12 Financial impact of cyber security attack

12.1 On 14 May 2021, the Health Service Executive (HSE) announced that it had been the subject of a very significant ransomware cyber attack which was impacting all of its systems involved in the provision of its core services. The HSE reported that some of its servers and workstations had been encrypted with Conti ransomware and that staff were unable to access impacted patient data.[1] In addition, it became aware that other health bodies, including hospitals, were also reporting that their information technology (IT) systems had been externally encrypted and that the Department of Health (the Department) had reported suspicious activity on its systems.

12.2 In a typical ransomware attack, a piece of software (malware) is activated which is designed to encrypt information on a device, rendering any files and the systems that they rely on unusable.[2] A demand is then made for a ransom in exchange for decryption. In the case of the HSE, a demand was received for a ransom of almost $20 million. The HSE has stated that it did not engage with the attackers and did not pay any ransom.

12.3 Subsequent to the attack, the HSE Board and Chief Executive Officer (CEO) engaged PricewaterhouseCoopers (PwC) to carry out a post incident review of the cyber attack and the circumstances surrounding the exfiltration of data from the HSE's IT systems. The final report contained detailed recommendations which were accepted by the HSE Board in November 2021.[3]

12.4 This examination was undertaken to review the impact of the cyber attack on the HSE and other health bodies, the HSE's cyber attack preparedness, the financial impact of the attack and the status of implementation of PwC recommendations.

Impact of the cyber attack on the HSE

12.5 At the time of the attack, the HSE had over 70,000 IT devices in approximately 4,000 locations. To contain the spread of the ransomware, the HSE shut down its Information and Communications Technology (ICT) network. The network shutdown affected all HSE systems whether they had been impacted by the data encryption or not.

12.6 On the advice of the National Cyber Security Centre (NCSC), the HSE engaged an external firm, Mandiant to provide it with expert response assistance.[4,5] On 21 May 2021, the attacker posted a link to a tool that would decrypt the encrypted files. Mandiant validated that the decryption tool worked, reverse engineered its capabilities, and produced a new decryption tool that was rolled out on the HSE IT systems.[6]

12.7 In a review of 550 organisations with data breaches over the period March 2021 to March 2022, IBM Security has calculated the average number of days to identify a data breach, and the average number of days to contain it.[7] Relative to the calculated averages, the HSE was notified of the data breach significantly earlier, but took longer to contain and recover from it (see Figure 12.1).

1 Conti is a human operated ransomware. In addition to stealing data, the attackers threaten to expose the data as well as encrypting it. This is known as a 'double extortion' ransomware.

2 Malware is a catch all term for any type of malicious software designed to harm or exploit any programmable device or network.

3 PwC's published report can be found here.

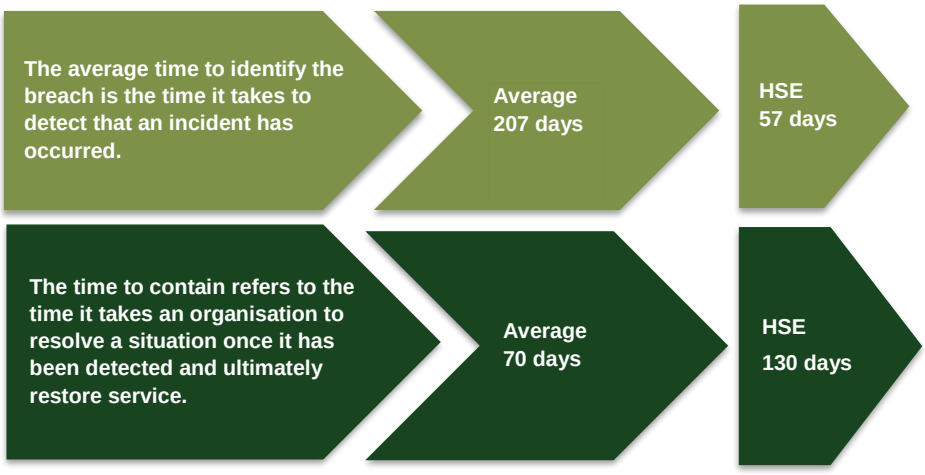
4 The NCSC is an operational section of the Department of the Environment, Climate and Communications. It is tasked with, *inter alia*, leading in the management of major cyber security incidents across Government and providing related guidance and advice.

5 Mandiant is a global specialist in cyber recovery and defence.

6 The reverse engineering process involved examination of the tool provided and obtaining the source code holding the decryption key. Software was developed to decrypt the HSE systems. The decryption software had to be uploaded to each device on the network before access was restored. Assistance in these tasks was provided by a number of organisations including the Defence Forces.

7 IBM Security publishes an annual report on the *Cost of a Data Breach* in association with the Ponemon Institute. The 2022 report can be found here.

Figure 12.1 Time taken to resolve data breaches[a]



Source: IBM Security *Cost of a Data Breach report 2022*, HSE and PwC

Note: a In its review, IBM has defined a data breach as an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk — either in electronic or paper format.

12.8 The timeline in Figure 12.2 summarises the key events and actions taken by the HSE in response to the attack on its systems.

Impact on other bodies

12.9 Prior to the cyber attack, a number of organisations which included voluntary hospitals, some HSE hospitals and the Department operated their own domain networks, but were also connected to the HSE network through an 'active domain trust'.[1,2]

12.10 In this type of trust network, users input their user name and password on their own network and are able to access information and services on the other network without being asked for additional authentication. For example, clinical staff in voluntary hospitals could access HSE shared national data systems.

12.11 The relationship of trust between the HSE and the Department, and the HSE and Beaumont Hospital, facilitated the attackers' access to the Department and Beaumont Hospital's ICT networks. However, the ongoing monitoring of network threats and the identification of suspicious activity allowed the Department and Beaumont Hospital to proactively respond to an attack on their networks, preventing widespread encryption of their ICT networks.

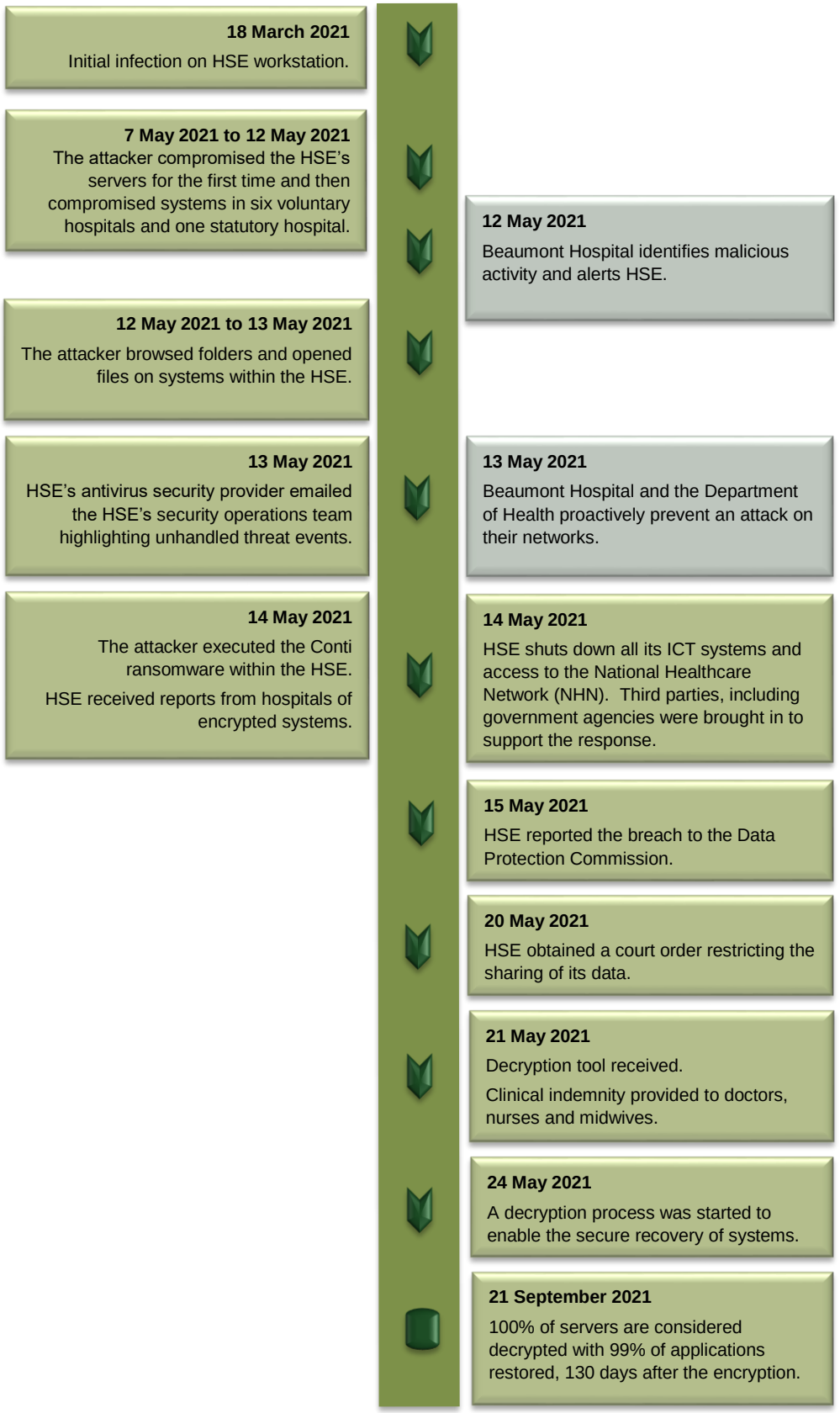
12.12 Sophos, the Department's monitoring provider, notified the Department of the attempt to install malicious software on its systems. The Department acted by contacting the NCSC and engaging Grant Thornton to provide assistance. The deployment of a security tool by the Department in collaboration with Grant Thornton prevented the ransomware from inflicting additional damage on its systems.

12.13 The sequence of events leading up to the attack on the Department and the actions taken by the Department are summarised in Figure 12.3.

1 Hospitals in the public system are HSE hospitals (statutory hospitals) or run by voluntary organisations (voluntary hospitals). Voluntary hospitals are separate legal and corporate entities.

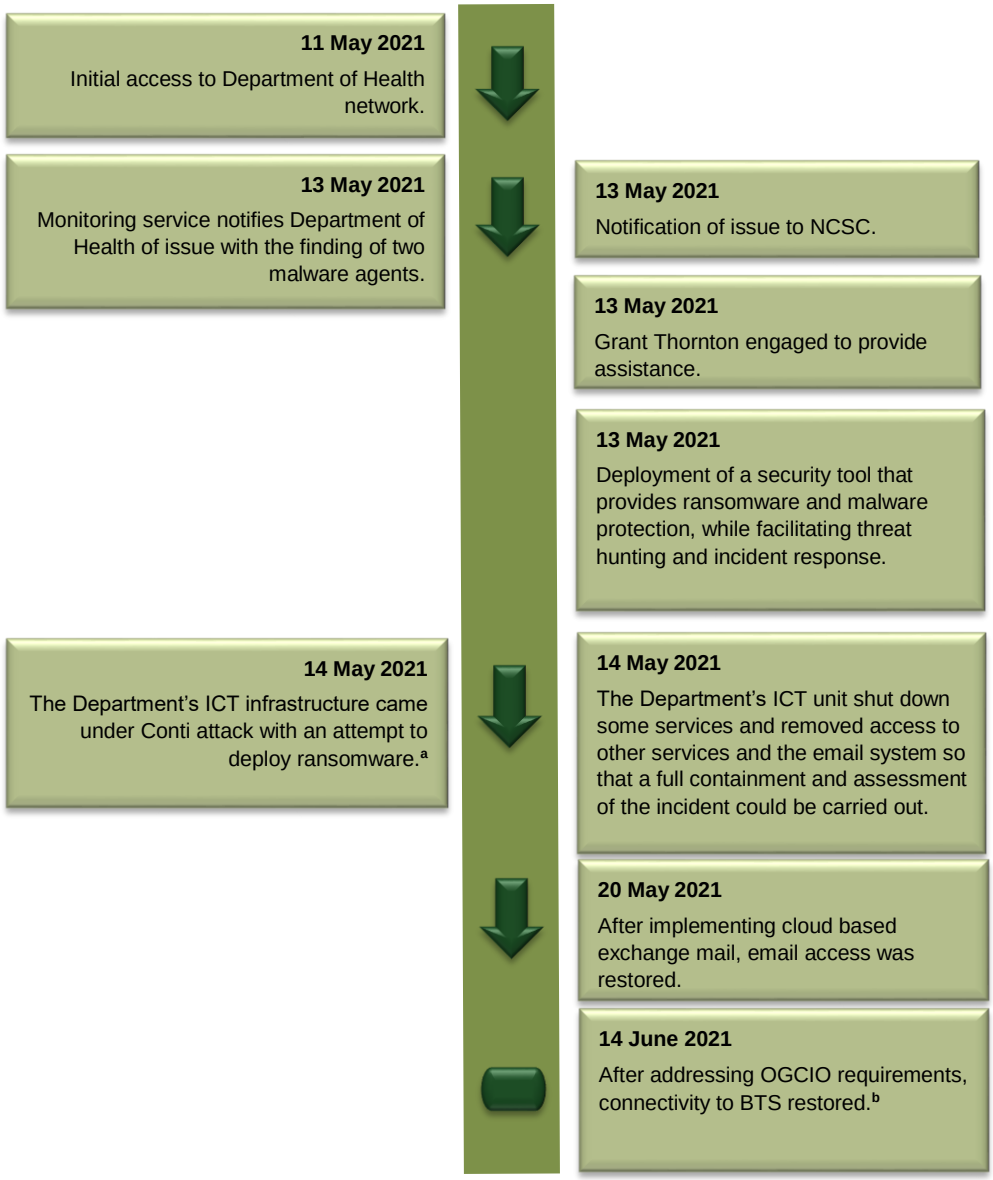
2 An active domain trust is a method of connecting two distinct active domains to allow authenticated users in one domain use resources and systems in the other domain.

Figure 12.2 Timeline of key events and actions taken in response to HSE cyber attack



Source: PwC *Conti cyber attack on the HSE,* independent post incident review

Figure 12.3 Timeline of key events and actions taken in response to the attack on the Department of Health



Source: Department of Health

Notes:
a ICT is the infrastructure that enables the operation of modern computer systems.
b The Office of the Government Chief Information Officer (OGCIO), through the Build to Share (BTS) programme, delivers a range of collaboration tools, platforms and services for public service bodies.

Impact on patient care

12.14 The patient care services most impacted by the cyber attack included radiology, pathology/laboratories, radiotherapy, maternity, primary care, and disability services. Some activities like blood tests took longer to complete. Other services closed completely.

- Radiation machines were shut down and radiation treatment ceased in the days following the cyber attack in five centres (St Luke's Rathgar, St Luke's Radiation Oncology Network facilities on the campuses of St James's and Beaumont Hospitals, Galway University and Cork University Hospitals). A plan was implemented for the provision of urgent patient care in the private hospital sector.
- X-rays and imaging services were available within hospital radiation departments. However, as the national integrated medical imaging system (NIMIS) which allows for sharing of x-rays and other images was put offline, staff were unable to access historic imaging and images could not be shared across the network.[1]

12.15 Where systems were unavailable, HSE staff had to develop manual workarounds to ensure continuity in the provision of services and to mitigate the impact on patient care. This included switching to paper systems to update health records which was slower than the normal processes.

12.16 Indirect impacts of the workarounds used included delayed patient admissions and discharges, difficulties with patient hand-overs and the recording of clinical information in a complete and timely manner. The absence of automated prompts to ensure that all required information was obtained may have resulted in certain clinical and non-clinical information not being recorded.

12.17 Following the restoration of clinical systems, significant resource effort was required to backload clinical information and to ensure that information was complete and accurate. However, the HSE has reported that some data is irretrievable and therefore the impact of the cyber attack will be long lasting and will affect clinical practice for some time.

Impact on the voluntary hospitals

12.18 The HSE has reported that voluntary hospitals were affected in different ways by the cyber attack.[2]

12.19 Beaumont Hospital was subject to an attempted ransomware attack. The hospital's monitoring system raised an alert that there was a potential issue and the hospital was able to take action to block access to its system. This occurred prior to the deployment of the ransomware on the HSE network which minimised the impact on the hospital's system.

1 NIMIS holds personally identifiable information for the population of Ireland which is shared with health service providers in the public health system.

12.20 Some voluntary hospitals were moderately impacted by the attack, with local systems generally not impacted. The key operational problems experienced in those cases were as a result of the HSE's removal of access to national systems.

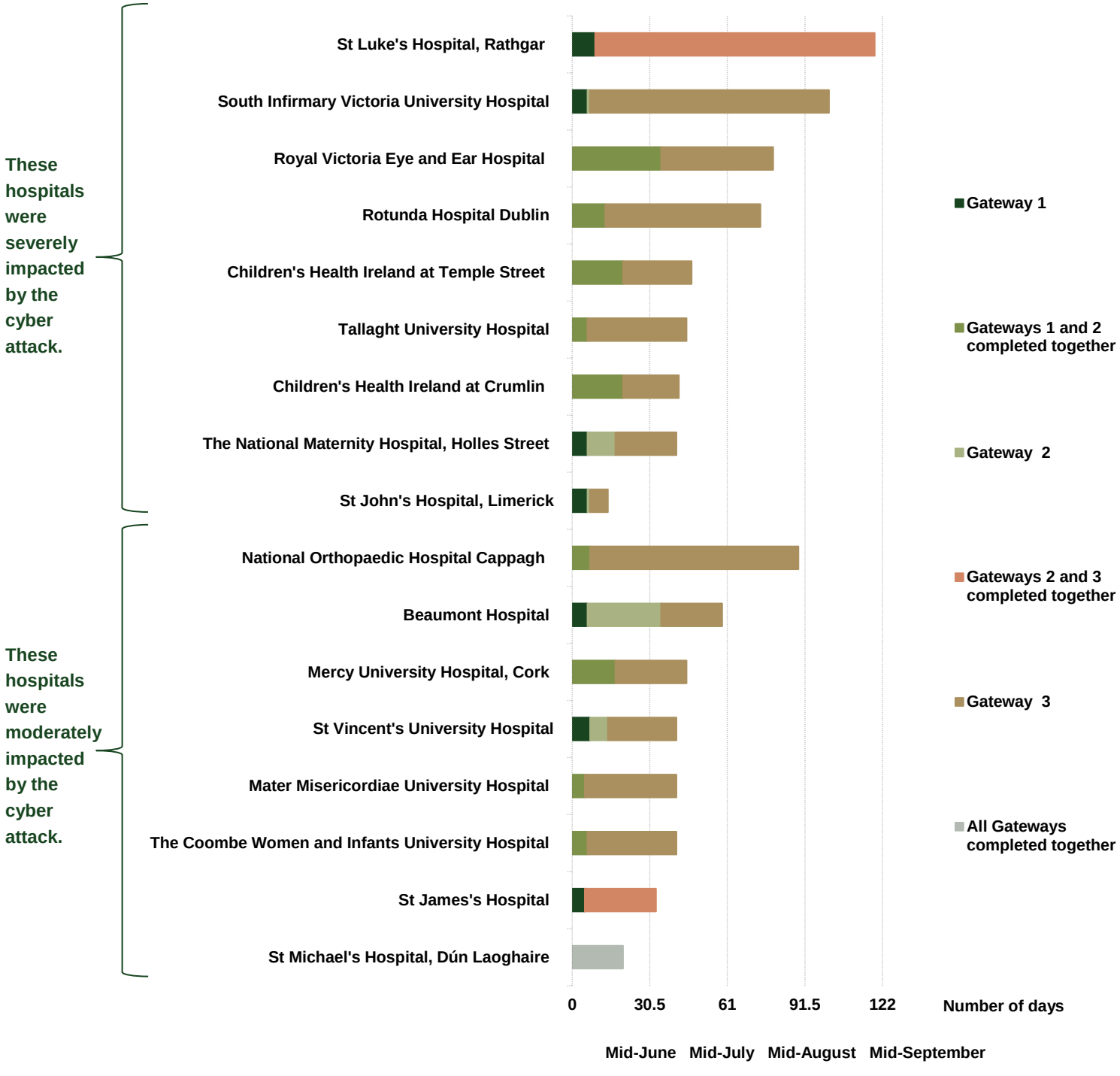
2 Information on the impact of the cyber attack on voluntary hospitals was provided by the HSE.

12.21 Some voluntary hospitals were severely impacted. In those cases, the hospitals' local systems were either encrypted or they were reliant on the main clinical system, hosted by the HSE, which was impacted.

12.22 Hospitals identified as having attacker activity had to agree a bespoke plan with the HSE and Mandiant based on the extent of the attack activity.[1] The restoration process involved three stages, called 'gateways' — Gateway 1 involved the restoration of internal systems without internet; Gateway 2 allowed some specific internet activity; while Gateway 3 allowed hospitals to resume normal internet-based activity. The restoration timeline for each hospital, by gateway, is set out in Figure 12.4.

1 Before restoring access to the network, Mandiant had to review the systems in the relevant hospitals to ensure that they were clear from indicators of compromise.

Figure 12.4 Restoration process timeline for each hospital by gateway[a]



Source: HSE

Note: a The restoration process took place over the period mid-May to 10 September 2021.

HSE's preparedness

12.23 PwC's post-incident review of the cyber attack found that the HSE was operating on a frail IT estate that had evolved rather than having been designed for resilience and security; and that part of the reason for the frailty of the IT estate was an over-reliance on legacy systems. PwC noted that while the design of the network made it easy for staff to access the applications they required, the network's flat nature exposed the HSE to the risk of cyber attacks from other organisations connected to the network as well as exposing other organisations to cyber attacks originating from the HSE network.

12.24 The risk of a cyber security incident had been considered by the HSE prior to the attack. The audit and risk committee (ARC) was briefed on cyber security in February 2020 and again in March 2021. The HSE stated that cyber risk was also on the corporate risk register and that the register is reviewed by the ARC and the HSE Board on a regular basis.

12.25 Internal audit also reported on the HSE's IT systems prior to the attack and its recommendations were accepted by HSE management. For example,

- In 2018, an internal audit of the NIMIS found that certain servers used outdated software — Microsoft Windows Server 2003 — supplier support for which ended in July 2015.[1] It also found that a number of web applications in use did not follow secure coding practices. Therefore, there was a risk that the HSE could be subject to an attack where a malicious user could trick normal users of the application to perform actions without their knowledge, obtain sensitive information, or insert malicious code into the application.
- In 2019, an internal audit of the HSE's national data backup and resilience infrastructure found that the HSE did not have a standardised approach for managing data backup and recovery across its data centres, and that the national backup and recovery policy had not been finalised. It also identified servers running unsupported software.

12.26 In the statements on internal control published with the HSE's 2019, 2020 and 2021 annual financial statements, the HSE acknowledged the weaknesses and stated that it was committed to improving controls in respect of cyber security.

12.27 The initial focus of the IT response in the aftermath of the attack was to try to restore the systems from the backup. However, the HSE stated that, due to the number of systems that would have to be restored mainly from disks or tapes, this process would have taken much longer than the process involved by obtaining the decryption tool.

12.28 Since the attack and to safeguard against a similar event occurring, the HSE has put in place an enhanced network monitoring service. Prior to the attack, there was limited monitoring of the network — a third party provided an antivirus monitoring service which operated from 8 am to 6 pm each day, with an on-call service outside those hours. The enhanced monitoring service provides 24-hour support. Additional measures, such as virus scanning software and a network monitoring device scanning all traffic which enters or leaves the network, has increased the HSE's preparedness to deal with similar attacks.

1 Vulnerability Assessment — National Integrated Medical Imaging System (NIMIS), June 2018.

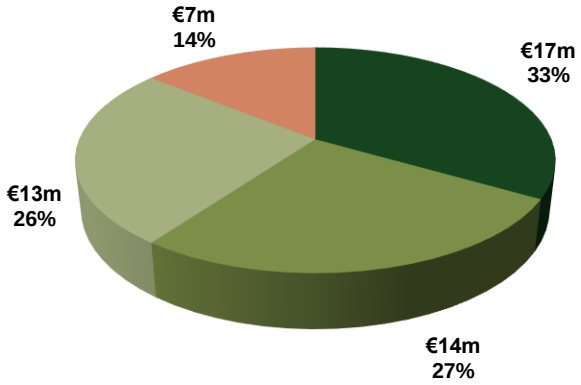
Costs of the attack

HSE costs

12.29 The financial implications of a cyber attack are significant, with costs ranging from those associated with the initial attack, to costs associated with recovery, rebuilding and enhancing the security of systems.

12.30 Following the cyber attack, the HSE incurred significant costs in recovering access to encrypted systems and in enhancing security across its ICT network (see Figure 12.5). In 2021, the HSE (excluding voluntary agencies) incurred revenue expenditure of €37 million and capital expenditure of €14 million.[1]

Figure 12.5 Costs of the cyber attack 2021[a]



Professional services	This includes costs such as vendor support (to build servers and applications) and strategic partner costs (investigation, remediation and security monitoring services, and engagement of external cyber security expertise).
HSE hospitals' cyber costs	This includes incremental costs (both pay and non-pay) incurred in the wider HSE as a result of the cyber attack.
ICT hardware	Replacement of legacy devices and purchase of monitoring infrastructure.
Other costs	This includes other costs such as the purchase of software and costs involved in the migration to Office 365 to facilitate the move to a more secure cloud based system.

Source: HSE

Note: a ICT hardware costs together with €537,000 included in professional services are capital costs, while the remaining costs are revenue related costs.

12.31 In addition, revenue costs incurred of around €4.4 million, mainly relating to Microsoft Office 365, have been expensed in 2022. The HSE has stated that it will incur other mitigating costs in 2022.

12.32 The full cost of the attack on the HSE has not been quantified. Costs incurred by the voluntary agencies are not included in any of the figures. Staff time incurred in addressing the technical aspects of the cyber attack and the additional time required to resume normal services have not been costed by the HSE.

12.33 The HSE was also unable to provide the staff costs associated with the maintenance of hard copy records while systems were down, and for the subsequent updating of electronic records once system access was restored.

1 €23.6 million of the total revenue expenditure and all of the €13.7 million capital expenditure were incurred directly by the HSE's Office of e-Health and Disruptive Technologies. This Office is responsible for the delivery of technology to support and improve healthcare in Ireland.

12.34 The HSE incurred legal costs of €2.6 million since the cyber attack.[1] This included securing a high court order to prevent, *inter alia*, the sharing of its data, without its consent. The HSE stated that no legal actions have been taken against it to date by individual patients. However, HSE patients, clients and staff whose personal information was stolen as part of the cyber attack had yet to be informed as at August 2022.

12.35 In addition to the costs incurred in 2021, the HSE has secured an increase in its recurrent funding from 2022 of €43 million for ICT expenditure of which €38 million is for immediate and shorter term actions to enable it to increase its capability to deal with future threats.

12.36 The HSE has prepared an initial plan to implement PwC's post-incident review recommendations and to cost the associated actions required. The HSE stated that initial estimates are that this will require almost €657 million over seven years for implementation of cyber security improvements.[2]

Impact of cyber attack on patients

12.37 Many patient appointments were cancelled in the aftermath of the cyber attack, which has led to an increase in waiting lists. However, the HSE noted that a significant number of appointments were cancelled due to Covid-19, rather than being directly due to the cyber attack. It is difficult to separate the impacts, which in any event would be difficult to cost.

Other health bodies' costs

The Department

12.38 As a result of the cyber attack, the Department incurred direct costs of almost €647,700 to deal with the immediate response and aftermath of the attack. It also incurred expenditure for an interim managed detection and response service of €305,000 and for professional advice of €22,000.

12.39 Prior to the attack, the Department had tendered for a monitoring service at a cost of €61,000 for three years. Following the attack, the Department decided to centralise all security options and implement a cloud-based email system. The licences for all staff cost €293,000 for 2021.

St James's Hospital

12.40 Following the attack, St. James's Hospital identified potential improvements to its network security. The hospital stated that it has provided the HSE with costings for additional measures to secure an increase in its annual ICT budget to include €2.8 million for non-pay costs, €482,000 for recurring pay costs and €2.2 million for capital expenditure.

Beaumont Hospital

12.41 Beaumont Hospital has estimated that as a result of the cyber attack, it incurred additional costs of €512,000 of which around €233,000 will be recurring annual costs.

1 The legal costs covered the period from May 2021 to the end of July 2022.

2 This is comprised of €127 million capital and €530 million revenue based on current estimates.

12.42 The fragility of Beaumont Hospital's IT system means that the hospital's focus is on delivering a patient records administration system as the hospital's current system is due to cease functioning on 31 December 2025.

PwC recommendations

12.43 PwC's post incident review into the cyber attack sought to

- urgently establish the facts regarding the HSE's technical and operational preparedness for a strategic risk of this nature
- identify the lessons from the incident and identify improvements to the HSE's preparedness for and response to other major risks; and
- share the lessons within the HSE and externally.

12.44 The PwC report includes a total of 83 key recommendations (see Figure 12.6).[1]

Figure 12.6 PwC key recommendations, September 2021

Area	Focus of review	Key recommendations
Overall	Transformational change[a]	22
Focus area 1	Technical investigation and response	15
Focus area 2[b]	Organisation wide preparedness and strategic response	24
Focus area 3	Preparedness of the HSE to manage cyber risks	22

Source: PwC *Conti cyber attack on the HSE,* independent post incident review

Notes:
a The PwC report includes ten strategic recommendations to deliver transformation change and twelve tactical recommendations which contribute to the implementation of the strategic recommendations.
b Six of the recommendations in focus area 2 were further sub-divided.

12.45 The HSE stated that as at June 2022, three of the recommendations have been fully implemented. It also stated that many of the recommendations will take a number of years to complete, others are an ongoing commitment and that the status of each recommendation does not fully capture the extent of ongoing work to ensure that the HSE is safe from a future attack.

12.46 The HSE also noted that some of the recommendations in the report contain duplicate elements which were analysed with PwC so that a refined and costed plan could be prepared which will be capable of being tracked to ensure the recommendations are implemented.

1 The HSE has stated that many of the key recommendations contain a number of sub recommendations totalling 245 recommendations overall.

12.47 PwC also identified a number of lessons for sharing with other bodies to inform their future preparedness for the threat of a cyber attack (see Annex 12A).

Conclusions and recommendations

12.48 The HSE was subject to a significant cyber attack in May 2021 which resulted in a large number of its systems being encrypted and the theft of patient private information. In response to the attack, the HSE shut down its network to prevent further harm being done by the attackers, but this resulted in severe disruption to the activities of legitimate users of the HSE systems. Full access to systems was not restored until late September 2021.

12.49 A post incident review by PwC into the attack found that Ireland's public health service was operating on a frail IT estate with an architecture that had evolved rather than having been designed for resilience and security. PwC determined that part of the reason for the frailty of the IT estate was an over-reliance on legacy systems.

12.50 Previous internal audits had also identified issues with the HSE's IT infrastructure, which included the continued use of outdated and unsupported software and some web applications not following secure coding practices.

12.51 The financial cost of the cyber attack on the HSE has been significant. However, the full cost of the attack and its long term impact on patient care have not been determined. The use of manual workarounds while systems were offline and the subsequent back loading of information also presented challenges in ensuring that recorded information is accurate, complete and accessible. The HSE has reported that difficulties in retrieving some data will affect clinical practice for some time.

12.52 In their post incident review of the attack, PwC set out a broad range of recommendations which were accepted by the HSE Board in November 2021. The HSE has prepared an initial plan to cost the implementation of the recommendations. Substantial investment in the HSE IT systems will be required to ensure that the systems are fit for purpose, that operational platforms are upgraded and to ensure that client and patient personal data is sufficiently protected from external threats.

Recommendation 12.1

The HSE's plan for the implementation of the PwC recommendations should clearly set out target deliverables, costs and timelines, against which progress can be measured.

Chief Executive Officer's response

Agreed.

The HSE has progressed an investment case which has been submitted to the Department of Health.

The HSE has established a sub-group of the Executive Management Team to oversee the implementation of the PwC recommendations.

Recommendation 12.2

ICT systems which do not have ongoing support should be replaced so that systems which store personal information are sufficiently secure.

Chief Executive Officer's response

Agreed in principle.

System replacement and upgrading is an ongoing requirement undertaken by the HSE and replacing older unsupported technology will take a number of years.

12.53 PwC's post incident review also found that the flat nature of the HSE's network exposed the HSE to the risk of cyber attacks from other organisations connected to its network as well as exposing those organisations to attacks originating from the HSE.

12.54 The relationship of trust between the systems used by the HSE and the Department, and those used by the HSE and Beaumont Hospital, facilitated the attackers' access to each entity's ICT network. However, better ongoing monitoring of network threats and suspicious activity by the Department and the hospital was successful in blocking the ransomware cyber attack on their systems and minimising the impact of the HSE cyber attack in those organisations.

Recommendation 12.3

The HSE should review the trust relationship arrangements currently in place to ensure that they reflect best practice and that the risk of cyber attacks originating from either party to each arrangement is appropriately addressed.

Chief Executive Officer's response

Agreed.

A number of key steps have been undertaken to improve the cyber posture of the organisation, including the recruitment of a Chief Information Security Officer to lead the end-to-end cyber security operations function.

12.55 At the time this examination was being finalised, patients, clients and staff of the HSE whose personal data was stolen as part of the cyber attack had yet to be informed about how they were affected.

Recommendation 12.4

The HSE should prioritise its engagement with the relevant stakeholders so that all those impacted are fully informed of the extent of their personal data stolen as part of the attack.

Chief Executive Officer's response

Agreed.

A notification process is underway which has been notified to the Data Protection Commissioner.

12.56 All organisations that operate online are at risk of a cyber attack. Significant personal data and confidential data is held by State bodies. There is a high reliance by these bodies on properly supported and functioning IT systems. The HSE included a request in its commission to the external consultants that they consider lessons learned from the cyber attack so that these can be shared with State and non-State organisations. These lessons have been shared publicly.

Annex 12A Recommendations for all public sector organisations to consider based on lessons learned from the HSE cyber attack

No.	Recommendation
1	Boards and/or executive leadership of organisations should ensure that they understand the extent to which their critical operations are dependent on technology.
2	Organisations should ensure they have a cybersecurity strategy that defines the key cybersecurity risks to the organisation, how those risks are being mitigated and the resourcing and investment to execute the strategy.
3	Organisations should perform a cybersecurity assessment specific to the threat of ransomware, given the heightened threat posed by ransomware attacks.
4	Organisations must possess an effective security monitoring capability that can detect and respond to the tools and techniques used by human-operated ransomware groups.
5	Testing of cybersecurity capability through the use of ethical hackers simulating end-to-end attack techniques (i.e. 'red team' testing) is essential to provide a threat-based perspective of an organisation's vulnerability to ransomware and other types of attacks.
6	Organisations should develop and exercise cybersecurity-specific incident response and crisis management plans that define how a response should be led, managed and coordinated.
7	Organisations should prioritise business continuity planning and disaster recovery planning that would ensure provision for continuity of critical operations and the ability to recover in the face of a ransomware attack that results in total loss of IT and associated data.
8	Organisations should establish contractual retainers with key third parties that may be required to support a crisis response.

Source: PwC *Conti cyber attack on the HSE*, independent post incident review