FH SPOTLIGHT

15 February 2013

FLEISHMAN HILLARD
INTERNATIONAL COMMUNICATIONS

EU Cybersecurity Strategy:

Threats, challenges and opportunities for business

INTRODUCTION

Until recently, cyber-attacks seemed the domain for script writers of science-fiction films and geeky teenagers operating from their bedroom computers. In the last year, however, the impact of cybercrime on the economy and the business sector in particular has become clear.

Companies in Europe and across the world are losing billions of Euros due to business interruption, industrial espionage, extortion, counterfeiting, data theft and data manipulation. Cyber-attacks can also seriously tarnish companies' reputation in a single strike, reduce consumer trust and result in a loss of market share. Attacks against power plants and electricity grids endanger not only the economy, but also people's safety and health.

A noticeable increase in the number of cyber incidents and research quantifying the actual impact of cybercrime have propelled the issue to the top of the national and European political agendas:

- In the UK, the Ministry of Defence put the cost of cybercrime to the UK at over 13 billion Euro per year.*
- In 2012, 93% of large companies and 75% of small businesses in the UK suffered cybersecurity breaches.

Since there are currently only limited notification requirements and with companies not eager to report attacks, these figures are probably only the tip of the iceberg. Whereas legitimate companies are losing billions, cyber criminals have created business models which generate huge turnover and profit right across the world. Since cybercrime is one of the fastest growing forms of crime, it is clear that governments and the private sector have to catch-up to protect, prevent and to be able to react adequately to all kinds of cyber incidents.

Publications and speeches reveal that only a quarter of companies have the right tools, people and contingency plans in place to deal with the growing phenomenon of cyber-attacks. This paper focuses on the public affairs and practical threats, challenges as well as opportunities for companies in Europe in the light of the EU's first Cybersecurity Strategy presented in February 2013.

* http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

The Cybersecurity package launched by the European Commission will affect many sectors including energy, transport, financial services, healthcare and Internet.

For more information

Christiaan Weiland
Senior Policy Adviser

Jessica Henderson
Account Director

Fleishman-Hillard Brussels
Square de Meeûs 35
1000 Brussels

Tel: +32 2 230 05 45

christiaan.weiland@fleishman.com
jessica.henderson@fleishman.com

EU's first Cybersecurity Strategy

In February 2013, the European Commission published its first "comprehensive" cybersecurity strategy. The policy document aims to improve resilience and security of network and information systems, fight cybercrime, and enable an adequate response to a cyber disruption.

- **International cooperation** is an important element of the proposed policy mix, because cybercrime is not confined to a single jurisdiction. Moreover, a cyber-attack in one country can have a knock-on effect in others. It is a global problem in need for international solutions and cooperation. Therefore, the EU will reinforce cooperation with countries such as the US and Japan as well as international organisations including the OECD, OSCE, UN and the ITU. With the Executive Order on Cybersecurity signed by the US President in February 2013, *it will be a challenge to create a transatlantic level playing field for internationally operating companies.* The voluntary nature of compliance for US industry to update infrastructure is quite different from the approach proposed in the NIS Directive by the Commission.
- **Cooperation between the public and private sector** is regarded as vital with the public sector providing the right policy and legal framework and the private sector ensuring cyber resilience across its networks and protecting its assets and individuals. *It should, however, be a true partnership on an equal level to create the resources and processes to prevent, detect and handle cybersecurity incidents.*
- The **EU should not become too dependent on foreign technologies** and the strategy therefore calls for the development of an integrated European market for secure ICT solutions by hardware, software and service providers, operators, as well as on-line operating companies such as banks and retailers. To realise this, the EU will allocate R&D funding to develop cybersecurity products. *It will be interesting to see how this protectionism will stroke with discussions over a EU-US Free Trade Agreement.*
- The EU and private sector should work with **insurance** companies to develop harmonized metrics to calculate cyber insurance schemes with lower premiums for companies which have invested in cybersecurity.

On a national level much work needs to be done. In 2012, only 10 of the 27 EU Member States had a national cybersecurity policy in place and the tools to track down and fight cybercrime. *This has led to fragmentation and unequal level of protection of businesses and citizens.*

The opportunity for companies is that this new strategy aims at completing the Digital Single Market, ensuring that the virtual backbone of the European economy and society is strong, secure and provides a stable and prosperous on-line environment for companies, governments and citizens alike. This is crucial since most Europeans rely on digital technologies, networks and services for their work and their day-to-day life.

Who are the perpetrators?

Perpetrators of cyber-attacks exploit the virtual anonymity of the web and they can range from students on their home computers to individually operating criminals, organized crime rings, politically motivated groups, (rogue) states, or terrorists. Threats can also come from competitors, third party suppliers as well as disgruntled employees or employees who, by accident, lose mobile devices (laptops, USB sticks) or download malware, which compromise the company's cybersecurity system.

EU Network Information Security (NIS) Directive: manage risks & notify incidents

Alongside the Cybersecurity Strategy, the Commission also presented a Directive proposing measures to ensure a harmonized level of network and information security across the EU.

In cooperation with all stakeholders, Member States should ensure prevention, detection, response, repair and recovery attuned to the level of seriousness of a cyber incident.

The proposal singles out a number of sectors which should ensure a secure and trustworthy digital environment throughout the EU:

- **"critical" infrastructure operators** in energy (oil, gas, electricity), transport (airlines, airports, traffic management, rail, logistics), banking, and healthcare services (electronic medical devices in hospitals and electronic patient records).
- **"key" Internet companies** such as payment services (Paypal), social networks (Facebook, LinkedIn, Twitter), search engines (Google, Yahoo), cloud services (Microsoft, Cisco, Apple), apps providers, e-commerce platforms (eBay, Expedia, Amazon), video sharing platforms (You Tube) and voice-over-Internet providers (Skype).

The Directive stipulates firstly that the above sectors which operate in the EU need to adopt **risk management** practices which include risk assessments and taking technical and organizational security measures through "voluntary" industry practices.

Secondly, the center-piece in the Directive for companies in the above sectors is the obligation to **notify** national authorities of major security incidents that have "a significant impact". *It has to be avoided that market operators have double or even triple notification requirements under this Directive and other existing EU and national rules. The focus should in first instance be on resolving the problem and damage control instead of administrative requirements.* Notification requirements already existed for the telecoms sector and Internet Service Providers and this Directive extends them to other market operators. Following the notification, national authorities may decide to inform the general public. **Industry needs** to *ensure that a company's commercial interests are not harmed in the process.* The Commission believes that reporting requirements will stimulate companies to put appropriate security processes in place. Such processes are not only needed to prevent cybercrime, but also to deal with natural disasters, technical problems or human error.

For companies, the circumstances to notify cyber incidents might change over time and the Commission may issue guidelines and issue instructions, because the Directive comprises Delegated Acts by which it can be adapted. *This room for maneuver creates a degree of legal uncertainty.*

Small companies are excluded from the risk management and notification requirements, although *their size does not exclude them from being confronted with or causing a cyber incident with wider ramifications for the economy and the public.*

National authorities would have the power to **investigate compliance** by means of requesting information from a company on its cybersecurity and by carrying out a security audit. Violations of the Directive shall lead to sanctions which will be laid down by the Member States on a national level. *This implies that sanctions and the enforcement thereof can differ from Member State to Member State, which creates uncertainty for transnationally operating companies.*

Hardware and software companies are exempted from the risk management and reporting obligations. *It remains to be seen how this exemption can work effectively in view of possible liabilities for operators and some computer hardware coming onto the market which already has virus and other malware installed on it before the consumer has even unpacked and installed the equipment.* The Member States can, however, on a national level expand the Directive's scope to include more sectors. The Directive only sets minimum rules allowing EU countries to go beyond these requirements.

The Directive opts for "industry-led" **security standards**, certification schemes and security labels agreed within existing European standardization bodies with the relevant stakeholders. However, in order to avoid fragmentation of standards, the *Commission states that it might be necessary to draft "harmonized standards" on an EU level.*

Finally, companies have to assess what the cost of compliance and possible government investigations are. *Note that the Directive makes market operators liable regardless of whether they carry out the maintenance of their network and information systems internally or outsource it.*

Besides policy & legislation: practical steps to prevent & prepare

The vast majority of companies is unprepared to both prevent a cyber-attack and to implement a contingency plan in case it would be hit by such an attack. Part of the problem is that a company's cybersecurity function is often disconnected from business management, because security expenses are in general not regarded as an investment, but merely as cost. Yet the potential impact can be considerable: loss of turnover, reputational damage, a loss of jobs, fines for data breaches, litigation, and in the worst case bankruptcy.

Companies have to realize though that investing in cybersecurity, in terms of prevention and contingency planning, can be used as a marketing tool towards prospective clients. Therefore, either with in-house resources or with the help of external specialists, companies should:

- Carry out a **risk assessment** of the security of their IT infrastructure and awareness levels of staff.
- **Adequately secure** its IT infrastructure which includes regularly updating anti-virus software, securing firewall, routers, and switches, make staff change passwords regularly, and password-protect and/or encrypt sensitive employee and key financial data. Data on mobile carriers of staff (laptops, USB sticks, mobile phones) should be encrypted and protected against loss.
- Require staff to **notify the loss** of any mobile device containing sensitive information on the company or on any third party.
- Introduce a **company policy** prohibiting staff **to download software** that is not identified as safe and secure and which has not been approved for use by the company.
- Ensure 24/7 **monitoring and evaluating** the cybersecurity against both internal and external threats.
- Appoint a **chief information officer** to organise and manage cybersecurity and who will ensure compliance with the company's cybersecurity policy and applicable EU and national rules.
- **Train all staff** to make them aware of the risks and impact of cyber incidents, how to prevent them and how to deal with the consequences if a cyber incident occurs.
- Make cybersecurity a recurring item **on the agenda of the Board of Management** in view of the major financial, reputational and legal impact of a potential cyber incident.
- Organise a **cyber-attack exercise** to test the IT infrastructure and staff as well as to assess how the company would be affected.
- Prepare a **contingency plan** on how to deal with a cyber incident in terms of media relations, investor relations, dealing with affected people, insurance, legal issues and public officials to contact for notification purposes and assistance in investigating and prosecuting the perpetrators. It should also identify which people in the company should be in charge and act in case of an incident.
- Ensure **adequate insurance** for cyber incidents and its consequences, because traditional liability insurance does usually not cover them.
- Sign compliance **contracts** with **third party suppliers** (salary administration, cloud) which might be linked to your IT infrastructure for the processing of personal or financial data.

Forms of cyber attacks, cyber crime

The Internet has created phenomenal opportunities for the economy and society as a whole. It has, however, also facilitated a rapidly growing and lucrative underground economy. The 'value chain' of classic crimes in the off-line world has been shortened substantially in the on-line world; theft, deception and fraud can be committed by using computers and networks without leaving a room. In addition, a new range of cyber crimes has emerged including:

- **Botnets** of master and remotely controlled zombie computers (i.e. 'hijacked' home laptops, computers at universities or hospitals of which the users are unaware) are created to carry out on-line attacks. These botnets can distribute spam, phishing e-mails, and malware. They can also be used for **Denial-of-Service** (DoS) attacks, by which a high volume of traffic is generated to a particular website to hinder or block normal communications with the site.
- **Malware** is short for malicious software that is aimed at causing damage, disruption, and annoyance. It can contain viruses, Trojans, worms, keystroke loggers, and it can operate botnets. Although in the past a thorough IT knowledge was needed to develop such malware, organised crime has ceased the opportunity to develop, sell and distribute malware and this has become a thriving business for them.
- **Phishing** is in particular targeted towards banks or credit cards customers with the creation of websites or e-mails having a legitimate appearance. In fact, they are luring customers to fake websites where they have to confirm their passwords and other confidential personal and financial data. This data is then used to commit ID fraud and bank accounts are illegally opened and credit cards obtained.
- **Program fraud of the 'salami' type** is a carried out via a software program by which small amounts from accounts are automatically 'sliced off' by the perpetrator. If the process is repeated on a large scale, from a great number of accounts and over a considerable period time the sums siphoned off can add up to substantial amounts.
- On-line fraud, caused by malware, phishing and salami type program fraud are the biggest growing areas of cybercrime.
- **Pharming** is another tactic by which users are redirected from a legitimate website to a spoof site, which installs malware on the users' computer.
- **Scareware** is software which suggests that a user's computer is infected with a virus and offers to scan the computer. If a user accepts, the results can be disastrous.
- In addition, the Internet has also facilitated the distributions of **criminal content** which can be defamatory, threating, discriminatory, obscene or pornographic.