Section 4.1 summarises from the detailed findings four strategic areas where transformational change is required, likely over a period of several years. Further details that underpin these can be found in Section 5.

Given the high risk exposure at present, we highlight in Section 4.2 some tactical recommendations for which immediate attention is required to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations.

Section 5 describes in detail a number of recommendations to address learnings that the HSE should take from the Incident, with a supporting key recommendation mapping in Appendix G.

4.1 Strategic recommendations

In order to deliver a significant and sustainable change in the exposure to cybersecurity risk, four areas of strategic focus are required across the HSE and other parties connected to the NHN:

- Governance of IT and cybersecurity;
- Leadership and transformation of the IT foundation on which provision of health services depends;
- Leadership and transformation of cybersecurity capability; and
- Development of clinical and services continuity and crisis management capability to encompass 'service-wide' events such as prolonged total outage of IT.

There are dependencies across these four areas and they need to be progressed in parallel. They are described in the strategic recommendations below, with further supporting recommendations provided in Section 5 of this report.

1. Implement an enhanced governance structure over IT and cybersecurity that will provide appropriate focus, attention and oversight.

1.1 Establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, share health data or access shared health services. Establish a 'code of connection' that sets minimum cybersecurity requirements for all parties and develop an assurance mechanism to ensure adherence.

One of the challenges faced by the HSE is that cybersecurity risk materialises as a 'common risk' to all organisations connected to the NHN given the interconnected nature of the IT systems. This has resulted from the direction of digital healthcare demanding greater interconnectivity, ability to share information and access to common services. Under the governance constructs of the health service, organisations have varying levels of autonomy over IT and cybersecurity decision making, yet the risk is shared - with organisations dependent on each other for cybersecurity. There is no 'code of connection' for all parties that connect to the NHN, share health data or use shared services in order to set a minimum baseline of security standards. The HSE's IT Security Policy was written in 2013, with the last update in 2014, and does not reflect the controls and capabilities required to manage cyber risk in 2021.

In order to manage the 'common risks' effectively, clarity is required over responsibilities and decision rights of all parties. In addition, the HSE must be able to set minimum standards for IT and cybersecurity, and ensure compliance to those standards by all organisations connected to the NHN. These minimum standards are required in order to ensure there is confidence in all organisations connected to the NHN that they are not themselves exposed due to inadequate cybersecurity controls in an organisation that they are connected to.

© 2021 PwC. All rights reserved.

1.2 Establish an executive level cybersecurity oversight committee to drive continuous assessment of cybersecurity risk and a cybersecurity transformation programme across the provision of health services.

The HSE has initiated a number of tactical improvements post the Incident to better secure systems as they have been recovered. However, this will not lead to the level of cyber risk reduction required to significantly and sustainably reduce the risk of further ransomware (or other) attacks.

Within the HSE, there is no dedicated executive oversight committee that provides direction and oversight to cybersecurity, both within the HSE and all organisations connected to the NHN. A known low level of cyber security maturity, including critical issues with cybersecurity capability, has persisted for years with little progress. An Information Security Project Board ceased operating in 2013.

A challenge faced in ensuring cybersecurity of health systems is balancing the need for ease-of-use, especially for clinical staff, with cybersecurity imperatives. For example, implementation of increased levels of cybersecurity controls such as ‘Multi Factor Authentication’ will have an impact on working procedures. It is therefore important that the cybersecurity oversight committee includes participation from user groups, so that culturally cybersecurity moves from being perceived as an IT challenge, to being perceived as ‘how we work’.

Finally, the cybersecurity oversight committee should be accountable for ensuring compliance with the evolving requirements of the EU NISD for essential services across the health service.

1.3 Establish an executive level oversight committee for IT.

With a fragmented set of decision rights over IT development and support across the provision of health services, a necessary enabler for driving transformational change will be the establishment of an executive level committee that can agree the priorities for IT development and investment, and align all interested parties behind a clear vision, strategy and plan.

This committee should be chaired by the Chief Technology & Transformation Officer (see Recommendation 2 below) and drive reporting on all aspects of IT hygiene (such as status of legacy systems) as well as progress in implementation of strategy. Critical to its success will be the participation of IT leaders from across the health service, in particular hospital groups, where a degree of autonomy over IT decisions remains. It will also be crucial in directing the evolution of an IT infrastructure and service provision that aligns with the objectives of Sláintecare, and establishment of appropriate levels of resourcing.

1.4 Establish a board committee (or repurpose an existing one) to oversee the transformation of IT and cybersecurity to deliver a future-fit, resilient technology base for provision of digitally-enabled health services, and ensure that IT and cybersecurity risks remain within a defined risk appetite. Consider the inclusion of further specialist non-executive members of the committee in order to provide additional expertise and insight to the committee.

Cybersecurity was recorded as a ‘High’ risk in the Corporate Risk Register in Q1 2019.[80] At the time of the Incident, the risk rating for cybersecurity on the Corporate Risk Register was 16, based on a likelihood scoring of 4 (likely, with a 75% probability) and an impact scoring of ‘Major’.[81] The HSE’s risk assessment tool is described in Appendix H.

Risks on the Register are subject to a quarterly review process and the quarterly reports are reviewed by the relevant Board Committee. The Performance and Delivery Committee of the Board reviewed the cyber risk with management in September 2020[82] and this was followed by a revised mitigation plan. The Committee includes two experienced IT leaders in large organisations, although they are not cybersecurity specialists. This revised mitigation plan had a number of actions due to be completed post the date of the Incident. The actions completed prior to the Incident did not materially impact the risk faced in this area.

The HSE’s IT-related risks had been presented at Board level on a number of occasions. However, the gravity of cybersecurity exposure was not fully articulated to the Board, given the HSE’s level of vulnerability to a cyber attack, or assessed against a defined risk appetite. Known issues with cybersecurity capability have made limited progress over the course of several years.

Other organisations with a critical cybersecurity exposure, and a need to drive significant technology transformation have found a dedicated committee of the board beneficial in order to raise the priority and focus to an appropriate level and ensure risks are appropriately communicated and understood.

[80] Q1, 2019 CRR COMBINED Document for April LT meeting.pdf

[81] CRR Q4 2020 Full Report post EMT meeting February 2021 v0.1 09 02 21.pdf

[82] Minutes-hse-performance-and-delivery-committee-18-september-2020.pdf

© 2021 PwC. All rights reserved.

Given the scale of change required across the provision of health services, it is recommended that a focused committee of the board is established, with relevant training provided. Consideration should be given to appointing additional individuals to that committee with specialist skills to act in a non-executive capacity and enhance the ability for the committee to support and oversee the IT and cybersecurity transformation. A key role for the committee will be to ensure that HSE requests for government funding (e.g. to DPER) to invest in addressing IT and cybersecurity issues are clearly articulated, and the risks associated with lack of investment are communicated and understood.

2. Establish a transformational Chief Technology & Transformation Officer (CTTO) and office to create a vision and architecture for a resilient and future-fit technology capability; to lead the delivery of the significant transformation programme that is required, and to build the increased function that will be necessary to execute such a scale of IT change.

The national health service is operating on a frail IT estate with an architecture that has evolved rather than be designed for resilience and security.

The NHN is primarily an unsegmented (or undivided) network, and can be described as a “flat” network, to make it easy for staff to access the IT applications they require. However, this design exposes the HSE to the risk of cyber attacks from other organisations connected to the NHN, as well as exposing other organisations to cyber attacks originating from the HSE - since once an attacker has a presence on the network they have ‘freedom to roam’. This network architecture, coupled with a complex and unmapped set of permissions for systems administrators to access systems across the NHN, enabled the Attacker to access a multitude of systems across many organisations connected to the NHN and create the large-scale impact that they did.

Part of the frailty of the IT estate is an over-reliance on legacy systems. [redacted] The HSE also has over 30,000 outdated Windows 7 legacy systems running on workstations. One reason cited for the continued proliferation of Windows 7 systems is that a key shared service for handling medical imaging, NIMIS, is not supported by the manufacturer to function on more modern Windows desktops without being upgraded. The upgrade has not been rolled out, despite Windows 7 being deemed ‘end-of-life’ by Microsoft in January 2020, with many organisations upgrading to Windows 10 several years prior to that. Some hospitals have implemented an unofficial workaround to enable NIMIS to operate on Windows 10 machines, with potential implications on the support and warranty arrangements for their use of the application, and work to minimise the dependency on Windows 7 is continuing.

The parts of the health service that were arguably best-equipped to maintain clinical services in the face of prolonged IT outages were those that rely on paper records for patient services. Whilst this was a positive feature in managing the Incident, it highlights the extent to which modernisation is required across the health service to enable the adoption of digital health services. The relative disadvantage in this Incident for organisations who are more dependent on technology services illustrates the critical need for resiliency to be built into the IT architecture and systems to foster the confidence required to enable future migration to more digital provision of health services.

Reducing cybersecurity risk requires both a transformation in cybersecurity capability (see recommendation 3) and IT transformation, to address the issues of a legacy IT estate and build cybersecurity and resilience into the IT architecture.

2.1 Appoint a permanent Chief Technology & Transformation Officer with the mandate and authority to develop and execute a multi-year technology transformation, build an appropriate level of IT resource for an organisation the scale of the HSE and oversee the running of technology services.

The HSE has operated since the end of 2018 with an interim Chief Information Officer with a limited practical mandate, authority and resource to effect change across all organisations connected to the NHN. The level of resourcing in critical IT functions is significantly lower than we would expect for an organisation with the size of IT estate that the HSE has; the IT organisation consists of approximately 350 FTE, serving a population of over 70,000 end-user devices. This observation has been consistently made in interviews, both within the HSE and from external parties who interfaced with them during the Incident, and was a known issue within HSE prior to the Attack with an additional 300 FTE approved for recruitment shortly before the Incident.

The lack of investment in IT resources over a sustained period of time has clearly limited the ability of the HSE to drive modernisation and maintain

© 2021 PwC. All rights reserved.

the IT estate to be resilient and secure. In addition, the scarce resource in critical IT functions resulted in significant key-person dependencies during the Incident management and recovery, which was undoubtedly a contributing factor to the extended length of the recovery process.

In interviews with hospitals and other providers, it was observed that this incident has highlighted the need to build greater IT resource within many of those organisations, as well as at HSE centre, including representation on leadership committees. The CTTO should develop a resourcing plan for the whole health service that will be sufficient to deliver a transformational strategy, and maintain a resilient and secure IT estate.

The CTTO should assume responsibility for all capabilities that currently sit within the OoCIO, as well as a broadened capability to drive rapid transformation. The CTTO should be a member of the EMT reporting to the CEO.

The ransomware incident has served to highlight the extent to which the provision of health services is dependent on an effective and resilient IT capability. The opportunity needs to be seized to reflect this increased understanding of the criticality of IT with a repositioning of leadership, funding and level of resource.

2.2 Under the office of the CTTO, develop an IT strategy to achieve a secure, resilient and future-fit IT architecture, required for the scale of the HSE organisation.

In order to deliver the transformation required to the technology foundation of the health service in Ireland, a clear strategy is required that can be used to secure commitment to execution across all organisations involved in the provision of health services, and the significant funding that will be required over many years.

The HSE has had a plan for the development of IT that has been used to secure funding for individual projects. However it has not been tied to a vision, strategy and architecture that is deliverable over a period of years and that provides the necessary level of resilience through investment in enabling IT architecture and fallback solutions in the event of core technology failure. Many interviewees expressed frustration with an apparent approach of investing in ‘new projects’ or ‘new features’ rather than the holistic delivery and maintenance of a technology foundation for health service provision.

The development of the IT strategy and target architecture also needs to explicitly address the architecture for deployment of medical devices. Whilst not in scope for this review, it is apparent that reliance is placed on medical device manufacturers to specify how they should be deployed within the overall IT architecture, with no HSE-mandated approach to ensuring they could not be impacted by a cyber attack.

A key requirement for the IT transformation plan that will be critical to the ability to recover from a similar incident in the future will be clear alignment between critical clinical services and the IT applications and infrastructure they depend on. The recovery activities following the ransomware incident would have benefited greatly from such a view, and speed of decision-making and recovery increased.

3. Appoint a Chief Information Security Officer (CISO) and establish a suitably resourced and skilled cybersecurity function. Develop and drive the implementation of a cybersecurity transformation programme.

The HSE has a very low level of cybersecurity maturity (Section 5.3 of this report gives an evaluation of maturity against the industry standard ‘NIST’ cybersecurity framework). Examples of the lack of cybersecurity controls in place at the time of the Incident include:

- The IT environment did not have many of the cybersecurity controls that are most effective at detecting and preventing human-operated ransomware attacks;
- There was no security monitoring capability that was able to effectively detect, investigate and respond to security alerts across HSE’s IT environment or the wider NHN;
- There was a lack of comprehensive effective patching (updates, bug fixes etc.) across the IT estate of all organisations connected to the NHN; and
- Reliance was placed on a single antivirus product that was not monitored or effectively maintained with updates across the estate. For example, the workstation on which the Attacker gained their initial foothold did not have antivirus signatures updated for over a year.

The low level of cybersecurity maturity, combined with the frailty of the IT estate, enabled the Attacker in this incident to achieve their objectives with relative ease. The Attacker was able to use well-known and simple attack techniques to move around the NHN,

© 2021 PwC. All rights reserved.

extract data and deploy ransomware software over large parts of the estate, without detection.

3.1 Appoint a CISO and establish a suitably resourced and skilled cybersecurity function.

The HSE has not had a single responsible owner for cybersecurity at either senior executive or management level, responsible for cybersecurity leadership and direction. This is highly unusual for an organisation of the HSE's size and complexity with reliance on technology for delivering critical operations and handling large amounts of sensitive data. As a consequence, there was no senior cybersecurity specialist able to ensure recognition of the risks that the organisation faced due to its cybersecurity posture and the growing threat environment.

The HSE lacked a detailed and holistic cybersecurity strategy, operating model and transformation plan that outlined the strategic, tactical and operational activities required to mitigate known weaknesses and reduce cyber risk exposure.

The CISO should be at National Director level, a direct report to the CTTO, and have appropriate access to the EMT and their agenda, to ensure that cybersecurity risks are understood and considered in all decision-making. They should be responsible for cybersecurity operations as well as driving strategic and tactical actions to transform cybersecurity capability, and providing updates to the Board. Whilst recruitment of a permanent CISO may take some time, appointment of an interim CISO should be considered in the short term.

The HSE also only had circa 15 FTE in cybersecurity roles, and they did not possess the expertise and experience to perform the tasks expected of them. For example, alerts were generated by antivirus software on key systems in the days leading up to the attack, which were passed to the cybersecurity team. However, there was insufficient expertise, and a lack of expertly-designed triaging processes to appreciate the significance of the alerts and take appropriately urgent action to prevent the attack resulting in significant disruption to systems. As a result, opportunities to prevent the crisis were missed.

A critical requirement for the HSE to begin to develop the ability to prevent and detect a similar incident in the future is the appointment of senior cybersecurity leadership and the development of a suitably skilled and resourced cybersecurity function. These skilled resources are currently scarce and the HSE may need to consider co-sourcing arrangements to support requirements in this area.

3.2 Develop and drive the execution of a multi-year cybersecurity transformation programme to deliver an acceptable level of cybersecurity capability for a national health service.

It is apparent that significant capability and controls need to be built and implemented across HSE and other organisations involved in the provision of health services, in order to achieve even a basic level of protection against cyber attacks. This will need to dovetail with the transformation of IT, but also extend beyond IT into 'the way people work' (see recommendation 1.2 above).

There will therefore need to be a multi-year programme to transform cybersecurity capability in a holistic way to ensure that the provision of health services in Ireland, and the data that those health services handle, becomes less vulnerable to cyber attacks. Further detail as to a suggested structure of the programme is given in Section 5.

4. Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk and enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

4.1 Implement a clinical and services continuity transformation programme reporting to the National Director for Governance and Risk. Establish an Operational Resilience Policy and Resilience Steering Committee to drive integration between resilience-related disciplines, and an overarching approach to resilience.

The HSE and associated organisations such as hospitals, CHOs, and GPs have dealt with a number of crises over recent years that have required development of clinical and services continuity plans and the 'muscle memory' that comes from repeatedly managing incidents. Indeed one voluntary hospital described the short-term outage of certain local IT systems as a regular occurrence that their Business-As-Usual processes were designed to accommodate.

It is apparent that much of the planning for clinical and services continuity (a more appropriate name for the 'business continuity' discipline in the HSE) has occurred at local level, for specific organisations, and there has not been a programme to ensure consistency of clinical and services continuity planning across all health service organisations and the HSE centre itself, and cross-sharing of leading thinking.

© 2021 PwC. All rights reserved.

In addition, as is the case with many other organisations, the scenario of sustained loss of IT across the entire health service has not been planned for, with specific considerations and playbooks. As a result, both within organisations and at the HSE centre, great efforts were required 'in the moment' to manage the impacts of the ransomware attack on clinical services, implement workarounds and manage patient risk. The success of these efforts was significantly due to the personal commitment, energy and ingenuity of individuals across all organisations, with no plans or playbooks for such an event that could be relied upon.

A particular challenge faced during the recovery process was the identification and prioritisation of critical systems for recovery. Processes were rapidly developed during the days and weeks following the Incident, to identify the most critical health services for recovery and to map them back to IT systems and infrastructure. However, the understanding and map of the dependencies between specific clinical services and IT systems had not been developed prior to the Incident. Development of this dependency map is a critical requirement for clinical and services continuity planning for future similar events.

During the recovery process in the days following the ransomware attack it became apparent that disaster recovery (DR) arrangements for IT systems were ad hoc and inconsistent. With the Attacker able to corrupt some primary data stores for disaster recovery, there was a requirement to identify secondary stores and attempt to recover from them. A workstream was initiated to attempt to locate them and test the viability of recovery. Were systems to have been recovered using this method, they would have been recovered to different points in time that backups were available for, and there was no confidence in the completeness (or in some cases tested viability) of recovery solutions. As a result, when the decryption key became available from the Attacker, the decision was made to abandon work to recover from backups, and instead recover systems from their production environment, using the decryption capability provided by the Attacker. It cannot be confidently asserted that all health services would have been able to recover in a timely manner (or even at all) without the provision of the decryption key by the Attacker.

The HSE has recognised that clinical and services continuity as a risk discipline has not developed at the pace needed with executive oversight and focus. A National Director for Governance and Risk (equivalent to a Chief Risk Officer) has been appointed, and assigned responsibility for establishing a clinical and services continuity framework, through which risk management and 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. A programme and resource is required to develop the consistency and breadth of planning across the health service, including establishing clear requirements for disaster recovery capability to be implemented by the IT transformation programme, and the mapping of clinical processes to IT systems and data.

In addition, the HSE should establish an Operational Resilience Policy and Steering Committee to drive integration between resilience-related disciplines across the organisation, such as incident management, crisis management, clinical and services continuity and enterprise risk management plus disciplines that can impact on resilience such as cybersecurity and physical security.

4.2 Enhance crisis management capabilities to encompass events such as wide-impact cyber attacks or large-scale loss of IT.

It is indisputable that the HSE has extensive experience in managing crises, for example in the critical role it has fulfilled for the nation in navigating the COVID-19 crisis. This has resulted in some effective mechanisms for crisis management not just being designed, but regularly used. In addition, significant effort has been expended in planning for large-scale external events that the health service will be required to manage such as a plane crash or security incident in a city. Mechanisms that have been developed from previous crises served well in managing this crisis - of particular note was the effectiveness of communications out to the general public and media.

However, the nature of the crisis resulting from the ransomware attack was different, and required elements of capability that have not previously been required. For example: communicating with all staff in the health service without internal emails or other IT collaboration tools; establishing a wide variety of communication channels and forums to gather information and feedback to prioritise recovery of systems, and issuing clear guidance to all parties impacted by the Incident that was relevant to their localised situation. Even establishing a coherent set of facts from which to build communications to the public proved to be challenging, as is typical in a ransomware recovery situation.

The establishment of a crisis management centre and working group, initially in a third party organisation's offices and subsequently in City West, were examples of crisis management structures that had to be developed 'in-the-moment' rather than

© 2021 PwC. All rights reserved.

being pre-planned. Support from the Defence Forces and other parties enabled an effective structure and set of information flows to be developed rapidly, but this evolved over several days and critical time was lost in the recovery process as a result.

The nature of a ransomware attack, resulting in effectively total loss of IT, makes it particularly challenging to manage with a unique set of issues to be navigated. Investment is required in crisis management planning, resourcing tools and processes in the HSE and associated organisations in order to be prepared to manage this kind of crisis in the future.

4.2 Immediate tactical actions

As highlighted above, there is a requirement for a transformational body of work over several years to make strategic changes to the governance, leadership and capability across IT, cybersecurity, clinical and services continuity and crisis management. Given the high risk exposure at present, we highlight in this section some tactical recommendations for which immediate attention is required to achieve urgent impact and to contribute to the development and implementation of the strategic recommendations. Further information on these, and other recommendations, is given in Section 5.

1. Response to the Incident

1.1 Complete the ongoing work being performed by the Legal and Data workstream and continue to work closely with the Data Protection Commissioner (DPC).

The HSE established a Legal and Data workstream to support the work of their Data Protection Officer (DPO) in coordinating the HSE's data protection investigation, engagement with An Garda Síochána, and subsequent reporting to the DPC.

Through forensic analysis of systems, and review of data sets, this workstream will need, to the extent possible, undertake the following actions:

- Assess the likelihood that the attacker took a copy of data from systems on the NHN;
- Assess the content of data sets at risk for personal data;
- Assess whether any potential breaches meet the threshold to be reported to the DPC;
- Determine the course of action to be taken, such as, informing data subjects and referring identified potential data breaches to other organisations.

The DPO should continue to work closely and maintain regular dialogue with the DPC until the conclusion of the HSE's data protection investigation (see key recommendation FA2.KR20 in section 5.2).

1.2 Continue to reconcile medical data stored and managed through interim processes post the ransomware attack and place centralised governance over these activities.

As the HSE has moved out of the 'crisis phase' of responding to the ransomware attack, it should put in place sustainable governance to manage and resolve the risks and issues originating from the Incident to HSE's data (see FA2. KR22.2 in section 5.2).

During the Incident, workarounds were implemented across the HSE, Hospital Groups/hospitals and CHOs to allow clinical services to continue operating. This often resulted in teams reverting back to paper-based records. There are multiple ongoing efforts to reconcile these paper based records with the data in recovered clinical applications. Until this is complete there is a risk
that clinical services are impacted by patients not having up-to-date medical records in the appropriate systems.

Members of staff used personal email accounts and devices for information sharing and communication. The HSE issued a communication in August 2021 to stand down the use of personal emails and ensure all data was deleted from local storage areas. However, some stakeholders from hospitals and CHOs reported they have not received clear guidance on the steps required to address this risk.

The HSE should establish centralised governance over these activities. This should initiate a review of the scope of work required to resolve these risks and issues, provide the necessary resources to prioritise this work and track it through to completion, across all HGs/hospitals and CHOs.

1.3 Collate and manage artefacts created in response to the Incident, including initial production of an asset register.

The HSE should collect, organise and document artefacts created as part of the response and recovery to the ransomware cyber attack.

The HSE was able to gather a significant amount of information during the response to the Incident,

© 2021 PwC. All rights reserved.

for example key information about the technology underpinning the clinical applications that were being used across the HSE, hospitals and CHOs. In addition, response processes and plans were developed that would be invaluable in the event of a similar attack in future.

These documents will provide a foundation for developing an up-to-date asset and application register, as well as plans that will assist in the response to future incidents (see key recommendation FA1.KR11 in section 5.1 for further detail).

1.4 Appoint an interim senior leader for cybersecurity (a CISO) to be responsible for driving forward tactical cybersecurity improvements, managing third-parties that provide cybersecurity services and leading the cybersecurity response to cyber incidents.

The HSE should appoint an interim senior leader for cybersecurity (a CISO) who has experience in rapidly reducing the vulnerability of organisations to threats, and designing cyber security transformation programmes (see key recommendation FA1.KR1 in section 5.1).

This role should be responsible for placing governance around cybersecurity improvements (see immediate tactical action 1.5), identifying a sustainable medium-term managed detection and response solution (see immediate tactical action 2.1), and leading the cybersecurity response to cyber incidents. The role should also be responsible for developing processes to manage third-parties that provide security services, and providing the expertise to oversee the successful delivery of these.

1.5 Formalise a programme and governance to respond to tactical recommendations arising from the Incident Response investigation and provide assurance over their implementation.

The HSE should mobilise a tactical cybersecurity improvement programme, with governance that feeds into the interim CISO (see immediate tactical action 1.4) and can provide updates on the programme's progress into the Board committee. Dedicated resources should be used to deliver this programme.

The programme should be structured around tactical work packages that can be delivered at pace using focused governance and reporting to drive accountability. The programme should also include a process to triage all third party recommendations, and fixes to security control gaps identified internally, into tactical or strategic activities.

HSE should also bring the governance of ongoing tactical IT and cybersecurity improvement projects, that have been initiated following recommendations from the retained Incident Response provider under the tactical cybersecurity improvement programme (see key recommendation FA1.KR7 and KR8 in section 5.1).

2. Security monitoring

2.1 Ensure that the HSE's Incident Response provider's managed defence service or an equivalent is maintained to detect and respond to incidents on endpoints (i.e. laptops, desktops, servers etc.) to provide protection to the entirety of the NHN.

The HSE has engaged their Incident Response provider to continue providing a managed detection and response service. This capability is the most crucial defence HSE has against further ransomware attacks at present, providing a valuable 'safety net' given the inherent weaknesses in cyber security controls across the estate (see key recommendation FA1.KR6 in section 5.1).

The HSE should identify a sustainable plan to ensure the HSE's Incident Response provider service or an equivalent service is continued across all organisations connected to the NHN. Whether through formalising the continuation of the current service, or replacing in parts of the NHN with a new service, the objective should be to ensure that equivalent levels of service are maintained, including: using Endpoint Detection and Response tooling to detect malicious activity on endpoints; 24/7 monitoring; and triage and investigation of security alerts.

2.2 Establish an initial cybersecurity incident monitoring and response capability to drive immediate improvement to the ability to detect and respond to cybersecurity events.

The HSE should drive immediate improvement to the ability to detect and respond to cybersecurity events, by augmenting the existing security operations function with additional team members with experience and expertise in cybersecurity monitoring and response. This augmented team should document, establish and operate an initial process to triage, investigate, contain and respond to cybersecurity events (see key recommendation FA1. KR11 a in section 5.1).

© 2021 PwC. All rights reserved.

3. Ability to respond to a similar incident in the near future

3.1 Review the process for managing internal crisis communications including resources.

The HSE should formalise and document the process required to manage internal communications during a crisis response similar to that required in the Incident, including cascading call trees and audience segmentation via secure 'out of band' notification and communication platforms (see key recommendation FA2.KR19 in section 5.2).

The HSE should assess the requirements of their internal communications process and plan for a crisis response similar to that required in the Incident and allocate adequate resources to grow the Internal Communications team (see key recommendation FA2.KR6 in section 5.2).

3.2 Develop a plan for response and management of an NHN-wide similar incident taking recent learnings into account.

The HSE should develop, document and exercise a plan for managing and coordinating a cybersecurity incident involving multiple organisations connected to the NHN. This plan should be invoked by any organisations connected to the NHN if they detected a security incident that may have wider implications.

The HSE IT and security teams should identify documents required to respond to a ransomware attack (e.g. network diagrams, asset list) and secure these in a cloud repository (see key recommendation FA1.KR11 f in section 5.1).

3.3 Establish retainers with appropriate SLAs for third party incident and crisis management response support, together with processes and sufficient internal expertise to direct and manage the third-parties.

The HSE should ensure it has a fit-for-purpose set of capabilities under retained contract with external providers to enable a more effective response to an incident similar to the Incident in the near future. This should include support for operation of crisis management functions, legal support and cybersecurity incident response services (see FA2.KR13 in section 5.2).

The HSE should also ensure that they have developed the processes to effectively manage these retained third-parties in the event of an incident, and that they have sufficient expertise to provide challenge and understand the implications of what the third-parties are reporting to them (see immediate tactical recommendation 1.4).

The HSE should work with the retained cybersecurity incident response provider to ensure they have sufficient understanding of the HSE's organisation and technology, and be available within defined service level agreements to assist the HSE respond to security alerts (see key recommendation FA1.KR11 f in section 5.1).

4. IT environment

4.1 Implement an upgrade to NIMIS to allow Windows 10 upgrade, thereby addressing known vulnerabilities and support issues associated with current wide deployment of Windows 7.

The HSE should prioritise the remediation of critical legacy systems. Immediate efforts should focus on prioritising the upgrade of the NIMIS system, as this is currently inhibiting the upgrade of a significant proportion of 30,000 Windows workstations from Windows 7 to Windows 10.

In considering the acceleration of the NIMIS upgrade, HSE should review if the configuration changes made in one hospital (Hospital A) to enable the application to run on Windows 10 can be more widely implemented, and supported by the vendor, to expedite the central Windows 10 rollout plans (see key recommendation FA1.KR11 g in section 5.1).

4.2 Formalise existing roles and responsibilities for IT across the entities accessing the NHN and establish SLAs for centrally-provided services, while also ensuring information security policies align with those responsibilities.

The HSE should establish clear responsibilities for IT and cybersecurity across all parties that connect to the NHN, or share health data, or access shared health services. This formalisation of responsibilities should include specification of Service Level Agreements (SLAs) for centrally-provided services, including availability requirements.

The HSE should define a code of connection that defines the minimum acceptable level of security controls necessary to connect into the NHN, to be agreed by all parties connected to the NHN, including requirements for central reporting of cybersecurity alerts and incidents. The HSE should establish a programme to monitor and enforce ongoing compliance with this code of conduct. Compliance with the code of connection should become part of the onboarding process of any connecting organisation (see key recommendation FA1.KR11 e in section 5.1).

© 2021 PwC. All rights reserved.