5.2 Focus area 2 - review of organisation wide preparedness and strategic response

Focus area 1	Focus area 2	Focus area 3
Review the technical investigation and response	Review the organisation-wide preparedness and strategic response	Review the preparedness of the HSE to manage cyber risks
	Key findings and recommendations	
	Conclusion	

Key findings and recommendations

Figure 13: Focus area 2 summary of key findings and recommendations

Themes	Areas	No. of key findings	No. of key recommendations
Prepare	Governance over crisis and business continuity management - HSE and across HGs and CHOs	2	2
	Incident/crisis management and clinical and services continuity planning - HSE and sample site hospitals and CHOs	3	3
	Crisis communications preparedness at the HSE	2	2
	Awareness, training and exercising capability - HSE, HG/ hospitals and CHOs	1	1
	Implementation of lessons learned	1	1
	Human factors and cultural contributors	1	1
Response	Notification and activation of NCMT and wider response workstreams	1	1
	Response structures, resourcing and logistics	2	2
	Information and data management in a crisis	3	3
	Response leadership, strategy setting and decision making	2	2
	Stakeholder management, crisis communications and reputation management	2	2
	Scenario planning	1	1
	Effectiveness of workarounds	1	1
Recovery	Services and data led recovery strategy	2	2
	Total no. of key findings & recommendations	**24**	**24**

In reviewing the organisation-wide preparedness and strategic response, we have incorporated guidelines and principles from ISO 22301:2019 'Security and resilience - Business continuity management systems (BCMS) - requirements', BS 11200:2014 'Crisis Management. Guidance and good practice' and PD CEN/TS 17091:2018 'Crisis management - Guidance for developing a strategic capability.

ISO 22301 defines business continuity as 'the capability of an organisation to continue the delivery of products and services within acceptable time frames at predefined capacity during a disruption'.[177] In the context of the HSE, the term clinical and services continuity is used throughout this section of the report. It refers to all acute and community services, as well as corporate services, including, but not limited to HR, procurement, finance, training, ICT etc.

[177] ISO 22301:2019 'Security and resilience - Business continuity management systems (BCMS) - requirements', p. 2.

The European Technical specification for Crisis Management, PD CEN/TS 17091:2018 specifies that organisations should be prepared for an ‘unprecedented or extraordinary event or situation that threatens an organization and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity, with clear, universally understood structures, roles and responsibilities’.[178] It defines crisis management as ‘the developed capability of an organization to prepare for, anticipate, respond to and recover from crises’[179] and states that an organisation’s crisis management capability is not normally part of routine organisational management, and should be consciously and deliberately built and sustained through capital, resource and time investment.

The findings and recommendations in this section are mapped against the key thematic areas derived from these standards *(see section 2.4 - Our review approach)*. The findings and recommendations follow a numbering convention of FA2.KFX (Focus Area 2: Key Finding X) and FA2.KRX (Focus Area 2: Key Recommendation X).

See Appendix F for a detailed organisational timeline.

Crisis Preparedness

Area 1: Governance over crisis and clinical and services continuity management in the HSE and across HGs and CHOs

Introduction and Context

The HSE has shown itself to be well versed and proficient in major emergency management, a capability that has been demonstrated through its response to several recent events, most notably the 2020 COVID-19 pandemic and the 2019 nurses’ strike. The integration of the Major Emergency Management Framework with the wider national emergency management capability enables a comprehensive approach to plan for, to respond and to coordinate recovery from major emergencies which threaten persons or infrastructure at a national as well as local level.

The organisation’s approach to incident and emergency management is detailed in the following preparation documents:

- A Framework for Major Emergency Management;
- Area Emergency Management Plans;
- Hospital Major Emergency Plans;
- Emergency Management Operational Delivery Plan; and
- Incident Management Framework.

FA2.KF1 Crisis management and clinical and services continuity were not integrated within an overarching Operational Resilience Programme, leading to siloed work streams and capabilities

There was little active integration between clinical and services continuity, crisis management and the other closely aligned disciplines to ensure they directly informed planning and that preparedness evolved to prevailing conditions. The HSE is a large and diverse organisation with complex operational structures. Initiatives to achieve greater integration of resilience disciplines were proposed in September 2019, when an Enterprise Risk Management (“ERM”) programme was discussed at the Board meeting.[180] Following this Review the HSE’s new CEO and Board and Audit and Risk Committee led a programme of work to further develop the corporate governance of risk. This included greater oversight at Board and ARC level for corporate risks, significant reviews of the Corporate Risk Register led by the EMT, work undertaken between the Board and the EMT to improve the risk management process, the establishment of a Corporate Risk Support Team and increased investment provided in the 2021 National Service Plan to strengthen the corporate level risk team.

A subsequent review of the HSE’s corporate services commenced in December 2019,[181] ultimately led to the proposal that a new role at National Director level would be established with responsibility for Governance and Risk (“ND G&R”). Responsibilities include the development of risk and business continuity management frameworks through which risk management and clinical and service continuity plans will be reviewed, maintained and validated. Responsibility for clinical and service continuity under the HSE’s accountability structure will remain with operational and functional managers.[182] Resilience

[178] PD CEN/TS 17091:2018 ‘Crisis management - Guidance for developing a strategic capability’, p. 8.
[179] PD CEN/TS 17091:2018 ‘Crisis management - Guidance for developing a strategic capability’, p. 8.
[180] Minutes-hse-board-meeting-27-09-2019
[181] Centre Review Slides June 2021
[182] HSE_CCR_Phase2_HealthcareStrategy_Gov&Risk(Extract)

was also highlighted as a priority at the Performance and Delivery Committee meeting in June of 2021.[183]

Board oversight of the wider risk and resilience capability is currently delivered through a number of different committees, under the consolidated oversight of the Audit & Risk Committee, as follows:

- Clinical and services continuity (currently described as business continuity) - Audit & Risk Committee; and previously People & Culture Committee until June 2020;
- Incident management - Safety & Quality Committee;
- Enterprise risk management - oversight and management - Audit and Risk Committee; and
- Cyber security - Performance & Delivery Committee.

The workstreams related to these risks often operated in silos. Additionally, when risks were identified, improvements to the HSE's response capability were not always informed by those risks. For example, the Board received a detailed briefing in November 2020 on the emerging cyber threats faced by the HSE and the increase of the ransomware risk to business continuity.[184,185] Nevertheless, the Cybersecurity and Business Continuity risk ratings in the CRR remained constant (at a 'High' rating of 16).[186,187,188,189]

Following the review of corporate services, the ND G&R (equivalent to a Chief Risk Officer) reports through the Chief Strategy Officer to the CEO, Audit & Risk Committee and Board on risk management. In a mature Operational Resilience Programme, we would expect to see the separate, but related disciplines of risk management, incident management, clinical and services continuity and crisis management integrated into a comprehensive resilience framework under the coordination of a senior executive, usually a Chief Risk Officer who has appropriate access to the EMT, the CEO and the Board. The framework allows for assurance over the operational capability that is being delivered by relevant owners.

FA2.KR1.1 Establish governance and oversight of an Operational Resilience Programme (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Nominate an executive with responsibility for operational resilience which will include the coordination of component parts of crisis management (including major emergency management), incident management, clinical and services continuity and enterprise risk management;
- Establish a HSE Resilience SteerCo to oversee the design and delivery of an Operational Resilience Programme, reporting into the Board. This SteerCo should include senior representatives from the EMT who own the respective resilience disciplines and related functions (e.g. cyber security), and any additional key clinical and services and operations representatives.

FA2.KR1.2 Establish an Operational Resilience Policy and Programme scope, strategy and structure (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Define an overarching policy that incorporates the above resilience disciplines. Clarify ownership of the programme (for example, under the ND G&R) and integration with existing policies. At a minimum, the policy should include a statement of leadership commitment, objectives and scope, roles and responsibilities, reference to relevant industry standards and an oversight regime;
- Define the Operational Resilience Programme scope, strategy and structure across the HSE and funded entities. Define the types of incidents in scope (e.g. physical, technological, people and cyber incidents) and how to build and maintain a capability to respond across the organisation. Define the operating model or the capability in terms of dedicated staff, reporting lines, roles and responsibilities within 'prepare' and 'respond and recover.' Specify which areas of the HSE and funded entities are included and identify accountable teams/individuals for delivering specific components of the programme. Agree the intended end state, the timetable to achieve the objectives and the resources required;

[183] https://www.hse.ie/eng/about/who/board-members/committees-of-the-board/performance-and-delivery-committee /mintues-hse-performance-and-delivery-committee-18th-june-2021.pdf
[184] Briefing for HSE Board on Cyber Security
[185] Cyber Security Awareness Draft V7.2
[186] CRR Full Report Post EMT 2nd Nov OCTOBER 2020 v0.2 03 11 20 FINAL
[187] CRR FULL Report Summary and Assessments HSE Board 23rd June 2020 pdf v0.1 23 06 20
[188] CRR Q1 2021 Review Report Final post EMT meeting 27 04 21 v1.0 27 04 21
[189] CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21

- Design consistent tools and templates to be used by the HSE and to be cascaded down as resources for funded entities. Assign responsible leads to complete these tools and templates, and develop documentation and capability at operational sites.

FA2.KR1.3 Establish assurance over the Operational Resilience Programme (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Develop programme reporting, including KPIs, a method and timetable for review, and risk management considerations. Ensure that operational resilience is a standing agenda at Board (or Board committee) meetings.

FA2.KR1.4 Embed the Operational Resilience capability via training and exercising (see strategic recommendation 4.2 in Section 4)

The HSE should:

- Ensure a commitment to maintain and test the resultant capability by designing an HSE-wide training and exercising programme. This includes a structured programme for delivering knowledge and skills training, and scenario-based exercises to all relevant stakeholders across the HSE and funded entities who have a role to play in any serious or significant incident or crisis; as well as additional training resources, validation programmes and independent Internal Audit review to the Board;
- Ensure ND G&R and at least one Board member has direct competency/experience in the area of operational resilience.

FA2.KF2 There was no effective governance or consistent ownership of clinical and services continuity across the HSE

There was no central Clinical and Services Continuity Management System Framework in place in the HSE prior to the cyber attack. Roles and responsibilities in respect of the management and oversight of clinical and services continuity were not documented, nor were there any structured governance mechanisms to implement, monitor and report progress on the objectives contained in the 2016 Business Continuity Policy.[190] In the absence of this framework, clinical and services continuity capability was not adequately resourced or embedded. This was identified in the review of the HSE's corporate services, initiated in 2019; and while enterprise risk management and clinical and services continuity are now consolidated under the National Director for Governance and Risk *(see also finding FA2.KF1)*, a significant body of work will be required to address this gap.

Due to the historic lack of governance and oversight over clinical and services continuity across HGs and the HSE funded entities, a fragmented and unvalidated capability was also apparent across individual hospitals and CHOs. There was no evidence of Clinical and Services Continuity Policies at any of the sample sites or of formalised steering committees with documented roles and responsibilities for the ongoing and continuous maintenance of the local Clinical and Services Continuity Management System. Senior members of the HSE commented that there was insufficient support and resources provided to HGs and CHOs to ensure standardised and consistent approaches to clinical and services continuity management at local site level. While continuity of services is implied in service level agreements with hospitals, there is no specific requirement to demonstrate a clinical and services continuity capability.[191] Internal Audit scrutiny of all organisations funded by the HSE is permitted in the Audit and Risk Committees ToRs. However, there was no evidence of any audit of the clinical and services continuity capability in the HSE or funded entities.[192]

FA2.KR2.1 Establish and document a formal governance structure to oversee clinical and services continuity in the HSE (see strategic recommendation 4.1 in Section 4)

The HSE should:

- Update the existing Clinical and Services Continuity Policy and present it to the Board for review and approval. This should be nested under the overarching Operational Resilience Policy *(see also recommendation FA2.KR1)* and clearly articulate the purpose, scope, applicability, review frequency, authority, Clinical and Services Continuity Management Framework, governance and monitoring of the policy and programme;
- Establish a programme of governance for clinical and services continuity - incorporated under the Operational Resilience Programme *(see recommendation FA2.KR1.1)* - which provides a central point of accountability for monitoring and reporting on the implementation, maintenance and validation of activities in line with policy objectives. Formally document roles and responsibilities, a Clinical and Services Continuity Steering Committee and an organisational chart.

[190] Business Continuity Management Policy 2016
[191] Site Workshop 6 and 11 (Hospital C and Hospital A)
[192] Audit and Risk Committee TORs

The scope should reference the HSE and all funded entities;

- Formalise robust reviews and challenges by appropriate personnel, of all stages of the Clinical and Services Continuity Programme, embedding Internal Audit into the clinical and services continuity lifecycle to provide independent assurance to the Board of the HSE's contingency capabilities;
- Secure formal clinical and services continuity qualifications for appropriate members of the steering committee/implementation team;
- Be prepared to consider the emerging requirements contained in the EU Critical Entities Resilience Directive ("CER").

FA2.KR2.2 Support funded entities (hospital groups, hospitals and CHOs) to establish governance over clinical and services continuity (see strategic recommendation 4.1 in Section 4)

The HSE should support funded entities (hospital groups, hospitals and CHOs) to:

- Implement Clinical and Services Continuity Steering Sub-Committees at HG, hospital and CHO levels, beneath the HSE Steering Committee; and establish a framework of governance. These groups should have a similar structure, terms of reference and roles and responsibilities as the overarching HSE group;
- Draft specific Clinical and Services Continuity Policies which complement the HSE's policy, according to the policy guidance listed above;
- Appoint relevant clinical and services continuity sponsors;
- Integrate clinical and services continuity into project and change management processes where appropriate.

Area 2: Incident / crisis management and clinical and services continuity planning at the HSE and sample site hospitals and CHOs

FA2.KF3 Clinical and Services Impact Analysis did not consistently inform clinical and services continuity workarounds

The Clinical and Services Impact Analysis[193] (referred to in standards as a Business Impact Analysis) identifies critical processes, and the associated people, premise, systems and infrastructure, which must be maintained to ensure a minimum viable organisation during an incident or crisis. Failure to conduct a comprehensive Clinical and Services Impact Analysis process hinders the development of adequate workarounds to maintain critical operations.

Standardised or formalised Clinical and Services Impact Analysis processes were not evident at HSE centre, support services, or sample hospital and CHO sites. Even those sample sites where the clinical and services continuity posture was proactive and mature (e.g. Site Workshop 11), a Clinical and Services Impact Analysis had not been conducted. Some hospital and CHO response teams reactively defined their recovery priorities during the initial phase of the attack because there was no Clinical and Services Impact Analysis. This diverted effort from the response towards tasks which should have been completed in advance of the cyber attack, eg., defining a schedule of systems for recovery based on pre-agreed Recovery Time Objectives ("RTOs") and Recovery Point Objectives ("RPOs"). Several interviewees noted that in the absence of a Clinical and Services Impact Analysis the early prioritisation scheme was driven by the OES list, before advancing to an approach that focused on clinical risks,[194] delaying the recovery of patient critical services *(see also finding FA2.KF17)*. The extent of the initial disruption and maintenance of essential services varied significantly across the sample sites. There was also significant variance in the effectiveness and availability of workarounds or recovery strategies to ensure consistency of critical patient services.

[193] ISO 22317 Societal security - Business continuity management systems - Guidelines for business impact analysis (BIA)
[194] Site Workshop 8 (Hospital B)

FA2.KR3.1 Establish and embed a clear and consistent approach to Clinical and Services Impact Analysis across the HSE to inform recovery prioritisation *(see strategic recommendation 4.1 in Section 4)*

To ensure a standardised organisation-wide approach to the Clinical and Services Impact Analysis process, the Executive Sponsor for clinical and services continuity at the HSE and each HG/hospital and CHO should:

- Establish and embed a formal Clinical and Services Impact Analysis process, with clear ownership at each level, including the criteria for the "RTOs"[195] and "RPOs"[196];
- Ensure the results of the Clinical and Services Impact Analysis are formally reviewed and approved on a periodic basis, by senior management, and following any significant systems/process, operational, regulatory or personnel change.

FA2.KR3.2 Design clinical and services continuity workarounds, based on the Clinical and Services Impact Analysis, to enable the HSE to continue providing critical services while responding to an incident or crisis *(see strategic recommendation 4.2 in Section 4)*

The HSE should:

- Design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis;
- Assess all workarounds to ensure they do not pose an unacceptable risk to patient care or to the HSE through the transfer of data or other assets between systems;
- Align workarounds for similar systems or processes across the HSE to improve their effectiveness and inform a consistent response;
- Reflect the workarounds in the relevant Clinical and Services Continuity Plan.

FA2.KF4 There was no standardised approach to clinical and services continuity planning across the HSE

There is no framework or mechanism in place at the HSE to ensure that the clinical and services continuity planning is aligned to the policy objectives. No integrated and comprehensive clinical and services continuity planning exists at the HSE. Additionally, while some hospitals had a level of clinical and services continuity planning in place, there was no evidence that this process was consistently formalised or conducted across sampled HGs, hospitals or CHOs, to deliver a local clinical and services continuity capability.[197] Where workarounds were in place, there was inconsistency in emphasis, layout and terminology and no evidence that the determination, adoption and resourcing of those workarounds had input or steer from the HSE centrally.

The absence of pre-prepared Clinical and Services Continuity Plans severely impacted the initial stages of the response to the cyber attack, as resources had to be diverted away from the response effort to compile essential information, create structures and prioritise services for recovery which should have been formalised and articulated during a preparatory phase.[198, 199] Recurring examples given in interviews of this were construction of call trees, compiling asset registers, critical service prioritisation and definition and use of alternative communications methods. Furthermore, recovery solutions were often inaccessible as hard copies were not available.

FA2.KR4 Develop and embed consistent Clinical and Services Continuity Plans at strategic, tactical and operational levels that align with the Clinical and Services Impact Analysis *(see strategic recommendation 4.2 in Section 4).*

To ensure that Clinical and Services Continuity Plans are compatible with the recovery objectives, the HSE should:

- Implement Clinical and Services Continuity Plans at strategic, tactical and operational levels of the HSE, HGs/hospitals and CHOs and that they formally document workarounds and the steps involved to resume normal operations;

[195] Recovery Time Objective (RTO) is the period of time following an incident within which a product and service or an activity is resumed or resources are recovered (ISO 22300:2021).

[196] Recovery Point Objective (RPO) is the point at which information used by an activity is restored to enable the activity to operate on resumption (ISO 22300:2021)

[197] A sample of example plans include: Hospital C Business Continuity Plan Dec 2019, Hospital F Pandemic Preparedness Plan, Hospital E Internal Emergency Response Plan, Midlands SAP Payroll Business Continuity Plan

[198] Site Workshop 11 (Hospital A)

[199] Information Management & Coordination Workshop

- Benchmark the Clinical and Services Continuity Plan construction against ISO 22331, and ensure they are compatible with future Sláintecare objectives;[200]

- Incorporate the testing of these steps into the clinical and services continuity management training and exercising schedule/programme (e.g. through desktop walkthrough of the resumption procedures to identify any gaps or unforeseen dependencies);

- Ensure soft and hard copies of Clinical and Services Continuity Plans are available in appropriate areas.

FA2.KF5 The HSE did not have an adequate internal Crisis Management Framework or plans to support the response to the Conti attack, nor had they planned for severe but plausible total loss scenarios

The Major Emergency Management and Incident Management Frameworks (as well as interim Emergency Management governance arrangements published in 2020) have been invoked on multiple occasions and delivered an agile and effective response to short term surge demands on health services.[201,202]

There is an inconsistent and interchangeable use of the terms 'major emergency management' and 'emergency management' and 'crisis management'. Crisis planning throughout the HSE was focused on the scenarios which would mobilise major emergency management teams, such as adverse weather, pandemic, epidemic, serious accidents and terrorist action. There was no Crisis Management Plan in place to guide the HSE's response to an internal crisis impacting the HSE itself, rather than an external crisis such as COVID-19 or Storm Emma; nor has it developed and exercised *scenario-specific* plans for the response to severe disruption scenarios, (e.g. total loss of premises, systems or people). A fundamental assumption of these plans is that all mission critical systems and infrastructure would remain available to the response teams. The HSE has not conducted any scenario planning for the total loss of a facility, system, process or service *(see also finding FA2.KF21)*. While risks were noted on the Corporate Risk Register (especially cyber security and clinical and services continuity), there was limited evidence to suggest the HSE undertakes subsequent scenario planning to:

- Identify potential triggers and escalators for the worst, best and most likely scenarios per risk;

- identify likely impacts;

- undertake mitigating actions despite the fact that cyber security and clinical and services continuity were identified as strategic risks.

Such scenario-specific plans would outline the likely impacts caused by highly plausible organisational crises, as well as the key considerations, and corresponding pre-agreed decisions to guide the strategic response to those events.

FA2.KR5.1 Design an end-to-end Crisis Management Framework (integrated with the existing MEM and IM Frameworks) and overseen by the HSE Resilience Steering Group *(see finding FA2.KR1.1 and strategic recommendation 4.2 in Section 4)*

The HSE should review the existing incident and emergency management structures, and the structures established during the attack and other recent events (e.g. COVID-19), to establish a new integrated end-to-end organisation-wide Crisis Management Framework that is fit-for-purpose across a wide variety of crisis types. This Framework should incorporate all resilience disciplines responsible for implementing organisational preparedness activities (e.g. emergency/incident/crisis response, and clinical and services continuity management), and identify accountable teams/individuals for specific components, as well as define all levels of response required during an actual event at strategic, tactical and operational levels. It should also integrate with the relevant elements of the organisation-wide Major Emergency Management and Incident Management Frameworks.

The Framework should include the following elements:

- Hierarchy of teams required for response. Typically this will include three layers - operational, tactical and strategic - with command and control escalating according to the nature and severity of the incident;

- Defined roles and responsibilities, and decision making authority, for all those involved in the identification, escalation, response to and management of incidents;

- Escalation thresholds and formalised communication channels;

- Guidance on how and when to invoke response structure in line with the Incident Classification and Severity Matrix *(see also finding FA2.KF14);*

[200] ISO 22331 Security and resilience - Business continuity management systems - Guidelines

[201] Incident Management Framework 2020

[202] A Framework for Major Emergency Management

- Agreed touchpoints and interaction between the HSE, and HGs and CHOs;
- Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).

FA2.KR5.2 Design a suite of crisis response plans and procedures to underpin the Crisis Management Framework *(see strategic recommendation 4.2 in Section 4)*

The HSE should design:

- A Crisis Management Plan providing detailed roles and responsibilities for key positions in the NCMT and supporting tactical teams (e.g. HG/hospital and CHO leadership), including checklists of activities and considerations, and details of third party support available;
- A Technical/Operational Coordination Guide providing the details of how the technical (e.g. IT Ops) and operational teams (e.g. clinical response teams) would coordinate and work together. This includes detailed roles and responsibilities, information flows, processes, checklists of key activities and considerations and details of third party support available;
- Scenario-specific plans providing detailed step-by-step operational guides for specific scenarios (e.g. analyst response to malware, fire response plan). The HSE should, using the risks identified in the Corporate Risk Register, conduct a threat profile review and readiness assessment to determine high likelihood, high impact scenarios and create scenario-specific plans for response. This should include severe but plausible total loss scenarios;
- Functional Response Plans providing detailed function-specific guidance for non-technical teams, for example a Legal/Regulatory Team and Communications Team *(see recommendation FA2.KR7);*
- Site-Specific Response Plans templates and guidance, providing resources for standardised clinical and services continuity and crisis management planning at sites across the organisation.

Area 3: Crisis communications preparedness at the HSE

FA2.KF6 The HSE's Internal Communications Team was under resourced

Having only been established in 2019, the HSE's Internal Communications Team was not large enough to coordinate communications to 130,000 staff[203] members. Whilst investment in the External Communications Team has increased to circa 76 full time employees (FTE), the Internal Communications Team consisted of circa six FTE.[204] Stakeholders noted that the Internal Communications Team had struggled to deliver on their growth strategy because immediate crises and operational requirements had consistently diverted the attention of the team.[205]

FA2.KR6 Ensure that the resources assigned to internal communications are sufficient *(see strategic recommendation 4.2 and tactical recommendation 3.1 in Section 4).*

An effective Internal Communications Team is critical to disseminate information and guidance to all 130,000 HSE staff[206] all operating across different levels of the response; this requires additional resources and staff to what is currently available. As part of their future crisis management planning, the HSE should assess the requirements of their crisis response communications strategy and allocate the resources necessary to grow the internal communications team, to reflect the HSE's current operational architecture, and taking into consideration the impacted and involved stakeholder base.

FA2.KF7 There was no documented HSE Crisis Communications Plan in place; and the crisis communications capability across HG/hospital and CHOs was fragmented

The HSE's external communications strategy in response to the ransomware attack, whilst well-executed, was based on previous experience for the organisation rather than a formally documented Crisis Communications Plan. The combined experience of the communications team, across multiple sectors (including PR, journalism and crisis communications) allowed them to create a governance structure for their workstream by 08:00 on the day of the attack

[203] https://www.google.com/url?q=https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf&sa=D&source=docs&ust=1634489485576000&usg=AOvVaw1RQuuJUGldbFXKLPmktsyu

[204] Comms Division Organisational Chart July 2021

[205] Communications & Stakeholder Management Workshop

[206] https://www.google.com/url?q=https://www.hse.ie/eng/staff/resources/our-workforce/workforce-reporting/health-service-personnel-census-aug-2021-v2.pdf&sa=D&source=docs&ust=1634489498604000&usg=AOvVaw10xqOINj8e5bZNoLDcNAVZ

and begin the process of integrating their response with other response and local communications teams.[207] Whilst the absence of standardised plans and processes did not impact their communications response to this incident, these are important documents to have when onboarding new joiners or working in collaboration with other teams, to ensure response activities are completed to a consistently high standard.

The HSE's national communications teams, and the HG and CHO communications teams operate under separate governance structures. Whilst the HSE's national communications teams have a well established communications network, developed through weekly meetings during the COVID-19 pandemic, the local communications teams have varying levels of experience and available resources. The absence of a consistent communications strategy across HGs and CHOs resulted in different messages being conveyed to patients; some were told to come in unless told otherwise whilst others were told to stay at home unless explicitly told to come into the hospital. This disparity in experience and subsequent strategy has been flagged in the Corporate Risk Register since February 2020 under the risk of damage to the HSE's 'Organisational reputation', with a corresponding action to *'enhance communications functions in new Regional Health Areas'*.[208]

FA2.KR7 Document the Communications Team's existing response structures, processes, tools and templates in a Crisis Communications Plan *(see tactical recommendation 3.1 in section 4)*

The HSE should document a formal Crisis Communications Plan to ensure consistent and efficient communications management across the organisation during an incident/crisis, and to guide the actions of new members of the HSE's Communications Team.

- The Communications Team should document the response processes, tools and templates, and structures they have found most effective during previous incidents, ensuring the resulting plan dovetails into any existing Major Emergency and Crisis Management Plans and processes, in line with the Crisis Management Framework *(see also finding FA2.KF5);*

- The Crisis Communications Plan should be reviewed in conjunction with the Crisis Communications Plans in place at the HGs and CHOs to ensure the structures and processes involved integrate effectively;

- Once finalised, all processes and templates, especially those requiring collaboration with other HSE teams, should be socialised and ratified to ensure they are fit for purpose and based on up-to-date information;

- The Crisis Communications Plan should be reviewed regularly to confirm the content is still correct and relevant, and to incorporate any lessons learnt from new incidents.

Area 4: Awareness, training and exercising capability at the HSE, HG/hospitals and CHOs

FA2.KF8 Awareness, training and exercising of the crisis management and clinical and services continuity capabilities were not formally embedded across HSE

Various emergency management exercises have been held across the HSE, covering responses to several scenarios such as extreme weather and exposure to infectious diseases. There was also evidence of more advanced training and exercising capabilities in place at some HGs and CHOs.[209, 210] However, there was no evidence of a HSE-wide training and exercising programme to ensure the right people, at the right levels, were trained in their functions, roles and responsibilities in a crisis.[211, 212] For example, there was isolated but limited evidence that staff involved in the Conti response had received training on the HSE's clinical and services continuity capability, priorities and plans prior to the crisis.

We found no evidence of strategic level exercises (delivered to its National Crisis Management Team), rehearsing the response to a clinical and services continuity event or crisis *impacting the HSE only,* e.g. the loss or denial of critical HSE systems or infrastructure, or a significant reputational issue. Additionally, while the HSE has participated in national multi agency major emergency exercises, they have not conducted any multi-team crisis desktop or simulation exercises in conjunction with

[207] Communications & Stakeholder Management Workshop
[208] CRR Full Report Summary and Risk Assessments v0.1 28 02 20
[209] Site Workshop 5 (Hospital F)
[210] Site Workshop 10 (Hospital I)
[211] Site Workshop 5 (Hospital F)
[212] Site Workshop 1 (CHO B)

key sites to simulate loss/denial scenarios of critical infrastructure. There was also a lack of evidence to show how the risks identified in the Corporate Risk Register informed the design of plausible scenario-based exercises.[213, 214, 215]

Whilst there were pockets of good practice across the organisation where local entities deliver frequent emergency management exercises, there was no evidence that the clinical and service continuity exercises delivered followed a standard approach or aligned to best practice design as outlined in industry standards. The absence of a comprehensive approach to integrated crisis management training and validation across the organisation has resulted in the following findings, evidenced in a sample of hospitals:

- Plans did not capture challenges which could have been identified during a rigorous validation process; for example, the unavailability of hard copies of Clinical and Services Continuity plans, an inability to install WiFi post attack, absence of call trees and no alternative communications plan;[216]
- The absence of well-articulated roles, responsibilities and crisis management structure (e.g. local level responders were unsure of their roles and the structures in place);[217]
- No clear decision making authority, including delegated decision making to HGs/hospitals and CHOs, that is clear to the National Crisis Management Team and executives, as well as supporting teams and structures[218];
- No Crisis Communications Plan or recognition for the need of a HSE-wide internal alert system or alternative communications channels[219] to allow cascading information between the HSE, CHOs and HGs;
- At the time of the cyber attack, there was no expertise in the HSE on how to stand up an integrated coordination centre. The HSE therefore initially relied on significant third party assistance and then the Defence Forces to establish a SITCEN and the templates and protocols necessary to achieve an integrated command centre *(see also finding FA2.KF15)*.[220]

FA2.KR8.1 Establish a formal training and exercising programme in support of the Operational Resilience Programme *(see also Finding FA2.KF1 and strategic recommendation 4.2 in section 4)*

The HSE should:

- Ensure this programme incorporates clinical and services continuity and crisis management requirements and that all relevant individuals and teams involved at every level of the HSE become familiar with their roles and responsibilities in a crisis or significant clinical and services continuity incident;
- Ensure it is aligned to *ISO 22398 Security and resilience - Guidelines for exercising and testing.* Define and implement standard training and exercising templates which articulate scope, objectives, assumptions, results, issues log and lessons learned.

FA2.KR8.2 Deliver training to staff in key responsible and supporting roles, and new managers *(see strategic recommendation 4.2 in section 4)*

The HSE should:

- Provide clinical and services continuity and crisis management training for staff in key responsible and supporting roles. Such staff should have knowledge of best practice in relation to each core element of an effective integrated command centre and of an effective Clinical and Services Continuity Management Programme including: risk assessment, Clinical and Services Impact Analysis, clinical and services continuity management strategy selection, plan testing techniques and processes for assessing effectiveness of plans;
- Include clinical and services continuity awareness training for new managers.

FA2.KR8.3 Conduct annual exercises to rehearse the operational resilience capability *(see strategic recommendation 4.2 in section 4)*

The HSE should:

- Conduct annual crisis management and clinical and services continuity desktop or simulation

[213] Site Workshop 2 (CHO A)
[214] Site Workshop 3 (Hospital E)
[215] Site Workshop 10 (Hospital I)
[216] Site Workshop 3, 9 and 11 (Hospital E, Hospital H and Hospital A)
[217] Site Workshop 4 (Hospital E)
[218] Site Workshop 4, 7 and 9 (Hospital E, Hospital G and Hospital H and) and Information Management & Coordination Workshop
[219] Site Workshop 9 (Hospital H)
[220] Site Workshop 4, 9 and 10 (Hospital E, Hospital H and Hospital I)

exercises with the NCMT and ensure scenarios extend beyond current focus to include other loss scenarios including loss/denial of mission critical infrastructure, unavailability of key persons, systems, processes and facilities;

- Conduct annual multi-team crisis management and clinical and services exercises involving key HSE functions (e.g. support services) and funded entities; increasing in complexity over time to continually build organisation-wide maturity and capability;
- Support the nominated responsible owner with responsibility for clinical and services continuity and crisis management to acquire relevant external training to maintain the currency of their expertise.

Area 5: Implementation of lessons learned

FA2.KF9 While there was a formal overarching post-incident review process and evidence of localised 'lessons learned' programmes, the process and outcomes were not consistently applied

The HSE Incident Management Framework outlines a process for conducting a post-incident review, followed by improvement planning and monitoring.[221] Whilst the HSE have not previously encountered an incident of this scale, they have been exposed to other significant incidents (COVID-19, nurses strike and WannaCry) over the last five years, each of which would have highlighted key learnings for improved crisis management maturity at localised level.

One example of lessons learned being incorporated, and a recurring theme from interviews[222], is that the NCMT meeting process, which was developed during the COVID-19 pandemic, was quickly adapted to respond to the Conti ransomware attack. This was demonstrated by the speed with which the NCMT first convened at 08:30 on 14 May and the clear governance and administrative structures put around their response activities.[223, 224] Another example is that, with communications platforms unavailable across the HSE, the Internal Communications Team were still able to publish information to the HSE website; this was due to a previous decision to reduce the website's dependency on the HSE infrastructure, based on lessons learned from previous IT disruptions.[225]

At the hospital and CHO level, several sample sites had proactively conducted after action assessments[226] of the response to clinical and services continuity events and applied these in a lessons learned programme. Notable examples of this were CUH with comprehensive post event analysis of Storm Emma and laboratory outages. Moreover, examples of populated lessons learned spreadsheets were shared, illustrating that a wider awareness about the importance of a lessons learned process is in place.[227]

However, there is insufficient overarching governance and process to ensure that lessons from incident and major emergency response are not just identified, but assigned ownership, addressed, and disseminated to inform structural improvements across the HSE and funded entities. Specifically, where individual reviews were conducted, there was a lack of evidence indicating lessons learned were shared more broadly with other areas of the HSE, and with HGs and CHOs. Actions for implementing lessons learned do not appear to have been assigned owners to ensure they are completed, indicating that while lessons may be identified, they do not systematically lead to improvement or change.

FA2.KR9 Review and refine the post-incident review process to ensure ongoing and continuous improvement of the response capability *(see strategic recommendation 4.2 in section 4)*

Formal and consistent post-incident reviews should be conducted following all incidents or near misses to capture both areas of positive performance and opportunities for improvement. The Operational Resilience Steering Group should ensure that all post incident reviews are reported centrally to enable learnings to be disseminated across the HSE and funded entities *(see also finding FA2.KF1).* Mitigating actions should be assigned a responsible owner and tracked centrally until their completion. The process should be reflected in the end-to-end Crisis Management Framework *(see also recommendation FA2.KR5.1).*

[221] Incident Management Framework 2020
[222] Information Management & Coordination Workshop
[223] Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
[224] Programme org chart v1 21.05.21
[225] Communications & Stakeholder Management Workshop
[226] Site Workshop 8 (Hospital B)
[227] Lessons Learned_ Programme Lessons v0.2

Area 6: Human factors and cultural contributors

FA2.KF10 Emergency response was ingrained in the HSE's core operations; HSE staff had a natural ability to respond to emergencies, despite a lack of organisational preparedness

At the time of the cyber attack the HSE was over a year into a multifaceted and prolonged crisis response to the COVID-19 pandemic. All workshop participants stated that staff from all levels across the HSE, impacted hospitals, CHOs and third parties went above and beyond to support the cyber attack response effort.[228,229,230,231]

In times of significant challenge or emergencies staff across the health service are able to demonstrate resilience, and exhibit efficient and quick decision making grounded in organisational values (e.g. prioritisation of patient service and care). A prevalent theme in interviews is that the staff are 'perpetually responding to emergencies'[232, 233, 234], and are therefore naturally skilled at it.

However, the significant majority of individuals interviewed also clearly stated that the HSE was not prepared to manage an event of this magnitude and scale.[235] Clinical and services continuity and crisis *preparedness,* as opposed to emergency *response,* was not evidenced as a corporate priority in the HSE. Interviewees commonly commented that a reactive posture to crisis had largely been normalised and accepted day-to-day practice.[236] The apparent normalisation of crises had led to a predominantly reactive posture towards crisis response, a confidence in the HSE's crisis management capability, and a reduced perceived need for significant advance preparation for wider incidents, organisational crisis or 'black swan' events.

The leadership style and decision-making process required during a crisis is necessarily different than that required during business as usual, even within high tempo, safety critical operations such as health care. Crises are associated with heightened stress that impacts on the decision-making process, which is made more complex by the constraints of time, the volume of decisions to be made and the scarcity of available information. For example, decisions had to be made in the response to the Conti attack where supporting data was not available and where IT and clinical priorities were not understood or aligned (e.g. the decision to disconnect appliances from the network, made in the absence of a clinical and services impact analysis outlining the critical systems, the impacts to be caused, and service level agreements for recovery).

The consequence of being in perpetual 'crisis response' mode can also create wellbeing impacts on staff members, as illustrated in this case by the level of stress and fatigue experienced by staff members dealing with both the COVID-19 and concurrent cyber attack crises.[237] Chronic stress without recovery, depletes energy reserves, leads to burnout and ultimately compromises the crisis response capability. This can subsequently compound the inability to act and lead clearly, and therefore has the potential to further increase the risk of patient safety incidents and clinical errors as well as further risk of harm to staff. Staff who had been deployed during the COVID-19 pandemic reported returning to their roles feeling fatigued before the ransomware attack; the concurrent crises were unlike anything they had ever encountered and the response was heavily fuelled by staff members' 'can-do attitude'.[238]

FA2.KR10 Instil a culture of preparedness in the HSE to reduce the negative impacts of disruption on its people *(see strategic recommendation 4.2 in section 4)*

The HSE should aim to create a culture that values and emphasises crisis preparedness as well as having confidence in natural ability to respond to major emergencies. In addition to scenario-specific plans to prepare for crisis scenarios (beyond the current scope of floods, adverse weather and aviation disasters) recommended below *(see also findings FA2.KF8 and FA2.KF21)*, the HSE should implement a comprehensive training and exercising programme to familiarise all crisis responders at operational (e.g. hospital/CHO, business support services, IT Security,

[228] Information Management & Coordination Workshop
[229] Site Workshop 5 (Hospital F)
[230] Site Workshop 6 (Hospital C)
[231] Site Workshop 1 (CHO B)
[232] Site Workshop 2 (CHO A)
[233] Site Workshop 4 (Hospital E)
[234] Site Workshop 6 (Hospital C)
[235] Information Management & Coordination Workshop
[236] Communications & Stakeholder Management Workshop
[237] Programme RAID Log
[238] Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

etc.), tactical (e.g. HSE, regional/area CMTs), and strategic (e.g. HSE NCMT) levels with their roles and responsibilities for crisis preparedness and response, as well as the unique key considerations and decisions required in various crisis scenarios *(see also finding FA2.KF8).* Conducting scenario-based desktop and simulation exercises will expose individuals to the (simulated) pressures they will experience, thereby reducing the negative impact imposed by external stressors and uncertainty in real life events. Transferring the skills gained in psychologically realistic exercises will facilitate more effective teamwork and decision making in actual crisis situations when they occur.

Crisis Response

Area 7: Notification and activation of NCMT and wider response workstreams

FA2.KF11 Core senior responders were notified and the NCMT invoked quickly; however, the notification of staff and wider stakeholders was ad hoc and did not follow a pre-planned notification process or channel

Core senior responders were notified quickly using best endeavours via phone on the morning of the attack, and the first NCMT meeting was held at 08:30 on the day of the Incident.[239] An initial 'blast' notification was also issued to HSE mobile devices at 14:00[240] via Vodafone and Three network providers[241], in an effort to inform wider HSE staff of the Incident. However, there was no evidence to show this process was formally prescribed and embedded in the Incident Management Framework,[242] Major Emergency Framework[243] or a Crisis Communications Plan, nor was it aligned to an incident severity matrix to ensure the correct level of response was activated and involved *(see also finding FA2.KF14)*. It was noted during interviews with several stakeholders, and in the *Lessons Learned Log* that receipt of the initial notification text was ad hoc and did not reach all HSE staff members and contractors.[244, 245, 246] This was in part because the recipient list did not include staff members or contractors on non-HSE devices.

Interviewees noted that as a result of the ad hoc notification process, some staff members and contractors first heard of the attack on the local news, or by experiencing the effects of the ransomware attack first hand. Others received multiple notices from various parties (including impacted hospitals) and through multiple channels, while some never received an initial notification.[247]

FA2.KR11 Design and implement an integrated notification and escalation process and acquire a means of mass notification to all HSE staff and contractors *(see tactical recommendation 3.1 in section 4)*

The HSE should implement a uniform and integrated notification and escalation process within the updated end-to-end response framework, supported by an Incident Classification and Severity Matrix and an 'Activation Membership' list detailing the stakeholders to be informed, across all levels of response, depending on the severity rating of that incident. This will allow critical responders to be notified of an event and convene at pace to instigate a response at the appropriate level to any incident or crisis impacting its operations or services.

The HSE should review whether the use of mobile phone network providers as a method of sending 'blast notifications' meets the required functionality for mass notification and, if not, should consider investing in a mass emergency notification and communications tool to improve its wider incident notification capability. The solution should include features for notifying all HSE staff members and contractors or smaller groups of staff about any serious incident, crisis or clinical and services continuity event (e.g., a data leak where formal notification and information needs to be disclosed with impacted persons, physical or medical events requiring safety instructions to be issued, or a total system outage/ransomware attack). Clear authority should be designated to an individual or individuals with an appropriate level of authority to send communications from this platform, to ensure all messages are consistent and have been signed off by the appropriate parties (e.g. legal).

[239] Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
[240] Minutes of Cyber Attack MI Meeting 12 pm - 14052021
[241] Information Management & Coordination Workshop
[242] Incident Management Framework 2020
[243] A-Framework-For-Major-Emergency-Management
[244] Lessons Learned_ Programme Lessons v0.2
[245] Site Workshop 2 (CHO A)
[246] Site Workshop 5 (Hospital F)
[247] Site Workshop 4 (Hospital E)

Area 8: Response structures, resourcing and logistics

FA2.KF12 The HSE did not follow a pre-defined and consistent crisis management structure in the initial phase of the response

Although the HSE ultimately established an effective crisis management structure during their response to the ransomware attack, it was designed reactively to apply to this specific incident.

The first NCMT meeting was convened less than four hours after the IT Critical Incident Process was invoked,[248] in part due to the familiarity of operating NCMT established during the COVID-19 response.[249] While invocation was prompt, several stakeholders noted that the initial supporting structures feeding into the NCMT were inconsistent and at times conflicted.[250] Both the Regional CMTs[251] and the Area CMTs[252] were initially stood up based on different documentation, and subsequently stood down when alternate response governance structures, linking directly to the HGs and CHOs, were agreed.

Technology-focused response and recovery workstreams were established in parallel to the CMTs but were not reflected in any of the initial Emergency Response or Incident Management documentation. Additionally, a clinical and integrated governance structure (which later became the integrated clinical and operational risk subgroup of the NCMT) was set up to capture risks, guide the operational response based on clinical priority, and in an effort to establish clear communications between clinical operations and IT. This was a critical group that ultimately influenced the prioritisation of the recovery of the IT systems to enable the resumption of clinical services Stakeholders noted that the legal workstream had not been considered as a required workstream for an emergency or incident response prior to the attack. Finally, it was identified in the *Lessons Learned Programme Log* that central reporting was difficult due to the way individual workstreams were established in silos and without clear central guidance *(see also finding FA2.KF18)*.[253]

The lack of integrated programme management was recognised as a risk by the HSE five days into the response.[254] This led to a request for assistance from the Defence Forces who established defined information management processes which were 'scalable and agile'[255] and could cope with the complexity of a cyber crisis. Stakeholders interviewed noted a recurring sentiment that the Defence Forces' intervention was critical in allowing the HSE to establish tighter governance, better communication flows and create mental space for responders to focus on remediation and recovery activities.[256, 257]

FA2.KR12 Establish a Crisis Situation Centre to manage an organisation-wide response to a crisis *(see recommendation FA2.KR5.1 and strategic recommendation 4.2 in Section 4)*

As part of the Crisis Management Framework *(see recommendation FA2.KR5.1)*, the HSE should establish a Crisis Situation Centre construct to be stood up during a crisis response. This should incorporate the learnings from the Situation Centre introduced by the Defence Forces during the Conti response and include the following elements:Guidance on how and when it should be invoked in line with the Incident Classification and Severity Matrix *(see also recommendation FA2.KR14);*

- Guidance on how and when it should be invoked in line with the Incident Classification and Severity Matrix (see also recommendation FA2.KR14);
- The hierarchy of teams required;
- Roles and responsibilities and delineated decision authority of each response level;
- Escalation thresholds and formalised communication channels;
- Agreed touchpoints and interaction between the Situation Centre and HGs and CHOs;
- Tools and templates to be used by all responders (across the HSE, HG and CHO levels) during an incident (e.g., situation report, classification and severity matrix, impact assessment, decision and action logs).

[248] Conti Cyber Response NCMT Structures Governance and Admin V1.10 31052021
[249] Information Management & Coordination Workshop
[250] Lessons Learned_ Programme Lessons v0.2; Information Management and Coordination Workshop
[251] Emergency Management Services Delivery Plan 2019 - Regional CMTs
[252] HSE EM Interim Governance Arrangements Jan 2020 - ACMTs
[253] Lessons Learned_ Programme Lessons v0.2
[254] Programme RAID Log
[255] Information Management & Coordination Workshop
[256] Information Management & Coordination Workshop
[257] Communications & Stakeholder Management Workshop

FA2.KF13 There was lack of oversight and structure to the coordination and integration of third party support

The HSE recognised the need for additional resources and specialist skills and engaged third parties for incident response,[258, 259] legal and forensics support early on. The impact of the Incident on a national scale encouraged goodwill from third party support and vendors, including the provision of pro bono work. The HSE was aware of the reliance they were placing on third parties and set objectives for each, to ensure they did not undertake activities beyond the required time period. The HSE also took ownership of tasks when sufficient progress was made and the internal resources became available.

It was noted in interviews that a significant amount of time was spent onboarding and integrating third parties, particularly educating them on the intricacies of the health sector and for example, differences between voluntary and statutory hospitals.[260] Stakeholders also noted that data gathering activities were duplicated because HSE staff did not have visibility of third party activity or miscommunication between third parties and internal teams. This diverted focus from other efforts during the critical early stages of the response. The visual representation of each team's priorities at CityWest several days into the response addressed some of these issues, as it allowed responders to deconflict their activities and re-engineer their approach where required.

FA2.KR13 Establish formal retainers with key third parties that may be required to support a crisis response *(see tactical recommendation 3.3 in Section 4)*

The HSE should consider the third party support that may be required during an incident, including: crisis response, external legal counsel and public relations. These retainers should include service level agreements, clear descriptions of third party roles and responsibilities, and pre-agreed legal requirements (such as non-disclosure agreements) to ensure partners can be engaged to support, and be integrated into, a response immediately and scale to the size of the response required.

Work should be conducted with third parties providing technical support to familiarise them with the HSE's IT network, architecture and systems, to facilitate quicker engagement during an incident. The role of retained third parties should be reflected in response plans or playbooks and they should be involved in regular cross-organisation conversations and training exercises with the HSE, the HGs and CHOs to rehearse efficient coordination and communication flows.

Area 9: Information and data management in a crisis

FA2.KF14 The initial impact assessment was hindered due to the absence of an HSE-wide incident severity matrix

There was no integrated HSE-wide Incident Classification and Severity Matrix to guide the initial impact assessment following the attack. The 'HSE Risk Impact Table' in the *HSE Incident Management Framework* lists five impact levels from Negligible to Extreme across eight different categories.[261] While those categories reflect a spectrum of operational, financial, compliance and reputational impacts, there was no evidence to indicate that the initial impact assessment conducted during the ransomware attack was based on this guidance and subsequently used to inform decisions made and actions taken. There was also no evidence provided of an Incident Severity Matrix for IT or cyber incidents, specifically.

The *Managing a Major Incident* document is designed to be used in a 'critical' incident that attracts '*more attention or has a greater impact than "normal" critical incidents*'; [262] however, there were no associated definitions for those thresholds. It was also unclear how the impact assessment from an IT incident would be aligned with that of the 'HSE Risk Impact Table'. In the absence of an *integrated* HSE-wide Incident Classification and Severity Matrix *(see also finding FA2.KF12)*, response teams did not have clear thresholds and criteria to assess the (actual and potential) business, operational, financial and reputational impacts of the cyber incident. As a result, the initial response centred on understanding 'the what', rather than quantifying the impact to inform and set the strategic response strategy for effective decision making.

[258] M_HSE_Intrusion Investigation Report - REDACTED (FINAL).pdf, 2021

[259] Minutes of Cyber Attack MI Meeting 10 am - 14052021

[260] Site Workshop 9 (Hospital H)

[261] HSE-2020-incident-management-framework-guidance

[262] Managing a Major Incident v1 1 and IT Security Incident Plan

FA2.KR14 Develop an integrated HSE-wide incident classification and severity matrix for assessing the organisational impact of an incident *(see strategic recommendation 4.2 in section 4)*

The HSE should ensure it includes clear criteria to determine the level of actual and/or potential likely impacts of the Incident, and align with or supersede the 'HSE Risk Impact Table'.[263] It should consider specific impact categories - operational, clinical, reputational, financial, regulatory/legal - and a method for estimating impact based on impact and likelihood.

This should be embedded across all organisational response plans and align with any technical severity matrices, such as those in a technical cyber response plan, to support consistency in response. This will ensure responders are using a consistent approach to anticipating immediate, ongoing and future impacts to support a shared situational awareness.

FA2.KF15 The lack of pre-defined information sharing processes led to inefficiencies in the creation of a shared understanding of the Incident

As mentioned in *finding FA2.KF12*, the tools and processes introduced by the Defence Forces on 18 May, enabled a more efficient meeting tempo and information management. Information sharing channels with HGs and CHOs via nominated liaison officers and coordinators subsequently also took shape.[264]

Several stakeholders noted that the sheer number of coordination and information sharing meetings required placed a strain on several critical HSE stakeholders, who struggled to attend all meetings and/or action response and recovery tasks.[265] Interviewees from several HGs and CHOs also reported that some initial meetings with the HSE were time consuming, oversubscribed and, at times, difficult to follow.[266] A recurring theme was that technical jargon generated confusion and delayed decisions and actions. The lack of in-report standards and a clear definition of what constituted 'Red', 'Amber' and 'Green' also led to initial confusion.[267]

There were instances when HGs and CHOs sent requests for clarification and further support, but did not receive a response and were unclear about how to proceed.[268] Similarly, some hospital stakeholders cited an example where ICT staff had been deployed to their site to clean laptops, but the hospital leadership were unaware that they were present and were still trying to work with the HSE to organise their attendance.[269] These differing understandings may also have been compounded by use of unapproved or informal channels for communicating with stakeholders; for example many interviewees noted they resorted to individualised phone calls, WhatsApp and text messages to relay or obtain information first hand where relationships existed.[270, 271]

FA2.KR15 Designate and train incident information managers (or coordinators) at all levels across an incident or crisis response to maintain a consistent overview of the situation as it develops *(see strategic recommendation 4.2 in section 4)*

Further to *recommendation FA2.KR12,* the HSE should ensure that each workstream beneath the SITCEN, at every command level and workstream, has an information manager (or coordinator) appointed as part of the Incident response team. This role should be implemented in all local hospital response teams, Regional/Area CMTs, and within each HSE workstream up to the NCMT. As the information manager completes their expected role (digesting all information to gain a view of the end-to-end incident), they should escalate their status and update upwards (as with the SITREPs). This will allow the SITCEN information manager to articulate one consolidated account of events, decisions and actions which will achieve situational awareness across all teams and parties involved.

To embed this capability the HSE should train those who have been assigned the role of information manager/coordinator and complete multi-team exercises to rehearse information sharing between teams to maintain situational awareness. Templates created as a result of the ransomware attack should be further developed and embedded into scenario-specific response plans, in order to support the information managers in their role. This structure and format should be used in all teams and work streams to maintain consistency.

[263] HSE-2020-incident-management-framework-guidance
[264] Information Management & Coordination Workshop
[265] Programme RAID log
[266] Programme RAID log
[267] Lessons Learned_ Programme Lessons v0.2
[268] Site Workshop 11 (Hospital A)
[269] Site Workshop 7 (Hospital G- identifier to be removed from final report)
[270] Site Workshop 1 (CHO B)
[271] Site Workshop 10 (Hospital I)

FA2.KF16 There was no pre-agreed 'out-of-band' technology solution to support coordination, collaboration and information sharing during a crisis response

The HSE's communications and information sharing platforms were severely impacted by the attack. A patchwork of technology solutions were brought together to address this gap. The NCSC introduced [redacted] - a secure online chat and file sharing platform - to support the HSE in coordinating and collaborating during the initial incident response. The HSE set up 'clean' email accounts for a handful of key responders on a new HSEmail.ie domain[272] and leadership issued a special derogation and guidelines for HSE staff to use personal emails for information sharing.[273]

The Defence Force SITCEN Information Manager established a directory and information sharing structure on a Teams instance to facilitate centralised coordination, collaboration and information sharing; however, it was noted that not all workstreams were storing their documentation in the Teams instance.[274]

More widely, HSE staff defaulted to the use of WhatsApp, text message and phone calls to share information. Stakeholders from HGs and CHOs also noted in interviews that, in some instances, they procured their own domains and IT infrastructure in order to communicate and share information.[275]

This ad hoc approach ultimately provided a means by which to share information; however, these solutions had not been pre-agreed, risk assessed or authorised for use by the HSE during 'prepare' phases prior to the Incident, nor were incident responders and staff made aware before the Incident that they should be used. As a result, the HSE, HGs and CHOs lacked a centralised and secure information sharing, collaboration and coordination platform from the outset of the Incident. This impeded the initial response efforts, as well as leading to a long data remediation tail *(see also finding FA2.KF23).*

FA2.KR16 Identify and acquire a secure and resilient 'out-of-band' technology solution to ensure an alternative means of information sharing and communication *(see tactical recommendation 3.1 in section 4)*

The HSE should ensure that the platform can facilitate email, file sharing, call hosting and the dissemination of communications to all staff and segmented audiences, and enable all responders to see situations reports, actions and decisions logs and other information necessary to support a shared understanding of the Incident.

Area 10: Response leadership, strategy setting and decision making

FA2.KF17 The overarching response strategy was underpinned by the core HSE value of patient care; however, the initial response was driven by technology priorities

It was widely acknowledged by stakeholders that the HSE's prioritisation strategy in the first week of the Incident was driven by the OES list, informed by regular communication between the HSE's OoCIO and COO functions and input from the CCO.[276,277,278]Stakeholders noted that the response strategy progressed to an approach that focused on clinical risks and the recovery of end-to-end clinical services, underpinned by the core HSE value of patient care, following the co-location of all responders to City West.[279]

The introduction of a 'higher organisational intent' directed at restoring systems that enable patient care was formalised on day 11 of the response and reflected in the daily SITCEN meeting rhythm, which were aligned to facilitate a service-led response strategy.[280, 281] This service-led approach was then consistently adopted and ensured patient care was at the heart of all decisions made. The HSE would have benefited from taking this approach earlier in the response to allow for a more efficient recovery

[272] RAID Log, HSEmail.ie was agreed on 17 May 2021
[273] Letter to all Staff - 1 on 26 May 2021
[274] Lessons Learned_ Programme Lessons v0.2
[275] Site Workshop 11 (Hospital A)
[276] Information Management & Coordination Workshop
[277] Clinical Risk Group Workshop
[278] Site Workshop 4 (Hospital E)
[279] Site Workshop 11 (Hospital A)
[280] 20210524-Morning Update Brief - FINAL
[281] 20210525-Morning Update Brief - FINAL

programme, ultimately reducing impact on patient care.

FA2.KR17 Ensure the 'higher organisational intent' is aligned to the organisational values and drives the response and recovery strategy; review the strategy regularly throughout the response as the situation develops *(see strategic recommendation 4.2 in section 4)*

In this incident, the strategic priority was the restoration and protection of systems underpinning patient care services. The HSE should ensure that all incident response strategies consider both the technical and business response priorities, and are informed by the impacts and requirements of the hospitals, HGs and CHO.

Patient care may not always be restricted to the maintenance of healthcare systems; the possible implications of patient data exposure should be considered in conjunction with discussions on patient care, and incorporated into the HSE's strategic intent during a response. Consideration should be given to how this strategy is cascaded to all levels of the organisation, to direct the actions of the tactical and operational response teams *(see finding FA2.KF19)* and to inform the activities of third party support.

The response strategy should be reviewed regularly during a response based on new information and circumstances to ensure it is still valid and appropriate. The development and implementation of a response strategy should be a key focus during crisis exercising, as this will facilitate a single consistent approach to response and recovery activities.

FA2.KF18 There was a lack of clearly defined and delineated decision making authority between the HSE, HGs and CHOs in the case of an HSE-wide crisis

Several interviewees noted that there was no strategic Crisis Management Plan or cyber response guide with a clearly defined and documented decision making process for senior leadership to follow, in the event of a total IT outage or cyber crisis.[282]

Senior HSE leadership exhibited agile, yet reactive, decision making in the absence of guidance that was driven by organisational values, and grounded in judgement and experience acquired from managing previous crises *(see also findings FA2.KF7 and FA2.KF19).* There was limited evidence of formal and documented decision-making authorities *between* the HSE, CHOs, HGs/hospitals during an HSE-wide crisis *(see also finding FA2.KF12)*. Existing service level agreements between these organisations did not include provision for these authorities,[283, 284, 285] and while the Incident Management Framework identifies the need for decision-making authority, no specific details were provided.[286] Interviewees reported that this led to some confusion at the beginning of the response.[287] The autonomy under which Voluntary hospitals operate makes centralised decision making more complex if the restrictions, constraints and permissions around decision making authority are not formally agreed and documented in advance.

For example, some hospital stakeholders reported that the unilateral HSE decision to disconnect national systems did not take into consideration the level of system dependencies between the HSE, HGs/hospitals and CHOs, and potential risks associated with rapid disconnection.[288] There was also no evidence to indicate that the authority for that decision was documented and agreed.[289290] Conversely, some hospital and CHO stakeholders noted that local decisions were taken contrary to HSE guidance when deemed in the hospital's or CHO's best interest.[291]

FA2.KR18 Agree delineated decision making authority across all teams in the organisation likely to be involved in an organisation-wide incident *(see strategic recommendation 4.2 in section 4)*

The HSE should establish an organisational crisis management structure, incorporating hospitals, HGs, CHOs and contracted third parties, which clearly defines the decision making authority at each level. This structure should be socialised and embedded as part of a regular training and exercising programme for all responders *(see finding FA2.KR8.3)* to ensure it meets the different priorities of all parties and remains fit for purpose. Additional training should be provided

[282] Lessons Learned_ Programme Lessons v0.2
[283] Site Workshop 6 (Hospital C)
[284] Information Management & Coordination Workshop
[285] Site Workshop 11 (Hospital A)
[286] Incident Management Framework 2020
[287] Site Workshop 4 (Hospital E)
[288] Programme RAID Log
[289] Site Workshop 6 (Hospital C
[290] Site Workshop 11 (Hospital A)
[291] Site Workshop 11 (Hospital A)

for the HSE, HG and CHO leadership to support them in:

- creating a shared situational awareness across multiple sites or locations;
- developing effective communication flows between senior leadership across multiple sites or locations;
- establishing clear decision making and delegated authority for senior leadership across multiple sites or locations.

Critical stakeholders or response team members at every level should therefore receive communication about, and be trained and exercised in, the predefined response structures to ensure the hooks and handovers within every level of the command model is understood and seamless during an incident.

Area 11: Stakeholder management, crisis communications and reputation management

FA2.KF19 The lack of internal communications tools and diffuse nature of the health service hindered the ability to send nuanced and targeted messages to staff

The HSE Communications team managed the external communications and media agenda effectively, ensuring the focus of reporting was consistently brought back to patient service and care implications. Through interviews and workshops it was evident that EMT members involved in media messages displayed a consistent and informed approach, receiving support and coaching from the experienced senior Communications team members before any public event.[292]

In contrast, the internal communications capability was stretched to meet the demands of the Incident *(see also finding FA2.KF6*). The absence of a comprehensive mass emergency notification and communications tool meant only staff with HSE devices received the initial 'blast' messages *(see also findings FA2.KF6 and FA2.KF7)*. There was no pre-prepared method by which to communicate with staff in a segmented manner, therefore there was no capability to target different messages to distinct groups of staff. This was exacerbated by the vast and diffuse structure of the HSE, including multiple disparate smaller community organisations. The Internal Communications team ultimately facilitated a workaround whereby updates were published on the publicly available HSE website, and staff were directed via phone calls and social media to check for updates.[293]

Stakeholders noted that improvements to the internal communications capability were made following WannaCry in 2017 - replacing the 'antiquated' intranet with a new website - and the internal Communications Team was formally established in 2019; however, the capability is not adequate for responding to crises of this magnitude.[294]

FA2.KR19 Familiarise the Internal Communications Team with the 'out of band' technology solution to enable focused and targeted communications during a crisis *(see also recommendation FA2.KR16 and tactical recommendation 3.1 in section 4)*

The HSE should set up user accounts for all staff members pre-incident on the selected 'out of band' communication platform to expedite transition to the new platform during a system outage. Staff members should be familiarised with the platform and its functionality ahead of an incident. Details for all alternative user accounts should be recorded centrally and stored offline to ensure contact information for all staff members is readily available during any disruption to the HSE's standard communications channels. Crisis response and communications workstream leads should establish cascading contact trees to notify staff of an incident, to initiate the use of the out of band platform, and to enact specific channels for the discussion of response and recovery activities between core responders. This will allow workstreams to maintain a central repository of useful information and act as an audit trail for post incident review and reporting.

FA2.KF20 Potential data exposure has heightened risk to patients and created long remediation requirements

The HSE took several steps to manage the impact of potential data exposure following the cyber attack, despite the absence of scenario-specific plans[295] and related workstream structures reflected in the MEM or IM Frameworks *(see also findings FA2.KF5*

[292] Communications & Stakeholder Management Workshop
[293] Communications & Stakeholder Management Workshop
[294] Communications & Stakeholder Management Workshop
[295] The Data Protection Breach Management Policy provides high level guidance but does not include specific steps for a ransomware scenario.

and FA2.KF12). They established the Legal and Data Workstream on the 19th of May to:

- Oversee the response and investigation from a legal and data protection perspective arising from the cyber attack;
- Maintain a consistent approach to data protection and legal actions to ensure all regulatory requirements are met;
- Support the Data Protection Officer (DPO) in coordinating the data protection investigation and reporting to the Data Protection and Commission;[296]
- Assist and report on the ongoing investigation of An Garda Síochána[297]

Related decisions, such as informing the Data Protection Commission (DPC),[298]obtaining a court order to prevent the publication and sharing of stolen data and setting up web monitoring services,[299] were actioned quickly to mitigate the potential impact of data loss. A Legal and Data Steering Committee was subsequently set up to oversee risk-based decisions relating to the approach to, and threshold for, breach notification to data subjects whose data may have been compromised and the wider public.[300] Third parties were also called on to support this risk assessment. This work is ongoing and may continue for an extended period of time as the HSE reviews and seeks to mitigate any risk to data subjects' rights and freedoms. While thresholds for notification have been identified, the HSE is in the early stages of scenario and resource planning of the actual notification process, including the liaison with the HSE Communications team on how these notifications should be rolled out. As such the HSE has not yet made any data subject notifications, and no standard resources or templates for notification exist, or have yet been tailored/created for this event. The HSE continues to work closely with funded entities to understand the extent of the potential data exposure and share their risk assessment methodology for notification threshold.

FA2.KR20 Review processes, plans and resourcing for response to future potential data breaches *(see strategic recommendation 4.2 in section 4)*

The HSE should ensure the appropriate resources, tools and templates are created with sufficient advance notice and time prior to notifying data subjects of a breach. Having initial notification letters, FAQ's, responses, and sufficiently trained resources to manage an influx of requests for information will be critical to ensuring a successful roll out of notification if and when required. The HSE should also review and document the processes established during the response to support their future preparedness. They should:

- Complete the work of the Legal and Data Workstream in response to the Incident. This includes reconciling all medical data stored and managed through interim processes post the attack, including data stored on personal devices/ accounts and in paper form;
- Embed the Legal and Data Workstream in the Crisis Management Framework *(see also recommendation FA2.KR5.1 and FA2.KR12);*
- Update the existing Data Protection Breach Management Policy to support the Legal and Data Workstream in future responses, including the data breach notification risk assessment;
- Rehearse the workstream's response both individually and as part of wider HSE exercising programme *(see also recommendation FA2.KR8.3);*
- Agree retainers with third parties for future web monitoring services;
- Ensure materials used to support the notification of data subjects, such as letters, FAQs and talking points, are agreed with the Communications Team;
- Conduct resource planning for future notification programmes; for example, call centres to respond to the significant influx of incoming requests once data subjects are notified.

Area 12: Scenario planning

FA2.KF21 Scenario planning did not inform response and recovery strategies

Stakeholders stated that, despite having dealt with a vast array of major emergencies, they felt ill-prepared for dealing with an IT outage or cyber crisis of this scale, or a specific ransomware attack *(see also finding FA2.KF8)*. Specifically, individuals initially struggled to comprehend the scale and size of the Incident, and felt unable to foresee the contingent

[296] Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021
[297] Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021
[298] DPC Report 15 July 2021
[299] Data Protection Monitoring Process
[300] Terms of Reference - Cyber Attack Legal and Data Workstream Steering Group June 2021

impacts that may occur over time.[301] As with many organisations impacted by ransomware attacks, there was initially a belief that the Incident would cause impact for several days to weeks, before a realisation dawned that these types of events, and their longer term impacts, play out over several weeks and months.

This uncertainty stemmed, in part, from a lack of any formal scenario planning process within the existing Major Emergency Management and Incident Management Frameworks and pre-prepared scenario-specific playbooks. Scenario-specific playbooks define the likely decisions and actions required of a senior team, given the potential risks and impacts of the scenario *(see also finding FA2.KF5).* The existence of a cyber response plan or ransomware playbook would have supported the NCMT's ability to foresee the likely impacts and consequences of the Conti attack, combatting what one stakeholder described as 'a failure of imagination'.

The HSE also does not have a formal overarching process or system to guide the use of scenario planning *during* crisis response, in order to inform the response and recovery strategy during an incident, irrespective of the nature of that event. This would involve identifying potential triggers and escalators for the worst, best and most likely scenarios; identifying consequent likely impacts; and implementing mitigating measures. While some stakeholders noted they were able to conduct hasty scenario planning during the Incident, particularly when determining patient care workarounds, this was performed in an ad hoc fashion at the hospital or CHO level.

FA2.KR21 Scenario planning should be informed by the risk register, the process embedded in the Crisis Management Plan, and the activity conducted throughout incident and crisis response *(see strategic recommendation 4.2 in section 4)*

The HSE should ensure that the risk register is used to drive the creation of severe but plausible scenarios against which the HSE should validate its resilience capability is validated. The process should be extended to engage individuals from the HSE's senior leadership team, risk management, clinical and services continuity and crisis management disciplines in regular scenario planning against the organisation's top risks.[302,303] This is best conducted in a workshop format to identify potential political, economic, sociological, technical, legal and regulatory, environmental and organisational impacts related to each of the HSE's top risks, and to then explore the worst, best and most likely scenarios for each.

Mitigating actions resulting from these workshops should be assigned to an owner with the appropriate level of authority to facilitate organisational change where required, and tracked throughout their lifecycle to confirm they are completed to an acceptable level. These actions and all other outputs from these activities should be used to inform preparation activities across resilience disciplines, to ensure that plans, processes and structures are fit for purpose; and where applicable specific response plans to be developed for the most plausible risks *(see also findings FA2.KR5.2).*

Scenario planning should be included in the Crisis Management Plan to support HSE to prepare for likely outcomes and mitigate subsequent impacts during a response.

Area 13: Effectiveness of workarounds

FA2.KF22 Emergency workarounds implemented across the HSE, HGs/hospitals and CHOs were ad hoc and not always based on predefined solutions or processes, and have caused long remediation tails.

It was widely reported that responders across the HSE, HGs/hospitals and CHOs implemented timely and agile workarounds that allowed core critical processes to continue in the absence of IT.[304, 305 306] The lack of preparedness for a cyber incident of this scale, including a lack of Clinical and Services Impact Analysis and scenario-specific playbooks for cyber response, meant that whilst many workarounds were pre-agreed and rehearsed, others were defined in an ad hoc manner; as there was no systematic approach to maintaining continuity of patient-critical processes *(see also findings FA2.KF3, FA2.KF4 and FA2.KF23).*

In some cases, predefined workarounds were familiar to responders and well-rehearsed, for example, where clinicians were able to switch from digital to paper-

[301] Information Management & Coordination Workshop

[302] The CRR should inform the development of severe but plausible scenarios against which Crisis Management Teams are exercised. The timing, nature and extent of testing should reflect the criticality of the underlying recovery solution / activity

[303] CRR Q1 2021 Review Report Final post EMT meeting 27 04 21 v1.0 27 04 21

[304] Site Workshop 6 (Hospital C)

[305] Communications & Stakeholder Management Workshop

[306] Information Management & Coordination Workshop

based procedures.[307] However, several stakeholders noted that the workarounds were primarily designed for individual systems or processes and proved to be time limited, thereby not suitable for continued use throughout the recovery from a total and lasting IT outage. Additionally, whilst staff in community service environments had experience relying on paper patient charts and were able to adapt quickly, the after action review (AAR) collated by the HSE identified that some staff (clinical and non-clinical) had never worked in a paper-based system and so risked missing relevant information from the different format used in paper documentation.[308] This introduced a risk of information loss if it was not ultimately uploaded into the patient data management system.

Other workarounds, although creative, were devised during the Incident and, as a result, had not been reviewed from an overarching security or risk perspective. Many workarounds were documented as issues in the Programme RAID Log,[309] such as the use of runners to convey lab samples and test results, and the use of whiteboards and shared excel sheets on standalone laptops to populate hospital bed bureaus, due to the increased risk of human error. The risks associated with the continuation of clinical treatment and the use of operational workarounds were assessed and communicated on a regular basis, including clinical guidance on how treatments should be prioritised and managed.[310, 311] Many of these workarounds carried a risk of loss or contamination of patient data, misplacement of patients and incorrect disclosure of patient data, all with a secondary risk of patient care being negatively impacted. One example quoted during interviews that illustrates the lack of accurate patient data, was of a surgeon questioning the whereabouts of a patient due for surgery, when that patient had already been operated on.

Several of the emergency workarounds established to support information sharing and allow individuals and teams to respond at pace, such as the use of personal emails and devices, WhatsApp and paper records, have resulted in an ongoing data remediation risk. Many stakeholders noted that some of the workarounds implemented were not designed with consideration of the need to consolidate and retrofit data when systems were restored.[312, 313] Whilst some interviewees noted they had hired extra resources to manually enter paper-based clinical information to restored systems, the absence of IT systems has resulted in large volumes of paper records, some of which are likely to include duplicate, incomplete or incorrect data that will need to be investigated and remediated. The backload of COVID-19 data in conjunction with the clinical data from the ransomware attack will likely take considerable time, people and resources to rectify.

The HSE issued a communication on 12 August 2021 to stand down the use of personal emails and ensure all data was deleted from local storage areas.[314] However, some stakeholders from hospitals and CHOs reported they have not received clear guidance on the steps required to address this risk. The absence of an assigned owner for the remediation of clinical data will make it difficult for staff members to direct enquiries relating to correct data handling and remediation, resulting in delayed resolution of the issue.

FA2.KR22.1 Design clinical and services continuity workarounds, informed by the Clinical and Services Impact Analysis *(see strategic recommendation 4.1 in section 4)*

The HSE should design and agree clinical and services continuity workarounds, for critical processes, with the agility and governance to be maintained for a prolonged period, and based on the Clinical and Services Impact Analysis *(see also recommendations FA2.KR3.1, FA2.KR4 and FA2.KR23).*

FA2.KR22.2 Design workarounds to support rapid data remediation post-incident or crisis *(see tactical recommendation 1.2 in section 4)*

The HSE should:

- Establish a pre-agreed out of band communications and information sharing platform *(see also finding FA2.KR16)* to ensure data generated by workarounds outside normal operations is captured in a format that can easily be retrofitted with the information held on HSE systems. As part of the organisation's stand-down process, each site and workstream should assign an individual with responsibility for overseeing the consolidation of patient and service data; and
- Reconcile all medical data stored and managed through interim processes post the attack,

[307] Site Workshop 11 (Hospital A)

[308] Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

[309] Programme RAID Log

[310] CCO Clinical Memo 1 15.05.2021

[311] CCO Clinical Memo 2 21.05.21

[312] Site Workshop 1 (CHO B)

[313] Site Workshop 5 (Hospital F)

[314] Temporary Use of Personal ICT Resources.msg

including data stored on personal devices/accounts and in paper form.

FA2.KR22.3 Rehearse workarounds in multi-team exercises *(see strategic recommendation 4.2 in section 4)*

The HSE, HGs and CHOs should participate in multi-team exercises to explore how high impact or likely scenarios could impact their operations. This is extremely important as it helps identify likely and potential impacts to the organisation and responders. These may often need a team and significant investment to resolve, however even the discussion and establishment of hypothetical workarounds will likely reduce the number of ineffective emergency protocols and allow space for creative thinking to consider the ideal solution for all parties involved *(see also recommendation FA2.KR8.3).*

FA2.KR22.4 Consider a review to establish the longer term clinical impacts of the Conti attack *(see strategic recommendation 4.2 in section 4)*

Finally, the HSE should consider conducting a review to understand the longer term clinical impacts that resulted from the Conti attack. This review should build on the findings of the draft research report into the effectiveness of the patient safety risk mitigation strategies following the Incident,[315] and inform future steps to improve the HSE resilience against potential future attacks and minimise the risk to patient care.

Crisis Recovery

Area 14: Services and data led recovery strategy

FA2.KF23 The lack of a comprehensive, current and accessible Clinical and Services Impact Analysis, Configuration Management Database, and asset register delayed recovery efforts

Whilst the HSE were clear in their intent to prioritise patient care and maintain its OES list, without an up to date clinical and services Impact Analysis or configuration management database (CMDB) response teams were initially unable to assess resource requirements and prioritise the recovery of critical services.

As part of the incident response, the HSE established a data workstream to build an understanding of all applications and their dependencies for recovery, collating data from unaffected systems, existing documentation and undocumented knowledge from HSE staff and supporting vendors. The requirement to build this list and then prioritise applications for recovery *during* the Incident, rather than being able to rely on an (offline and accessible) *pre-prepared* Clinical and Services Impact Analysis, Configuration Management Database and asset register, delayed recovery efforts. The HSE also noted in their *Lessons Learned Log* that the complexity and disparate ownership of the HSE IT combined with the lack of an overarching impact assessment *(see also finding FA2.KF14)*, made it difficult to plan the recovery efforts.[316]

The recovery priorities set centrally by the HSE initially focused on the priority restoration of core national applications, e.g., NIMIS.[317] While this approach was widely agreed, the subsequent prioritisation of the smaller and more disparate applications, particularly at the hospital and CHO level, was less straightforward. Stakeholders noted that following the restoration of core national applications, some peripheral applications used by CHOs (such as [redacted]) to communicate with patients and carers, were not prioritised adequately given their place underpinning critical CHO services, due to a lack of perceived importance.

Services were prioritised into three classifications: category A (national core applications), category B (major clinical applications) and category C (priority applications).[318] Applications moved between these categories throughout the response based on recommendations made during the daily Major Incident meetings. Responders attempted to prioritise systems based on the effectiveness of workarounds, and how long they could be maintained. However, this approach did not consider the connections between systems requiring restoration. A recurring finding was that several applications reported to be 'green' were not yet functional at the time of reporting, due to a lack of data on the dependencies between impacted infrastructure, applications and data. One example of this is when access to IPMS was initially blocked by delays in the restoration of Active Directory and Citrix,[319] a delay that took over two weeks to fix, postponing the resumption of business as usual services. The recovery of systems requires the restoration of trusted network connections and information exchanges, all of which

[315] Healy, O. Dr. A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare IT failure, Dated 30th September 2021.

[316] Lessons Learned_ Programme Lessons v0.2

[317] App Priority List - 20210601 1415 and Site Workshop 7 (Hospital G)

[318] Minutes of Cyber Attack MI Meeting 11 am - 18052021

[319] Programme RAID Log

rely on a clear understanding of which systems are interconnected, and what is required for them to work together.

There was also limited consideration of how the IT landscape differed at a central and local level; CHOs and HGs found that third parties brought in to support the prioritisation and restoration of applications did not have a strong understanding of the local environments and their requirements for recovery, impeding the ability to set clear and sequenced recovery priorities.

FA2.KR23 Ensure the Clinical and Services Impact Analysis is informed by an up-to-date asset register and Configuration Management Database *(see also findings FA2.KF3 and FA2.KF22.1 and tactical recommendation 1.3 in Section 4)*

As part of this process, the HSE should work with CHOs and HGs to develop a clear overview of the interdependencies between all departments and local sites using HSE infrastructure or services, with the aim to create a prioritised list for systems at both a central and local level. This should be informed by a service model for delivering patient care. The HSE should reconcile all medical data stored and managed through interim processes post the attack, including data stored on personal devices/accounts and in paper form *(see also finding FA2.KR22.2).*

Contingency plans should be developed by the business owners and IT teams to maintain priority and critical services (as defined in a Clinical and Services Impact Analysis) during the disruption of one or more key systems. These plans should be socialised and embedded across the organisation, and a version of them stored offline, to ensure they can be implemented effectively during an incident. In the event of an incident impacting multiple systems, as within the Conti attack, recovery prioritisation should be addressed on a regular basis from the beginning of the response, to direct resources to the appropriate systems and services from the offset.

FA2.KF24 Recovery efforts were hindered by the lack of a predefined recovery process and targeted supporting resources

Several stakeholders noted that recovery efforts were hindered by the lack of resources and inability to allocate them in the most efficient manner. As mentioned in *finding FA2.KF3*, without a Clinical and Services Impact Analysis to clearly articulate priorities and sequences of recovery, the HSE, HGs and CHOs were unable to create an informed recovery strategy in the initial days. This, coupled with the absence of information available on the HSE's assets and services *(see also finding FA2.KF23)*, meant that technical teams relied on queries and information submitted to a central mailbox set up for the response and on data gathered from vendors and suppliers. The speed with which applications could therefore be prioritised and communicated to the technical recovery teams was not therefore optimal.

Specifically, responders noted that the absence of a predefined priority list and overall process flow meant the Tech and Data Ops teams were at risk of under- and over-utilisation due to workflow issues.[320] This extended to third party support who relied on central coordination from the HSE to direct their recovery efforts. There were missed opportunities to recover applications in parallel and technical responders risked being redeployed onto other recovery areas,[321] delaying or preventing their return to application restoration once a new set of priorities was established. Indeed where responders were left without targeted guidance on what to restore they relied on informal conversations to determine which teams were struggling, and directed their attention there.

FA2.KR24 Map and document the people and technology resources and processes required to recover all critical systems in a pre-defined sequence *(see tactical recommendation 1.3 in Section 4)*

The HSE should ensure that the Cyber Incident Response Playbook[322] documents a pathway to recovery that maps the people, processes and technology requirements of each system, to provide a pathway to recovery in the event of single or multiple system failure. During a major outage or disruption, recovery priorities should be agreed with central and local response and IT teams and communicated to all responders to streamline the recovery of integrated and independent systems. Once recovery priorities have been agreed, incident response mechanisms need to be invoked that provide the most effective communication and coordination between teams.

Central coordination meetings should be held with the asset and application register acting as a tool to guide recovery activities. A read-only, and regularly updated, list of prioritised applications should be made available to all technical recovery teams to direct their activities and keep them informed of the actions being undertaken across the response.

[320] Lessons Learned_ Programme Lessons v0.2

[321] Programme RAID Log

[322] Recommendation FA1: 4.1.1, Focus area 1- Technical investigation and response report

To achieve this an operational rhythm needs to be established by:

- Setting up a meeting cadence *at* and *between* each response level e.g., operational or "Bronze" (HG and CHO) meeting followed by a tactical or "Silver" (HSE) meeting, then a strategic or "Gold" (EMT) meeting to share a cascade of updates increasing in importance, escalating priorities.[323] This waterfall flow between the command levels should also be used in reverse to share decisions and actions simultaneously to all teams and impacted sites;
- Each meeting following a set agenda to ensure all required areas are covered off, particularly in terms of situational awareness of the Incident;
- Use of uniform templates for collecting incident updates, action tracking and required decisions.

It is recommended that at each level of response there is a dedicated role to ensure coordination within and between teams. This can be the role of a Crisis Coordinator or SITCEN Information Manager (see also *finding FA2.KF15).*

Focus area 2 conclusion

Despite a lack of pre-prepared structures and processes, the HSE exhibited an agile and reactive response to the Conti ransomware attack in May 2021. Prior learnings, behaviours and processes, many of which were exercised during the COVID-19 response, were leveraged to ensure critical systems and processes were recovered, and to deliver safety critical patient care across the country. The lengths to which staff and vendors went to keep patients safe and facilitate a recovery within the operating constraints is a direct reflection of the leadership that was employed during this crisis. The behaviours, structures and processes designed reactively during the response to the attack should be leveraged and embedded into new crisis structures, to ensure the HSE is better able to respond at pace to future risks when they materialise.

Individuals within the HSE have described it as an organisation constantly responding to crises. To date, the HSE's approach to preparedness for disruptive events has been driven through the Major Emergency Management Framework. Events previously in scope of the Framework can be categorised as short term, national events caused by adverse weather or accidents, which created a temporary surge in demand on the HSE's clinical and acute services. The normalisation of crisis events in the HSE has generated a sense of over confidence throughout the organisation, whereby the forward planning has become restricted to contingencies for predictable or recognisable threats and risks. Specifically, the HSE's crisis planning has been based on the assumption that all critical infrastructure and processes would be available to support a crisis response. There was therefore no contingency planning for a cyber attack, or any other scenario involving the denial or loss of infrastructure, people, or facilities.

Prior to the cyber attack, outside of the Major Emergency Management Framework, there was no integrated organisation-wide Crisis Management Framework in place to deal with a major *internal* crisis event. In the absence of documented plans, the HSE's COVID-19 response imparted a degree of inherent preparedness, which manifested itself in a flexible and agile response from all of its people across all levels. However, the structures required to respond to the crisis caused by the ransomware attack were only achieved with assistance from the Defence Forces in the weeks following the attack. The lack of pre-planned contingencies contributed to increased levels of stress and fatigue in HSE staff during the initial stages of the response and recovery. The HSE requires a Crisis Management Framework, which sits alongside the MEM Framework, but with a separate focus on responding to crises which do not necessitate an interagency response.

Clinical and services continuity has not been a corporate priority in the HSE until recently, when enterprise risk management and clinical and services continuity were consolidated under the National Director for Governance and Risk. Consequently the level of clinical and services continuity and crisis preparedness across the organisation varies significantly. Due to a historic lack of governance and oversight, a fragmented and incoherent clinical and services continuity capability has evolved across the organisation. This delayed the implementation of an initial coherent response and recovery effort during the Incident.

There are many learnings to be taken from any response to an incident this significant. The HSE must expand upon initiatives already taken and implement a coherent operational resilience capability, including clinical and services continuity and crisis management, across the organisation. Key actions for the HSE to take to establish organisation-wide preparedness to significant incidents and crises disrupting its operations include:

- Define the governance arrangements and structures to ensure clear and ongoing oversight,

[323] "Gold, Silver, Bronze" is industry standard phraseology to refer to strategic/tactical/operational level decision making bodies in emergency and crisis management

management, and reporting of the operational resilience disciplines, with a particular focus on implementation and integration of the crisis and clinical and services continuity disciplines;

- Establish the Crisis Management Framework, detailing levels of response and supporting teams and processes to manage any significant incident or disruption impacting HSE operations;
- Develop supporting crisis documentation, including strategic, tactical and operational plans, procedures, tools and templates; scenario specific playbooks for pre-defined threats and risks, supported by clearly defined clinical and services continuity strategies, a resourcing assessment and cost base analysis of chosen solutions;
- Cascade the Framework, tools and templates throughout the organisation, and to HGs and CHOs, to ensure a coherent and standardised response across all parties involved in a crisis response;
- Embed crisis management and clinical and services continuity across the organisation by establishing a formalised HSE-wide training and exercising programme and schedule to develop awareness, familiarity, and competence for all stakeholders involved in incident response.