digital commerce
- Ex-CEO, Richard Smith, called to testify before the Senate Banking Committee

Interview: If you are online, hackers will constantly scan for your vulnerabilities

We interview **Benjamin Särkkä**, Head of NITSIRT (Nordea IT Security Incident Response Team) at Nordea's Cyber Defence Centre, on potential new cyber threats, how criminals profit from cyberattacks, what companies can do if they are affected, and how they can best protect themselves against cybercrimes.

Benjamin Särkkä

EB: We see plenty of media headlines about cyber threats to large corporates. Is the number of threats growing, and are they becoming more serious? If so, why?

BS: I wouldn't say that the number of threats has increased dramatically, but companies have become better at identifying them. That is why there is more noise about it in the media.

But we are seeing more players in the field of cybercrime today. This is partly because those people who have good 'business models' for cybercrime, who are able to monetise the stolen information or whatever they do, have run their businesses for quite a long time now, and have been able to create 'subsidiaries' to their main businesses. This gives them capacity for more attacks.

Today, we live in a very connected world, which means that attacks could potentially have much more serious outcomes. If hackers were able to attack a hospital, it could actually be a matter of life and death, shutting down critical machines used in healthcare, or delaying surgeries.

There are a number of new physical threats emerging as the world becomes more and more connected

I am guessing there have already been – unreported – incidents like ships being electronically hijacked by hackers demanding money to give back control. Another scary example for the future is self-driving cars. Looking five to ten years ahead, the majority of new cars will probably be self-driving. Imagine being in a situation where someone takes control of your car, locks the doors, starts to drive towards the edge of a bridge and demands money to give back control. This is something that could actually happen, at least in theory. There are a number of new physical threats emerging as the world becomes more and more connected.

Societies are also vulnerable to cyber sabotage. What if someone figures out a way to disconnect a whole country from the internet? Imagine how much damage that would inflict. We have already seen one example of this in the Ukraine, when another country infiltrated and manipulated its internet and systems with multiple strains of malware. The effects included when the hacker group "Black energy" successfully turned off the electricity for millions of people in the Ukraine. The same group has been attributed with the malware NotPetya that accidentally infected A.P. Møller-Mærsk's systems last year, costing the company hundreds of millions of dollars, just because it happened to have exposure to a specific country.

You are not even safe from these kinds of crimes in your own home. If you are unlucky, someone could access and take control of your personal computer and blackmail you with the threat that your private photos and other data will be made public if you don't pay them. Hence, it's not only large corporates that are potential victims of cyber criminals.

EB: Who are behind the cyber threats, including major ones like the big WannaCry and NotPetya attacks in 2017? Individuals, hacker organisations, organised crime, or even state-sponsored entities?

BS: Taking NotPetya as an example, that malware is actually based on code developed by the US National Security Agency (NSA). The code strings named *Eternal Blue* and *Eternal Romance* leaked, became available in the black market, and have now been used by other state-sponsored entities to manipulate another country's network systems. In my personal view, this is almost as bad as losing the codes for nuclear weapons to criminals. There should definitely be more controls in place. These

cyberattacks may not have as severe an impact on society and the environment as nuclear missiles, but they can really do a lot of damage.

In general, it is very hard to track who is behind cybercrimes

In situations like with NotPetya, it is hard to identify and make a single person or organisation accountable for the crimes committed. In general, it is very hard to track who is behind cybercrimes, because anyone can buy a server and use tools that have been leaked on the internet. What we can see, however, is that cyber criminals are more active in some regions, Russia and Asia being two of them, and all governments are equally keen on cracking down on such activity.

To show the complexity of pursuing cyber criminals, say that you could find evidence that some specific malware comes from China and there could be a political motive for it to be used for example in an attack on Taiwan. It could be the case that someone is using that particular situation to cover their own tracks and motivation behind the attack.

Basically, there are three types of 'bad guys' online: state-sponsored hackers, organised criminals and cyber terrorists/ hacktivists

Basically, there are three types of 'bad guys' online: *state-sponsored hackers*, whose main focus is to cause damage to their enemy; *organised criminals*, whose main aim is to make money; and *cyber terrorists and hacktivists*, who are driven by ideology. The end goal for them is usually not financial, but rather expressing their ideology. One example of such an attack is when Visa and MasterCard decided to disable donations to *Wikileaks*. After the announcement, they experienced a massive attack from the hacker organisation *Anonymous*, which prevented them from doing any business at all for a period of time. These three groups all use the same tools but for different purposes.

EB: What are the cyber criminals' motivations? Money? Influence? Anything else?

BS: Some 20 years ago, there was an underground culture where hackers just wanted to show off their skills rather than make money on them, but I don't think it exists anymore. Today, these talents have moved on to ethical hacking, meaning that they look for vulnerabilities in companies' IT systems and are financially rewarded for finding them. Criminals are usually motivated by money and power.

EB: How can criminals profit from cyberattacks? Are some industries or companies more exposed to threats than others?

BS: The easiest way to profit from cyberattacks is to use ransomware, meaning that you take the victim's files hostage and demand a ransom payment in order to give them back. However, ransomware requires a lot of manual support and effort.

You can also sublet computers that you have been able to take control of as resources for others to use as a botnet. They can then do whatever they want with those computers such as send out spam e-mails or use them as an attack network.

Another way to make an income is to sell credit card and personal information that you have illegally acquired online. You can also be a malware writer, meaning that you create malware code and sell it to others to use in malware attacks. There is actually huge potential to earn money from cybercrime.

The new crypto currencies also enable another possible income stream. Let's say that you control one million computers in a botnet...you can then use it to mine crypto currencies. If you set this up, you basically get money straight into your pocket with minimal effort.

When it comes to espionage and sabotage, I think that all companies are equally exposed

I think that industrials and financials are easy targets among corporates, since they handle money flows and possess information that is traditionally attractive for criminals. Looking at espionage and sabotage, I think all companies are equally exposed. For example, the gaming industry has plenty of intellectual property, pharma companies have a lot of R&D projects, and the defence industry has a lot of patents and classified information stored. Basically, all companies today possess sensitive information of some kind or another. It would be devastating for them if it was stolen or leaked.

However, I would not say that the financial industry is targeted the most. We are very skilled in detecting and blocking potential attacks, and thus looking at statistics it may

look like we have encountered more attacks, but that is not necessarily the case. If you are on the internet, hackers will try to get in.

EB: What are the typical cyberattacks directed at large corporates? How vulnerable are corporates to such attacks?

BS: The most common ways to attack companies are via phishing and spam emails. Ransomware, for example, is often spread via phishing. Companies that have no control over incoming traffic face a big risk of a ransomware attack.

A company can also be attacked via its business logic system. Criminals can create fake invoices, put them into the system, and without anyone noticing, companies can accidentally pay out millions of dollars to a fake creditor.

There could also potentially be huge reputational damage from a cyberattack, which many companies, especially banks, are very vulnerable to.

The easiest and cheapest way to cause trouble for a company is to carry out a distributed denial of service (DDoS) attack, which floods the victim's network with traffic, causing it to eventually crash. DDoS attacks are hard to protect against but on the other hand don't cause much damage other than some downtime.

It is very uncommon that one specific company is targeted; often companies are collateral damage

It is very uncommon that one specific company is targeted; more often, companies face collateral damage, as in A.P. Møller-Mærsk's case. Cyber criminals constantly scan the internet for vulnerabilities, if they find something that a lot of companies have, they send the malware out to all of them. Hackers typically want to use as few resources as possible to get maximum payment.

EB: What can corporates do to defend against cyberattacks?

It is of utmost importance to have the basics of cyber defence in place

BS: As a corporate, you need to have the basics in place. This means that you have your IT systems patched, your passwords in order, knowledge about potential cyber threats and what kind of security programs your business needs, as well as how they work. If you can tick all these boxes, you are very safe. However, as your business grows, the 'basics' become more and more complex, and it is of great importance that you always have control over it. On top of the basics, you can have network segmentations, machine learning, etc. But none of that extra protection will help if the basics are not in order.

I would say that password policy and patching are the most important defences against cyberattacks.

EB: What can corporates who are victims of cyberattacks do in terms of damage control during an attack, and to recover afterwards?

BS: I think that one of the most important things to do after an attack is to inform all potential stakeholders of the incident, and to be transparent about what has happened and what is being done to fix it. It is also very important to have a plan for how to get back to normal, which you have prepared and practiced, so that you know what to do in such a situation and who is responsible for what, and so on.

EB: How big has the cybercrime threat become? How well-prepared are large corporates? Are they investing enough to protect themselves?

If a method arises that makes it possible to benefit from your vulnerability, it will be used

BS: If your business is connected to the internet, you are constantly being scanned for vulnerabilities, and you probably have one somewhere in your system. If a method arises that makes it possible to benefit from your vulnerability, it will be used. This applies not only to corporates, but to individuals as well.

It is very different from company to company as to how prepared they are, so it is hard to say on a general level. A large company is not necessarily more prepared than a small one; it is all about what security focus, priorities and culture you have.

Nordea

This page is intentionally blank.

Disclaimer and legal disclosures

Disclaimer

Nordea Markets and Nordea Corporate and Investment Banking are departments of Nordea Bank AB (publ) and its branches Nordea Danmark, filial af Nordea Bank AB (publ),Sverige, Nordea Bank AB (publ), filial i Finland and Nordea Bank AB (publ), filial i Norge.

The information provided herein is intended for background information only and for the sole use of the intended recipient. The views and other information provided herein are the current views of Nordea Markets and Nordea Corporate and Investment Banking as of the date of this document and are subject to change without notice. This document is not investment research. This notice is not an exhaustive description of the subject discussed or the product described herein, or of their related risks, and it should not be relied on as such, nor is it a substitute for the judgment of the recipient.

The information provided herein is not intended to constitute and does not constitute investment advice nor is the information intended as an offer or solicitation for the purchase or sale of any financial instrument. The information contained herein has no regard to the specific investment objectives, the financial situation or particular needs of any particular recipient. Relevant and specific professional advice should always be obtained before making any investment or credit decision. It is important to note that past performance is not indicative of future results.

Neither Nordea Markets nor Nordea Corporate and Investment Banking is, nor does either purport to be, an adviser as to legal, taxation, accounting or regulatory matters in any jurisdiction.

Nordea Bank AB (publ), Company registration number/VAT number 516406-0120/SE663000019501. The board is domiciled in Stockholm, Sweden.

Completion date: 16 March 2018, 12:05 CET

Nordea Bank AB (publ)	Nordea Danmark, filial af Nordea Bank AB (publ), Sverige	Nordea Bank AB (publ), filial i Finland	Nordea Bank AB (publ), filial i Norge
Nordea Markets Division, Equities	**Nordea Markets Division, Equities**	**Nordea Markets Division, Equities**	**Nordea Markets Division, Equities**
Visiting address: Smålandsgatan 15 SE-105 71 Stockholm Sweden Tel: +46 8 614 7000 Fax: +46 8 534 911 60	Visiting address: Grønjordsvej 10 DK-2300 Copenhagen S Denmark Tel: +45 3333 3333 Fax: +45 3333 1520	Visiting address: Aleksis Kiven katu 7, Helsinki FI-00020 Nordea Finland Tel: +358 9 1651 Fax: +358 9 165 59710	Visiting address: Essendropsgate 7 N-0107 Oslo Norway Tel: +47 2248 5000 Fax: +47 2256 8650

Reg.no. 516406-0120
Smålandsgatan 17
Stockholm

Nordea

Nordea Bank AB (publ)
Smålandsgatan 15 SE-105 71 Stockholm Sweden