Development of a Ransomware Investigation Playbook for the Financial Sector, in compliance with ISO/IEC 27043

Diarmaid Clancy

A thesis submitted in fulfilment of the requirements for the degree of

MSc. in Computer Science

Supervisors: Cormac Doherty/Joe Carthy

UCD Centre for Cybersecurity and Cybercrime Investigation
University College Dublin

May 5, 2022

Abstract

Within the field of digital forensics, incident response and investigation, many groups have developed and evolved their own methods and procedures for conducting investigations of incidents in the digital space, until the creation of *ISO/IEC 27043* in 2015. This was an attempt to harmonise existing methods into a single model, however the Standard is intentionally generalist and non-industry specific. This is why we have developed an augmented version tailored for the financial services sector, in the hope that this will assist the reader in both comprehending and implementing *ISO/IEC 27043* within their own organisation, thus increasing compliance. Specifically, we have developed and evaluated a playbook for ransomware incident investigation that is practical without sacrificing compliance.

Acknowledgments

I would like to thank my supervisor Dr. Cormac Doherty for his excellent guidance, knowledge and advice throughout this masters, as well as all the staff at CCI for their valuable input. I would also like to thank the Irish Defence Forces for providing an invaluable opportunity to discuss and evaluate this research. Finally I want to thank all those that helped push me to finish, especially towards the end.

This research was made possible by a scholarship from the Banking and Payments Federation of Ireland.

Table of Contents

Chapter 1: **Introduction**

This chapter presents the background and motivation for the research undertaken in this thesis. Next, the research question, aim and objectives are described. Then, the contributions of this thesis to existing work are presented. The chapter concludes with a description of the structure of the thesis.

1.1 Thesis Motivation

Technology has integrated almost every aspect of daily life and has become indispensable for businesses ranging from the sole trader to huge corporations. All of our systems and everyday services are increasingly integrated with it but also dependant on it. With this dependence also comes an increased vulnerability to "cyber attack" either directly (eg. being the victim of "phishing" or "ransomware") or indirectly (eg. unable to access a service that is offline after themselves falling victim to an attack).

This increased integration of technology means that the nature of incidents is also changing. In the past, common incidents that might occur would include cheque fraud, physical theft (eg. armed robbery of a branch), and other incidents in "brick and mortar" locations such as fire and flooding. These incidents still occur, but they are now facilitated or augmented by technology (eg. ATM skimming, online payment fraud, theft of online banking access codes, etc.). Furthermore, incidents that previously affected a physical location such as a fire can now also affect part of a digital system (like a server room). Finally there are novel incident types such as network connectivity issues and malware/ransomware.

According to a 2019 report by Accenture[1], Banking and Utilities industries continue

to have the highest cybercrime related costs out of any industry, and this cost is increasing by around 11% every year. The same report indicates that malware is the most expensive type of attack and the cost of ransomware attacks alone increased 21% over the previous year. SANS and other cybersecurity organisations regularly report on the huge ransoms companies are having to pay criminals to regain access to their data (usually in the millions or tens of millions).

Money is what drives cybercrime[1][2] and financial institutions are a lucrative target[3]. To counter this threat, the Banking and Payments Federation of Ireland[1] founded the High-Tech Crime Forum for members to exchange information on the current threat landscape. The Financial Service Cybersecurity Community is the operational and Incident Response component of that group. Retail banks in Ireland, along with other BPFI members and the FSCC, have invested in funding for cybersecurity research such as this thesis, to bolster the protection of Ireland's financial sector.

In particular, there is a requirement for formal procedures for incident response and for conducting the increasing number of digital investigations that follow these diverse incidents[4][5]. A prerequisite for a successful investigation is good preparation, part of which is the awareness of threats currently facing the organisation. This intelligence is highly useful in building solid defences, however there is an unfortunate lack of cooperation and information sharing within the industry, which has become a secondary challenge on top of the investigation itself[6][7].

1.2 Research Question and Objectives

Within an organisation's information security management policy, there should exist an overall plan for handling information security incidents and vulnerabilities[8][9]. This would then include multiple documents covering procedures for the various aspects

[1] https://bpfi.ie/

of the plan. It may also include a high level outline of the incident management flow, which in turn would reference more detailed documentation for each of the steps. We will borrow from military vocabulary and define these as Standard Operating Procedures (SOPs).

There can be a large gap between an organisation's plan for an incident and an organisation knowing it is prepared for an incident. The main goal of this thesis is to provide a set of SOPs based on international standards for readiness, incident response and digital investigation in the form of a "playbook", tailored especially for the financial services sector. As such, this body of work (specifically chapters 2-5) draws heavily from *ISO/IEC 27043*[10], with additional input from *ISO/IEC 27035-2*[11], *ISO/IEC 27035-3*[12], *ISO/IEC 27037*[13], *ISO/IEC 27042*[14] and other relevant sources, the input from related standards being to provide a richer explanation of the processes.

The best way to demonstrate such a tailored playbook would be to create one for a specific category of incident and then evaluate its performance against said incident type. Due to its current prevalance and high cost to many industries[1] we have chosen to focus on the investigation of a ransomware incident. Thus our research question is defined as: **Can a playbook be developed from *ISO/IEC 27043* that is both effective in a ransomware investigation while remaining compliant with the Standard?**

1.3 Thesis Contributions

The contribution of this thesis is to provide the banking and wider financial sector (but particularly the FSCC) with an easily digestible "playbook" for ransomware investigation that is compliant with *ISO/IEC 27043*, which also includes input from related standards where appropriate, in order to have in one place all the general knowledge required to prepare for and conduct a digital investigation of a ransomware incident.

The thesis itself will also provide a comprehensive overview of *ISO/IEC 27043* and thus the entire incident management and investigation process with additional information and explanation (though the details of certain topics must be left to other documents). This then provides the basis on which an organisation can create additional playbooks for the investigation of other incident types that are also compliant with ISO Standards.

1.4 Structure of the Thesis

The rest of this thesis is organised as follows. Chapter 2 is review of the background research on this topic, followed by a comprehensive overview of *ISO/IEC 27043* in Chapter 3, Chapter 4 presents the development of the playbook and an evaluation of it in Chapter 5. Finally, the thesis presents conclusions and possible future work in Chapter 6.

The ransomware investigation playbook developed as part of this thesis is attached in its final form as Appendix F

Chapter 2: **Background Research**

This chapter will present a number of background topics related to this research including: a review of the ISO 27000 family of Standards, related non-ISO Standards, and the background to *ISO/IEC 27043* itself and the so called "harmonised model" for a digital investigation. It will also define several key terms that are common in this area of research.

We will first differentiate a security event from a security incident: the former is something unexpected that occurs and reported to a monitoring team, where it may then get passed back to the security team and escalated to an incident, at which point the incident response plan should be activated and a full investigation may follow[15]. Note that an event does not always lead to an incident (an unsuccessful attack for example, or a false positive).

A security incident occurs when an entity attempts to gain unauthorised access to an organisation's data infrastructure or security policy, putting sensitive information at risk[9]. Inside or outside, attackers make up the primary source of attempts. Attackers are a threat to organisations because they can target any vulnerability in infrastructure using various techniques at any time. Four common security incidents are distributed denial-of-service (DDoS) attack, malware, ransomware, phishing and insider threats:

— A DDoS attack is an attacker's attempt to congest traffic to a target application or an internet application, bombarding them with a high volume of requests.

— Malicious software, or malware, is software created to damage, disrupt or gain illegitimate access to a client, computer, server or computer network. Ransomware, a form of malware, threatens to destroy or withhold a victim's data or files unless a ransom is paid to unencrypt and restore access.

— Phishing is a fraudulent attempt, usually by email, to obtain sensitive information while masquerading as a reputable entity or person. It leverages human emotion to create a sense of urgency and elicit a reaction. Since phishing is ubiquitous in work environments, it's a constant threat, ranking as the top infection vector in the IBM X-Force Threat Intelligence Index 2020.

— Insider threats come from users who have authorized and legitimate access to a company's assets and either deliberately or accidentally abuse them. Insiders typically know where an organization's sensitive data lives and have elevated levels of entry, regardless of whether they have malicious intentions or not.

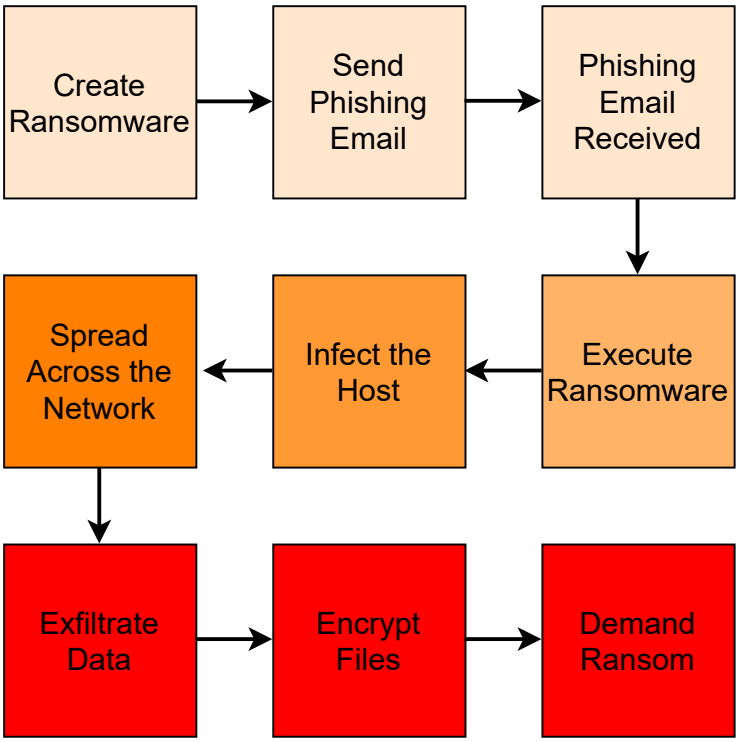

Figure 2.1: Ransomware execution flow.

In this research we will focus on an incident investigation in the case of ransomware. As mentioned above, ransomware is a form of malware that encrypts files at operating system level or databases to prevent users to access them[3]. After encrypting the data, the attackers demand payment to recover the files. The payment is usually demanded in cryptocurrency. It is not uncommon for the ransomware to also exfiltrate a large number of files to later be used as a "double extortion" technique (confidential

files will be leaked or sold if the victim does not pay the ransom).
Ransomware will usually infect the systems via a malicious attachment in an email or via a malicious website. The intrusion point for this kind of malware are the careless end-users who don't recognise the suspicious content, link or attachments in email. Once ransomware infects a machine, it uses the logged on user's credentials to spread across the network. Also, vulnerabilities at operating system level help the ransomware to spread further in the target systems.

In contrast to incident response, which is merely the immediate actions taken once an incident is declared, incident investigation is a slower and more thorough process which can also include an incident response. This is the case of *ISO/IEC 27043 "Information technology - Security techniques - Incident investigation principles and processes"*.

2.1 Review of the ISO 27000 Family of Standards

The *ISO/IEC 27001* standard, published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), is known as "Information technology - Security techniques - Information security management systems - Requirements". The most recent edition of this is dated 2013 and revises the previous edition published in 2005. *ISO/IEC 27001* specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). The ISMS presents a systematic approach to keep sensitive information secure[9][16]. It manages people, processes and IT systems through applying risk management processes. The ISMS suits not only large organisations but also small and medium businesses.

ISO/IEC 27001 laid the foundation for the larger family of standards *ISO/IEC 27000* which consists of inter-related standards and guidelines, already published or under development, and contains a number of significant structural components:

— *ISO/IEC 27001*: normative standards describing ISMS requirements.

— *ISO/IEC 27006*: certification body requirements (for those certifying conformity with *ISO/IEC 27001*).

— *ISO/IEC 27009*: additional requirement framework for sector-specific implementations of the ISMS.

Other standards and guidelines within the family provide guidance for various aspects of an ISMS implementation, addressing a generic process as well as sector-specific guidance. We will provide a brief summary of the standards most related to this work in the remainder of this section.

2.1.1 ISO/IEC 27035 (all parts)

"Information security incident management" is a three-part standard that provides organizations with a structured and planned approach to the management of security incident management. It is composed of:

— *ISO/IEC 27035-1*: "Part 1: Principles of incident management" provides basic concepts and phases of information security incident management and combines these concepts with principles in a structured approach to detecting, reporting, assessing and responding to incidents, and applying lessons learnt.

— *ISO/IEC 27035-2*: "Part 2: Guidelines to plan and prepare for incident response" provides (as the name suggests) guidelines focused on the "Plan and Prepare" and "Lessons Learned" phases from *ISO/IEC 27035-1*.

— *ISO/IEC 27035-3*: "Part 3: Guidelines for ICT incident response operations" was only published in late 2020 and gives practical guidelines for information security incident response in ICT security operations from a people, processes and technology perspective. It also covers incident detection, reporting, triage, analysis, response, containment, eradication, recovery and conclusion.

2.1.2 ISO/IEC 27037

"Guidelines for identification, collection, acquisition and preservation of digital evidence" provides guidelines for specific activities in the handling of digital evidence, which are identification, collection, acquisition and preservation of potential digital evidence (PDE). This can assure that sufficient PDE is captured to allow the investigation to proceed appropriately.

2.1.3 ISO/IEC 27038

Some documents can contain information that must not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that is not to be disclosed is called "redaction". The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information must not be recoverable. Hence, care needs to be taken so that redacted information is permanently removed from the digital document (e.g. it must not be simply hidden within non-displayable portions of the document). *ISO/IEC 27038* "Information technology - Security techniques - Specification for digital redaction" provides methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

2.1.4 ISO/IEC 27040

"Information technology - Security techniques - Storage security" provides detailed technical guidance on how organizations may define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security ap-

plies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use. Security mechanisms like encryption and sanitization can affect one's ability to investigate by introducing obfuscation mechanisms. They have to be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

2.1.5 ISO/IEC 27041

It is important that methods and processes deployed during an investigation can be shown to be appropriate. "Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method" provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

2.1.6 ISO/IEC 27042

"Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence" describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence, and effective reporting of findings. It also provides guidance on appropriate mechanisms for demonstrating proficiency and competence of the investigative team.

2.1.7 ISO/IEC 27050 (all parts)

"Information technology - Electronic discovery" covers the process of discovering pertinent Electronically Stored Information (ESI) or data by one or more parties involved in an investigation or litigation, or similar proceeding. This Standard is still actively being worked on, with new versions as recent as 2021.

— *27050-1*: "Part 1: Overview and concepts" defines terms and concepts relating to electronic discovery (ED).

— *27050-2*: "Part 2: Guidance for governance and management of electronic discovery" provides guidance regarding compliance and policy for technical and non-technical personnel at senior management levels within an organisation.

— *27050-3*: "Part 3: Code of practice for electronic discovery" provides requirements and recommendations on activities in ED, including, but not limited to, identification, preservation, collection, processing, review, analysis and production of ESI.

— *27050-4*: "Part 4: Technical readiness" provides guidance on the ways an organization can plan and prepare for, and implement ED from the perspective of both technology and processes.

2.1.8 ISO/IEC 30121

"Information technology - Governance of digital forensic risk framework" provides a framework for governing bodies of organisations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organisation for digital investigations before they occur. This International Standard applies to the development of strategic processes (and decisions) relating to the retention, availability, access, and cost effectiveness of digital evidence disclosure. It is applicable to all types and sizes of organisations. Forensic readiness assures that an organisation

has made appropriate preparation for potential securty events and incidents. Actions may occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation, information technology (IT) has to be strategically deployed to maximize the effectiveness of evidential availability, accessibility, and cost efficiency.

2.2 Review of Related Non-ISO Standards

In addition to numerous Standards from the ISO/IEC corpus there are also several non-ISO standards widely used in the information security industry, most notably by the United States National Institute of Standards and Technology (NIST), the Sysadmin, Audit, Network and Security Institute (SANS), but also by the Forum of Incident Response and Security Teams (FIRST) and the United Kingdom's Association of Chief Police Officers (ACPO). In this section we will provide a background to those standards most relevant to this research.

2.2.1 ACPO Principles

A set of four principles widely used in the investigative community are the "guidelines in the handling of electronic evidence" put forth by ACPO[17]. These are as follows:

— **Principle 1:** No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.

— **Principle 2:** In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

— **Principle 3:** An audit trail or other record of all processes applied to digital

evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

— **Principle 4:** The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

These principles do not strictly match up to individual clauses in *ISO/IEC 27043* Standard, however they can be applied as best practice principles throughout the entire investigation process and should be kept in mind. In a corporate investigation (such as one conducted within a bank) where the investigators are not necessarily law enforcement agents these principles should still be applied, as this will aid an investigation that remains internal and give credibility to the organisation should the investigation require a court case as well as allowing them to interface more easily with law enforcement if required.

2.2.2 Traffic Light Protocol for Communications

When it comes to information sharing, it is beneficial to have a clear and well-defined protocol for classification of information and its restriction to specific audiences. Simple and intuitive, the well-established *Traffic Light Protocol* was created by the UK Government's National Infrastructure Security Coordination Centre in the early 2000s and for which specifications were later defined by FIRST[18]. This protocol specifies four coloured designations, which can be used on paper, electronic documents, email, etc. These designations are defined as follows:

— **TLP:RED** = Not for disclosure, restricted to participants only.
Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED

information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

— **TLP:AMBER** = Limited disclosure, restricted to participants' organisations.
Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. As this may or may not include selected additional persons, sources are at liberty to specify additional intended limits of the sharing: **these must be adhered to.**

— **TLP:GREEN** = Limited disclosure, restricted to the community.
Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

— **TLP:WHITE** = Disclosure is not limited.
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Precise definitions of the colours used, usage guide and other additional information, the reader should consult *TLP - FIRST Standard Definitions and Usage Guidance*[1]. This method is also used by the European Network and Information Security Agency (ENISA)[19], and described in Annex C of *ISO/IEC 27010*[7]. Common usecases for TLP are corporate email and document exchange.

[1]Which can be obtained at https://www.first.org/tlp/

2.2.3 NIST & SANS Incident Response Plans

A large amount of incident response plans used in industry today are based on two main approaches: the NIST four phase method and the SANS 6 step method[3][20]. They are broadly the same as each other with SANS breaking down their response plan into slightly more specific steps. We will present the main components of the NIST methodology here, as it is more closely related to the playbook developed later in this thesis, with comments on where the SANS steps fit in. The four NIST phases are as follows:

— Preparation: To prepare for incidents, a list of IT assets such as networks, servers and endpoints is compiled, identifying their importance and which ones are critical or hold sensitive data. Monitoring is set up so there is a baseline of normal activity. One should determine which types of security events should be investigated, and create detailed response steps for common types of incidents. This is equivalent to *SANS Step 1 - Preparation*.

— Detection & Analysis: **Detection** involves collecting data from IT systems, security tools, publicly available information and people inside and outside the organisation, and identifying precursors (signs that an incident may happen in the future) and indicators (data showing that an incident has happened or is happening now). **Analysis** involves identifying a baseline of normal activity for the affected systems, correlating related events and seeing if and how they deviate from normal behavior. This is equivalent to *SANS Step 2 - Identification*.

— Containment, Eradication, & Recovery: **Containment** aims to isolate the malware or malicious actor and to stop their spread through the network. Here is where the response team will attempt to identify Command & Control (C2) traffic and servers. (*SANS Step 3 - Containment*).

Eradication aims to remove all elements of the threat from the system. This might include identifying all affected hosts, removing malware, and closing or resetting passwords for breached user accounts. (*SANS Step 4 - Eradication*).

Recovery aims to restore systems and recover normal operations as quickly as

possible, taking steps to ensure the same assets are not attacked again. (*SANS Step 5 - Recovery*).

— Post-Incident Activity: In this phase the root cause of the incident should be established, and the response as a whole should be examined from a learning perspective (ie. what went well and what didn't?). The goals of this phase are improvements to the system to reduce the impact of future incidents, and also improvements of the response itself (team and/or procedures) if required. This is equivalent to *SANS Step 6 - Lessons Learned*.

2.3 ISO/IEC 27043 and the Harmonised Model

Many groups and researchers (such as the U.S. Department of Justice, the Association of Chief Police Officers (UK), Ó'Ciardhuáin, etc.)[21][22][23] had developed and evolved their own methods and procedures for conducting digital forensic investigations (DFI)[5][24][25], essentially on an ad hoc basis, and it was not until 2015 that a standardised set of processes was created[26][4]. This was *ISO/IEC 27043* which attempted to harmonise many of the existing methods published by different organisations into a single "umbrella" model[4].

This organic evolution of procedures led to a number of disparities[27]: different number of investigation processes included, different scope of process models, different scope of the processes with the same names within different process models, different hierarchy levels[28] and even different concepts applied to the construction of the process model. The harmonised digital investigation process model is comprehensive and inclusive of all the benefits conveyed by previous models and its use should ultimately enhance the efficiency, effectiveness, and robustness of digital investigations[29][30].

Within the model, a process is defined as a single unit: each process covers a single part of the overall investigation[31]. A class is a collection of processes that share

a common theme: the *Concurrent processes* class contains processes that happen in tandem with the rest of the investigation; the *Readiness processes* class deals with pre-incident investigation preparedness and setup; the *Initialisation processes* class deals with the initial commencement of the investigation and first steps of the response; the *Acquisitive processes* class deals with the physical investigation where potential digital evidence is identified and handled; Finally, the *Investigative processes* class deals with uncovering answers from the digital evidence.

A top level view of how these classes make up the investigation process is presented in Figure 2.2. Each of the sections describing the four main classes of processes in Chapter 3 will include a more detailed diagram of the process layout. For a complete expanded diagram of the entire investigation and all the processes, please refer to Appendix B.

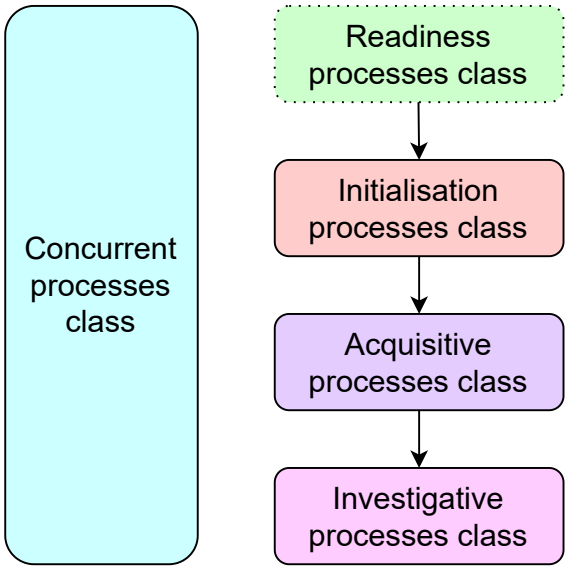

Figure 2.2: The various classes of digital investigation processes[10].

As the *Readiness* class happens separately to the rest of the model (as it may be actioned on far in advance or not at all), the actual starting point for the digital forensic investigation is the *incident detection* process (within the *Initialisation* class). In the next chapter we will present a comprehensive overview of *ISO/IEC 27043* and all of its processes.

Chapter 3: **Overview of ISO/IEC 27043**

3.1 Readiness Processes

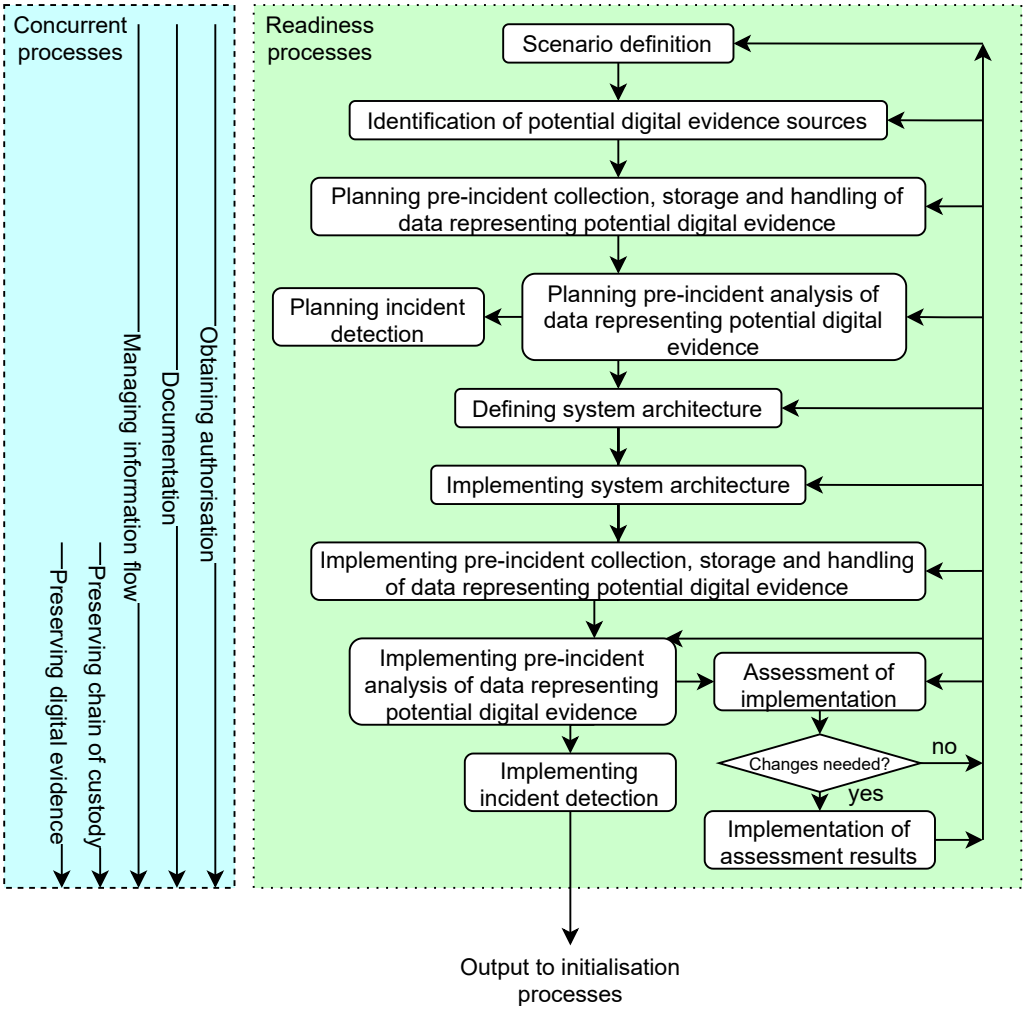

Figure 3.1: The readiness processes[10].

The Readiness class of processes (Figure 3.1) includes all the processes dealing with setting up an organisation in a way they are properly equipped to conduct an effective digital investigation while minimising time and cost. According to the standard

(*ISO/IEC 27043*[10]) this class is optional and is the responsibility of the organisation and not the investigator, however with the increasing number and sophistication of cyber-attacks in Ireland and around the world, this section becomes ever more important for any organisation at risk of attack. For this reason, this section is noticeably longer than the others, as a solid defence comes from proper preparation[11].

There are four main incentives for any organisation implementing these processes[31]: Prevent interruption or minimise interference with the organisation's normal business operations; Minimise cost of investigations (direct costs like investigators, or indirect costs such as loss of revenue due to the incident); Preserve or improve the current level of information security within the organisation; Maximise the use of potential digital evidence.

The processes presented in this section are divided into three subsections:

1. *Planning:* contains processes related to planning activities, which includes: scenario definition; defining the system architecture; planning of incident detection; identification of potential digital evidence sources; planning of pre-incident collection, storage and handling of data representing potential digital evidence, and any required pre-incident analysis of that data. (see 3.1.1)
2. *Implementation:* contains processes that implement what was planned in the previous phase: implementation of system architecture and incident detection, as well as the implementation of pre-incident collection, storage and handling of data representing potential digital evidence and its analysis. (see 3.1.2)
3. *Assessment:* contains processes that cover assessment of the current implementation and how to implement any feedback from that assessment by iterating back over the two other phases. (see 3.1.3)

Finally, the processes in this class are iterative, meaning that the procedures and implementation should be periodically reviewed and the feedback should be used to go back and improve and processes where deficiencies (or out of date procedures) were

noticed. For example, when during the *assessment of implementation* process, one notes that a certain defined system architecture has not been properly implemented, one would need to go back to the *implementing system architecture* process.

3.1.1 Planning

3.1.1.1 Scenario definition

The first step to being properly prepared it to examine all probable incident scenarios likely to occur within the organisation (based on currently expected threats)[32]. In particular any scenario where digital evidence might be required should be well thought through. For example, a ransomware attack is currently a common threat to large organisations so in this process we would define the characteristics of different scenarios in that theme (eg. single machine has been infected vs half our network has been infected, do we treat these differently?)

It is also recommended that for each scenario identified a proper risk assessment is performed. A risk assessment would enable one to better identify possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the risk assessed from vulnerabilities, threats or other scenarios, one will be able to better decide on the required controls in later processes. This will enable an organisation to take into account the risk level, costs and benefits of possible controls used to reduce the identified risk. An example of a simple control measure in the case of ransomware is not allowing the download of executable email attachments.

3.1.1.2 Identification of potential digital evidence sources

The potential sources of digital evidence within an organisation should be identified in this process. Identifying useful sources early on will be very beneficial should an investigation be required. The choice of source will depend on the organisation's

individual needs and technology, but various forms of log files are a common choice, as are CCTV cameras. However, one should not just collate every possible log of everything, as this will increase noise and drown out potentially relevant information. In the case of the ransomware example, we would want to try and preserve a sample of the malware for later analysis (with possible identification of command & control (C2) information), as well as access and execution logs to identify how it got in and how it moved around.

Some of the identified sources may not be available. For example, if the system is not set up to have access logs, then access logs will not be available as a source of data in the case of a digital investigation. In that case measures should be taken to make the identified sources available (for example, by turning on logging on the system).

3.1.1.3 Planning pre-incident gathering, storage, and handling of data representing potential digital evidence

In this process, one should define SOPs for pre-incident gathering, storage and handling of data representing potential digital evidence (i.e. what methods and tools will be used or would be required to respond to the defined scenarios?). The organisation should also make sure employees are trained in them or at the very least made aware of their existence and where they can refer to for clarification (including on taxonomies and shared standards).

The methods used for gathering, storage and handling have to conform to digital investigation principles in order for digital evidence to be admissible in court. These principles are covered in subsection 3.5.4 and subsection 3.5.5.

The retention period of the data will be determined based on the following factors: risk assessment; laws within the particular jurisdiction; regulations; business-specific requirements; and previous experience with matters that could influence the cost or efficiency of this process.

When attending the scene of an incident, such as a datacentre or onsite in a bank, the investigator will often require a variety of tools (e.g. precision screwdrivers, data cables, collection drives, etc.). Exactly which tools are required will depend on the task at hand and there may be times when an investigator only realises they need a particular tool when they are already at the scene (which could then cause significant delays). For this reason it is advisable to develop a "go-bag" in advance that will contain all the tools the investigator might need. For larger organisations several identical kits should be available (as their may be multiple investigators in multiple locations). The kits should also be audited on a regular basis to ensure components have not gone missing since previous uses.

The contents of the go-bag are entirely up to the organisation and different organisations will have different requirements. We have compiled a list of items that we believe will cover the needs of most investigators working in this sector and for reference have also provided the item lists of the go-bags used by An Garda Síochána DFRs and the (Irish) National Cyber Security Centre. These are available in Appendix E. The discussion of how these were compiled is in section 4.2.

3.1.1.4 Planning pre-incident analysis of data representing potential digital evidence

In this process, one should define SOPs for pre-incident analysis of data representing potential digital evidence. Essentially this means planning how logs and other data will be monitored in order to detect an incident. As the aim of the analysis is the detection of said incident, procedures defined in this process should define exactly what constitutes an incident and how it will be detected.

It is recommended that at this stage a monitoring system specialised in the detection of incidents is decided upon. This system can also be any one of the following: intrusion prevention systems, intrusion detection systems, change tracking systems, log processing systems, etc.

The use of an intrusion detection and prevention system (IDPS) is advisable[33] (in addition to just anti-virus software). Its purpose is to passively monitor, detect and log inappropriate, incorrect, suspicious or anomalous activity that may represent an intrusion and provide an alert and/or provide an automated response when these activities are detected[34]. In order to achieve reasonably complete coverage of potential intrusions, an organisation should combine host-based (ie. monitoring solutions installed on each host such as antivirus or system process monitors) and network-based approaches[35] (ie. a firewall server monitoring connections and traffic, or AI-powered traffic monitoring, such as anomaly detection software), as each type of IDPS has its strengths and limitations (for example, host-based solutions have good visibility on program execution and suspicious file changes but poor/no awareness of changes on the network, while network-based solutions can have a good overall picture of the network, but limited or no knowledge of a single process on an individual machine). For a comprehensive guide on understanding and choosing an IDPS the reader should refer to *NIST.SP.800-94*. There are a variety of commercially available or open-source IDPS products and services on the market, however they are not "plug and play" technology and organisations should be familiar with the contents of *ISO/IEC 27039* prior to deploying one.

At this point we need to briefly touch on another field: that of Threat Intelligence. If done correctly, the product of this intelligence will be (amongst other things) a variety of indicators that can be used within an IDPS to identify various threats. This is particularly useful when one leverages the power of existing Threat intelligence sources (such as Virus Total, FireHOL's IP address list and many others), as this gives access to readily availble indicators of threats around the world. It is recommended that in this process consideration is given as to how the organisation will employ threat intelligence in its defensive strategy[36][37][38].

There are four sub-types of threat intelligence:

— **Strategic:** high-level information, consumed at board level or by other se-

nior decision-makers. Usually non-technical this would cover things such as the financial impact of a cyberattack on the organisation.

— **Operational:** information about specific impending attacks against the organisation and would be consumed by higher-level security staff such as security managers or heads of Incident Response teams.

— **Tactical:** often referred to as Tactics, Techniques, and Procedures (TTPs) and is information about how threat actors are conducting attacks. It is consumed by defenders and incident responders to ensure that their systems are prepared for current threats.

— **Technical:** is information (or, more often, data) such as IP addresses and MD5 sums that is normally consumed through technical means (e.g. as indicators or input for software). This is often of very short-term value.

When an organisation is conducting its own threat intelligence gathering, it's crucial that it is requirements focused and defines the questions that need to be answered. There is little point obtaining information that cannot be acted upon (such as unrelated threats or enormous volumes of data that the organisation has no means to process anyway). Once requirements have been decided, the next steps are to identify the sources from which information and data will be collected, the analysis necessary to produce actionable intelligence, dissemination and evaluation. Thus the threat intelligence lifecycle is as follows:

— **Requirements:** what specifically are we looking for? What do we want to know?

— **Collection:** acquiring the information or data that is expected, this can come from a large variety of sources such as news feeds, paid-for services, forums, whitepapers, or even human sources.

— **Analysis:** turning data into information that can be actioned, this process can be simple (e.g. parsing a file) or more complicated (e.g. looking for a trend across multiple sources).

— **Dissemination:** an intelligence 'product' is created and distributed to relevant parties (product may be a simple report or YARA rule, but may be more complicated like a whitepaper).

— **Evaluation:** does the product meet the original requirements? If it does then it can help decide the next requirements. If it does not then the cause should be found and remedied (e.g. unrealistic requirements? wrong sources? poor analysis? etc.).

In the case of the organisation being targeted by an APT group, incidents themselves will be especially useful in building a picture of the APT's methods and intentions. Lockheed Martin Corporation defined the notion of a "kill chain" (Figure 3.2), a series of steps that model an attacker's intrusion and how much progress they made. The idea is to have mitigations in place for as many of these steps as possible and to detect and stop the intrusion in the earlier steps. Even in the face of a novel attack, or one using so called "zero-days" (as yet unfixed exploits), the incident will provide indicators and can reveal information on the attacker's TTPs, and each incident will allow the defenders to develop new mitigations and push detection down to earlier phases of the chain[38][39].

3.1.1.5 Planning incident detection

In this process, one should define actions to be performed when an incident is detected. (Note this is not the same as planning *how* to detect an incident, which is covered in the previous subsection). One should also include in the plan the definition of what constitutes an incident. We define an incident as the escalation of events to a security situation leading to financial loss, loss of service, reputational damage, etc.

Good threat modelling is key when planning incident detection. In other words the organisation must determine what are the most probable threats to them and what attacks from those actors are likely to look like, and then monitor for indicators of those types of attacks. (For example this could include monitoring certain common

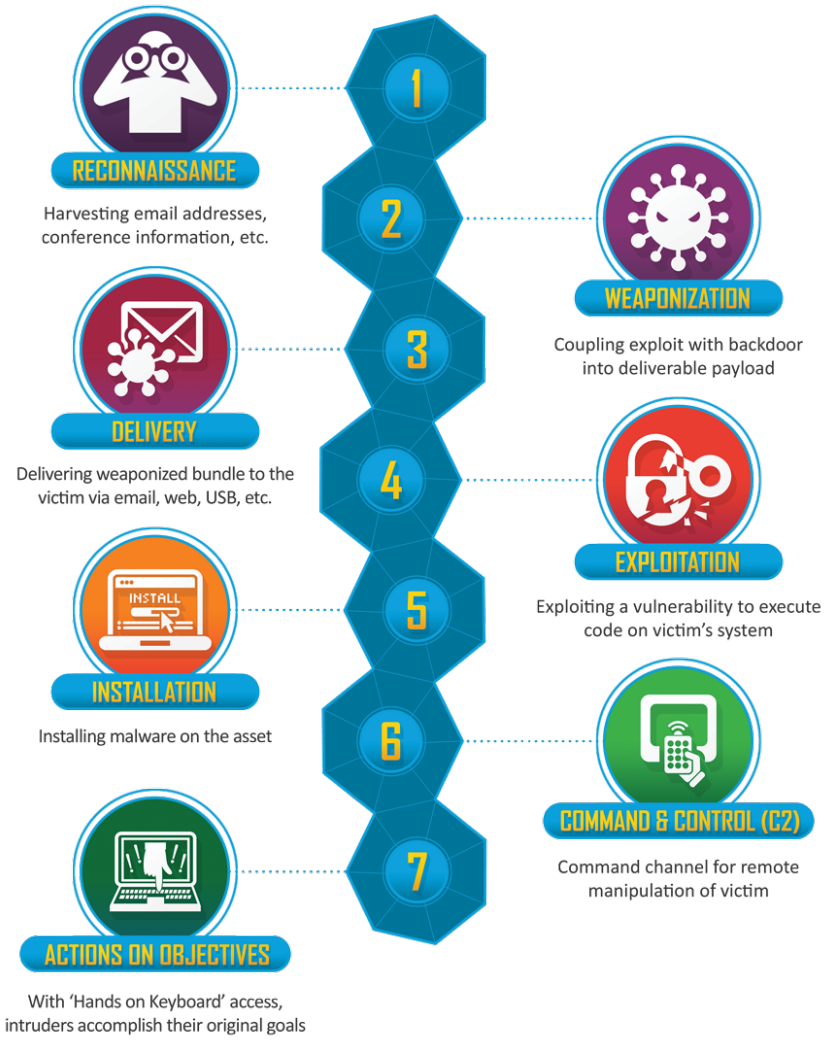

Figure 3.2: Cyber Kill Chain[39]

vulnerabilities and exposures (CVE) that affect equipment used in the organisation, or negative mentions on social media if that is a concern).

Incident detection involves not just the electronic equipment but also the human element, therefore the organisation should ensure that a security conscious culture is actively promoted at all levels and make sure that users are aware of the value of information security incident management and are motivated to report incidents. As noted in clause 7.2 of *ISO/IEC 27001*, this should involve determining the necessary competence of persons doing work that affects the organisation's information security performance, ensure that they are competent (on the basis of appropriate education, training, or experience) and if they are not then take actions to acquire the necessary competence (such as relevant training), and evaluate the effectiveness. The

organisation should also retain appropriate documented information as evidence of competence.

When an incident occurs, there should be incident report forms available for use. Deciding the type and design of these forms can happen in this process and they should be revised periodically. An internationally standardised format is recommended, for example that defined in *ISO/IEC 27035-2*. We have attached these to this thesis as Appendix D.

3.1.1.6 Defining system architecture

In this process, the system architecture for the organisation should be defined. This should take into account what has been decided in all the previous readiness processes (and any feedback from assessment of the current system). The system architecture in this context refers to the organisational structure of an information system, including necessary computer equipment, a communications network, and related software. (So for example, one would decide where the monitoring system chosen in subsection 3.1.1 fits into the overall system architecture).

The aim of this process is to customise the system architecture (specifically the electronic storage and transportation of data and/or information within the architecture) in such a manner as to facilitate the accomplishment of objectives defined in the readiness processes. In other words the system architecture should be secure and resilient to attack, while also facilitating investigation of any incident that might occur. A key point of this facilitation is to identify potential data and/or information sources within the architecture (or identify somewhere to put such a source if it doesn't exist).

Please note that this process would usually be the responsibility of an industry trained and competent security/network architect or that is familiar with the system architecture, so it will not be covered further in this document.

3.1.2 Implementation

3.1.2.1 Implementing system architecture

In this process, the system architecture defined in subsection 3.1.1 should be implemented. This includes the installation of any new hardware, software and/or policies required by the system design. Related documentation should also be updated to reflect these changes.

3.1.2.2 Implementing pre-incident gathering, storage, and handling of data representing potential digital evidence

In this process, the procedures for pre-incident gathering, storage and handling of data representing potential digital evidence (as defined in subsection 3.1.1) should be implemented. For example, this could include the implementation of logging software and hardware (if this was not already done), with time stamping and digital signature mechanisms in place, or the implementation of customized software to gather the data of importance (i.e. system usage data).

3.1.2.3 Implementing pre-incident analysis of data representing potential digital evidence

In this process, the procedures discussed in subsection 3.1.1 relating to pre-incident analysis of data representing potential digital evidence should be implemented. This would include the implementation of, for example, change-tracking software (such as a file integrity checker), intrusion detection/prevention software (such as "snort") and/or anti-virus software.

3.1.2.4 Implementing incident detection

In this process, one should implement the actions defined in subsection 3.1.1 (planning for incident detection), however the implementation of incident detection is also dependant on the previous process (see subsection 3.1.2), as the detection occurs based on the analysis performed. This is bascially sounding the alarm (or not) and other actions from the point the incident is detected.

During this process one should also decide on what information about the incident should be passed on to the rest of the digital investigation process. A well developed information security policy, and the accompanying procedures will include details on standards and taxonomy used for incident classification (such as VERIS, CVE and CVSS)[40], how to escalate an incident up to the relavent people, and how to deal with unintended discovery of classified materials.

This process represents an interface to the rest of the digital investigation process. It is an overlap between the *Readiness* phase and an investigation itself, as a digital investigation cannot start until an incident is actually detected, so essentially this process is a trigger for everything else.

3.1.3 Assessment

3.1.3.1 Assessment of implementation

In this process one performs an assessment specifically of the results of all the *Implementation* processes and compares these against the digital investigation readiness goals of the organisation (which is not the same as an assessment of the performance of a full real-life investigation, that comes from a later process). The output of this process should be a list of any required changes to the implementation or SOPs, if it is deemed any are required.

The organization should schedule regular checking and testing of the systems and procedures defined in the readiness processes to highlight potential flaws and future problems. One such method of assessment is organising exercises. These simulated scenarios can range from severe, complex incidents based on realistic attacks, failures or faults to simple discussion-based table top exercises. The setup will depend on the pre-defined goals of the exercise. These exercises may also involve external parties who are involved in the management of information security incidents (e.g. other member banks or the NCSC). Care should be taken however, to ensure all involved are aware that they are not dealing with a real attack and thus prevent people from triggering actions that might have much larger implications.

As an example, the results of the exercise could provide answers to the following questions: Did the procedures implemented in the *Readiness* processes work as intended? Were any procedures or tools identified that would have been of assistance in a particular process? Was the communication of the incident to all relevant parties effective throughout the detection, reporting and response processes? Are there any procedures or methods that would have aided in the detection of the incident?

The capabilities of the organisation's Incident Response Team should be adequate to address the current threats facing said organisation, however threats are constantly evolving, as is the technology used within the organisation, therefore these capabilities will also need to change. Threat Intelligence, such as that provided by monitoring characteristics and frequency of incidents throughout the cyber environment, is a valuable source of information that will allow team members to stay ahead of the curve and so should have a place in the organisation's Security Operations Centre (provided, of course, that good quality sources are used).

Finally, it is recommended that, at this stage, a legal review is carried out for all procedures, controls, and architectures defined previously. The revision should show, amongst others, whether or not there is conformity with the legal environment and digital forensics principles of the organisation's particular jurisdiction, in order to assure admissibility of potential digital evidence in court.

3.1.3.2 Implementation of assessment results

In this process one should implement any required changes to implementation or SOPs, based on the results of the assessment covered in the previous subsection. This process is optional, as it depends on that assessment, which may decide that the system is currently optimal and no further changes are required.

While deciding recommendations for changes in one or more of the previous processes, the main decision is whether to go back to one of the processes in the *Planning* phase, or to one in the *Implementation* phase. For example, one might decide that the implementation of a certain component was poorly done (e.g. log-in authorization controls have been poorly implemented in the system architecture) or one might decide that an additional scenario for a new type of threat should be defined and additional procedures put in place to deal with this.

Finally, there may be results from the assessment that are not strictly related to the incident management, but could help to streamline the operation of the organisation. For example, insufficient staffing during handling of the incident could lead to a recommendation to improve scheduling of leave, and poor cooperation (poor support, very slow to deliver critical updates) from software or hardware vendors could help to refine these same.

3.2 Initialisation Processes

In this section we present the *Initialisation* class of processes (Figure 3.3), which deal with processes that will occur in the first stages of an incident investigation, triggered by the detection of an incident itself. This process class is about reacting effectively to the incident, and laying a good foundation that the rest of the investigation will build upon. As such, it is very important that relevant procedures are executed correctly during these processes, and that any potential disruption caused by mistakes is minimised.

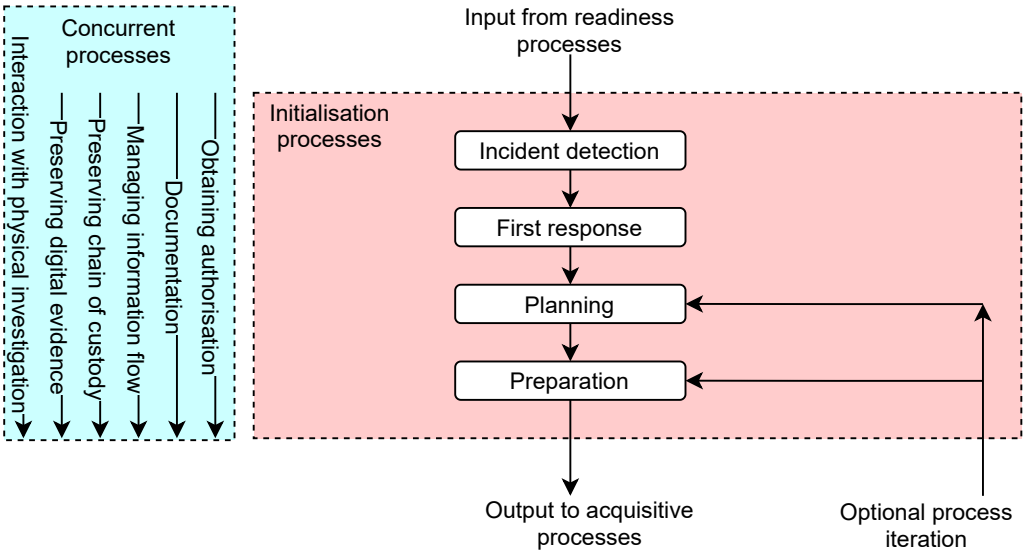

Figure 3.3: The initialisation processes[10].

This section will describe the *Incident detection*, *First response*, *Planning* and *Preparation* processes. Addtional information is also available in *ISO/IEC 27035-2* and *ISO/IEC 27037*.

3.2.1 Incident detection

Incident detection systems must be in place before beginning this process. For details on the implementation of the incident detection system and examples, see subsection 3.1.2.

This process includes not only the detection of the incident itself, but also the description and labelling/classification of the incident, as this will be required to decide the direction that the investigation will take. For example the investigation would take a different course if the incident was described as "ransomware trojan infection of multiple machines", than if it was described as "unauthorised access to teller's machine". Thus this process may be seen as three discrete steps: detection of the incident, followed by its classification and finally its description. The classification and description should be done using information available prior to detection and not from any interaction with systems that might affect digital evidence.

To this end an incident classification scale should be used to grade events/incidents. In any event, the decision should be based on the actual or projected adverse impacts on the organisation's business operations. There are existing classification systems such as the *FIRST Common Vulnerability Scoring System (CVSS)*, the UK government's *Structured Warning Information Format (SWIF)*, and what is defined in *ISO/IEC 27035-2*. Drawing on elements from all of these we propose an intuitive practical categorisation revolving on the concept of priority. This is also closely related to what the Irish Defence Forces use. For an example of how this could be applied, please refer to the table below.

	System Importance & Business Loss	Example incident
Priority 1 (P1)	Critical infrastructure and/or business paralysis or damage such that cost to recover is enormous. May also include severe damage to public interest.	Wisespread ransomware infection on a network with data exfiltration.
Priority 2 (P2)	Prolonged interruption to services, or serious damage to key business data, high associated cost.	Compromise of organisation's website which then redirects users and steals their credentials.
Priority 3 (P3)	Short term or significant interruption to business operations, bearable but non-negligible cost or negative effects. Little effect on general public but damage to interests of individuals.	Client-facing machine crashing for short period.

Table 3.1: Incident prioritisation.

3.2.2 First response

This process will be the initial response after an incident has been detected. This response may include many different actions (such as disconnecting equipment from a networked environment, isolating infected machines, freezing an account, etc.) but the exact actions will be dictated by the type and severity of the incident, and the procedures in place. Regardless of the type of incident however, it is important that any actions taken do not negatively impact on the ability to perform a digital investigation (for example, powering off equipment, or carelessly changing files on a live system, could corrupt or destroy potential evidence).

The first responder should perform certain general actions to secure and protect the location of the potential digital evidence as soon as they arrive on site:

— Heighten monitoring and alerting of the network and systems.

— Secure and take control of the area containing the devices (in the case of remote machines this could mean cutting of access to an outside actor, or simply ensuring someone at the datacentre is on standby for further instructions).

— Determine who is the individual in charge of the location.

— Contact the person designated in the SOPs as responsible for that part of the organisation or network (for example this could be a line manager, the Secrutiy Operations Centre (SOC) or a sysadmin).

— Ensure that individuals are moved away from the devices and power supplies.

— If a device is ON do not switch it OFF and if a device is OFF do not switch it ON.

— Document anyone who has access to the location (including virtual access if these machines are intended to allow remote connection) and anyone who may have a reason to be involved with the incident scene.

— In pysical locations keep an eye open for any devices or peripherals that shouldn't be there (such as Hak5's Bash Bunny, Lan Turtle, Packet Squirrel, and various other similar devices available on the market).

— If possible, document the scene with all components and cables in their original position. If applicable, label the ports and cables so that system may be validated and reconstructed at a later date.

The first response process is an entire topic by itself and so a full definition is outside the scope of *ISO/IEC 27043*[10], however much more detailed information is available in *ISO/IEC 27037*[13] and *ISO/IEC 27035-3*[12].

3.2.3 Planning

After the first response the investigator must now make a plan for the rest of the investigation, which will include development of relevant procedures and deciding what methodologies and tools are to be used. What to consider in the plan includes, but is not limited to the following:

— What type of collection/acquisition methods to be applied (and are they available or do they need to be obtained)?

— What equipment may be needed on-site?

— What is the level of volatility of data and information related to the potential digital evidence?

— Is remote access to any digital device possible and does it pose a threat to evidential integrity?

— What happens if data/equipment is damaged?

— Could data have been compromised?

— Could the digital device have been configured to destroy (e.g. using a logic-bomb), spoil or obfuscate data if switched off or accessed in an uncontrolled way?

— Are there any physical hazards to individual(s) present?

— What additional human resources (e.g. additional investigators, IT staff, overtime hours, etc) might be required?

— What is the deliverable of the investigation (i.e. what type of report)?

If controls from the *Readiness* class have been implemented, the investigator should avail of them and plan how to best use their results, as this may aid or speed up the investigation and help to avoid duplication of work. This planning process will have a

significant impact on the efficiency and success of all other processes, therefore care should be taken to ensure it is done properly.

3.2.4 Preparation

The preparation process is the last step of the investigation *Initialisation* class, it involves preparing relevant resources necessary for the investigation (those that will have been decided in the *planning* subsection). This might include (but is not limited to) the preparation of relevant equipment (hardware and software), human resources, raising awareness (within the organisation or with the authorities/public, depending on the incident), verifying investigators are prepared for the current task, documentation of the systems/tools and double-checking the go-bag discussed in subsection 3.1.1 is ready (specifically that no items are missing, though this should be verified periodically anyway). Preparation also has to be made to implement any procedures defined in the previous subsection (such as preparing a report design if it has not already been done).

At this stage there should be a briefing for the investigators from the relevant party (such as the line manager in charge of the affected department, or the security team who first detected/responded to the incident), with information disclosed in line with the TLP outlined in subsection 3.5.3. This briefing is important in order for the investigators to understand the incident and to know what to expect (or what not to). The briefing should contain sufficient information that the investigators do not need to be further briefed.

Below is a list of suggested items that should be part of the briefing (non exhaustive):

— Type of incident (if known).

— Date and time of incident (if known).

— Designation of the area under investigation (e.g. which bank or which section).

— Investigation plan (collection, acquisition, network activity?, any volatile data?, etc.).

— How and where the potential digital evidence will be transported/stored after collection or acquisition.

— Specific tools needed to acquire the potential digital evidence.

— Required equipment and manuals related to digital devices.

— Logistics of bringing any equipment to the incident scene.

— Any applicable factors that may prohibit collecting any devices and their contents.

— Assignment of roles and responsibilities of investigation team members at the incident scene.

— Whether other authorities are expected to be involved in the investigation.

— Legal aspects and implications.

— Investigation time frame.

— Reminder to team members to switch off Bluetooth and Wi-Fi on their devices (so as not to create noise or interfere with other devices).

— Reminder of the importance of documentation.

— Reminder not to allow unauthorised individuals to interact with devices.

— Relevant HR information (e.g. if overtime will be required).

As with the *planning* process, correct execution of this process is very important for the investigation as it will ensure investigators are properly prepared and will not compromise the investigation or damage evidence through lack of skill, preparation or training.

3.3 Acquisitive Processes

In this section we present the *Acquisitive* class of processes (Figure 3.4), which deal with processes that are concerned with acquisition of digital evidence. Although the complete digital evidence handling process includes other activities (i.e. presentation, disposal, etc.) these are covered under other sections, so the scope of this section relates only to the initial handling process which consists of identification, collection, acquisition, and preservation of potential digital evidence. Note that the dashed line for the *Potential digital evidence acquisition* process indicates that it is optional at this stage as it can be done in the investigative processes class, however we will describe it here rather than later.

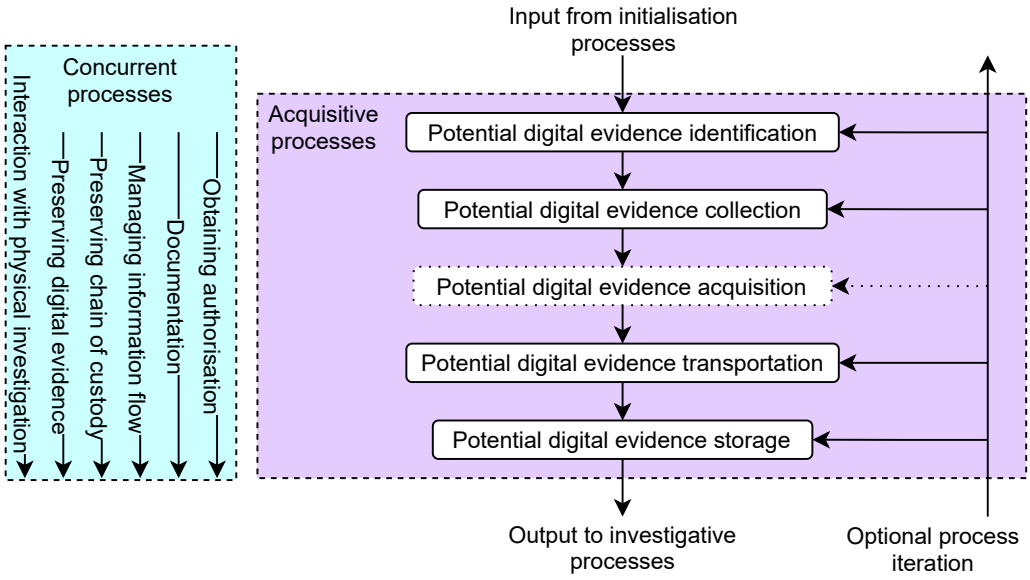

Figure 3.4: The acquisitive processes[10].

Digital evidence can be required for a number of scenarios, each of which has a different balance between evidential quality, timeliness of analysis, restoration of service and cost of digital evidence collection. Therefore an organisation should have a prioritisation process to identify the needs and balances of the aforementioned points. This will involve an evaluation of the material available being carried out in order to determine

what potential digital evidence should be collected and in what order. The person who's role it is to perform this triage process is known as a Digital Evidence First Responder (DEFR). The DEFR is an individual who is authorised, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence.

In most organisations, digital evidence is governed by three fundamental principles: relevance, reliability and sufficiency. These three principles are important to all investigations, not just those for digital evidence to be admissible in court. These can be satisfied as follows:

— *Relevance:* It should be possible to demonstrate that material acquired contains information of value in assisting the investigation of the incident and that there is a good reason for it to have been acquired. The DEFR should be able to describe the procedures followed and explain how they decided each item was relevant.

— *Reliability:* All processes used in handling potential digital evidence should be auditable and repeatable. The results of applying such processes should be reproducible (though in the case of volatile data this may not be possible so the procedure itself must be well documented).

— *Sufficiency:* The DEFR should have taken into consideration that enough material has been gathered to allow a proper investigation to be carried out. They should also be able to give an indication of the total amount of material considered and how they decided what (and what not) to acquire. It is important that the DEFR understands this concept in order to prioritise the effort properly when time or cost is a concern.

This section will describe the *Potential digital evidence identification*, *Potential digital evidence collection*, *Potential digital evidence acquisition*, *Potential digital evidence transportation* and *Potential digital evidence storage and preservation* processes. Further details for each of these processes are available in *ISO/IEC 27037* as well as other supporting information.

3.3.1 Potential digital evidence identification

This is either the first or second process to be performed at the scene of the incident (depending on whether the *first response* process included an on-site component or not). In terms of time this will actually overlap with previous processes (in particular *first response*), but it should be considered as a separate process because it specifically looks at identifying potential digital evidence.

Potential digital evidence may be physical or logical. The physical form includes tangible objects or devices (a USB key inserted into a machine for example). The logical form refers to the virtual representation of data within a device (for example, a malicious executable file). A digital investigation will usually involve mostly the logical form.

Evidence must first, by some method, be identified as such before it can be processed and applied, and often there can be a huge amount of potential evidence. Therefore it is of vital importance that this identification happens at the scene of the incident, as if it is not, potential evidence may become changed and unusable or simply unavailable at a later point in the investigation. This is especially important when an incident happens in a cloud or networked environment[41], an environment with exceptionally large amounts of data (such as a datacentre) or in an environment where live investigations should be performed (and the DEFR should be aware of these challenges).

The DEFR should systematically carry out a thorough search for items that may contain potential digital evidence. Different types of digital devices that may contain evidence can easily be overlooked (e.g. due to small size), disguised or mixed in with other irrelevant material.

In prioritising collection or acquisition of potential digital evidence, generally one should attempt to maximise the amount of data collected. However it may be necessary to prioritise volatile items or items with especially relevant evidential value (i.e. those that are most likely to contain data relating directly to the incident under investigation),

therefore it is imperative for the DEFR to understand the reason the potential digital evidence is being collected or acquired (so they can prioritise effectively).

Potential digital evidence can be broken into two categories: volatile and non-volatile. Volatile data can be easily destroyed or lost forever if due care to protect the data is not applied. For example, removing the power supply from a digital device may result in loss of volatile data. Non-volatile data remains on the media even if the power supply is removed. Prioritisation by volatility is only applicable if the specific circumstances of the case being investigated require this. Generally it is better to acquire the most volatile potential digital evidence first, but the exact order would be situation dependent (for example if an open encrypted container is present, it may be better to acquire files from that before attempting to acquire the RAM). When encryption or malware is suspected, it is desirable to examine the volatile data. Although unlikely in an investigation conducted by the financial sector, it is possible that digital devices containing potential digital evidence may also be a source of physical evidence (e.g. fingerprints, DNA, etc.) in which case DEFRs need to take care not to spoil such evidence before proceeding to the next activities.

3.3.2 Potential digital evidence collection

Once digital evidence has been identified, it must be collected so as it can be analysed at a later stage. It must be collected in a way that preserves its integrity. This is important in order to be able to draw any sort of formal conclusions from the investigation, but especially important if the evidence will be used in court. If the evidence is intended for use in court then incorrect handling and collection procedures may result in that evidence being discounted entirely, regardless of what it might prove.

As defined in *ISO/IEC 27043*, collection is a process in the digital evidence handling process where devices that may contain potential digital evidence are removed from their original location to a laboratory or another controlled environment for later ac-

quisition and analysis. However in some cases (such as a remote server or customer device) this process can simply be gaining access to the device in a way that permits the acquisition process to take place. Devices containing potential digital evidence may be in one of two states: when the system is powered on or when the system is powered off. Different approaches and tools are required, depending on the state of the device. For more details on these approaches, see diagrams and accompanying information in Clause 7 of *ISO/IEC 27037* (essentially if the device is **on** do not swicth it **off**, if the device is **off** do not switch it **on**).

This collection process includes documenting the whole approach, as well as the packaging of these devices prior to transportation. It is also important for the DEFR to collect any material that might relate to the potential digital evidence (e.g. paper with passwords noted down). Finally, details on digital devices not collected should be documented with justification for their exclusion.

3.3.3 Potential digital evidence acquisition

Once potential digital evidence has been collected, it has to be acquired in order to permit its analysis. For example, a physical drive has been collected and now the access logs containing potential evidence must be acquired. This process involves producing a digital evidence copy (e.g. complete hard disk, partition, selected files) and documenting the methods used and activities performed (for example, a write blocker is often used to prevent accidental modification of a drive's contents). It is common practice for these copies to be made verifiable using hash functions (see *ISO/IEC 10118-2*[42]) of all the bits contained within each media item that contains potential digital evidence.

Proper data acquisition of protected devices with additional security controls such as data encryption, or mission critical systems that cannot be shutdown should be considered. In these instances, a DEFR may perform a logical acquisition, which

targets only specific data types, directories or locations. Refer to *ISO/IEC 27037* for guidance on this.

Again as mentioned in the previous subsection, adhering to strict legal regulations during this process is important to avoid evidence being classed as unusable. However note also that improper acquisition may destroy evidence (for example, attempting to acquire a file from a live system infected with advanced malware may cause the malware to deactivate itself or attempt to wipe the machine).

This process is optional at this stage, since it is not always possible to acquire one or more images of the evidence after it has been collected, however it often happens that image acquisition only takes place within a laboratory and thus this process might not happen until the first step of the *Investigation* class. It should be noted however that despite it being optional, this process must happen exactly once, either here or in the *Investigation* class (because if acquisition is not done then there will not be much to investigate, and if it is done twice then this may cause confusion and result in a waste of resources).

3.3.4 Potential digital evidence transportation

During this process, potential digital evidence is to be transported to a location where it is to be stored and analysis can later be performed. Transportation can be done physically or electronically. If the evidence is transported electronically, special precautions have to be taken to preserve the integrity and chain of custody, such as encrypting and digitally signing data.

During packaging and transporting, the DEFR needs to be aware of the possible presence of electrostatic discharge that may damage the evidential value of potential digital evidence. The DEFR should ensure that computers and digital devices are packaged securely during transportation to prevent damage from shock and vibration. The

transportation process should allow for an environment that allows control of the level of humidity, temperature and moisture such that it is suitable for the digital devices. Avoid keeping potential digital evidence and digital devices in the transporting vehicle for prolonged periods and avoid them being in the presence of Ultra Violet. Documents of the transportation and verification of the package integrity should become part of the chain of custody. For more information on the chain of custody refer to subsection 3.5.4.

3.3.5 Potential digital evidence storage and preservation

The storage of potential digital evidence might be needed if analysis cannot be performed right away or if there is a legal requirement to keep digital evidence for a certain period of time. Preservation of the integrity of the evidence and the chain of custody is of utmost importance during this process. Care must also be taken not to damage the media containing potential digital evidence due to shock, temperature, humidity, pollution, loss of power, malfunction, etc.

In the best-case scenario, there should be no damage to the data itself or any metadata associated with it (e.g. date and time-stamps). The DEFR should be able to demonstrate that the evidence has not been modified since it was collected or acquired, or provide the rationale and documented actions if unavoidable changes were made. Note that in some cases the confidentiality of potential digital evidence is a requirement (either legal or business), it should be preserved in a manner that ensures the confidentiality of the data.

The collected digital device(s) and acquired potential digital evidence should be stored in a preservation facility that applies physical security controls such as access control systems, surveillance systems or another controlled environment for digital evidence preservation. The main objectives of the physical security are to protect and prevent loss, damage and tampering, as well as enable auditability. The collected digital

device(s) should be wrapped or placed in appropriate packaging suitable for the nature of the device. Shock resistant packaging can be used to avoid physical damage to any components of the device(s). Devices sensitive to static electricity should be secured in an anti-static bag. Additional detailed storage guidelines available in *ISO/IEC 27037*.

3.4 Investigative Processes

In this section we present the *Investigative* class of processes (Figure 3.5) which deal with investigation of the incident that is the cause of the digital investigation and is concerned with analysing the evidence, interpreting results from the analysis, reporting on results of the *digital evidence interpretation* process and presenting these results in a court of law or to the relevant parties involved (e.g. regional/area managers, shareholders, Security Operations Centre (SOC)/Network Operations Centre (NOC) team leader). Finally, the digital investigation draws to a close within the *investigation closure* process.

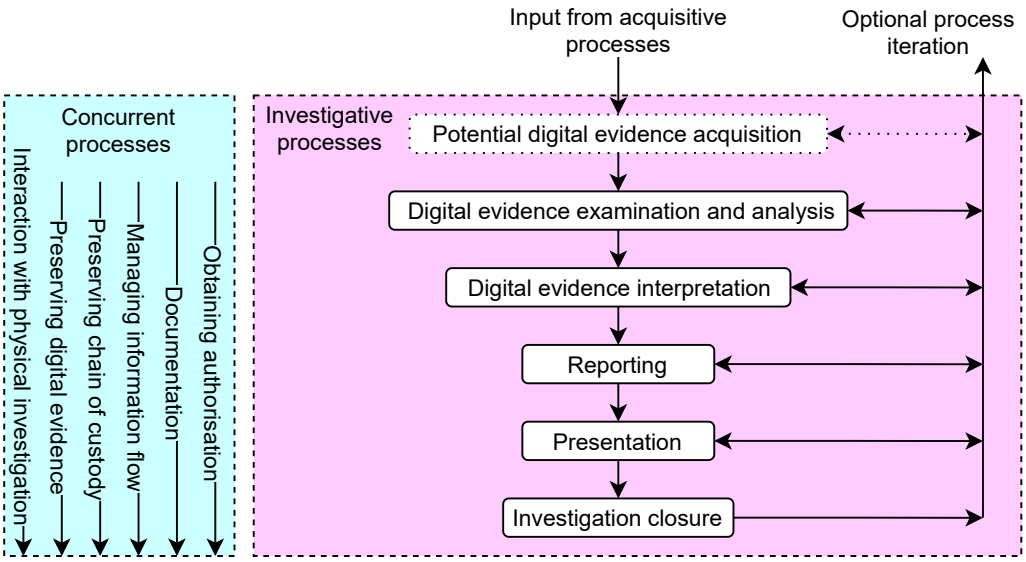

Figure 3.5: The investigative processes[10].

Prior to an investigation being conducted, it is difficult to know what action (if any) will be taken once the incident is understood. Therefore, the primary purpose of an investigation is to develop understanding of an incident. Investigation can result in improved remediation, improvements to security measures and controls for the future, disciplinary action against personnel or civil or criminal court proceedings against those responsible for the incident.

Investigators have a duty to ensure that they report their findings as fully and impartially as possible. In order to achieve this, the team should adopt a structured approach to the investigation. Investigators should be aware of areas of uncertainty in their findings and aim to prove their hypothesis (of what has happened) beyong reasonable doubt. Uncertainty should be considered inversely proportional to the quality and quantity of evidence in support of a hypothesis, in other words, the more supporting and convincing evidence there is, the more certain investigators should be of the findings.

It is assumed that at this stage of the investigation potential digital evidence bas been acquired and is available (as this process was optional in the *Acquisitive* class, it may not yet have been done, thus it is represented with a dashed line in Figure 3.5). For details of this process, see the *Potential digital evidence acquisition* subsection 3.3.3, as this will not be covered again in this section.

This section will describe the *Potential digital evidence examination and analysis*, *Digital evidence interpretation*, *Reporting*, *Presentation* and *Investigation closure* processes. Further details on some of these processes are available in *ISO/IEC 27042* as well as other supporting information.

3.4.1 Potential digital evidence examination and analysis

Examination and analysis of potential digital evidence involves the use of a large number of techniques to identify digital evidence as well as reconstructing it, if needed. In order to formulate a hypothesis on how the incident occurred, one should define what its exact characteristics are and who is to be held responsible. Formulating a hypothesis in this context basically involves the reconstruction of a sequence of events that have led to the current state of the system being investigated. The challenge of present-day digital investigations is the diversity, volume and complexity of the data to be analysed.

As volumes of data to be examined and analysed can be vast, accredited automated techniques are often employed to complement manual validation techniques. These should be decided in the *planning* process during the *Initialisation* phase (see 3.2.3) and the procedures specified in *ISO/IEC 27041* should be followed when selecting them [43]. The user should be competent to use the tools in the context of the investigation.

This process is likely to be an iterative one as each item of digital evidence identified can lead to the re-consideration of other digital evidence. Sufficient contextual information (about the incident, system affected and sources of evidence) should also be available to allow the investigator to make informed decisions about each item under consideration. Investigators and their support staff must therefore be competent to carry out their roles in the analysis. Competence may be defined/measured in terms of the individual processes they will carry out (do they have an appropriate qualification or experience?), or as a set of well-defined competencies against which they can be assessed (a relevant industry certification for example). Where there is a chance of damage to potential digital evidence, appropriate measures should be taken to minimise the likelihood, or the effects, of any such damage (e.g. using a write blocker to minimise the chance of inadvertently modifying the contents of a drive). However, if some form of damage is inevitable or strictly necessary, the investigative team should be able to explain the effects of their actions and provide justification for doing so.

The most common method for analysing potential digital evidence is known as "static analysis" (in this case meaning the analysis of any non-live digital evidence) which would normally be carried out on a copy of the original to avoid accidental damage or obfuscation to potential evidence, however in some circumstances it may be necessary or beneficial to examine a "live" version instead (for example, to observe behaviour of a piece of malware). Further details of the types and methods of analysis are outside the scope of this document and the reader should refer to *ISO/IEC 27042*. Additionally, from this point onwards, "potential digital evidence" becomes "digital evidence" according to the definitions of "potential digital evidence" and "digital evidence" (see appendix A).

3.4.2 Digital evidence interpretation

In this process the results from the previous process (subsection 3.4.1) should be interpreted. Interpretation of any evidence is dependent on the information available about the circumstances surrounding the creation of that item of evidence (for example, if evidence was found of a sophisticated strain of malware, this could potentially be interpreted as a direct attack against the organisation). To be able to carry out a proper interpretation, information from persons involved in the day-to-day running of the system(s) which are being investigated, is often required. Information about the purpose of the investigation and a definition of the scope of the investigation are also required and should be provided to the investigator.

When assessing evidence care must be taken to distinguish facts that have been found and information that has been inferred. For example, the presence of a file on a device is a fact. If that file was an attachment to an email in an inbox, it can be inferred that the file was created on the device due to being received in an email, hence this is inferred information. When reporting facts and inferred information, the distinction between the two needs to be stated and the reasoning behind the inference should be clear.

As the main goal of this process is to provide an explanation for the digital artefacts identified in subsection 3.4.1 (within the context of the investigation), then if the contextual information changes the interpretation may also have to change. The investigator should also document their reasoning for this explanation. A further objective of this process is to classify the interpreted evidence according to relevance. This means that the evidence (according to the interpretation) is organised in such a way that it distinguishes which digital artefacts are more important than others. This decision process is at the discretion of one or more competent investigators. For more details on the process of interpretation, the reader should refer to *ISO/IEC 27042*.

3.4.3 Reporting

The interpretation produced in the previous process (subsection 3.4.2) forms the main output of the investigation, i.e. the report. According to the exact wording of the standard (*ISO/IEC 27043*) "the report should, where economical, be printed on paper", however, it is the opinion of the author that a digital version should also be prepared (and could be distributed as a PDF document if needed). One should also refer to the *Traffic Light Protocol* presented in subsection 3.5.3 to ensure the correct designation is used (depending on the contents of the report, the people whom it may be shared with could be more or less restricted).

Prior to commencing the investigation, the nature and purpose of the final report should be decided by the person in charge of the investigation. This should be used to guide the investigative process and may consist of a set of questions to be answered, an indication of the likely readers of the report and details of any constraints and limitations which apply to the investigation.

The report should be written in simple language and should be clear, concise and unambiguous in its statements. It should also be understandable for a wide audience whom do not necessarily possess a technical understanding of incident investigations. Such audiences include, but not limited to, managers, shareholders, employees, legal team, prosecutors and judges. It is possible that during an investigation, the number of digital evidence artefacts could be many. Therefore, one should take care to list all relevant digital evidence in the report in order to assure that no valuable evidence is omitted. For a detailed list of suggested report content, one can consult *ISO/IEC 27042*[14].

The author(s) of a report should always be aware of the potential impact of the report on all the applicable audiences as mentioned above. Authors of such reports should also keep in mind possible consequences of potentially wrong or misinterpreted reports. Therefore, the report should elaborate on issues such as which potential evidence was collected/acquired, which analysis techniques were performed and what

outcome results from this. Sometimes no clear outcome is possible based on the available evidence. In such a case, the report should state clearly the assumptions made, how probable these are and the conclusions arising from the assumptions. It is essential to emphasise the hypothetical character of such conclusions.

3.4.4 Presentation

The report created during the previous process (subsection 3.4.3) is to be presented to all stakeholders. In the case of an internal company incident, stakeholders may be the company management team, shareholders and the employees involved. In the case of a court case the stakeholders include the judge, jury, accused, solicitors/barristers and prosecutors, as well as any other interested party.

The main purpose of this process is to conduct a live demonstration of the results of the report (including conclusion/hypothesis and relative evidence). This demonstration can be performed using questions and answers, as an oral presentation, as an expert witness testimony or whatever is suitable for the case. This demonstration also includes proving the validity of the conclusion/hypothesis if/when it is challenged. Thus, the one who presents the hypothesis should be prepared for it and should preferably have had insight into the *reporting* process. Additionally, if the findings of the report could be relevant to the security of other member banks or the industry as a whole, then the information should be shared with them.

3.4.5 Investigation closure

This process concludes the investigation and a decision is to be made on the validity of the hypothesis presented in the previous process (subsection 3.4.4). The digital investigation process is iterative, so after completing this process one can go back to any of the earlier processes that follow the *first response* process. For example,

if the investigation concludes that there is insufficient evidence for a conviction, the investigators could return to the *Potential digital evidence examination and analysis* process (subsection 3.4.1) to attempt to gather more convincing evidence.

This process should also include the following sub-processes:

— record acceptance or rejection of the hypothesis;

— deciding on the need to iterate to a previous process (see example above);

— returning evidence if needed (for example if equipment was seized for the investigation);

— destruction of evidence if needed (depending on the laws in the organisations jurisdiction). The way in which evidence is destroyed, or whether it is destroyed at all, or whether it needs to be stored for a certain period of time after the case has been completed, all depends on the local laws. More information on the destruction of data can be found in *ISO/IEC 27040*. More information on storage of data can be found in *ISO 15489-1*;

— distribution of relevant information to all stakeholders (i.e. deciding the acceptance or rejection of the hypothesis, communicating the need to iterate to a previous process, providing any documents from the *presentation* process or sharing information with other member banks);

— debriefing and lessons learned. For example, if the investigation concludes that due to a vulnerability in a particular system, a successful cyber-attack was carried out against the organisation by a bad actor, the organisation might wish to iterate through the *Readiness* processes to fix the vulnerable implementation and/or update relevant procedures.

3.5 Concurrent Processes

Throughout the whole digital investigation there are several processes that do not fit within a single class (eg. within *Readiness*, *Initialisation*, *Acquisition* or *Investigation*), but rather take place alongside the rest of the investigation processes. These processes are the following: *obtaining authorisation*, *documentation*, *managing information flow*, *preserving chain of custody*, *preserving digital evidence*, and *interaction with physical investigation*. In this section we will cover each of these processes in more detail.

These processes are defined as *Concurrent processes* and are principles which should be applied throughout the digital investigation (see Figure 2.2 or Appendix B), as they are applicable to many other processes within the investigation. For example, documentation is important at every stage as all tasks throughout the investigation should be properly documented and logged.

The processes presented in this section are justified as these principles should be translated into actionable items. It is also important these processes (especially the preservation of evidence and chain of custody) run concurrently with all others in order to assure full admissibility of the digital evidence in court. Other processes such as obtaining authorisation and documentation are obviously required throughout the investigation.

3.5.1 Obtaining authorisation

For each process performed during the digital investigation, proper authorisation should be obtained. Such authorisation might be required from management, government authorities (Ombudsman, Data Protection Commissioner), system owners, system custodians, users, etc. It is important to obtain proper authorisation for actions performed during the digital investigation process in order not to infringe on the rights of system

owners or its users but also to assure that no legal rules are infringed and that evidence obtained will be admissible in court. Exactly what type of authorisation is needed would depend on both the legal environment and the organisational environment where the investigation is taking place.

3.5.2 Documentation

Each process performed should be documented in order to assure that it can be reproduced (for verification by an independent third party for example) and that chain of custody is preserved. Good documentation will also improve efficiency and increase the likelihood of a successful investigation. Proper documentation should also be demonstrated during the *Presentation* process (see subsection 3.4.4). This is closely related to APCO Principle 3 (see subsection 2.2.1).

During the *Readiness* processes, this process will include documentation of the outputs of the planning processes and especially the procedures that have been defined during those processes. Details of the systems and software in use (and links to relevant user manuals in case they should be required) should also be documented.

During the *Initialisation* processes, documentation will include any alerts from the incident detection, notes of actions taken during the first response, and details of the plan for the rest of the investigation.

During the *Acquisitive* processes, this process should include documentation of the incident scene if applicable, which would be performed at the scene of the incident and would include written (or typed) documentation of activities, photographs, videos, sketches and labelling any potential digital evidence. All activities performed in relation to the investigation should be recorded, as should details of the architecture and components of the system where the incident occurred (if applicable). This could include such things as serial numbers, time and date setting (if the digital devices are

powered on) or anything visible on a digital device screen (e.g. active programs and documents).

During the *Investigative* processes, specifically throughout the *Potential digital evidence examination and analysis* process, each person carrying out any process should keep accurate and detailed notes of their actions and the results of those actions. These should be sufficiently detailed to allow another similarly competent person to repeat those actions and achieve the same results. The notes should include details of relevant information received and decisions taken, including reasons for the decision.

3.5.3 Managing information flow

A structured set of protocols to control information flow should exist between each of the processes and among the different stakeholders. It is important to identify and describe information flows so that they can be secured and supported technologically. For example, an information flow could refer to the exchange of investigation progress reports via email between an investigator and their superior. Protection of this information flow could be in the form of, for example, encryption with PGP to ensure confidentiality and the use of digital signatures to guarantee authenticity. Similar protections should also apply to all of the incident response planning discussed in the *Readiness* class.

Additionally, there should be a protocol in place to dictate how information is to be shared. Chosen because of its simplicity and intuitiveness, the use of the well-established *Traffic Light Protocol* is recommended (see subsection 2.2.2).

Common usecases for TLP are corporate email and document exchange, though one should take care that it does not become a hinderance by being misused (for example, if everything is in TLP:RED it either becomes impossible to share any information, or the meaning of TLP:RED itself gets diluted and genuinely sensitive information is no

longer properly distinguished). To avoid misuse persons using it should be provided with the above definitions when they are introduced to the system and optionally can receive additional training (such as a short practical quiz with some examples).

3.5.4 Preserving chain of custody

In any investigation, the investigator should be able to account for all the acquired data and devices at the time it is within their custody. All legal requirements should be complied with and as before, any actions should be properly documented in order to preserve chain of custody as the evidence is handled by several parties. See also ACPO Principle 3 (subsection 2.2.1).

This process is to be performed from the *incident detection* process (subsection 3.2.1) until the last process, however the creation and set up of SOPs covering how this will be done should happen in the *Planning* processes of the *Readiness* class (see subsection 3.1.1). It also runs concurrently with two of the *Implementation* processes, see subsections 3.1.2 and 3.1.2.

The chain of custody record is a document identifying the chronology of the movement and handling of the potential digital evidence (see Appendix C for an example). It should be created at the start of the collection or acquisition process. This will typically be accomplished by tracing the history of the item from the time it was identified, collected or acquired by the investigating team up to the present status and location. The chain of custody record itself may comprise more than one document (for example, a separate document for a device sent to a specialist laboratory for analysis). The chain of custody should be maintained throughout the lifetime of the evidence and preserved for a certain period of time after the end of the lifetime of the evidence (depending on local jurisdiction).

As a minimum, the chain of custody record should contain the following:

— Unique evidence identifier;

— Who accessed the evidence and the time and location it took place;

— Who checked the evidence in and out from the evidence preservation facility, when it happened why it was checked out (which case and the purpose) and the relevant authority (if applicable);

— Any unavoidable changes to the potential digital evidence, as well as the name of the individual responsible and the justification for the introduction of the change.

3.5.5 Preserving digital evidence

Preserving digital evidence means to preserve the integrity of the original digital evidence. In order for this to be achieved, strict procedures should be put in place from the time the incident is detected until such time as the investigation is closed. These procedures should be defined in the organisation's SOPs during the *Planning* processes of the *Readiness* class (see subsection 3.1.1). Additionally this process runs concurrently with two of the *Implementation* processes, see subsections 3.1.2 and 3.1.2. In relation to this process, one should also take note of ACPO Principle 1 and Principle 2, which are closely related.

The procedures should ensure that the original evidence is not changed and more importantly, they should ensure that there is no means by which the original evidence may be changed, destroyed, stolen, lost, etc. This includes assessing and documenting the integrity of digital evidence after processing it (for example, after transporting the evidence or after performing analysis on it, the integrity of the evidence should be confirmed). See also the *Potential digital evidence storage and preservation* process (subsection 3.3.5) for details on storage.

3.5.6 Interaction with physical investigation

The digital investigation can interconnect with the physical investigation or even be dependant on it, if that investigation is conducted in relation to the same incident. In fact, it is often the case that the physical investigation needs assistance from the digital forensic investigation. For example, a digital investigation (of computers, mobile phones, social network activities, email communication, communication via chat rooms and forums etc.) could help to reveal communication between cyber-criminals. On the other hand, the digital investigation might also need assistance from a physical investigation. An example could be interviewing witnesses (which is an activity within the physical investigation) to supplement results of the digital forensic investigation in the case of an employee using proprietary company information for personal benefit.

Therefore the interaction between the two investigations is important for the preservation of the integrity of digital evidence, protecting the digital evidence from damage and preserving the chain of custody. It is also important that a cooperative relationship between the two investigations is established as this will enable investigators to work more efficiently and adapt more easily to any changes in scope or investigation objectives that might arise.

This process starts from the *first response* process (subsection 3.2.2), but the planning and setup of SOPs for it should happen during the *Planning* processes of the *Readiness* class (see subsection 3.1.1).

Chapter 4: **Development of the Playbook**

In this chapter we will present and discuss the playbook that has been developed as the main deliverable of this research. The playbook developed here is specific to a ransomware incident investigation and was developed from industry best practice while also ensuring compliance with *ISO/IEC 27043*. The full playbook in its raw form is attached to this thesis as Appendix F.

As mentioned in Chapter 2, the industry standard for incident response plans is either the NIST 4 phase method or SANS 6 steps method. Both of these provide a good basis for our own playbook, however in order to maintain compliance with *ISO/IEC 27043* some adjustments and additions are needed (such as the *Concurrent* or *Investigative* processes). In the interest of comparison we will briefly explain where the NIST/SANS steps fit into *ISO/IEC 27043*: *Preparation* is essentially the same as the *Planning* processes in the *Readiness* class while *Detection & Analysis* lines up with the *Incident detection* and *First response* processes of the *Initialisation* class. *Containment, Eradication, & Recovery* also mostly fits into that *First response* process (*Recovery* is outside of *ISO/IEC 27043*'s scope). Finally, *Post-Incident Activity* ties nicely to the *Reporting*, *Presentation* and *Investigation closure* processes of the *Investigative* class.

The playbook is divided into 4 main sections: *Guiding Principles*; *Pre-Incident*; *Incident Detection, First Response and Recovery*; and *Incident Investigation and Post-Incident*. This format was chosen to combine exisiting industry practices with *ISO/IEC 27043*'s processes in a user-friendly layout while still remaining fully compliant. The rest of this chapter will give a more detailed breakdown of what processes have been included in which sections.

4.1 Guiding Principles

This section contains all of the *Concurrent* class processes except for *Interaction with physical investigation* as this process is not applicable in our ransomware scenario (at least not in the way it is defined in *ISO/IEC 27043*).

This was chosen as the first phase as these principles should be kept in mind throughout the incident and ensuing investigation, and it is not much use to the reader to only discover them at the end of the document. The main points are control of information, documentation and taskings, all of which will be applicable for the entire process. Doing these things well will naturally improve every other process and foster an efficient professional environment[12].

4.2 Pre-Incident

This section contains all of the *Readiness* class processes. They are not all mapped one-to-one with specific steps but from a compliance standpoint all elements of the processes are covered by the broader scopes of the three subsections *Planning*, *Implementation*, and *Assessment*. Just as deifined in the ISO[10], this section happens in advance of any incident or investigation, in the hope of mitigating those same. As such it would expected to regularly review this section in particular and implement changes where appropriate.

Planning is a mostly "pen and paper" task focused on gathering information required for a better defence (threat intelligence, assest lists) and defining procedures. This is also the best place to make any changes to playbooks (including this one) based on information collected or threats detected. We may optionally also identify equipment requirements for the Incident Response Team themselves (such as laptops, screens, whiteboards, etc.), although this outside the scope of a ransomware specific playbook

and would be better defined elsewhere and simply referenced.

In this part of the playbook we mention a "Go-Bag", this is effectively a list of items that an investigator or responder considers essential to have on hand when an incident occurs. We have suggested our own in Appendix E, though the response team should add or remove to suit their own use cases. The one suggested in this body of work is closer to that of (and inspired from) the NCSC than An Garda Síochána's as the latter is tailored more for a traditional crime scene containing elements of IT, compared to the former being entirely focused on cybercrime. Addtional notes on specific choices are detailed in that Appendix.

Implementation is more hands on and attempts to turn all of the theoretical work of the previous step into actioned items and working defences. This step is where we would update and patch hosts on the network, configure defensive software such as anti-virus, create detection rules for common and currently faced threats and give training to staff and responders.

Finally, *Assessment* should be an opportunity to test the plan, this can be done with a "live" exercise, or just a tabletop version. A live one is usually more realistic but is generally more expensive and time consuming to organise[11][44]. Any lessons learned from these exercises should be fed back into the development of the procedures so the next one is smoother[20] (and participants are better prepared for the real thing). Not explicitly mentioned in the playbook but perhaps worth a consideration is the use of smaller scale drills for common attack vectors, such as emails with supicious attachements or wording to see how well staff are detecting and reporting them.

4.3 Incident Detection, First Response and Recovery

This section is very much the "action" part of the playbook and because of this it is by far the most detailed. In terms of *ISO/IEC 27043* compliance this section contains all of the *Initialisation* processes but in particular the *Incident detection* and *First response* processes. While not aligned to a specific step, elements of several steps in this section also cover the first 2 processes of the *Acquisitive* class, *Potential digital evidence identification* and *Potential digital evidence collection*. Additionally this section includes procedures for *Recovery*, which is not itself defined in *ISO/IEC 27043* but still has an important place in a ransomware playbook.

The primary focus of this section will be on containing and neutralising the threat, and then getting systems back up and running. First steps are detection, classification and the triage[45], before taking action and escalating to others. After identifying the incident and analysing it on the related systems, next we contain the risk, isolate infected system from the still-clean environment and start removing the malware. Due to the critical nature of ransomware and the effect it may have on other systems[3] some steps in this section may get merged together or happen out of order.

At one point in this section, there is a mention invoking a "Data Loss" playbook, this is not defined within the thesis as it is considered outside its scope, and would need to be obtained elsewhere. It is usally a lot less technical however and large parts are covered by exisiting legislation such as GDPR[46][47].

The recovery phase of the playbook is the only significant part that has no equivalent in *ISO/IEC 27043*, however this is still a crucial part of a practical ransomware incident playbook so it is detailed here. Restoring the functionality back to the level before the malware infection and removing the containment measures are the goals for the recovery phase.

A particular point of note in this last part is the decision to pay the ransom or not.

This needs to be decided at the board/executive level who should first contact An Garda Síochána and report the cybercrime. However it should be noted that paying the ransom does not guarantee access to the encrypted data or systems[3]. Even if the ransom is paid, threat actors may still carry out the following actions:

— Demand more money.
— Continue to infect the organisations' devices (or others).
— Re-target the organisation with a new attack.
— Copy, leak, or sell the data.

Additionally the payment may be used to fund and support other illicit activities. As noted in the PWC report on the infamous HSE ransomware attack[2], a precedent was set by Ireland for **not** paying the ransom.

4.4 Incident Investigation and Post-Incident

This section returns to the core of *ISO/IEC 27043* and is generally absent or skimmed over in the NIST/SANS methodologies. It contains the remaining three processes from the *Acquisition*, namely *Potential digital evidence acquisition*, *Potential digital evidence transportation* and *Potential digital evidence storage and preservation*. Additionally it contains all of the processes in the *Investigative* class and thus rounds of the whole process.

The *Potential digital evidence transmission and storage* subsection covers *Potential digital evidence transportation* and *Potential digital evidence storage and preservation*, while the *Digital evidence acquisition, examination and interpretation* subsection integrates the *Potential digital evidence acquisition*, *Potential digital evidence examination and analysis* and *Digital evidence interpretation* processes. The *Reporting* and *Presentation* processes are combined under the eponymous subsection, and finally the *Investigation closure* process along with lessons learned is present in the last subsection.

Chapter 5: **Evaluation of the Playbook**

In order to evaluate the effectiveness of *ISO/IEC 27043* in helping to investigate incidents as part of a compliant playbook, it had to be tested against either a real or simulated incident (as this would be the best way to reveal any strengths and weaknesses[44]). Additionally it seemed a reasonable idea to also evaluate its use by a team rather than an individual (as this would be more realistic).

Being able to evaluate it directly in the financial sector would probably have been ideal, however, another opportunity presented itself in the form of a large military cyber training exercise with the Irish Defence Forces. This was actually a very suitable alternative as the Defence Forces also provide assistance to outside groups if there is a risk to national interest (most notably the relatively recent attack on the HSE). It also provided a unique opportunity to observe other organisations own response plans in motion and exchange ideas and information with various industry partners (including some from an Irish bank's security team). This exchange provided not only a practical test of the playbook we have developed, but also an element of industry peer review that might have otherwise been difficult to obtain.

This military exercise is known as Cyber Coalition. Held annually for over a decade now, it is NATO's flagship annual collective cyber defence exercise and one of the largest in the world. There is no competitive element to this particular exercise, but rather it is large scale learning, training and information sharing exercise with a range of possible scenarios (based on real events or current threats). As a partner nation Ireland sometimes participates. Exact details of the exercise contents can not be published, but in this edition Ireland chose two incidents to practice, one of which was a ransomware scenario (eerily similar to that of the HSE). It was on this scenario that we were given the opportunity to evaluate the playbook developed here and compare it to exisiting methods.

The Defence Forces incident response plan is mainly based off the NIST methodology and so offers us a good comparison to the rest of the industry. In terms of content both are very similar with regards to the "action" part (identification, first response, eradication and recovery), but differ a lot more on the investigation and compliance aspects. It was noted however that while sections such as our *Guiding Principles* don't appear in their playbook, they are implemented anyway in practice as part of wider organisation Standard Operating Procedures.

In terms of performance and usability again both methods achieved roughly the same outcome on the "action" section(s), however we did observe that the remainder of the *ISO/IEC 27043* based playbook has certain disadvantages in terms of speed and flexibility due to its compliance requirements. For example, the need to slow down the early steps when speed of response might be key, in order to preserve and collect as much potential digital evidence as possible for later analysis during the more formal investigation. The NIST based playbook would act a lot quicker and performs the investigation almost on the fly, however in doing so not only was there more destruction of evidence but the investigation write up afterwards was also more challenging due to the fragmentation of some information.

To conclude this evaluation, the *ISO/IEC 27043* compliant playbook we have created definitely has merits in terms of strict preservation of evidence and a thorough investigative process overall, however due to the urgent nature of the response required for a ransomware investigation (and perhaps the worthwhile sacrifice of evidence to instead preserve system integrity and achieve a rapid recovery), this playbook was not able to display its full potential and might have done better against a more traditional forensic investigation scenario. Despite these shortcomings, it does retain one key advantage of the NIST methodology, and that is its compliance aspect for any organisation wishing to or having already obtained *ISO/IEC 27001* certification.

Chapter 6: **Conclusions**

In order to be successful, the incident response policy should be created and implemented as an enterprise-wide process, therefore all stakeholders or their representatives should be involved and the policy should be approved by a member of top management. Personnel need to be able to recognise an incident, know what to do and understand the benefits of the organisation's approach. Management needs to be supportive of the policy to ensure that the organisation commits to maintaining their incident response capabilities ("make sure that your incident response plan is up to date and tested, rather than a letter to your successor"). A worthwhile read regarding organisation-wide security awareness is the *SANS Security Awareness Roadmap* poster[48].

An organisation's Incident Response Team (IRT) plays a vital role in their overall information security. It requires collaboration of all personnel to detect, resolve and investigate incidents that occur, therefore it must be viewed as trustworthy by the whole organisation as well as external partners. Especially for external partners, this trust is earned through the reputation of how well it handles cybersecurity incidents, in addition to a proven track record of compliance with industry standards.

We sought to answer the following question: **Can a playbook be developed from *ISO/IEC 27043* that is both effective in a ransomware investigation while remaining compliant with the Standard?** To that end we successfully developed a playbook in line with these requirements and evaluated it against a very realistic exercise scenario utilising a full IRT. The results were satisfactory although improvements could still be made. Future research could apply this Standard and playbook style to a more traditional forensic investigation scenario, which might achieve better results. This playbook did however fulfill its principal goal of maintaining compliance with *ISO/IEC 27043* in a practical, real-world investigation.

Several more minor conclusions also emerged from the evaluation and the wider industry: the first was the importance of command and control (as wielded by the tead lead/incident handler) in the investigation to avoid any destruction of evidence or loss of data. During the exercise some mistakes were made by the team which ultimately lead to portions of data being unrecoverable where they should not have been. This was caused by a failure to ensure team members actually stuck to the defined procedures throughout the entire process.

The second was that getting hit with ransomware is a worst case scenario, the attackers will almost certainly have exfiltrated data from the system and sell/publish it if the ransom is not paid. If the ransom is paid then the organisation is funding and incentivising organised crime, and they may decide to sell/publish the data anyway. Given the extremely precarious position this would put the organisation in, it should be obvious that it is in the best interest of any organisation to invest time and resources in to preparation and especially prevention.

And finally, collaborative exercises on a small or large scale serve to encourage the exchange of knowledge, threat intelligence, good practices and experience with other industry partners, particularly in the case of Ireland as the cybersecurity community is small but many organisations will face the same threats and these exchanges will help strengthen the overall industry.

The author hopes that with the information and guidance provided in this thesis (and accompanying ransomware investigation playbook), the reader will be able to better design and implement procedures for digital investigations within their organisation in compliance with *ISO/IEC 27043* and thus ensure greater compliance with *ISO/IEC 27001*.

Appendix A: **Definitions and Abbreviations**

A.1 Terms and definitions

Acquisition: process of creating a potential digital evidence copy.

Analysis: process of evaluating potential digital evidence in order to assess its relevance to the investigation (potential digital evidence, which is determined to be relevant, becomes digital evidence).

Attack: attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Chain of Custody: the documentation showing the full process of acquisition, transfer and handling of physical or electronic materials.

Collection: process of gathering the physical items that contain potential digital evidence.

Competence: ability to apply knowledge and skills to achieve intended results.

Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control: measure that is modifying/reducing risk.

Digital evidence: information or data, stored or transmitted in binary form, that may be relied on as evidence

Digital Evidence First Responder: individual who is authorised, trained and qualified to act first at an incident scene in performing digital evidence collection and acquisition with the responsibility for handling that evidence.

Digital Evidence Specialist: individual who can carry out the tasks of a DEFR and has additional specialised skills.

Digital investigation: use of scientifically derived and proven methods towards the identification, collection, transportation, storage, analysis, interpretation, presentation, distribution, return, and/or destruction of digital evidence derived from digital sources, while obtaining proper authorisations for all activities, properly documenting

all activities, preserving digital evidence, and maintaining the chain of custody, for the purpose of facilitating or furthering the reconstruction of events found to be incidents requiring a digital investigation, whether of criminal nature or not.

Examination: set of processes applied to identify and retrieve relevant potential digital evidence from one or more sources.

Identification: process involving the search for, recognition, and documentation of potential digital evidence.

Incident: single or a series of unwanted or unexpected information security breaches or events, whether of criminal nature or not, that have a significant probability of compromising business operations or threatening information security.

Information security: preservation of confidentiality, integrity and availability of information.

Information security incident management: processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.

Integrity: property of accuracy and completeness.

Interpretation: synthesis of an explanation, within agreed limits, for the factual information about evidence resulting from the set of examinations and analysis making up the investigation.

Investigation: application of examinations, analysis, and interpretation to aid understanding of an incident.

Investigator: member of the investigative team, including the investigative lead.

Logic-bomb a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Malware: Malicious computer software that interferes with normal computer functions or sends personal data about the user to unauthorized parties over the Internet.

Method: definition of an operation which can be used to produce data or derive information as an output from specified inputs. Ideally, a method should be atomic (i.e. it should not perform more than one function).

Monitoring: determining the status of a system, a process or an activity (to determine the status, there may be a need to check, supervise or critically observe).

Phishing: The act of sending email that falsely claims to be from a legitimate organisation. Usually combined with a threat or request for information (imminent account

closure, a bill payment is due, or udate account information). The email will ask the recipient to supply confidential information, such as bank account details, PINs or passwords. These details are then used to conduct fraud, gain system access or steal further information.

Policy: intentions and direction of an organization as formally expressed by its top management.

Potential digital evidence: information or data, stored or transmitted in binary form, which has not yet been determined, through the process of examination and analysis, to be relevant to the investigation.

Preservation: process to maintain and safeguard the integrity and/or original condition of the potential digital evidence and digital evidence.

Process: set of activities that have a common goal and last for a limited period of time.

Ransomware: Malware that encrypts the files of a computer or data of a user and requires a payment to be made by the victim to the attacker (usually in Bitcoin) in order for the victim to regain access to the files/data.

Readiness: process of being prepared for a digital investigation before an incident has occurred.

Stakeholder: person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Threat: potential cause of an unwanted incident, which may result in harm to a system or organisation.

Validation: confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

Volatile data: data that is especially prone to change and can be easily modified.

Vulnerability: weakness of an asset or control that can be exploited by one or more threats.

YARA rule: a rule for the pattern-matching software "YARA".

A.2 Abbreviated terms

ACPO: Association of Chief Police Officers.

APT: Advanced Persistent Threat.

ATM: Automated Teller Machine.

AV: Anti-Virus.

BPFI: Banking and Payments Federation of Ireland.

C2: Command & Control.

CCTV: Closed Circuit Television.

CIRT: Computer Incident Response Team.

CVE: Common Vulnerabilities and Exposures.

CVSS: Common Vulnerability Scoring System.

DDoS: Distributed Denial of Service.

DEFR: Digital Evidence First Responder.

DES: Digital Evidence Specialist.

DFR: Digital First Responder.

DNS: Domain Name System.

EDR: Endpoint Detection and Response.

FIRST: Forum of Incident Response and Security Teams.

FSCC: Financial Service Cybersecurity Community.

HSE: Health Service Executive.

IDS: Intrusion Detection System.

IOC: Indicator Of Compromise.

IP: Internet Protocol.

ISP: Internet Service Provider.

LAN: Local Area Network.

MD5: Message-Digest algorithm 5.

NCSC: National Cyber Security Centre.

NIST: National Institute of Standards and Technology.

NOC: Network Operations Centre.

RAM: Random Access Memory.

RDP: Remote Desktop Protocol.

SANS: Sysadmin, Audit, Network and Security.

SIEM: Security Incident and Event Manager.

SOC: Security Operations Centre.

SOP: Standard Operating Procedure.

TLP: Traffic Light Protocol.

TTP: Tactics, Techniques, and Procedures.

USB: Universal Serial Bus.

VERIS: Vocabulary for Event Recording and Incident Sharing.

VPN: Virtual Private Network.

YARA: Yet Another Recursive Acronym.

WiFi: Wireless Fidelity.

Appendix B: **Full Digital Investigation Process**

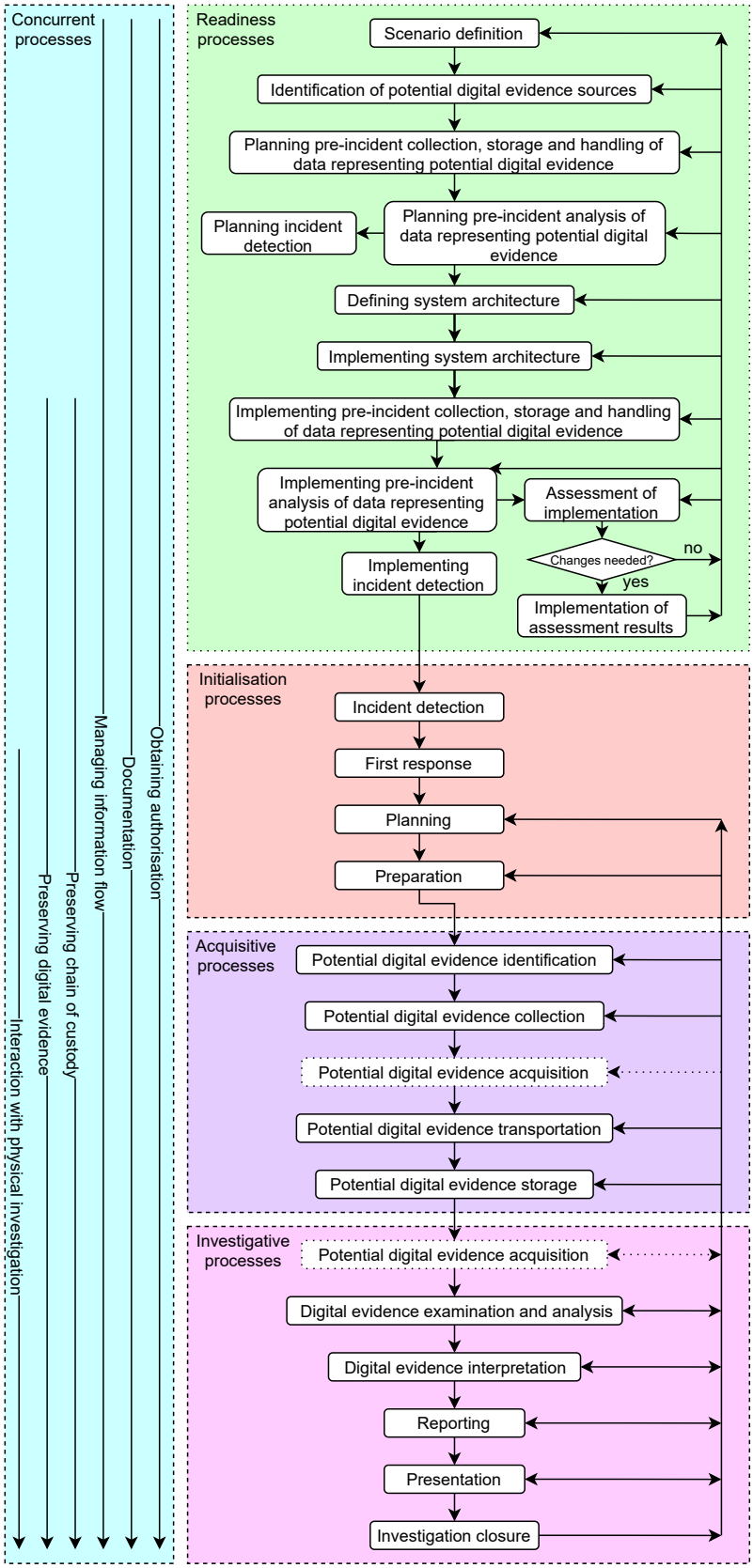

Figure B.1: Fully expanded process diagram[10]

Appendix C: **Example Chain of Custody Form**

Print Form

PROPERTY / EVIDENCE CHAIN OF CUSTODY FORM

APLCS, LLC (http://www.aplcs.com)

Case Name:		**Reason Obtained:**	
Case Number:			
Item Number:	**Evidence Type / Manufacturer:**	**Model Number:**	**Serial Number:**
Content Owner / Title:	**Content Description:**		
Content Owner Contact Information:			
Forensic Agent:	**Creation Method:**	**HASH Value:**	**Creation Date/Time:**
Forensic Agent Contact Information:			

CHAIN OF CUSTODY

Tracking Number	Date / Time	Released By	Received By	Reason for Change
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: _____

Page: 1 of _____

CHAIN OF CUSTODY				
Tracking Number	**Date / Time**	**Released By**	**Received By**	**Reason for Change**
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	
	Date:	Name / Title	Name / Title	
	Time:	Signature	Signature	

Item Number: ______________________ **Page:** _____ **of** _____

Figure C.1: Sample chain of custody form (APLCS, LLC)

Appendix D: **ISO27035 Security Incident Forms**

INFORMATION SECURITY EVENT REPORT			Page 1 of 1
1. Date of event		**3. Related event and/or incident identity numbers** *(if applicable)*	
2. Event number[2]			
4. REPORTING PERSON DETAILS			
4.1 Name		**4.2 Address**	
4.3 Organization		**4.4 Department**	
4.5 Telephone		**4.6 E-mail**	
5. INFORMATION SECURITY EVENT DESCRIPTION			
5.1 Description of the event: What occurred How occurred Why occurred Initial views on components/assets affected Adverse business impacts Any vulnerabilities identified			
6. INFORMATION SECURITY EVENT DETAILS			
6.1 Date and time the event occurred			
6.2 Date and time the event was discovered			
6.3 Date and time the event was reported			
6.4 Is the response to this event closed?	**YES** ☐ **NO** ☐ *(tick as appropriate)*		
6.5 If yes, specify how long the event has lasted *(in days/hours/minutes)*			

Figure D.1: Sample information security event report[11]

INFORMATION SECURITY INCIDENT REPORT			Page 1 of 6
1. Date of incident		3. Related event and/or incident identity numbers *(if applicable)*	
2. Incident number[3]			
4. POINT OF CONTACT MEMBER DETAILS			
4.1 Name		4.2 Address	
4.3 Organization		4.4 Department	
4.5 Telephone		4.6 E-mail	
5. IRT MEMBER DETAILS			
5.1 Name		5.2 Address	
5.3 Organization		5.4 Department	
5.5 Telephone		5.6 E-mail	
6. INFORMATION SECURITY INCIDENT DESCRIPTION			
6.1 Further description of the incident: What occurred How occurred Why occurred Initial views on components/assets affected Adverse business impacts Any vulnerabilities identified			
7. INFORMATION SECURITY INCIDENT DETAILS			
7.1 Date and time the incident occurred			
7.2 Date and time the incident was discovered			
7.3 Date and time the incident was reported			
7.4 Identity/contact details of reporting person			
7.5 Is the incident over?	YES ☐ NO ☐ *(tick as appropriate)*		
7.6 If yes, specify how long the event has lasted *(in days/hours/minutes)*			

Figure D.2: Sample information security incident report 1 of 6[11]

INFORMATION SECURITY INCIDENT REPORT	Page 2 of 6

8. INFORMATION SECURITY INCIDENT CATEGORY

(Tick one, then complete related section below.)
8.1 Actual *(incident has occurred)* ☐
8.2 Suspected *(incident thought to have occurred but not confirmed)* ☐

(One of) **8.3 Natural disaster** ☐ *(indicate threat types involved)*

☐ **Earthquake** ☐ **Volcano** ☐ **Flood** ☐ **Violent wind**
☐ **Lightning** ☐ **Tsunami** ☐ **Collapse** ☐ **Other**

Specify:

(One of) **8.4 Social unrest** ☐ *(indicate threat types involved)*

☐ **Protest** ☐ **Terrorist assault** ☐ **War** ☐ **Other**

Specify:

(One of) **8.5 Physical damage** ☐ *(indicate threat types involved)*

☐ **Fire** ☐ **Water** ☐ **Electrostatic**
☐ **Abominable environment** (such as pollution, dust, corrosion, freezing)
☐ **Destruction of equipment** ☐ **Destruction of media** ☐ **Theft of equipment**
☐ **Theft of media** ☐ **Loss of equipment** ☐ **Loss of media**
☐ **Tampering with equipment** ☐ **Tampering with media** ☐ **Other**

Specify:

(One of) **8.6 Infrastructure failure** ☐ *(indicate threat types involved)*

☐ **Power-supply failure** ☐ **Networking failure** ☐ **Air-conditioning failure**
☐ **Water-supply failure** ☐ **Other**

Specify:

(One of) **8.7 Radiation disturbance** ☐ *(indicate threat types involved)*

☐ **electromagnetic radiation** ☐ **lectromagnetic pulse** ☐ **Electronic jamming**
☐ **Voltage fluctuation** ☐ **Thermal radiation** ☐ **Other**

Specify:

(One of) **8.8 Technical failure** ☐ *(indicate threat types involved)*

☐ **Hardware failure** ☐ **Software malfunction**
☐ **Overloading (saturating the capacity of information systems)**
☐ **Breach of maintainability** ☐ **Other**

Specify:

Figure D.3: Sample information security incident report 2 of 6[11]

INFORMATION SECURITY INCIDENT REPORT	Page 3 of 6

8. INFORMATION SECURITY INCIDENT CATEGORY

(One of) **8.9 Malware** ☐ *(indicate threat types involved)*

☐ Network worm ☐ Trojan horse ☐ Botnet ☐ Blended attacks
☐ Malicious code embedded web page ☐ Malicious code hosting site ☐ Other

Specify:

(One of) **8.10 Technical attack** ☐ *(indicate threat types involved)*

☐ Network scanning ☐ Exploitation of vulnerability ☐ Exploitation of backdoor
☐ Login attempts, interference ☐ Denial of Service (DoS) ☐ Other

Specify:

(One of) **8.11 Breach of rule** ☐ *(indicate threat types involved)*

☐ Unauthorized use of resources ☐ Breach of copyright ☐ Other

Specify:

(One of) **8.12 Compromise of functions** ☐ *(indicate threat types involved)*

☐ Abuse of rights ☐ Forging of rights ☐ Denial of actions ☐ Mis-operations
☐ Breach of personnel availability ☐ Other

Specify:

(One of) **8.13 Compromise of information** ☐ *(indicate threat types involved)*

☐ Interception ☐ Spying ☐ Eavesdropping ☐ Disclosure
☐ Masquerade ☐ Social engineering ☐ Network phishing ☐ Theft of data
☐ Loss of data ☐ Tampering with data ☐ Data error ☐ Data flow analysis
☐ Position detection ☐ Other

Specify:

(One of) **8.14 Harmful contents** ☐ *(indicate threat types involved)*

☐ Illegal contents ☐ Panic contents ☐ Malicious contents
☐ Abusive contents ☐ Other

Specify:

8.15 Others ☐ *(If not yet established whether incident belongs to the above category, tick here)*

Specify:

Figure D.4: Sample information security incident report 3 of 6[11]

INFORMATION SECURITY INCIDENT REPORT	Page 4 of 6

9. COMPONENTS/ASSETS AFFECTED [4]

Components/assets affected *(if any)*	*(Provide descriptions of the components/assets affected by or related to the incident, including serial, licence and version numbers where relevant.)*
9.1 Information/data	
9.2 Hardware	
9.3 Software	
9.4 Communications	
9.5 Documentation	
9.6 Processes	
9.7 Other	

10. ADVERSE BUSINESS IMPACT/EFFECT OF INCIDENT

For each of the following, tick if relevant, then against "value" record the level(s) of adverse business impact, covering all parties affected by the incident, on a scale of 1 to 10 using the guidelines for the categories of: Financial loss/disruption to business operations; Commercial and economic interests; Personal information; Legal and regulatory obligations; Management and business operations; and Loss of goodwill. Record the code letters for the applicable guidelines against "guideline" and, if actual costs are known, enter these against "cost".

		VALUE	GUIDELINE(S)	COST
10.1 Breach of confidentiality *(i.e. unauthorized disclosure)*	☐			
10.2 Breach of integrity *(i.e. unauthorized modification)*	☐			
10.3 Breach of availability *(i.e. unavailability)*	☐			
10.4 Breach of non-repudiation	☐			
10.5 Destruction	☐			

11. TOTAL RECOVERY COSTS FROM INCIDENT

(Where possible, the actual total costs of recovery for the incident as a whole should be shown, against "value" using the 1 to 10 scale and against "cost" in actuals.)	VALUE	GUIDELINES	COST

Figure D.5: Sample information security incident report 4 of 6[11]

INFORMATION SECURITY INCIDENT REPORT	Page 5 of 6
12. INCIDENT RESOLUTION	
12.1 Incident investigation commenced date	
12.2 Incident investigator(s) names(s)	
12.3 Incident end date	
12.4 Impact end date	
12.5 Incident investigation completion date	
12.6 Reference and location of investigation report	
13. PERSON(S)/PERPETRATOR(S) INVOLVED *(if incident caused by people)*	
(One of) **Person** ☐ **Legally established organization/institution** ☐ **Organized group** ☐ **Accident** ☐ **No perpetrator** ☐ *(e.g. natural elements, equipment failure, human error)*	
14. DESCRIPTION OF PERPETRATOR	
15. ACTUAL OR PERCEIVED MOTIVATION	
(One of) **Criminal/financial gain** ☐ **Pastime/hacking** ☐ **Political/terrorism** ☐ **Revenge** ☐ **Other** ☐ *Specify:*	
16. ACTIONS TAKEN TO RESOLVE INCIDENT	
(e.g. 'no action', 'in-house action', 'internal investigation', 'external' investigation by ...')	
17. ACTIONS PLANNED TO RESOLVE INCIDENT	
(e.g. see above examples)	
18. ACTIONS OUTSTANDING	
(e.g. investigation is still required by other personnel)	

Figure D.6: Sample information security incident report 5 of 6[11]

INFORMATION SECURITY INCIDENT REPORT	Page 6 of 6

19. CONCLUSION

(tick to indicate the incident is considered major or minor, and include a short narrative to justify the conclusion)

Major ☐ **Minor** ☐

(indicate any other conclusions)

20. INTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security Manager or other responsible official)	**Information Security Manager/Responsible Official** ☐ **IRT Manager** ☐ **Site Manager** *(state which site)* ☐ **Information Systems Manager** ☐ **Report Originator** ☐ **Report Originator's Manager/Line User Management affected** ☐ **Other** ☐ *(specify, e.g., help desk, Human Resources, management, internal audit)*

21. EXTERNAL INDIVIDUALS/ENTITIES NOTIFIED

(This detail to be completely by the relevant person with information security responsibilities, stating the actions required. As relevant this may be adjusted by the organization's Information Security manager or other responsible official)	**Police** ☐ **Other** ☐ *(specify, e.g., regulatory body, external IRT)*

21. SIGN-OFFS

ORIGINATOR		REVIEWER		REVIEWER	
Digital signature		**Digital signature**		**Digital signature**	
Name		**Name**		**Name**	
Role		**Role**		**Role**	
Date		**Date**		**Date**	

Figure D.7: Sample information security incident report 6 of 6[11]

INFORMATION SECURITY VULNERABILITY REPORT			Page 1 of 1
1. Date vulnerability identified		**2. Vulnerability number**[5]	
3. REPORTING PERSON DETAILS			
3.1 Name		**3.2 Address**	
3.3 Organization		**3.4 Department**	
3.5 Telephone		**3.6 E-mail**	
4. INFORMATION SECURITY VULNERABILITY DESCRIPTION			
4.1 Date and time the vulnerability reported			
4.2 Description in narrative terms of the perceived information security vulnerability: *(How vulnerability noticed Characteristics of vulnerability (physical, technical etc) If technical, what IT/networking components/assets concerned Components/assets that might be affected if vulnerability were to be exploited Potential adverse business impacts if vulnerability were to be exploited)*			
5. INFORMATION SECURITY VULNERABILITY RESOLUTION			
5.1 Has vulnerability been confirmed? *(tick as appropriate)*		**YES** ☐ **NO** ☐	
5.2 Date and time of vulnerability confirmation			
5.3 Name of person authorizing		**5.4 Address**	
5.5 Organization			
5.6 Telephone		**5.7 E-mail**	
5.8 Has vulnerability been resolved? *(tick as appropriate)*		**YES** ☐ **NO** ☐	
5.9 Description in narrative terms of how information security vulnerability has been resolved, with date and name of person authorising resolution			

Figure D.8: Sample information security vulnerability report[11]

Appendix E: **Go-Bag Contents Lists**

Our proposed Go Bag

Below is the list of items we believe an investigator should have available at the scene of a digital incident (which may have been malicious, e.g. malware, but is not necessarily, e.g. a server failure). It is intended to be relatively complete, however organisations should tailor it to their specific needs, and once they have agreed on the list it should be standardised in their policy documents.

Miscellaneous:

- Wall charger with USB port (see "Cables" for types of mobile phone charging wires)
- Large capacity (min 10400 mAh) power bank (in case wall charging is not an option), must be checked regularly to ensure fully charged
- Write Blocker (Laptop may be configured in such a way that a seperate write blocker is not required)
- Blank CDs & DVDs
- Raspberry Pi (and suitable SD cards)
- Lan tap
- A suitable bag to contain this equipment (that is easily portable on foot)

Laptop:

- CD/DVD drive (or a USB connected one)
- Ethernet port (many modern laptops will no longer have large ports so a suitable dock with Ethernet/SD Card/VGA/HDMI ports may be used)
- Pre-configured analysis VMs
- Pre-configured virtual appliances
- Pre-installed required/relevant software
- Suitable power cable & charger

Cables:

- Ethernet cable
- USB to Mini USB (for some older digital cameras and devices)
- USB to Micro USB (for most Android phones, tablets and other devices)
- USB to Lighting (for Apple phones later than 5)

— USB to Type-C USB (for most recent Android phones and new thunderbolt devices)
— Alternatively, an all in one phone charger cable (USB male one end, various male connectors other end)
— Power booster cable for external hard drives (some older devices may not be able to provide enough juice to USB powered external drives)
— Extension lead (min 4 outlet, recommended to have surge protection and individual power switches, could also include USB outlets)
— VGA cable
— HDMI cable
— Firewire cable (for some old machines and servers, check type compatible with laptop)
— Thunderbolt cable (for versions 1 and 2, for 3 a Type-C USB can be used)
— DB9 RS232 cable (female to female)
— DB9 RS232 adapter (to USB or RJ45, male to male)

N.B.: Only one cable of each type is listed here, but depending on what other equipment is present in the kit, extra cables may be required (eg. extra ethernet and Micro USB cables for a Raspberry Pi).

USB external hard drives (collection drives):

— Main drive: recommended capacity: minimum 4TB, formatted in NTFS
— Backup drive: recommended capacity: 2TB, formatted in FAT32

N.B.: Some devices running Mac OS or Linux may not be able operate an NTFS drive without additional software, hence the backup drive formatted in FAT32 (the most ubiquitous external drive file system), however where possible NTFS should be used as FAT32 has several limitations: drive volume is limited to 2TB, maximum single file size is 4GB, file permissions are not preserved. Where neither NTFS nor FAT32 can be used through a combination of access issues/file limits then ExFAT is a possible alternative, however it may also require additional software and does not preserve file permissions.

There should be no issue with USB 3.0 even on older USB 2.0 ports as it is designed to be backwards compatible, however some ports may not be able to provide sufficient power to the drives, in which case a power booster cable should be used (see "Cables")

Screwdriver set to include:

— Precision/watchmakers type
— Torx type (anti-tamper variant, which will also fit standard torx)
— Pozidriv/Phillips for cage nuts

Investigations kit:

— Gloves
— Torch
— Digital Camera (with appropriate storage capacity)
— Map of Search Site
— Search Log
— Adhesive Exhibit Labels
— Exhibits Book
— Black Markers
— Anti-static Bags
— Flat Pack Boxes
— Faraday bags for phones/tablets/small devices

Playbook, contains:

— This recommended equipment list
— Step-by-step guide for standard procedures

Additional notes:

The investigator should also consider in advance their own well-being while at the scene as they could potentially be there for a number of hours. As such they should include items such as food for the day (as their may not be conventional shops nearby) and a warm jacket (data-centres can be chilly!).

It has been noted in other organisations where go-bags are employed that over time items from these kits would get "borrowed" and not returned, thus it is important the go-bag also includes a complete list of the contents (e.g. on a sheet of paper) so that a quick audit can determine if anything needs to be replaced. Potentially, certain individuals could be assigned the responsibility of signing in or out the kits and ensuring they are complete.

Ireland's National Cyber Security Centre Grab Bag

Contents of the grab bag currently in use with NCSC.

— USB C adapter
— USB Hub
— HDMI Cable
— VGA Cable
— DVI cable
— HDMI to DVI Cable
— HDMI to VGA adaptor
— USB Keyboard
— USB Mouse
— 9" (Small) HDMI Screen
— Technical Screwdriver set
— WD40 Silicone based
— Can of compressed air
— Label Machine
— Markers
— Pens
— Notepad

— BIOS MBR Live USB (USB 3.0) DEFT, CAINE
— GPT EFI Live USB (USB 3.0)
— Linux Live USB Key (USB 3.0)
— Linux Live CD/DVD
— Blank CD/DVD
— Blank USB (USB 3.0)
— Evidence drive 3TB+
— SATA/IDE to USB 3.0 connector with power
— USB write blocker

— LAN tap
— Hub/Switch pre programmed

— Alfa wireless adapter - Wifi network monitor

— 4G Dongle

— Laptop (Etcher,tcpdump, Moloch, wireshark, dd, dcfldd, guymager, sleuthkit+autopsy, hexviewer, pdfanalysis, officedoc analysis, fred+regripper (registry), browser tools (sqlite), psttotext(email), adb, aflogical(Mobile), aircrack(wifi), ophcrack(passwords), openvpn (connents to owncloud))

— Raspberry Pi 3 (WiFi, ssh-server, tcpdump, openvpn)

— Live Data forensics USB:

— FREETOOL FiRST (plug and play detection for encryption, bitcoin wallets, etc.)

— Roastlamb - RAM analysis

— Sysinternals(malware)

— Whatsrunning(malware)

— FTK Imager lite (live imaging - RAM and crypto volumes/disks)

— regshot(malware)

— pestudio (malware)

— And a bag for the contents.

New An Garda Síochána Digital First Responder Bag

In 2020, due to the overwhelming volume of digital evidence at the Centre of Excellent (Garda National Cybercrime Bureau), An Garda Síochána introduced the new role of Digital First Responder. Gardai in this role are trained to perform identification and collection of potential digital evidence sources at a crime scene where a number digital devices are present (not just suspected cybercrime cases). To this end, each first responder is issued with the following equipment.

— Multi-socket extension lead with USB charging ports (for powering both large and small equipment).

— 4 x 32GB Micro SD Card (with adapter to regular size) (for use in photographing or video of exhibits in situ or to document your process).

— 3.5in HDD Protection Box (to protect hard drives from impact and shock).

— anti-static bags, larger and smaller sizes (to protect devices from electromagnetic shock or interference).

— 2 x 128 GB USB key (to store forensic tools or to collect output).

— Canon Camera (for use in photographing and video of exhibits or workstations in situ or to document your processes).

— Tripod with camera holder (to assist with photographing or video of exhibits or workstations in situ or to document your processes).

— Toshiba 2TB hard drive with USB Cable (for storing forensic tools & collection of data output).

— TP Link USB hub with power Supply and USB Cable (to assist with suspect devices with limited port access).

— Faraday bags (to isolate a device from wifi and cell network communications).

— A hard-walled briefcase to contain the above items.

Appendix F: **Ransomware Investigation Playbook**

Guiding Principles

As this playbook is intended to be *ISO/IEC 27043* compliant the following concurrent processes also need to run throughout the investigation.

— Ensure that any persons participating in the investigation have been authorised to do so (for example if private companies or external experts are brought in to assist the investigation that management is aware and has approved their participation).

— Document everything you are doing as much as possible, this helps rebuild the timeline of events but it also helps people joining the investigation quickly get up to date (avoiding duplication of work), it will be crucial for anyone reviwing the incident in the future and it will be the best source of lessons learned to improve future investigations.

— Maintain good control over information flow, both what is released (eg. to the press) and how it is shared among the team. An enhanced chat platform such as "Slack" or "Rocket Chat" are good choices. All the team members should communicate in the shared space so that information is not lost or duplicated, which also helps documentation.

— Recommended to use PGP encryption when communicating about sensitive information via email.

— Recommended to use the Traffic Light Protocol when sending documents or information to other parties (and ensure they understand the designations!)

— Maintain a chain of custody record that details who accessed systems, files, evidence and the timestamps and location (virtual or physical) of when this happened.

— Document any unavoidable changes to the potential digital evidence, as well as the who was responsible for it and the justification for the change.

— The lead investigator should maintain control of everyone else involved and allocate taskings to them as appropriate. This is crucial to avoid individuals acting on their own initiative and jumping in, potentially destroying evidence in the process.

Pre-Incident

Planning

— **Scenario definition:** This playbook is for a ransomware infection on one or more machines of a Bank's network.

— Maintain an updated asset list that includes asset owner, emergency contacts, priority (how essential is the asset to business operations?), and pre-authorised actions ("in case of fire, break glass"). Type of asset inventories needed:

  – Endpoints
  – Servers
  – Network equipment
  – Security appliances
  – Network ranges (Public, Private, and VPN)

— Make up a list of items for a "Go-Bag" that an investigator will bring with them to the scene of an incident. A suggested contents list can be found in Appendix E.

— Review threat intelligence for:

  – Threats against the organisation
  – The sector
  – Common patterns
  – Developing risks and vulnerabilities

— Maintain a list of domains owned by Company (to help prevent acting against your own domains) and of users that can register domains.

— Identify any potential requirements for new hardware or software (such as change-tracking software, intrusion detection/prevention software, anti-virus software, etc.). It may also be decided that no changes are needed as existing architecture is sufficient.

Implementation

— Install and configure any new software and hardware identified in the previous planning steps

— Put together a "Go-Bag" based on the list of items described in the previous step and ensure it is maintained and available.

— Ensure access to documentation, including out of hours/offline documentation for topics such as Phishing attacks and malicious emails; Ransomware; How-to guide for reporting a suspected cyber incident.

— Ensure tool access for the whole Incident Response Team. There are too many tools for an exhaustive list here, but common ones include Cyberchef, Ghidra, Wireshark, Nmap, Flare VM, Kali Linux, etc...

— Make sure that users know how to report phishing.

— Put detections in place for the spawning of these (often maliciously used) Microsoft Office products:

  – PowerShell (Very powerful Windows system administration, command and script execution tool).
  – CMD (Windows command line terminal, able to execute a variety of commands).
  – WMI (Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.)
  – MSHTA (Mshta.exe component provides the Microsoft HTML Application Host, which allows execution of .HTA (HTML Application) files.)

— Create email templates to:

  – Notify employees of ongoing phishing campaigns against the Company
  – Contact hosting companies to take down malicious domains hosted on their infrastructure
  – Ask 3rd party (Microsoft, etc.) to act against phishing on their platform

Assessment

— Assess the playbook to make sure that all aspects are working. Suggested method is to run a "live" test scenario or a tabletop exercise. This should happen after the playbook is published and at least once a year thereafter. Confirm any contact info used for escaltion is still valid.

— Feed the results of the tests back into the earlier preparation and implementation steps, especially if there were issues or inefficiencies.

Incident Detection, First Response and Recovery

The "live" part of the scenario, here the primary focus will be on containing and neutralising the threat, and then getting systems back up and running, but there are also several important steps that are key to the investigation and incident post-mortem that will happen later in *Incident Investigation and Post-Incident*.

Identification & Analysis Phase

This is the initial detection of a security incident, we want to analyse and triage it in order to escalate if required.

1. **Detect the threat via common sources of alerts and notifications:**
   - Tickets from Helpdesk or Support team.
   - SIEM (Security information and event management) is a set of tools and services that combine security events management (SEM) and security information management (SIM) capabilities to enable analysts to review log and event data, understand and prepare for threats, and retrieve and report on log data).
   - AV/EDR (Anti-Virus, Endpoint Detection and Response) is the process of monitoring and detecting, in real-time, any suspicious activity or events occurring at the endpoint. The goal of EDR solutions is to allow your company visibility into threats on a detailed timeline and provide real-time alerts in the event of an attack).
   - Reports/Graphs from DNS (Domain Name System) or Proxy.
   - Users reporting.
   - Third parties such as ISP (Internet Service Provider) or Mail Providers (Office365).
   - Computers acting unusual, slow or crashing.

2. **Collect data on affected files:**
   - Hash.
   - Reputation.
   - Publisher.
   - Behaviour.

3. **Collect data about possible command and control (C2) domains:**
   - Reputation.
   - Registrar.
   - Owner.
   - IP (geo location, other domains using the IP, etc.).

— Multistage/Redirect.
— Site platform (eg. WordPress/Joomla/custom...).

4. Determine the type of ransomware (i.e., what is the family, variant, or flavour?):

— Find any related messages and take an offline copy of it:
  – graphical user interfaces (GUIs) for the malware itself.
  – text or html files, sometimes opened automatically after encryption.
  – image files, often as wallpaper on infected systems.
  – contact emails in encrypted file extensions.
  – pop-ups after trying to open an encrypted file.
  – voice messages
— Analyse the messages looking for clues to the ransomware type:
  – ransomware name.
  – language, structure, phrases, artwork.
  – contact email.
  – format of the user id.
  – ransom demand specifics (e.g., digital currency, gift cards).
  – payment address in case of digital currency.
  – support chat or support page.
— Analyse affected and/or new files. Check:
  – file renaming scheme of encrypted files including extension (e.g. .crypt, .cry, .locked) and base name.
  – file corruption vs encryption.
  – targeted file types and locations.
  – owning user/group of affected files.
  – icon for encrypted files.
  – file markers.
  – existence of file listings, key files or other data files.
— Analyse affected software or system types. Some ransomware variants only affect certain tools (e.g., databases) or platforms (e.g., NAS products).
— Upload indicators to automated categorization services like Virus Total, Crypto Sheriff, ID Ransomware, or similar. This can help with:
  – Knowing the TTPs.
  – Finding the vector.
  – Identifying potential lateral movement techniques (Windows Management Interface, PSExec, RDP, etc.).
  – If there is a decrypter?
  – Which operating systems are targeted.

5. Identify the system type. This will help to determine the teams needed and the impact.

— Servers (OS version, Kernel).
— Workstations (OS version, Service pack).
— Databases.

— Shared Drives.
— SAN (Storage Area Network).
— Backups.

6. Determine the scope:

— Which systems are affected?
  – Scan for concrete indicators of compromise (IOCs) such as files/hashes, processes, network connections, etc. Use endpoint protection/EDR, endpoint telemetry, system logs, etc.
  – Check similar systems for infection (e.g., similar users, groups, data, tools, department, configuration, patch status): check IAM tools, permissions management tools, directory services, etc.
  – Find external command and control (C2), if present, and find other systems connecting to it: check firewall or IDS logs, system logs/EDR, DNS logs, netflow or router logs, etc.
— What data is affected? (e.g., file types, department or group, affected software) .
  – Find anomalous changes to file metadata such as mass changes to creation or modification times. Check file metadata search tools.
  – Find changes to normally-stable or critical data files. Check file integrity monitoring tools.

7. Assess the impact to prioritize and motivate resources

— Assess functional impact: impact to business or mission.
  – How much money is lost or at risk?
  – How many (and which) missions are degraded or at risk?
— Assess information impact: impact to confidentiality, integrity, and availability of data.
  – How critical is the data to the business/mission?
  – How sensitive is the data? (e.g., trade secrets).
  – What is the regulatory status of data (e.g., GDPR).
  – What systems have been affected? Servers will be more critical than a workstation.
  – What user accounts are associated with the infection? A domain administrator account will be more critical than a standard user account.
— There is a table 3.1 in Chapter 2 can be used to determine the response level that should be applied.

8. Collect potential digital evidence (PDE) for later investigation

— What is the level of volatility of data and information related to the PDE?
— Is remote access to any digital device possible and does it pose a threat to evidential integrity?
— Could data have been compromised?
— Could the digital device have been configured to destroy (e.g. using a logic-bomb), spoil or obfuscate data if switched off or accessed in an uncontrolled way?

9. Stop backups. We need to protect the backups from being overwritten, if there are backups

- Make sure that there is an offline copy of the backup.
- Disable future backups.

10. Find the infection vector. Check the tactics captured in the Initial Access tactic of MITRE ATT&CK. Common specifics and data sources include:

- Phishing/Email attachment: check email logs, email security appliances and services, e-discovery tools, etc.
- Insecure remote desktop protocol (RDP): check vulnerability scanning results, firewall configurations, etc.
- Self-propagation (worm or virus) (check host telemetry/EDR, system logs, forensic analysis, etc.).
- Infection via removable drives (worm or virus).
- Delivered by other malware or attacker tool: expand investigation to include additional attacker tools or malware.
- Drive-by download (a file that is downloaded in the background when the user visits a compromised but legitimate website).
- Vulnerability (Remote code execution? Cross-site scripting? . . .).
- Remote services (Weak or default password? Brute force? . . .).
- Lost device.
- Human error.

11. Was data exfiltrated?

- If so invoke the Data Loss playbook (not defined here).
- Notify users if their personal data may have been compromised.
- Notify local authorities if type of data requires it.

12. Communications (if not done already)

- If this incident is a P1 as defined in table 3.1 then a War Room should be established
  - Using the information gathered so far it can be decided who should be included in the War Room.
  - Appoint the most qualified person (not always the most senior) as the incident handler, they will be in charge of distributing taskings and tracking the overall progress.
- Update
  - Security team
  - Admin teams
  - Affected entities

Containment & Eradication

We now want to contain the risk, isolate infected systems, start removing the malware and moving towards a state where we can begin to recover the systems.

1. Methods of containment:

- Block system to system communication:
  - If there is an EDR solution or one can be installed then the EDR solution can be used to isolate the host.
  - Local firewall (can be circumvented if still compromised).
  - Shutdown virtual interface.
  - Shutdown switch port.
- Shutdown **non-encrypted** systems but **do not** shutdown **encrypted** systems as they might not restart.
- It might be necessary in some cases to call the owner of an infected system if help desk or remote tools can not achieve containment. This could include getting the owner to install updates, stop a service or even disconnect the system from the network manually.
- Disconnect all shared drives.
- If the machines are on remote connection like VPN, disable VPN connection. So, the mapped drives will be inaccessible and the risk will decrease.
- Block the suspicious destination IP addresses on firewall based on their reputation – if any suspicious IPs, URLs, domains have been blocked at the previous phase, that can be skipped.
- Disable the user account of the victim of the incident. This could include disabling any accounts that have authenticated to the infected system.
- Block any current sessions with that user on other systems.
- Change the privileged accounts' passwords in case they have been compromised too.
- Set up filters to block emails containing the ransomware.
- If a hash or name of file containing the ransomware is obtained this can be blocked on the AV/EDR or IPS.
- Disabling of email accounts might be needed if compromised.
- If an infection propagating and can not be controlled by the above methods it might be necessary to disconnect a whole subnet from the network.

2. Update Signatures and Block lists:

- Update AV/EDR, IDS/IPS and Firewalls with any new signatures released.
- Re-scan environment.
- Make sure all IOCs discovered have been added to any block lists.

3. Eradication:

- Scan the infected machines and remove malware if possible.

- If the malware couldn't be cleaned, remove the target machine(s) from the network. Once removed try and remove the malware manually and apply any updates and patches. Scan the system again to confirm that the malware has been removed. This is not an option if the user account on the compromised host was admin or root.
- It may not be possible to remove the malware or it could take too long and use up too many resources; in this case rebuilding the system will be needed. This includes reinstalling the OS and applications from a known good copy or if available rolling back to a good OS version. Some reasons to perform a rebuild:
  - Attacker gained administrator level access.
  - System files were replaced.
  - The host is still unstable after the malware has been removed.
  - If there is any doubt about the nature of the infection.
- Reset the passwords of all accounts involved with the infected systems.
- Active Directory clean up:
  - Change kbrtgt password twice (KRB stands for Kerberos and TGT is Ticket Granting Ticket), because keeps a password history of 2.
  - Reset all privilege accounts.
- If a domain admin account has been compromised:
  - Restore Active Directory from backup taken from before the breach.
  - Rebuild Active Directory if there is no safe backup.

Systems should be checked again periodically to confirm that the infection was successfully removed or that it was not reinfected.

4. **Before moving on:**
   - Has the root cause been identified?
   - Have all impacted accounts including temporary accounts passwords' been reset?
   - CSIRT confident that there is no evidence of more malware?
   - Are all systems configured to prevent a repeat occurrence of this malware?
   - If any new IOCs or TTPs discovered move back to the analysis phase.

Recovery

Now that the malware has been eradicated we want to restore the functionality back to the level before the infection and remove temporary containment measures.

- First, try to recover the encrypted files from clean backups to a clean location, not the infected machine itself. It may encrypt the recovered files aswell.
- If there is no healthy backup of the corrupted files, risk analysis must be performed with IT and related Business Department. If the Business Department decides that the lost data is not too critical, there will be no further actions to take to recover the files (and we can go straight to cleaning/re-imaging the systems).

— If the Business Department decides that the encrypted files are critical for business processes, then attempt the following options:

  – Check if the lost data can be reproduced using other files or systems. For instance, if the lost files are reports which are generated on an application, check if they can be regenerated with the desired format and content.
  – Try to decrypt the files on systems using decryptors for well-known ransomware types (if it can be identified). Consulting a security vendor who are experts on these kinds of attacks may be an on option to try to decrypt the files.
  – If the lost data cannot be reproduced and can't be decrypted, paying the ransom may be the only option. Note however that by paying the ransom you are funding organised crime and incentivising further attacks on your organisation or others. If this option will be considered, then the following actions must be taken:
    * Get approval from higher management and legal team to pay the ransom.
    * Check if the cyber insurance can be used for payment.
    * Contact the attackers and ask them to decrypt some specific files for assurance that they still can recover files.
    * Negotiate the price down with the threat actors.
    * Make the payment (most likely in cryptocurrency).
  – Backup the recovered files to two offline systems, since the decryption will most likely happen on the infected machine and we can't rely on those systems. We may need to restore those files from offline backups to new built systems

— If cleaning of the machine is not possible, completely re-image the system and restore from the most reliable and most current backups.

— Patch all vulnerabilities of severity "critical" and "high". This applies to operating systems, applications, and network appliances.

— After taking those actions, conduct a full vulnerability scan to make sure the system is now secure against a re-infection or a similar attack.

— Finally, remove containment rules from the firewall, network switch and anti-virus (but do not remove any rules for the malicious domains and files themselves).

Incident Investigation and Post-Incident

Potential digital evidence transmission and storage

— Where possible data should be compressed in an archive format (zip, tar, rar) before being moved or transmitted.

— If potential digital evidence is transmitted electronically on an open network then it must be encrypted first (on a secure private network this isn't necessary). If transported physically the storage devices used should all be logged in the chain of custody.

— If storing the data in drives for a long period of time they should be secured in a virtual or physical facility with strict access controls. The data should also be documented as much possible so a potential future analyst can find it and doesn't waste time redoing what has already been done.

Digital evidence acquisition, examination and interpretation

— Acquire relevant data from the victim systems (from drives contining images of those systems).

— If accessing the live system be sure to use a write blocker where possible.

— There should already be a record of hashes of all important files. This should be made available to the person doing the investigation.

— When analysing a file check the hash first to make sure it has not been changed since it was acquired.

— Reconstruct the sequence of events that have lead to the current state of the system.

— In the case of a large volume of data, automation tools may be used provided the user is competent with the tool and its use is documented (in case the results are challenged).

— Always use a sandboxed environment for analysing and detonating malware samples. If a network is required the sandbox host must remain completely isolated from other hosts in the network. This might be done to run a packet capture that could not be obtained on a live host.

— Interpret the evidence in order to definitively determine the root cause of the Incident.

Report and presentation

— Create an incident report. This document will essentially be the deliverable of the investigation for the majority of stakeholders and so should avoid too much technical description or jargon where possible, while still providing complete

picture of the investigation process. The report should contain at least the following items:

  - Incident date and time.
  - Affected systems (scope).
  - Affected business processes.
  - Approximate cost (it doesn't have to be monetary cost, it can be duration of interruption of business, etc).
  - Actions taken.
  - Results.

— If the results of the investigation will be used in court as evidence or if they will be shared with others in the community dealing with a similar issue, then a seperate report with all of the most technical details and step-by-step guides should be created. This should be done by a technical person who was involved in the investigation.

— Present the report to senior management (a slide-deck presentation followed by a Q&A session is recommended as the full report document may be very long).

— Ideally the report should then be shared with other industry players (other member banks, the NCSC, An Garda Síochána, etc.) so that the broader Irish cybersecurity community may benefit from any lessons learned.

Investigation closure and lessons learned

— Review both the response and the investigation as a whole: what worked and what didn't? Make sure lessons learned are turned into actionable items and implemented to reduce the likelihood of another successful attack.

— Scan all systems to make sure AV signatures are updated and OS security updates are installed.

— Update firewall rules to prevent connections to malicious addresses and also internally to limit the spread of any malware.

— Review email filtering and security to make sure there are rules in place for phishing, impersonation, sender identity checking, etc.

— Review access rights of users to limit their scope to only what they need (to reduce effect of a compromised account).

— Inform legal department if any legal actions needs to be taken if needed and provide sufficient information.

— Inform all users about the incident (without exposing sensitive corporate information) and organise awareness training on the topic relevant to the breach (for example Phishing or Supply Chain Attacks).

— Check backup schedules to make sure that the systems can be recovered in another possible future event. Check the auditing settings on systems to make sure that sufficient data can be gathered from the logs in case any further events.

Bibliography

[1] Accenture. *The Cost Of Cybercrime*. Ninth Annual Cost of Cybercrime Study, 2019. Retrieved on 27/Nov/2021 from `https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf`

[2] PWC, HSE. *Conti cyber attack on the HSE*. Independent Post Incident Review, 2021.

[3] CCCS. *RANSOMWARE PLAYBOOK*. Canadian Centre for Cyber Security, 2021.

[4] A. Valjarević, H. S. Venter. *A Comprehensive and Harmonized Digital Forensic Investigation Process Model*. Journal of forensic sciences, Vol. 60, Issue 6, 2015.

[5] A. Agrawal et al. *Systematic Digital Forensic Investigation Model*. International Journal of Computer Science Security, Vol. 5, No. 1, 2011.

[6] ENISA. *Report on Cyber Security Information Sharing in the Energy Sector*. European Union Agency for Network and Information Security, 2016.

[7] ISO/IEC 27010:2015. *Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[8] ISO/IEC 27035-1:2016. *Information technology - Security - Information security incident management - Part 1: Principles of incident management*. Retrieved on 26/Feb/2020 from UCD Library NSAI Database.

[9] ISO/IEC 27001:2015. *Information technology - Security techniques - Information security management systems - Requirements*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[10] ISO/IEC 27043:2016. *Information technology - Security techniques - Incident investigation principles and processes*. Retrieved on 26/Feb/2020 from UCD Library National Standards Authority of Ireland (NSAI) Database.

[11] ISO/IEC 27035-2:2016. *Information technology - Security - Information security incident management - Part 2: Guidelines to plan and prepare for incident response*. Retrieved on 26/Feb/2020 from UCD Library NSAI Database.

[12] ISO/IEC 27035-3:2020. *Information technology - Security - Information security incident management - Part 3: Guidelines for ICT incident response operations*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[13] ISO/IEC 27037:2012. *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*. Retrieved on 26/Feb/2020 from UCD Library NSAI Database.

[14] ISO/IEC 27042:2015. *Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence*. Retrieved on 26/Feb/2020 from UCD Library NSAI Database.

[15] ISO/IEC 27000:2016. *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[16] OGCIO. *An Overview of ISO/IEC 27000 family of Information Security Management System Standards*. Office of the Government Chief Information Officer (HK), 2019.

[17] ACPO. *ACPO Good Practice Guide for Digital Evidence*. Association of Chief Police Officers (UK), 2011.

[18] FIRST. *Traffic Light Protocol (TLP)*. FIRST Standards Definitions and Usage Guidance - Version 1.0, 2016.

[19] J. De Muynck, S. Portesi, ENISA. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. European Union Agency for Network and Information Security, 2015.

[20] P. Chichonski, T. Millar, et al. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61, 2012. Retrieved on 27/Nov/2021 from `https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final`

[21] R. Leigland, A. Krings. *A Formalization of Digital Forensics*. International Journal of Digital Evidence, 2004.

[22] R. Rowlingson. *A Ten Step Process for Forensic Readiness*. International Journal of Digital Evidence, 2004.

[23] S. Ó. Ciardhuáin. *An Extended Model of Cybercrime Investigations*. International Journal of Digital Evidence, 2004.

[24] E. Casey, R. Curtis. *Forensic Analysis*. Handbook of Digital Forensics and Investigation, Elsevier Academic Press, 2010.

[25] R. Hankins, T. Uehara, J. Liu. *A Comparative Study of Forensic Science and Computer Forensics*. Third IEEE International Conference on Secure Software Integration and Reliability Improvement, 2009.

[26] A. Valjarević, H. S. Venter, R. Petrović. *ISO/IEC 27043:2015 - Role and application*. 24th Telecommunications forum TELFOR, Belgrade, Serbia, 2016.

[27] E. Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. New York: Academic Press, 2011.

[28] N. L. Beebe, J.G. Clark. *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process*. Journal of Digital Investigation, 2005.

[29] A. Valjarević, H. S. Venter. *Harmonised Digital Forensic Investigation Process Model*. International workshop on Digital Forensics in the Cloud (IWDFC)/Information Security South Africa conference proceedings, 2012.

[30] A. Valjarević, H. S. Venter. *Towards a Harmonized Digital Forensic Investigation Readiness Process Model*. Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics proceedings/Advances in Digital Forensics, 2013.

[31] H. S. Venter. *Digital forensic readiness processes and procedures for investigators*. Page 72, Dagstuhl Seminar 14092, 2014.

[32] IIROC/OCRCVM. *Cyber Incident Management Planning Guide*. Investment Industry Regulatory Organization of Canada, 2016.

[33] K. Scarfone, P. Mell. *Guide to Intrusion Detection and Prevention Systems*. NIST Special Publication 800-94, 2007. Retrieved on 27/Nov/2021 from `https://csrc.nist.gov/publications/detail/sp/800-94/final`

[34] ISO/IEC 27039:2015. *Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[35] L. O. Nweke. *Digital Forensics: Validation of Network Artifacts Based on Stochastic and Probabilistic Modeling of Internal Consistency of Artifacts*. Masters Thesis, Sapienza Universita Di Roma, 2018.

[36] D. Chismon, M. Ruks. *Threat Intelligence: Collecting, Analysing, Evaluating*. MWR InfoSecurity, CPNI, CERT-UK, 2015.

[37] SANS Institute. *Cyber Threat Intelligence Consumption*. Poster, 2021. Retrieved on 27/Nov/2021 from `https://www.sans.org/posters/cyber-threat-intelligence-consumption/`

[38] E. M. Hutchins, M. J. Cloppert, R. M. Amin. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. Lockheed Martin Corporation, 2010.

[39] Lockheed Martin. *Cyber Kill Chain*. Retrieved on 27/Nov/2021 from `https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html`

[40] M. Pollitt. *Applying Traditional Forensic Taxonomy to Digital Forensics*. Advances in Digital Forensics IV, IFIP TC11.9 Conference Proceedings, 2009.

[41] A. Pichan, M. Lazarescu, S. T. Soh. *Cloud forensics: technical challenges, solutions and comparative analysis*. Digital Investigation 13, Elsevier, 2015.

[42] ISO/IEC 10118-2:2010. *Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[43] ISO/IEC 27041:2015. *Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[44] M. B. Line, I. A. Tondel, M. G. Jaatun. *Information security incident management: Planning for failure*. Eighth International Conference on IT Security Incident Management and IT Forensics, 2014.

[45] D. Y. Kao, G. J. Wu. *A Digital Triage Forensics Framework of Window Malware Forensic Toolkit*. 49th Annual IEEE International Carnahan Conference on Security Technology, 2015.

[46] ISO 15489-1:2016. *Information and documentation - Records management - Part 1: General*. Retrieved on 27/Nov/2021 from UCD Library NSAI Database.

[47] M. Bartock, J. Cichonski, M. Souppaya, et al. *Guide for Cybersecurity Event Recovery*. NIST Special Publication 800-184, 2016. Retrieved on 27/Nov/2021 from `https://csrc.nist.gov/publications/detail/sp/800-184/final`

[48] SANS Institute. *Security Awareness Roadmap*. Poster, 2021. Retrieved on 27/Nov/2021 from `https://www.sans.org/posters/security-awareness-roadmap-managing-your-human-risk/`