Deliverable 8.2 – Practical sector guidance supporting technological advancements through sector specific crime-proofed applications

Deliverable submitted on 31 January 2017 in fulfilment of the requirements of the FP7 project, E-CRIME Economic Impact of Cyber Crime

Project Acronym	E-CRIME
Project full title	The economic impacts of cyber crime
Website	www.ecrime-project.eu
Grant Agreement	#607775
Funding Scheme	FP7-SEC-2013-1
Deliverable number:	D8.2
Title:	Practical sector guidance supporting technological advancements through sector specific crime-proofed applications
Due date:	31.01.2017
Actual subm. date:	31.01.2017
Contact:	
Authors:	Sten Mases, Joe Cunningham
Reviewers:	
Dissemination Level:	Public

Table of Contents

Summary

This deliverable presents an initial list of business and technological requirements for sector-specific, crime-proofed applications in the selected e-crime sectors – finance, retail, transport, healthcare and energy. These requirements are based upon the opportunities identified in WP7 and findings from WP2 and WP3. Special attention is given to privacy-by-design considerations. The final requirements will provide practical, sector-specific guidance on crime-proofed applications advancements, including the identification of key functionalities, and other technological counter-measures for the selected non-ICT sector.

This report is divided into four sections. The first section gives a summary of opportunities identified in earlier deliverables. The second section provides guidance on crime-proofed application advancements. The third section lists business and technological requirements per sector and the forth section covers the main principles of privacy-by-design.

As a result, this report contains practical guidance that can be exploited by organisations from the selected sectors who want to improve the security of their applications.

8.2.1 – Summary of opportunities identified in earlier deliverables

This deliverable purports to provide practical sector-specific guidance for the prevention and management of cybercrime to E-Crime's five non-ICT sectors by identifying relevant business and technological requirements for the crime-proofed applications associated with each sector. It aims to do this against the background of prior findings of the E-Crime project, thus demonstrating that those findings have practical manifestations and impact. It will help at the outset to have on the table an overview of some the results and findings of prior deliverables produced by the project. The salient work packages here are work packages 2, 3 and 7, and this section of the report provides an overview of them.

1. Findings from WP2

WP2 was largely taken up with primarily framework issues associated with the E-Crime project: the engagement with a number of basic, foundational tasks which need to be completed at the outset of the inquiry and prior to the pursuit of the remaining tasks of the project. These tasks included

(i) the completion of a fresh taxonomy of cybercrime, suitable for use in the remainder of the project;
(ii) a framework for measuring the impact of cybercrime, to be utilised especially in work package 6, where the economic impacts on selected EU member states of cybercrime are mapped;
(iii) a mapping of representative criminal and victim journey, against the background of the taxonomy provided.

Let us briefly examine these in turn.

The Taxonomy. The taxonomy distinguishes between different kinds of cybercrime on the basis of the aim of the criminal. There are four of these kinds identified: criminal online financial activity; activities causing the breakdown, interruption or incorrect operation of services or infrastructures; the theft or hijacking of processing capacity; and the theft of information, secrets, or other intellectual assets. For each of these there are a further four distinctions to draw in terms of four further salient properties of the criminal activity (thus delivering us in-principle sixteen kinds of category of crime): whether it is a targeted or a non-targeted attack; whether the target is of a high or a low value; whether it is aimed at consumers or companies/organisations; and whether it is a direct crime or an infrastructure crime.

Conceptualising the Impact of Cybercrime. The main contribution of WP2 here is the suggestion, taken up and operated with as part of the remaining work packages, that the costs of cybercrime should not be identified merely with the direct costs of cybercrime, understood as the monetary or equivalent losses to the victim of the crime, but also with a number of further consequences of crime. Direct consequences include the money withdrawn from victim accounts, the time and effort required in order to redress the

loss, as well as hidden costs such as the negative psychological effect on the victim. The further indirect costs, which it is the distinctive contribution of WP2 to draw attention to, include losses imposed on society by cybercrime, such as reductions in trust on the part of users; efforts required to clean infected devices; and defence costs, or monetary equivalents thereof, for example, in the form of the costs of staff training, security services, and security products.

Journey Mapping. A journey map, or script, is a sequence of causally related actions, groups of which can be divided into stages and indeed sub-stages, with the intention of providing a theoretically and practically useful model of the relevant phenomenon. WP2 provides eight journey maps from the perspective of the victim, and nine from the point of view of the perpetrator, focusing on a selection of cybercrimes, and including, in each case, a general journey map. For example, the general victim journey map divides the victim journey into three broad categories: a vector, which tracks the kind of crime to which the victim is subjected; an action or omission engaged in by the victim, such as use of a certain device; and the damages suffered.

2. Findings from WP3

WP3 purports to assess the existing cybercrime policies and countermeasures within selected EU member states. In particular, it purports to provide an overview of the interaction between and effectiveness of existing cybercrime technologies and technological trends; to assess the dominant policies and regulatory frameworks in the relevant member states, and at EU level, regarding cybercrime; and to engage in an ongoing monitoring of technology and policy developments during the lifetime of the project. Of these, it will be useful to summarise the review of existing cybercrime technologies and legislative frameworks.

Existing Technologies. WP3.1 develops a set of flexible criteria to test the usefulness and efficacy of existing cybercrime technologies, including criteria such as whether the technology prevents crime, identify crime. Reduce the potential impact of the crime, successfully identify the criminal, the technologies' usability and aptness to be integrated with existing business practices, and so on. There is then a selection of twenty representative examples of such technologies tested against these criteria, including access control, cryptographic and authentication technologies.

Existing Legal Frameworks. WP3.2 highlights two ways in which existing legal frameworks fall short. First, the Council of Europe Convention on Cybercrime has failed to attract signatories from all states, and as a result has failed to achieve the level of harmonisation that is desirable, and the Convention also allows for reservations to me made to it by signatories, further diminishing its effect. Second, existing legal structures do not maximise the effectiveness of cross-border cooperation, due to differing capacities, resources, and legal structures between member states. One recommendation made here is the promotion of standardised security exercises, awareness, and training in information security standards across member states.

3. Opportunities Identified by WP7

The main task of WP7 is to identify opportunities for the promotion of cybersecurity that currently exist within E-Crime's targeted sectors. A helpful way to summarise the opportunities identified is to look at a set of four dimensions identified in the final section of WP7, along which opportunities can be found for the development of cybercrime management strategies relevant to each sector.

The Political Dimension. The covers the opportunities available to governments to enhance cybercrime management in ways that would affect E-Crime's five sectors. First, there are opportunities relating to orchestrating the study of economic/sociological phenomena which can enhance our understanding of cybercrime, thereby indirectly strengthening the fight against it, for example: the study of the link between social and economic development with crime and security issues in a society rich with ICT infrastructures, the study of the link between cybercrime and cyberterrorism, and detailing a list of prominent ICT related threats to organisations and citizens. Second, governments can aid in the communication between organisations and states in order to help undermine cybercrime, for example by promoting cooperation at national, regional and international levels, promoting effective cyber diplomacy, and enabling effective communication between public and private sectors. A final opportunity is the orchestration of organisational and structural elements, for example the development of trust, preservation of the human right to privacy, and the earmarking of national and European budgets.

Legal Dimension. This covers the prevention opportunities available to legal enforcement agencies. These include, first, the definition of a legal framework compatible with international law and which enables collaboration between member states. Second, a clear and precise legal definition of 'whistle-blower' status, to ensure that individuals working for organisations at which there is known cybercrime occurring are able to speak out with legal protection. Third, the implementation of legal requirements which enhance the report of technical incidents. And finally, the up-dating of existing international cybercrime legislation in the light of the Cybercrime Convention of the Council of Europe.

Organisational Dimension. This covers the opportunities available to organisations for tackling cybercrime. It includes the development of strategies for the identification of vulnerabilities and risks in a given organisation; developing a culture of auditing, regulatory compliance, and a motivation on the part of employees to comply with security policies; and embedding security risk analysis into decisions that are taken regarding change in managerial processes.

Technological Dimension. This final dimension covers the opportunities available at the technological level for managing cybercrime. This includes ensuring that the applications produced are in accordance with the dictates of the security and privacy-by-design philosophies; producing security solutions that are user-centric and preserve functionality; and the development of confidence building measures.

8.2.2 – Guidance on crime-proofed application advancements

It is impossible to create usable applications that would be 100% secure against e-crime. The complexity of modern software systems always enables the would-be criminal to find some part that can be misused. The main question is how costly it is to successfully attack an application. In order to protect an application, it is enough to raise the security level high enough so that the cost of committing e-crime would be higher than the potential benefit. If attacking an application is too costly, then this application can be considered crime-proofed in our context.

From the defender's perspective it is important to optimise the costs for cybersecurity. If the risk related to e-crime is acceptable, then it is not necessary to spend resources for security. Unfortunately the risks relating to cyber threats are often underestimated due to optimistic bias [1]. People might understand that there are cyber threats, but they nevertheless find it unlikely that the accident will happen to them. All the following measures for improving security must start from ongoing security training raising the motivation to implement those guidelines properly.

In general, it is important to address cybersecurity issues in a holistic way. No software can be crime-proofed if users are not handling this software properly. In addition to the secure software and secure user behaviour secure hardware is also needed to ensure that a system can be secure. If one of the aspects of this holistic approach fails, then improving the other aspects might not help much. It is essential to understand that while this report focuses on the software side, the recommendations given here are not of much value without a holistic approach to cybersecurity.

In order to create crime-proofed applications, security must be built-in from the very beginning. Attempts to secure previously built insecure applications are already conceptually destined to fail. A proper application development must include security considerations already in the planning and design phase.

A classic software development life cycle can consist of multiple activities such as planning and visualization, requirement analysis, software modelling and design, coding, documentation, testing, deployment and maintenance [2]. In each part of the cycle it is important to consider security. There are many projects that describe the requirements at different stages of the SDLC (Software Development Life Cycle). In the next chapter there is a list of some common guidelines provided that can help to create crime-proofed applications.

Common guidelines

There are many projects that introduce the concept of security into the SDLC and provide guidance for developing crime-proofed applications. Some of them are well established standards, while others take more of an advisory approach. While some of them are more focused on one particular country, the guidance they provide is mostly universally usable.

Here is a list of some well-known projects:

1. ISO/IEC 27000 series (ISO 27001, ISO 27002…)
2. Common Criteria (ISO/IEC 15408)
3. OWASP SAMM (Software Assurance Maturity Model)
4. UK Cyber Essentials (CREST)
5. NIST Cybersecurity Framework and NIST SP800-53
6. ENISA National Cyber Security Strategy Good Practice Guide
7. Australian Department of State Development (DSD) Strategies to Mitigate Targeted Cyber Intrusions
8. U.S. Department of Homeland Security Cyber Resilience Review (DHS CRR)
9. ISACA COBIT (Control Objectives for Information and Related Technologies)
10. McGraw's Touchpoints
11. Microsoft Security Development Lifecycle
12. $(ISC)^2$ Common Body of Knowledge
13. The Center for Internet Security Critical Security Controls (CIS CSC)
14. HITRUST Common Security Framework (CSF)
15. HIPAA Security Rule
16. Payment Card Industry Data Security Standard (PCI DSS)
17. NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) Cyber Security

In the following sections there will be a short overview of some of the mentioned guidelines. For others, a reference is provided for further information. After the general overview concerning cross-sector guidelines, there will be sector specific guidance given for E-Crime's five areas of focus: the financial, retail, transport, healthcare and energy sectors.

1. ISO 270000 series

ISO/IEC standards are published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Those standards are probably the most well-known standards internationally. ISO/IEC 27000 series (also known as ISO/IEC 27k) comprise good case practice recommendations regarding information security. The following is a list of some relevant ISO/IEC standards:

- ISO/IEC 27000 — Information security management systems - Overview and vocabulary
- ISO/IEC 27001 — Information security management systems - Requirements
- ISO/IEC 27002 — Code of practice for information security controls
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27015 — Information security management guidelines for financial services
- ISO/IEC 27019 — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry

- ISO/IEC 27799 — Health informatics - Information security management in health care ISO/IEC 27002

ISO 27000 series is known to be adopted mostly by larger companies due to its overly costly and complex approach for many small organisations [3].

There are also many other ISO/IEC standards that might be relevant for a particular field, such as ISO/TR 13569 — Financial services - Information security guidelines.

2. Common Criteria (ISO/IEC 15408)

The Common Criteria (CC)[1] is an international program used by 26 nations in which IT products are certified against standard specifications (Protection Profiles). Protection Profiles represent the baseline set of security requirements for technology classes. [4]

In the U.S. the National Information Assurance Partnership (NIAP) is responsible for the U.S. implementation of the Common Criteria. NIAP also works with NATO and international standards bodies (ISO) to share Common Criteria evaluation experiences and avoid the duplication of effort[2].

In Canada the Communications Security Establishment (CSE) operates a product certification capability under this program, referred to as the Canadian CC Scheme.

In Europe, the national bodies of 10 countries are participating in the SOG-IS (Senior Officials Group Information Systems Security) agreement [3]. SOG-IS participants work together to coordinate the standardisation of Common Criteria protection profiles and certification policies between European Certification Bodies.

3. OWASP SAMM (Software Assurance Maturity Model)

The Open Web Application Security Project[4] (OWASP) is a worldwide not-for-profit charitable organization focused on improving the security of software. The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. Previously known as OWASP CLASP [5], it is now merged into OWASP SAMM.

OWASP also comprises many other relevant projects such as OWASP Top 10[5], OWASP ASVS[6].

[1] CC official site - http://www.commoncriteriaportal.org/
[2] NIAP official site - https://www.niap-ccevs.org/
[3] SOG-IS official site - http://www.sogis.org/
[4] OWASP official site - https://www.owasp.org/
[5] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
[6] https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

4. UK Cyber Essentials (CREST)

The National Cyber Security Centre of the UK has provided many types of guidance regarding cyber security.[7] A subset of that guidance is formalised under the name of Cyber Essentials.

The Cyber Essentials scheme is a cyber security standard, which organisations can be assessed and certified against. It identifies the security controls that an organisation must have in place within their IT systems in order to have confidence that they are addressing cyber security effectively and mitigating the risk from Internet-based threats. Whilst providing a basic but essential level of protection, the Cyber Essentials scheme enables organisations that believe they are practicing robust cyber security to benefit by making this a unique selling point thereby enabling business. Upon certification, they can then demonstrate to their customers that their data is adequately protected and that they take cyber security seriously.[8]

The UK is also enforcing Cyber Essentials by setting it as a requirement in some specific cases, e.g. every company supplying the UK Ministry of Defence is required to hold the Cyber Essentials certificate.

5. NIST Cybersecurity Framework and NIST SP800-53

The U.S. National Institute of Standards and Technology[9] (NIST) has created multiple relevant documents regarding cybersecurity.

NIST Cybersecurity Framework[10] focuses on *using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. Ultimately, the Framework is aimed at reducing and better managing cybersecurity risks*.[11]

NIST Special Publication 800-53 ("Security and Privacy Controls for Federal Information Systems and Organizations") provides a *catalogue of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk.* [12]

6. Other projects providing guidance

In the following table there is an additional list of projects that can provide guidance regarding cybersecurity.

[7] https://www.ncsc.gov.uk/guidance
[8] http://www.cyberessentials.org/background/
[9] NIST official site - https://www.nist.gov/
[10] https://www.nist.gov/cyberframework/
[11] https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf
[12] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Name of the project/framework	Reference, link	Focus area
ENISA National Cyber Security Strategy Good Practice Guide	https://www.enisa.europa.eu/ publications/ncss-good-practice-guide	General
Australian Department of State Development (DSD) Strategies to Mitigate Targeted Cyber Intrusions	http://www.asd.gov.au/ infosec/mitigationstrategies.htm	General
U.S. Department of Homeland Security Cyber Resilience Review (DHS CRR)	https://www.us-cert.gov/ ccubedvp/assessments	General
ISACA COBIT (Control Objectives for Information and Related Technologies)	https://cobitonline.isaca.org/	General
McGraw's Touchpoints	http://www.swsec.com/ resources/touchpoints/	General
Microsoft Security Development Lifecycle	http://www.microsoft.com/ security/sdl/	General
$(ISC)^2$ Common Body of Knowledge	https://www.isc2.org/cbk/	General
The Center for Internet Security Critical Security Controls (CIS CSC)	https://www.cisecurity.org/ critical-controls.cfm	General
BSI (British Standards Institution) PAS (publicly available specification) 555 Cyber security risk. Governance and management. Specification	http://shop.bsigroup.com/en/ProductDetail/ ?pid=000000000030261972	
HITRUST Common Security Framework (CSF)	https://hitrustalliance.net/ hitrust-csf/	Healthcare
HIPAA Security Rule	https://www.hhs.gov/hipaa/for-professionals/security/index.html	Healthcare
Payment Card Industry Data Security Standard (PCI DSS)	https://www.pcisecuritystandards.org/ pci_security/standards_overview	Finance
NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) Cyber Security	http://www.nerc.com/pa/ Stand/Pages/CIPStandards.aspx	Energy

Table 1 - list of projects providing guidance regarding cybersecurity

Sector-specific guidelines

In this section the sector specific guidance will be given for the five Non-ICT focus sectors of the E-Crime project; the financial, retail, transport, healthcare and energy sectors. We will give specific guidance on how applications can be designed, tested and assessed, and deployed in a secure way.

1. Financial sector

The financial sector is a very attractive target for cybercriminals. Financial technology, also known as FinTech, focuses on finding new ways to connect financial institutions and technology [6]. Therefore, it is essential for the financial sector to implement good security practices from the very beginning of the software development life cycle.

In the development phase it is beneficial to bring out specific use cases (a description of how the user can use the application for specific tasks) that are expected from this application. For example, there can be a description how a user logs in to an online bank and performs a transfer to another account. It is also a good idea to specify misuse cases – specific actions that the user should not be able to do. For example, normally a user should not be able to make a transfer worth millions of euros while having only a hundred euros in his/her account.

In the testing and assessing phases all those use and misuse cases defined in the development phase should be assessed to ensure that the application enables all the use cases and restricts all the misuse cases from happening. In the testing and assessing phase it is useful to look at sector-specific victim journeys that are brought out in WP2 of the E-CRIME project. Some examples of the potential sector-specific attacks are also given in the tool that is described in WP8.4.

In the deployment phase it is necessary to have a backup plan – i.e. if the deployment causes any problems, then an immediate roll-back to the previously working version of the application must be possible. It is good case practice to keep the newly deployed system running in parallel with the old system to ensure that the deployment was really successful. All deployed parts of systems should be thoroughly tested beforehand.

In addition to the cross sector cybersecurity guidelines, there are many that target specifically the financial sector, for example the following:

- PCI DSS provides helpful guidance for securing monetary transactions.
- ISO/IEC 27015 (“Information security management guidelines for financial services”) is specifically focusing on financial sector.
- ISO/TR 13569 Financial services - Information security guidelines.
- ISO 22307 Financial services - Privacy impact assessment

Financial institutions are often large organisations capable of enforcing extensive standards, such as ISO/IEC 27k series. Also they are often required to follow particular standards in order to comply with regulations and laws.

2. Retail sector

The retail sector has to face the risk of business interruptions, loss or theft of private data and also potential fraud. In order to manage the cyber risks successfully, it is beneficial to follow the general cybersecurity guidelines with a focus on privacy-by-design. It is also important to conduct proper security and performance testing for the new systems in the retail sector.

In the development phase it is helpful to bring out specific use cases (descriptions of how the user can use the applications for specific tasks) that are expected from this application. For example, there can be a description of how a user logs in to an online shop, chooses a product and pays for this product with his/her credit card. It is also a good idea to specify misuse cases – specific actions that the user should not be able to do. For example, normally a user should not be able to add negative amounts of products to his/her virtual basket.

In the testing and assessing phases all those use cases and misuse cases defined in the development phase should be assessed to ensure that the application enables all the use cases and restricts all the misuse cases from happening. In the testing and assessing phases it is useful to look at sector-specific victim journeys that are brought out in WP2 of the E-CRIME project. Some examples of the potential sector-specific attacks are also given in the tool that is described inWP8.4. When testing applications in the retail sector it is vital to also test the processes from payment through to successful delivery.

In the deployment phase it is necessary to have a backup plan – i.e. if the deployment causes any problems, then an immediate roll-back to the previously working version of the application must be possible. It is good case practice to keep the newly deployed system running in parallel with the old system to ensure that the deployment was really successful. All deployed parts of systems should be thoroughly tested beforehand. Any third party add-ons should be handled with care as they are a common attack vector for cyber criminals.

3. Transport sector

The key cyber risks in the transport sector are the denial of service situations (both accidental and malicious). Physical asset damage or loss and transport e-ticketing fraud are also relevant risks in this sector. Concrete mitigation methodologies vary based on the type of transportation (e.g. air, sea, and land transport all have their distinct peculiarities). In general, it is a good idea to follow the general cybersecurity guidelines and make sure that there are backup plans ready in case of the unavailability of the service. For web-based e-ticketing services it is beneficial to follow OWASP guidelines such as OWASP SAMM and OWASP ASVS.

In the development phase of an application in the transport sector it is beneficial to bring out specific use cases (a description of how the user can use the application for specific tasks) that are expected from this application. For example, there can be a description of how a user buys an airplane ticket. It is also good idea to specify misuse cases – specific actions that the user should not be able to do. For example, a user should not be able to book connected flights where the layover time between the two flights is negative.

In the testing and assessing phases all those use cases and misuse cases defined in the development phase should be assessed to ensure that the application enables all the use cases and restricts all the misuse cases from happening. In the testing and assessing phases it is useful to look at sector-specific victim journeys that are brought out in WP2 of the E-CRIME project. Some examples of the potential sector-specific attacks are also given in the tool that is described in WP8.4.

In the deployment phase it is necessary to ensure an appropriate backup plan is in place. In the transportation sector it is essential that all the services would fail safely. That means that if the airplane navigation systems have a temporary error then the plain would not make any sudden changes in its path – instead it should notify the pilot and be able to rely on backup systems.

4. Healthcare sector

Healthcare specific cyber risks are a liability due to regulatory statutes and unauthorised access to confidential information. Therefore, in addition to following cross sector best practices for cybersecurity, special care should be given for implementing privacy-by-design concepts. Also it is useful to follow (or at least investigate thoroughly) guidelines specifically targeting healthcare such as ISO 27799:2008 Information security management in health using ISO/IEC 27002 and the HITRUST Common Security Framework (CSF).

In the development phase it is recommended to bring out specific use cases (a description of how the user can use the application for specific tasks) that are expected from this application. For example, there can be a description how a user logs in to their e-health system and views their medical information. It is also good idea to specify misuse cases – specific actions that the user should not be able to do. For example, a normal user should not be able to see medical information of other people.

In the testing and assessing phases all those use cases and misuse cases defined in the development phase should be assessed to ensure that the application enables all the use cases and restricts all the misuse cases from happening. In the testing and assessing phases it is useful to look at the sector-specific victim journeys that are brought out in WP2 of E-CRIME project. Some examples of the potential sector-specific attacks are also given in the tool that is described in WP8.4. In the healthcare sector it is essential to put extra attention into privacy-by-design concepts which are mentioned further in 8.2.4. It is also crucial to ensure that role management is done carefully so that users of the application can only do what they are supposed to do and nothing more.

In the deployment phase it is necessary to have a backup plan – i.e. if the deployment causes any problems, then an immediate roll-back to the previously working version of the application must be possible. Also, it is needed that the healthcare application dealing with life-critical functions would be very robust. Even in the case of a failure the system should be able to recover quickly without long delays. All deployed parts of systems should be thoroughly tested beforehand.

5. Energy sector

Energy sector specific cyber risks are a disruption to operations in the generation, transmission and distribution systems, and also cause physical damage and loss of intellectual property. Therefore, in addition to following general cybersecurity practices, it is beneficial to put in extra effort toward ensuring the security of SCADA systems as well as proper implementation of defence in depth. Also, it is useful to implement guidelines that are specific to the field such as ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.

In the development phase of the energy sector specific application, it is beneficial to bring out specific use cases (a description of how the user can use the application for specific tasks) that are expected from this application. For example, there can be a description how a user monitors a specific part of a power plant and switches it off in case of need. It is also good idea to specify misuse cases – specific actions that the user should not be able to do. For example, a normal user wanting to see his/her electricity bill should not be able to switch off a power plant. In the energy sector it is essential to use proper segmentation of the applications so that if one of the applications is damaged then it would not affect the work of other applications.

In the testing and assessing phase all those use cases and misuse cases defined in the development phase should be assessed to ensure that the application enables all the use cases and restricts all the misuse cases from happening. In the testing and assessing phases it is useful to look at the sector-specific victim journeys that are brought out in WP2 of E-CRIME project. Some examples of the potential sector-specific attacks are also given in the tool that is described in WP8.4. In the energy sector it is vital to test the security of the industrial control systems.

In the deployment phase it is necessary to have a backup plan – i.e. if the deployment causes any problems, then an immediate roll-back to the previously working version of the application must be possible. It is good case practice to keep the newly deployed system running in parallel with the old system to ensure that the deployment was really successful. All deployed parts of systems should be thoroughly tested beforehand.

8.2.3 – Business and technological requirements per sector

Different sectors impose different business and technological requirements for crime-proofed applications. In general, it could be said that business and technological requirements are strongly intertwined. While requirement areas are mostly the same, the business side focuses more on the operational management and business processes, and the technological side can be seen as the enabler for the business side. The exact technical requirements depend on the individual case, but general types of requirements can be observed that are characteristic for a specific sector. In this section we will first go over cross sector requirements and then at requirement areas across five focus sectors: the financial, retail, transport, healthcare and energy sectors.

Cross sector requirements

There are five focus areas addressed by the E-CRIME project: financial, retail, transport, healthcare and energy sectors. While all these sectors have distinctive characteristics, there are also many commonalities regarding different business and technological requirements. Those requirements include:

- Confidentiality and privacy of sensitive information, for example customer data, employee data, business know-how. Therefore, it is important to use privacy-by-design concepts.
- Integrity of data, such as access logs, customer data.
- Availability of services, including protection against denial of service attacks, timely backups.
- Business continuity – in case of a cyber-attack or other cyber incident it is essential to have necessary measures in place for timely recovery.
- Legal compliance – each sector has their own legal norms and regulations that any legal organisation has to comply with.
- Timely analysis of big data in order to make efficient management decisions.
- Network security implemented on the basis of good case practices (firewall, intrusion detection system, etc). If the networking part is outsourced, then the organisation which uses the service should ensure that the service provider is following good case practices.
- Honeypots and other deceptive methods to slow down potential attackers while learning about the emerging threats. Especially for larger systems, such as critical infrastructure.
- Following basic security concepts such as input validation and whitelisting.

Financial sector

Financial sector has to track different systems dealing with currency rates, loans, payments and other financial data. Any faulty (malicious or erroneous) change in the data can cause significant monetary losses as well as reputation damage for the financial organisation. Therefore, it is of utmost importance

to maintain the integrity of the data. The main business and technological requirements in the financial sector are as follows:

- Integrity of data is essential in the financial sector. Transferring or displaying wrong amounts can cause direct financial losses as well as serious reputational damage.
- Service availability is less critical for online transactions (where a 10-minute downtime can be left unnoticed by an ordinary customer), but more critical for card payments. Any delays in card payments can cause significant inconveniences for the customer.
- Confidentiality of payment data – loss of e.g. credit card data can directly cause financial losses.

Retail sector

The retail sector has many similarities to the financial sector as both have direct contact with money and are therefore an attractive target for cyber-criminals who are motivated by financial gain. [7]

- Integrity of data, e.g. payment information, information regarding the objects that are sold. Misinformation might cause significant monetary losses and customer dissatisfaction.
- Prevention of unauthorised duplication of digital data.
- Traceability of goods. For digital goods it is important to ensure nonrepudiation. For physical goods it is important to ensure timely delivery to the right location.
  It is also important to have an overview of the amount of goods in near-real time in order to maximise logistical effectiveness.
- Confidentiality of payment data – e.g. loss of credit card data can directly cause financial losses.

Transport sector

Transport sector covers a wide area of diverse systems. Traditional means of transport are constantly being improved and an increasing amount of transportation machines are being connected to the Internet. While new means of transport such as drones and self-driving cars are raising new privacy and safety concerns, the main sector specific business and technological requirements for the transport sector are still connected to tracking the payment for the transportation and the transportation itself.

- Traceability of physical goods in order to ensure timely delivery to the right location.
- Confidentiality of payment data – loss of e.g. credit card data can directly cause financial losses.

Healthcare sector

A characteristic trait for business and technological requirements in the healthcare sector is sensitive nature of patient data. In addition, faults in the healthcare systems can often have fatal results – i.e. not only monetary losses, but also human victims. Therefore, it is essential to ensure the safety of the patient as well as the confidentiality of sensitive information.

- Privacy and confidentiality – the healthcare sector is especially sensitive regarding privacy, because it handles lots of delicate information. On the one hand, it is important to keep the data private, but on the other hand it is needed to share the data with relevant authorities (e.g. doctors need adequate and timely information regarding their patients).
- Robustness of the system – healthcare systems should guarantee safety of the patients even if there are some bugs in the system or if the system inputs are faulty.

Energy sector

Energy sector is the basis for other sectors. The modern society is highly dependent on constantly available energy sources and disturbances in the energy sector can have devastating effects for all other fields. The main business and technological requirements in the energy sector include the following:

- Availability is the main concern. E.g. power shortage in cold climate can have deadly results.
- Optimising resources based on big data analytics. E.g. smart grid enables the management of large infrastructures much more effectively.
- APT – as the energy sector is one of the main parts of the critical infrastructure in every country, it is a likely an attractive target for foreign countries to be used in cyber warfare – e.g. the case of Ukraine where approximately 225 000 customers were affected by a cyber-attack [8]. Therefore, the defence in depth should be implemented vigorously.

8.2.4 – Privacy-by-Design and Cybersecurity in Non-ICT Sectors

We live in a world of smart phones, smart cars, tablets, apps, online shopping, and social media. The opportunity for companies, and indeed states, to collect, store, aggregate and disseminate personal information about their consumers and citizens has never been greater. Although this information will often be used to improve goods and services its existence raises many fundamental questions from the point of view of privacy and cybersecurity. What amount and what kinds of personal data is it proportionate for organisations to store and aggregate and how should the necessity of protecting consumer privacy managed? How are legal frameworks tailored to take into account the protection of personal data? The following report is split into three sections. §1 provides a more developed overview of these issues, with particular attention paid to the concept of privacy-by-design and how a commitment to privacy-by-design has been legally implemented in the US and Europe. §2 provides an overview of the design strategies which can be used to implement privacy-by-design. Finally, §3 offers an overview of how these considerations interact with the five non-ICT sectors on which the E-CRIME focuses.

1. Privacy-by-Design and its Legal Ratification

The Personally Identifiable Information (PII) of a user is any information about them which can be used readily, on else in conjunction with other information about the user, to identify who that individual is, determine their whereabouts, or make contact with them. Prime examples of PII include names, physical addresses, email addresses and telephone numbers, national insurance numbers, passport information, IP addresses associated with the user, the user's past locations, as well as digital media in which the user appears. Organisations are now collecting, storing, agglomerating, and disseminating more user PII than at any other time, and they are doing so in myriad ways. The protection of PII by organisations – that is, the provision for and practice of keeping PII secure and therefore private – is implicitly required by Article 8 of the European Convention on Human Rights, which provides a legal right to a person's "private and family life, his home and correspondence", and is required explicitly by Article 8 of the Charter of Fundamental Rights of the European Union, which requires "protection of personal data". How are organisations to go about protecting the PII they store and agglomerate?

One approach is simply to add PET components such as authentication protocols, end-to-end encryption, and private information retrieval software, on top of an existing system. However, it is now standard to require that privacy be built-into the design and implementation of a system [9]. The idea that organisations ought to be committed to proceeding in this way is known as *privacy-by-design* – a concept introduced by Ann Cavoukian in the 1990s [10]. Privacy-by-design can be understood as a set of norms or principles concerning the relationship between the protection of PII and the design and implementation of systems and applications, the purpose of which is to embed "privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle" where it is thought that this "is necessary to fully protect privacy" [11]. Cavoukian herself sets out seven foundational principles [10] for Privacy-by-Design: (1) that privacy strategies should be proactive and preventative, rather than reactive and remedial; (2) that the aim of securing privacy should be the default

setting of the relevant system – the user does not have to take out any action to ensure that it is secured; (3) that privacy is embedded into the design of the system – a part of its core functioning and not a mere add-on; (4) that securing privacy is consistent with the full functionality of the system; (5) that PII is kept end-to-end secure: data is to be securely collected, retained, and then destroyed when no longer needed, and all of this in a timely fashion; (6) that the organisation is operating in accordance with these objectives, and that this is independently verifiable; and finally (7) that the privacy interests of the user be ascribed paramount importance: strong privacy defaults, appropriate notices, and all of this in a user-friendly fashion.

Privacy-by-design does not provide a set of concrete methods for implementing the basic privacy-by-design idea: it is, rather, an abstract design philosophy. In §2 we will look at some privacy design strategies which can be utilised in the service of privacy-by-design, and this will make the idea more concrete. For now, privacy-by-design can be illustrated by considering a simple example. Suppose we wish to create a freemium game app for a mobile device, part of the functioning of which involves tracking and storing the user's real-time location, and which requires users to have a user-account with some associated bank/credit card-details. This app would involve the processing of (at least) two different kinds of particularly sensitive PII: real-time location and financial details. When designing the app, we could build-in the features of the app which involve processing the relevant PII whilst bracketing off considerations of privacy until the completion of the process – adding on the relevant PETs after we have a completed product. Taking a privacy-by-design approach would require us precisely not to bracket-off privacy considerations during the design process. Considering user privacy – which privacy enhancing strategies to use and PETs to build-in – should permeate the whole design process, from development to implementation to evaluation.

Privacy-by-design is a concept which has been taken up by law-makers in the US and Europe. Starting with the US, in March 2012 the Federal Trade Commission (FTC) published a report entitled *Protecting Consumer Privacy in an Era of Rapid Change* [12] which lays down a privacy protection framework the first component of which is a commitment to privacy-by-design. In particular, the framework includes the principle that: "Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy." [12] Although the framework is not legally binding, the FTC does intend the framework to be considered by the US Congress as it considers privacy legislation. However, the most substantial legal commitment to privacy-by-design is to be found in the European Union's General Data Protection Regulation (GDPR), adopted in April 2016 and due to come into force in May 2018. The GDPR is legally binding on all member states and it replaces the non-legally binding Data Protection Directive. The GDPR has scope over every organisation and individual based in the EU and, in an important step beyond the Data Protection Directive, applies to organisations which are based outside the EU, just as long as they process the PII of EU residents. It does not apply, however, to the processing of PII for law enforcement purposes or national security activities. The GDPR constitutes, amongst other things, a legal ratification of the concept of privacy-by-design: it requires all agents over which it has scope to abide by privacy-by-design norms. Because the GDRP applies to all member states of the EU and to many non-EU based organisations, it renders possible cross-border data agglomeration and transfer without the need for *ad hoc* agreements between organisations.

2. Implementing Privacy-by-Design

How should developers go about implementing the idea of privacy-by-design during the development of a system? As Hoepman [13] points out, numerous PETs exist which can be freely built-into a system during the implementation phase of the design process but "at the start of the project, during the concept development and analysis phases, the developer stands basically empty handed" [13]. To remedy this problem, Hoepman introduces the notion of a *design strategy*: a fundamental, strategic choice the developer can make at the outset of the design process, and he outlines eight design strategies which might be adopted for the purpose of implementing privacy-by-design. He derives these strategies from the European Data Protection Directive, but they could just as easily have been derived from its legally binding successor: the GDPR. Hence, following at least a sub-set of the relevant set of strategies is way of going some way towards ensuring compliance with the GDPR. Figure 1 provides Hoepman's illustration of how they can be applied to a database system and Table 2 outlines Hoepman's privacy design strategies.

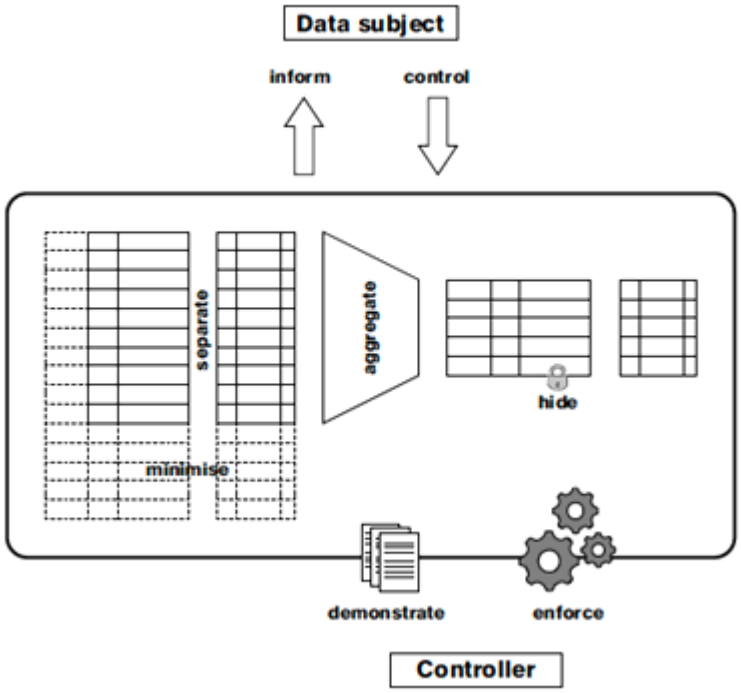

Figure 1 - The database metaphor of the eight privacy design strategies

Table 2 - Hoepman's Privacy Design Strategies

Name	**Principle**	**Elaboration & Justification**
MINIMISE	The amount of PII processed should be restricted to the minimum.	Privacy impact is limited by ensuring that no unnecessary PII is collected. Applying this strategy involves determining whether the processing of PII is *proportional* and whether there is no other, less identifying data the processing of which might achieve the same purpose.
HIDE	Any PII, and their interrelationships, should be hidden from plain view.	Hidden data cannot easily be abused. From whom the PII is to be hidden is context-sensitive.
SEPARATE	PII should be processed in a distributed fashion, in separate compartments whenever possible.	This precludes the construction of a complete profile for a single user. Implementing it requires distributed processing of data stored in separate databases.
AGGREGATE	PII should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.	Aggregating data and making it more coarse-grained renders the data less sensitive and more difficult to attribute to a single person.
INFORM	Data subjects should be adequately informed whenever PII is processed.	Users should be informed of which data is being processed and when, and of any third-party interaction.
CONTROL	Data subjects should be provided agency over the processing of their PII.	Users should be able to view, update, modify or delete their PII at will. Indeed, without means of controlling PII there is little need to be informed of it.
ENFORCE	A privacy policy compatible with legal requirements should be in place and should be enforced.	This ensures that there is in fact a privacy policy in place: a system of norms, compatible with legal requirements.
DEMONSTRATE	There must be a data-controller who can demonstrate compliance with the privacy policy and any applicable legal requirements.	This goes one step further than ENFORCE by requiring it to be provable that the relevant policy is operative.

3. Privacy-by-Design in E-CRIME'S Non-ICT Sectors

Privacy-by-design is often overlooked within the development, deployment, and integration of applications within the non-ICT sectors which the E-CRIME project focuses on, that is: healthcare, energy, financial services, retail, and transport. Not only is this a shortcoming in-itself, but with the implementation of the GDPR around the corner it is also a legal shortcoming. In this section, we go through each sector, highlighting some kinds of PII stored and agglomerated for that sector, and highlighting how the privacy design strategies described in §2 might apply to that sector.

Healthcare

Medical information associated with an individual, which includes, for example, the user's name and address, medical history, and medical insurance details or health service number, is a particularly direct form of PII. It is now standard to store such information electronically using technologies such as Electronic Health Records and to use online patient-provider portals which, amongst other things, enable the user to examine their medical records at will. How is privacy-by-design to be implemented in the context of applications used in the healthcare sector? The implementation of HIDE, INFORM, CONTROL, ENFORCE, and DEMONSTRATE to the sector is straightforward. Indeed, the existence of patient-provider portals constitutes the implementation of INFORM and CONTROL. And password protections supplied via encrypted connections for the healthcare professional and the patient using a patient-provider portal are the norm. However, the implementation of MINMISE, SEPARATE, and AGGREGATE could cause functionality issues in this sector. Minimal health data is of no use to the professional or patient: it is necessary for the success of treatment that the patient's identity is stored along with their medical history and medical insurance details/health service number, and it is therefore entirely proportionate for such PII to be processed in the medical setting. Similarly, such data needs to be available to professional and patient all-together and at a fine level of detail in order for it to be useful.

Energy

The energy sector does not in general process PII which is as sensitive as that processed by the healthcare sector. Energy usage, consumer account numbers, consumer email addresses and physical addresses, and bank details are examples of typical PII processed by the sector. This data is typically rendered accessible to the consumer via a password-protected online account. How do our privacy design strategies interact with the energy sector? Just as with healthcare, the implementation of HIDE, INFORM, CONTROL, ENFORCE, and DEMONSTRATE to the sector is straightforward and would not obviously reduce functionality. But unlike healthcare, the MINIMISE, SEPARATE, and AGGREGATE strategies can also be applied seemingly without loss of functionality. Regarding MINIMISE, it is not proportional, for example, for energy companies to collect details of every member of the relevant household. SEPARATE could also be directly implemented: whilst there might be a need for physical addresses to be stored together with energy meter identification numbers, there is no

obvious need for that information to be stored alongside user financial details. Likewise, AGGREGATE is readily implementable: usage history, for example, can be stored at a coarse level of detail whilst still being useful.

Financial Services

For the financial services sector, privacy is of the utmost importance. Not only is the familiar kind of PII processed – names, addresses, dates of birth – but a rich set of financial data for each individual and organisation is also processed. With respect to high-street banks, such data is made readily available to customers via online banking applications. Again, the implementation of INFORM, CONTROL, ENFORCE, and DEMONSTRATE is straightforward. INFORM and CONTROL can be implemented via the relevant online banking applications, for example. Regarding HIDE, due to the sensitivity of the financial information accessible via online banking, high-street banks have built into the design of their online banking applications layers of protection including, for example, access codes, membership numbers, and PINsentry card readers sent out to users, where these are typically used in tandem. Such privacy protection reduces the speed at which users can access their material, where this counts as a minor detriment to the functionality of such systems. Regarding MINIMISE, the functionality of the relevant systems requires names, contact details, financial histories and card details of the relevant user. However, there is room to apply the SEPARATE and AGGREGATE strategies: there is no need for membership numbers and PIN numbers to be stored together, or together with the user's names and addresses, and data such as financial transactions can be stored in a coarse-grained way.

Retail

The retail sector tends to process PII in several ways: via individual financial transactions, where the user's card details and time of transaction is recorded, via company mailing lists, where the user's name, email address, and perhaps physical address are recorded, and increasingly via the use of loyalty cards which are assigned to a unique user and with which unique user-data is associated, such as transaction history. Another way in which PII is stored is via the video surveillance of customers. ENFORCE and DEMONSTRATE are readily implementable. Although INFORM and CONTROL are implementable with respect to the consumer's financial transactions, mailing lists and loyalty cards, the implementation of INFORM with respect to video surveillance can come only in the form of warning signs telling the consumer that such surveillance is in operation, and there is little room for CONTROL. There is room for the minimisation of PII with respect to mailing lists: only email addresses and names need be taken, and different components of the address can be stored separately. Regarding card transactions, such data need only be processed in a coarse-grained manner and the electronic transactions subject to security measures. Thus, there is room to promote the MINMISE, HIDE, SEPARATE, and AGGREGATE strategies.

Transport

The transport sector tends to process PII via individual financial transactions that often come in the form of the use of smart-ticketing: electronic travel cards onto which consumers can upload credit and contactless-card payments being the most obvious examples. Another way in which PII is stored is via the video surveillance of users. Much of what was said regarding the retail sector applies here too.

Conclusions

The main task of this this deliverable was to give practical sector guidance supporting technological advancements through sector specific crime-proofed applications. In addition to sector-specific guidance it also provided more insight into the concepts of privacy-by-design: how to operationalise privacy-by-design and how to apply that concept to our sectors.

This report outlined the requirements regarding application development for the five Non-ICT focus areas of the E-Crime project – the financial, retail, transport, healthcare and energy sectors. As mentioned in this report, there are many guidelines available for creating more secure applications. Unfortunately, those guidelines are often not followed. The reasons can include optimistic bias (that security incidents are not likely to happen to me) [1], insufficient amount of cybersecurity specialists [14], [15] or the lack of holistic approach. Further research regarding cybersecurity motivational aspects could be useful in order to address psychological side of improving security.

It is not enough to secure the software – it is also needed to secure the hardware and improve the human factor. While WP8 of the E-CRIME project also includes a tool that can be used for security awareness training, more research regarding effective process for securing the human factor would be needed as well as research for quantifying cybersecurity related competencies.

Additionally, the impact of national and international initiatives such as UK Cyber Essentials[13] should be researched more thoroughly in order to locate the most efficient and effective ways to enforce e-crime prevention.

[13] UK Cyber Essentials is described on page 10 of the current report

References

[1] H. S. Rhee, Y. U. Ryu, and C. T. Kim, "Unrealistic optimism on information security management," *Comput. Secur.*, vol. 31, no. 2, pp. 221–232, 2012.

[2] V. Rastogi, "Software Development Life Cycle Models- Comparison , Consequences," *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 1, pp. 168–172, 2015.

[3] A. Gillies, "Improving the quality of information security management systems with ISO27000," *TQM J.*, vol. 23, no. 4, pp. 367–376, 2011.

[4] "Common Criteria - Communications Security Establishment." [Online]. Available: https://www.cse-cst.gc.ca/en/canadian-common-criteria-scheme/main.

[5] N. Sankhwar, "SDL , CLASP & TOUCHPOINTS : A Comparison and Alignment of CLASP with Waterfall Model," vol. 2, no. 3, pp. 365–376, 2015.

[6] D. W. Arner, J. Barberis, and B. P. Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm?," *Univ. Hong Kong Fac. Law Res. Pap.*, vol. 2015/047, pp. 1689–1699, 2015.

[7] S. Jones, M. Wilikens, P. Morris, and M. Masera, "Trust Requirements in E-Business," *Commun. ACM*, vol. 43, no. 12, pp. 81–87, 2000.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," *IEEE Trans. Power Syst.*, vol. 8950, no. c, pp. 1–1, 2016.

[9] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Metayer, R. Tirtea, and S. Schiffner, *Privacy and Data Protection by Design - from policy to engineering*, no. December. 2015.

[10] A. Cavoukian, "Privac y by Design," *Identity Inf. Soc.*, vol. 3, no. 2, pp. 1–12, 2010.

[11] 32nd International Conference of Data Protection and Privacy Commissioners, "Resolution on Privacy by Design," 2010, pp. 1–2.

[12] Federal Trade Commision (FTC), "Protecting Consumer in an Era of Rapid Change: Recommendations for businesses and policymakers," *Fed. Trade Commision*, no. March, pp. 1–112, 2012.

[13] J.-H. Hoepman, "Privacy Design Strategies," Springer Berlin Heidelberg, 2014, pp. 446–459.

[14] T. Caldwell, "Plugging the cyber-security skills gap," *Comput. Fraud Secur.*, vol. 2013, no. 7, pp. 5–10, 2013.

[15] Vogel and Rebecca, "Closing the cybersecurity skills gap," *Salus J.*, vol. 4, no. 2, p. 32, 2016.