E-CRIME Policy Brief

Recommendations for non-ICT sectors

The E-CRIME Project (the economic impacts of cyber crime) is a three-year project that ran from April 2014 to March 2017. The aim of the project is to reconstruct the spread and development of cyber crime in non-information and communications technology (non-ICT) sectors from the perspective of its economic impact on the key fabrics (i.e., economic and social) and different levels of the European society, while also identifying and developing concrete measures to manage and deter cyber crime. (Website: http://ecrime-project.eu)

The ECRIME project focussed on mapping and mitigating the effects of economic cyber crime in five non-ICT sectors (retail, finance, transport, energy and health) by providing practical recommendations for implementation that will aid in reducing successful cyber attacks, and mitigate/minimise the impact of those that have an impact. These are presented here, divided into *sector-neutral recommendations* that cut across all sectors, complemented by *industry specific* recommendations.

General Recommendations

Better perimeter and service knowledge:

- Map the technology/asset chain the critical service depends on, and the impact of their disruptions.
- Map the interdependencies between networks, applications, and operating systems.
- Identify the servers containing sensitive data.

Prioritize Patch management:

- Define a patch management cycle (notification, testing, prioritizing, deploying, and monitoring).
- Prioritize deployment on critical infrastructures the critical service depends on.

Reduce complexity and opportunities:

- Reduce the complexity of networks, applications, and operating systems, to reduce also the "surface" available for attacks.
- Often, there are many applications within a company which perform similar functions; platform optimization will save time and resources spent to monitor and patch devices.
- Reducing the attack surface will reduce the opportunities for the hacker to find blind spots.

Strengthen internal collaboration:

- Avoid conflicts between business units (business owners, information technology, and security departments).
- Join skills and capabilities and work together to define and implement security requirements (i.e. CERT).

Increase education and training:

- Managers and employees don't know security policy related to the use of ICT infrastructures, PCs or mobile devices.
- There is a lack of training and exercises inside companies; this impedes the speed of the incident handling process.

Use of Honeypots (often underestimated):

- Traps set to detect, deflect or counteract attempts at unauthorized use of information systems.
- Such devices gather information regarding an intruder or attacker in the system.

Use of disinformation and deception:

- False repository with false intellectual proprieties or data not useful for the attackers
- It allows to identify the attack motives
- It allows also to make attackers to invest money without profit

Knowledge of your enemies:

- Monitor blogs/forum, media, chat to understand the sentiment around the company and if someone intend to attack your organization
- Monitor black market (i.e. services, malware, databases of credentials, emails and so on)
- Learn hacker operating model (pattern of attacks could be similar against different companies)

Hack yourself:

- Start to think and act as a hacker. In this way, you can really test the protection levels of your infrastructures and take the right countermeasures (penetration testing, vulnerability assessment …)

Strengthen integration and data traffic analysis:

- Data are usually collected but rarely analyzed and correlated. Usually only for forensics
- Big Data is the future and security must be confident with them to understand patterns, correlations and so on
- There are new solutions dealing also with behavioral pattern or "pattern of life" that describe the normal online activity of employees … (anomaly-based IDS)
- Integration of security platform

Build a security in-house capability:

- Security could not be transfer to external suppliers. It will create an uncomfortable dependency
- Companies are re-thinking security bringing back at home competencies and skilled resources

Limit the BYOD:

- Internet of things will enlarge the interactions with personal devices used also for work
- Clear policy shall be defined and strict controls put in place (mandatory authorisation process, password protection, control of risky application, limit the use of business application with sensitive data …)

Strengthen external architectures:

- SOC/CERT and Security departments must strengthen concrete collaborations
- It is impossible to have the overview of all the threats and vulnerabilities present in cyberspace
- The collaboration shall go one step further the signature of MoUs

Moving target architectures:

- The design of architectures could be done to shift the program's attack surface, also reducing it (Moving target)
- Different types of architectures based on microkernels and separation kernels

Sector Specific Recommendations

Finance

Individuals:

- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.
- Make use of, and show patience in the use of, two-factor authentication solutions operated with by high-street banks.

Companies:

- Players should take multiple measures to improve supply chain security, the scope of which should include the provision of supplies for financial institutions, and covering each point of the financial mesh – receiving and supplying, for instance, in case of cloud computing; this involves joint responsibility and systematic cooperation between actors.
- Set up regular/mandatory security tests and stress tests to improve network security and resilience.
- Plan a wide training campaign (Securing the Humans) targeting employees, with the intention of improving their awareness of cybersecurity issues and fraud schemes.
- Establish and enforce strict policies and procedures concerning wire transfer authorisation schemes.
- Perform by regular base ethical hacking activities especially from the internal side aimed to reduce such critical attack surface.
- In the case of outsourced systems check very carefully with the partner his security practices; negotiate a timely monitoring activity looking for evidence of the countermeasures applied.
- Update on regular basis the ATM operating system and middleware infrastructure; monitor against physical attacks to the ATM premises; install and keep updated antimalware/HIPS systems at the ATM premises; enable logging on ATM systems and send the logs to a central facility (to a dedicated SIEM); segregate the ATM infrastructure and monitor very carefully the connections from/to other networks.
- Collect and send to the SOC facility the “unconventional” logs (ATM, Mobile & NFC transactions, Social Media, Threat Intelligence) to cross-check and reduce the notification time of suspicious behaviours.
- Define adequate budget and strategies to train the SOC personnel aimed to keep them updated with the latest cybersecurity issues.

National/EU Level:

- Establish a European Security Guidebook to define a common set of guidelines for implementing common operative security standards regarding prevention, detection and response to security concerns, as well as for how to assess the cost-benefits of information security investments.
- Improve cybersecurity awareness among citizens and employees and build cybersecurity culture in general both within the sector and in the community
- Increase international cooperation in security intelligence and cybercrime investigation and prosecution.

Retail

Individuals:

- Use strong passwords with multi-factor authentication.
- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.
- Ensure that the organisation being relied on is compliant with the PCI (Payment Card Industry Data Security Standard).

Companies:

- Keep Operating Systems patched and all software updated, including anti-malware solutions.
- Implement end-to-end encryption to the payment process.
- Use a next-generation firewall that implements intrusion prevention system (IPS).
- Use a misuse detection approach to detect cyber-attacks, for example: make use of the set of attack signatures in the intrusion detection system.
- Adopt a security policy that trusts nothing (networks, resources, etc.) and no one (vendors, internal personnel, etc.), and then work by adding needed exceptions.
- Organizations that handle payment systems should comply with standards, such as PCI-DSS. These standards provide a widely accepted set of effective policies and procedures that aim to reduce the exposure of companies to cyber-attacks.

- Adopt new secure technologies such as the EMV payment card technology.
- Train internal personnel making employees aware of cyber threats, security rules, and threat actors TTPs (Techniques, Tactics, and Procedures).
- Be complaint with the PCI (Payment Card Industry Data Security Standard)
- Periodically conduct vulnerability assessment and penetration tests on your platform.
- Secure your infrastructure by adopting a layered defence model that puts together several components, including firewalls, intrusion detection systems, and physical network segregation.

National/EU Level:

- Encourage information sharing with respect to cyber intelligence and best practices under the platforms created by the NIS Directive.
- Improving awareness and education on cybersecurity especially among SMEs. Awareness programmes are explored in more detail in the following part of this report.
- Encourage taking out cyber insurance in a voluntary manner.

<u>Transport</u>

Individuals:

- Keep the number of devices used on travel networks (e.g. smart tickets) to a minimum.
- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.

Companies:

- Keep the Operating System patched and all software updated.
- Install an anti-malware solution and keep it updated.
- Train internal personnel making employees aware of cyber threats, security rules, and threat actors TTPs (Techniques, Tactics, and Procedures).
- Enforce a Corporate Email Security Policy that lets employees know what is allowed and what is not. The policy needs to include a general Email Usage Policy, an Email Retention Policy and of course an Email Security Policy.
- Use Anti-phishing and spam protection systems.
- Use host intrusion prevention systems in infrastructure. It is important to highlight that HIPS usually leverage known attack patterns, so-called signatures, to identify malicious activity. Signatures must always be up to date.
- Adopt the “Principle Least Privilege” for each application running on every system.
- Use a Firewall with proper security rules to monitor and control the incoming and outgoing network traffic. Periodically review the set of predetermined security rules.
- Protect end-points with Host Intrusion HIDS.
- Use Network Intrusion Detection Systems to monitor the traffic and enable the early detection of malicious activity.
- Periodically conduct Vulnerability Assessment and Penetration Testing.
- Be sure that software updates are digitally signed and transmitted through trusted channels.
- Adopt multi-factor authentication (i.e. “2FA based on mobile devices, smart cards, USB token) to access systems used to manage/store sensitive data.
- Use VPN connections to access systems for maintenance activities.
- Implement risk management in multi-stakeholder environments including external contractors and dependencies.
- Take security by design and by default as a principle in daily operation and taking cyber security insurance policies.
- Conduct risk test and participate in similar exercises. Annually review and update cyber security processes, practices and infrastructures.

National/EU Level:

- Promote more public-private collaboration at both national and EU levels.
- Facilitate a common EU approach (a comprehensive strategy and framework) to cybersecurity.

- Integrate and converge security efforts from other sectors
- Foster harmonized sector-specific cybersecurity standards

Healthcare

Individuals:

- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.

Companies:

- Plan training sessions to the management to increase the awareness about the criticality of the sensitive data treatment process and the associated costs in case of data breach. A successful campaign could reach the objective of increasing and optimize the budget available to the data protection tasks.
- Plan a wide training campaign (Securing the Humans) targeting employees to improve their awareness about cybersecurity issues.
- Maintain an updated map both of the asset where the sensitive data are stored and the flow and methods used for data management operations.
- Develop and keep update the policies about the security design requirements (roles and responsibilities, software applications, protocols accepted, encryption level, authorized connections available to partner and maintenance operations).
- Obtain from suppliers the security implementation measures adopted and double check they are compliant to the requirement stated in the organization security policies.
- Incorporate cybersecurity as a mandatory policy consideration in health care governance at board level.
- Increase information and best practices sharing within the health care agents and with other non-ICT sectors
- Initiate or improve the educational program for insiders and employees, in order to increase cybersecurity awareness.
- Increase investment in cybersecurity in the future deployment of safer devices and services, update legacy devices and services, and hire more ICT staff.
- Establish a cybersecurity team and internal procedures both to improve network security and to respond to cyber incidents.
- Encrypt sensitive personal data collected/processed by the sector at least to the storage level.
- Establish independent OSs (operating systems) in case of network breakdown or disruption.

National/EU Level:

- Increase information and best practices sharing within the health care agents and with other non-ICT sectors.
- Initiate or improve the educational program for insiders and employees, in order to increase cybersecurity awareness.
- To the extent that healthcare is under national control with respect to the relevant state, many of the other recommendations offered to companies would also apply to national-level governments.

Energy sector

Individuals:

- Take heed of awareness programmes and trust initiatives enacted by the relevant organisation.
- If relying on a wireless user interface, pay attention to whether the relevant company has behaved in a security-conscious manner in implementing the use of such devices.

Companies:

- Promote consumer awareness and education on the changes to the energy systems. This should be compulsory for energy companies due to the high risk of human weakness.

- Review the architecture of information systems: pay special attention in the segregation and monitoring ICT components related to Industrial Control Systems (SCADA & DCS).
- The energy industry is strategic: launch a cybersecurity awareness campaign tailored to the specific sector.
- Monitor remote connection activities and anomalies.
- Introduce cybersecurity requirements in the procurement process of SCADA/DCS systems.
- Perform security assessment within acceptance test of Industrial Control Systems phase.
- Enable a deep logging auditing process at the ICS premises.
- Perform a deep scrutiny of the risks coming from the introduction of the IoT devices in the network; isolate the networks connecting IoT devices from the main information system; check for an acceptable baseline and monitor anomalies.

National/EU Level:

- Set up a set of minimum sector-specific security standards at the EU level including mandatory security risk assessments, compliance with specific security certifications, and establish regulatory sanctions.
- Information sharing should be a policy priority by means of standardization and facilitation within and beyond the sector including other CII sectors across Member States and ICS-SCADA operators and incident handlers.
- Harmonize industrial security requirements among member states; the EC should facilitate agreement between member states regarding a minimum level of harmonization on security and resiliency requirements and standards.
- Promote consumer awareness and education on the changes to the energy systems. This should be compulsory for energy companies due to the high risk of human weakness.
- Establish a common approach for smart energy communication system design and integration, including creating communication standards and guidelines for a common reference architecture, technical and operational requirements for smart energy, remote updates and reconfiguration and a reference risk assessment framework and methodology.