The Health and Care Cybersecurity Challenge

Mitigating the Risk with Cisco

Important Notice

“The guidance provided in this report is of a generic nature and cannot be specific to your organisation or operations. Please contact your Cisco partner or Account Manager to discuss your specific requirements. The guidance is provided in good faith based upon reference materials sourced from the NHS, Department of Health and other Healthcare organisations up to the date of publication. Errors and omissions are excepted. No warranty is given or implied.”

Contents

1. Introduction and Purpose

A more connected world offers many benefits but also introduces new threats, as organisational boundaries blur and exploits become more sophisticated but also easier to use. This change in the threat domain is a constant challenge for all organisations, including those operating in health and care, and the increasing prevalence of new threats such as ransomware, demonstrates that attackers are adapting at a faster pace and organisations are struggling to respond.

And as we enter the next generation of the Internet, a new wave of connected devices and 'things' open up that threat landscape even further. The Internet of Things (IoT) will see billions of elements becoming connected, from trees to cars and buildings, introducing new 'back doors' which must be considered as much a part of the security domain as any IT system.

The 2017 'Wannacry' event brought cybersecurity into the public domain. UK health and care organisations were however, already challenged by the security implications of moving towards health and social care integration, regional business models and more fluid organisational boundaries caused by growing demand for mobile access to information.

Contents

The 2016 National Data Guardian (NDG) 'Review of Data Security, Consent and Opt-Outs' called for tougher penalties and better controls of data and information. Its recommendations included a modernised Information Governance Toolkit (ITK), improved cybersecurity controls, data protection enhancements and harsher penalties for malicious data breaches.

More recently, NHS England's guidance, partly in response to 'Wannacry', included 22 security recommendations, while the 'Lessons Learned Review' discusses aspects ranging from development of local action plans, executive leadership, skills and awareness to contingency planning. The profile of cybersecurity in particular was heightened even further when the Care Quality Commission announced plans to include it in their assessment framework, to include validation that the various data security standards are being met. This new strategy coincided with significant investment to strengthen capabilities centrally through HSCN (Health and Social Care Network) together with funding initiatives for NHS organisations. Local Authorities meanwhile, are to undergo audits to assess their cybersecurity posture with the promise of funding to follow.

Inevitably, there are many considerations for any organisation involved in the delivery of health and care services, including:

- The fact that organisations are delivering public facing services
- The stakeholder landscape is ever-expanding
- Many legacy systems remain in place.

So where should you begin?

Cisco is one of the largest enterprise class cybersecurity companies in the world. Our solutions work together systematically to identify, prevent and remediate cyber threats. In this document we discuss these challenges in more detail and describe how an architectural approach and systematic design offers the best mitigation.

Contents

2. Components for a Secure Platform

Developing a secure platform should not be seen solely as a technology problem.

It requires the understanding and management of a wide range of domains. Effective security transcends the entire spectrum of people, policy, process and technology. If these aspects are not considered in combination, unnecessary complexity and gaps in coverage emerge, increasing risk.

Security should also be considered across its entire lifecycle.

It is not a 'point in time' problem, but one that varies over time depending on a wide variety of factors. Security requires constant review and adjustment and cannot simply be ticked off as part of an annual compliance exercise.

It is therefore important that cybersecurity thinking starts at the top of the organisation, setting the strategy, direction and culture needed to support critical business outcomes.
Once set, the technology elements can be identified and built as an end-to-end integrated system, mitigating the risks and enabling the business to deliver against its objectives.

"Security is not a 'point in time' problem"

2.1 People and Process

A common theme running through all of these recommendations is the need for cyber to be embraced by senior NHS leadership. Indeed, a key recommendation within the 'Lessons Learned Review' is for the appointment of a board level individual to act as the data security lead, together with regular board reviews of cybersecurity risks and associated counter measures. This level of ownership raises the profile of cybersecurity and awareness of the implications as it:

- Identifies the impact that a cyber incident can have on a health and care organisation's operations.
- Removes the long established misunderstanding that cybersecurity is just a technology problem.
- Changes culture, embedding the idea that cyber is not just the responsibility of the IT organisation, but that each member of staff has a responsibility and role to play. Rather than seeing users be as the 'weakest' link in the security chain, they should be seen as any organisation's first line of defence and a powerful asset in the event of a security incident.
- Places focus on the most critical risks, identifying and protecting that which matters the most. This relationship must be two-way; while senior leaders set the priorities, it is the responsibility of the technical leaders to articulate security risk and impact in clear business language.
- Ensures that the right skills and awareness exist across an organisation. Improving cyber skills is not about all staff members becoming experts, but about giving them a solid appreciation of the impact that their actions can have on the wider organisation -and where they should go if they suspect a breach or other cyber incident has occurred.

Contents

2.1 People and Process (Continued)

On this point, it is important to note that improving skills is not a panacea. Staff will continue to make mistakes – links will be clicked on, controls will be worked around and unsanctioned applications will be utilised. In fact, the National Data Guardian review clearly highlights that many security breaches in the health and care sector are the result of accidental or well-intentioned actions of staff simply trying to do their job.

With this in mind, security should not come at the cost of usability. It is a common anecdote among clinical staff that the vast numbers of different systems they have to use can result in staff writing passwords down or leaving systems logged in. This is just one example of where poor implementation of a security control has a significant impact on user workflow and consequently, introduces unnecessary risk to the organisation.

The WannaCry outbreak was something of a wake-up call – not just for the NHS but for other public sector organisations. Another consideration should be to ensure new policy and capability is consistent across the health and social care continuum to an STP (Sustainability and Transformation Partnership) or ICS (Integrated Care System) level as a minimum.WannaCry has in fact become a positive catalyst, underlining the need for organisations to not only focus on building defensive security capabilities – an approach that has dominated the security domain for many years – but to also think about what happens when their defences fail.

The health and care environment is no stranger to dealing with crises and is therefore ideally placed to apply the necessary rigour in developing robust incident response plans and importantly, testing these to ensure that deliver the necessary business continuity when needed.

Contents

2.2 Technology Domains

As identified above, security should not be confined to a technological set of considerations and corresponding solutions. However, it is also clear that technology has an important role to play in supporting business objectives and outcomes.

The National Data Guardian Review and DH 'Lessons Learned Review' touch only lightly on technology, mainly in relation to legacy systems, a major area of vulnerability for the NHS and many other organisations. Addressing this issue may initially appear to be a simple case of patching and renewing obsolete or unsupported applications. However, the reality is far more complex:

- Cost – investment in IT must always be balanced against the wider needs of the health and care system; maintaining the most up to date systems isn't always possible when budgets are constrained.
- Embedded Systems – some legacy systems in the health and care sector are embedded as a component in a larger business or clinical system, which can make patching and updating impossible.
- Patching immediately isn't always possible – keeping all systems patched and up-to-date is a mammoth undertaking and even with the best processes in place, there are many reasons why some systems can remain out of date, including:

1. lack of ability to patch
2. difficulties securing a change window to take a system down
3. staff members being on holiday during a patch cycle.

Whilst reducing the number of legacy systems will have an associated impact on the level of vulnerability, it cannot be focussed on in isolation. Strategies need to be developed to identify and address systems where for the reasons outlined before, updating and patching isn't possible.

Alongside legacy systems is an increasing challenge associated with connected medical devices. The NHS is no stranger to the recent IoT revolution; in fact, it could be argued that the NHS was an adopter of connected devices well before the term IoT was even coined. What has changed is the volume and type of devices that are being connected to the network. In the past, connected devices were large, static clinical diagnostic equipment such as MRI or CT scanners. Today, the range is far more diverse and mobile, requiring a fundamentally different approach to addressing the risks associated with these devices. These can be broken down in to two main areas:

- Risk to the device from the network – protecting the device from malware infection or other misuse that could have a range of impacts from simple loss of service through to manipulation of data
- Risks to the environment from the device – The rapid development of new and innovative connected medical devices is delivering real clinical benefits but the developers of these devices aren't always putting security at the heart of their design and development process. Security lessons learnt in the desktop operating system space over many decades (such as implementing security development standards, patching and software lifecycle management) must be re-learnt by an entirely new set of vendors.

Contents

2.2 Technology Domains (Continued)

One way in which these risks can be addressed are through the use of intelligent, dynamic network segmentation. This mechanism will help to reduce the access both to and from these devices and through linking such a system to the right threat detection capability can also be used to quarantine devices rapidly if unusual patterns of activity are detected.

Operational security capability

Another important consideration – and one that is intrinsically linked to some of the recommendations from the National Data Guardian and 'Lessons Learned Review – is the approach taken to building an operational security capability. That is to say, how they collect, normalise and take action on security related events generated by the various security infrastructure components. This organisational capability feeds directly into improving the ability to rapidly respond to security incidents, since it represents the core capability needed to understand:

- where a threat is coming from
- how it might be propagating
- directing where action can be taken to quarantine and remediate affected systems.

Building an operational capability requires investment not only in technology, but in people able to analyse, interpret and respond in the face of an incident. One approach that could be taken to building this capability is to address the operational need at a regional or STP level.

Pooling resources into a shared security operations facility that supports a much wider set of organisations not only achieves economies of scale but also helps to reduce the burden of finding and retaining sufficiently skilled resources.

Other challenges in the technology domain also need to be considered:

- Continued availability of infrastructure equipment
- Rapid identification and remediation of malware
- The built environment, e.g. building management systems and access control systems
- Mobile and remote connectivity out into the community and potentially into the home
- Partnering with, and connecting to, other organisations and agencies.

These concerns drive a need for a variety of protections such as control plane protection, rate limiting, posturing and microsegmentation. The key is to:

- Consider as many use cases as possible
- Understand the risk
- Build a portfolio of potentially reusable capability.

For example, building in microsegmentation capability would help mitigate risks associated with both connected medical devices and third party building management systems.

Section 3 expands on this principle, outlining how security should operate as a system, while in section 4 we go on to show how Cisco solutions can provide these required capabilities.

Contents

3. An Architectural Approach to Security

Taking an architectural approach means treating security as an end-to-end system, rather than a distinct set of individual components. The overall security system should be easier to manage. At the same time it should be capable of sharing vital contextual and threat information for a more responsive and effective outcome.

Such an approach should adopt the following guiding principles:

- A policy shift that considers security to be an enabler;
- Organisations must accept that it is no longer a case of if but when a security breach occurs;
- Security controls must transcend the traditional 'block' approach and instead focus on improving detection and remediation times;
- Security should be developed as a system; distinct components should not operate in isolation but should instead integrate to provide more accurate threat detection and reduce management complexity.

An architectural approach is fundamentally driven by the needs of the business. By first identifying the information assets and systems that support the business, an assessment can be performed to determine the relative impact in the event of a compromise.

Compromise in this sense should be considered across all three aspects of information security, i.e. confidentiality, integrity and availability. This is an important shift, given that all too often, emphasis is placed on loss of confidentiality, when in fact a loss in availability or integrity can have a far greater impact, particularly in a clinical setting.

Once the assets are understood and the impacts analysed, it is then important to consider the threat. We have identified a number of areas for consideration above, but also recommend close inspection of the National Data Guardian and Lessons Learned reviews with equal focus on both internal and external threats.

As with any architectural approach, understanding the business context helps identify the capabilities that the technology needs to deliver, which in turn improves user experience. Security should therefore be considered systematically, moving away from point solutions that plug holes as they appear. Security controls then become transparent to the end-user and prevent the need to bypass a control due to its impact on their workflow.

A further benefit of developing a business-focussed security architecture is that it helps develop control traceability. That is to say, a clear justification can be built to ensure controls effectively address real business risk and gaps in coverage are clearly understood. This level of traceability also helps with developing metrics around security performance – a subject which often proves difficult, especially when trying to translate the meaning of technical metrics such as the number of blocked pieces of malware into business metrics and performance indicators.

In summary, an architectural approach to security fundamentally shifts the perception from being a 'cost centre' or an 'insurance policy', to a more integrated set of capabilities that support tangible business outcomes.

Contents

4. Mitigating the Risk - Solutions from Cisco

Having considered the threat domain for health and care organisations and the recommended architectural approach, we now look at Cisco's solutions and how they operate systematically in order to provide the best possible protections.

4.1 Threat Intelligence

Attackers have unlimited attempts and resources, so defenders must win each and every time. To combat these threats, security needs to go beyond tracking and detection to push the boundaries of today's security technologies and work against tomorrow's exploits.

The Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world. Comprised of world-class researchers, analysts and engineers, these teams are supported by unrivalled telemetry and sophisticated systems to create accurate, rapid and actionable threat intelligence for Cisco customers, products and services. Talos defends Cisco customers against known and emerging threats through the development of new threat detection engines, and by providing continual updates directly to Cisco products. In addition to providing protection, this vast intelligence data set can also be used to enrich incident investigations through the use of Cisco ThreatGrid, Umbrella Investigate and AMP Visibility.

The Cisco security ecosystem covers email, networks, cloud, web, endpoints and everything in between. Talos therefore benefits from more visibility than any other security vendor, through the sheer size and breadth of Cisco's security portfolio and the incoming telemetry from customers and products. This unique visibility delivers greater context from many data points during an incident or campaign. This, along with other resources such as open-source communities and internal vulnerability discovery, enables Talos to move faster and create more comprehensive assessments of ongoing threats.

"Attackers have unlimited attempts and resources, so defenders have to win each and every time."

Contents

4.2 Network Visibility and Segmentation

Recent years have seen a dramatic increase in the number of devices connected to the network, including handheld or mobile devices and medical devices. Combined with the increasing complexity of network design, it is increasingly difficult to understand what is happening on a network at any given time and identify potential threats.

Cisco's Network Visibility and Segmentation solution set comprises three component parts that work together support threat detection, secure access and software-defined segmentation capabilities.

- Working with well-known network flow collection protocols, Cisco Stealthwatch uses your existing network to gain visibility and understand what is happening on the network. It also uses machine learning and behavioural analytics to understand malicious patterns of activity and can also apply this detection to encrypted traffic flows without the need for decryption.
- Cisco identity Services Engine (ISE) provides access control policy using the details of users and devices across wired, wireless and virtual networks. This includes the ability to recognise a large number of medical devices and assign access policy accordingly with our Medical NAC solution.
- Segmentation down to a micro level is achieved using TrustSec security group tags managed by ISE. Tagging is simpler and much more scalable than traditional VLAN segmentation and for example might include groups of user, devices or services – as well as medical devices as described above.

4.3 Advanced Malware Protection

Historically, security has been focussed on prevention of attacks and rigid perimeters predominantly built with firewalls and intrusion detection systems. More recently, there has been broad acceptance that compromises will happen and the focus has shifted to a 'before, during and after' approach.

Cisco's Advanced Malware Protection (AMP) solutions help with breach prevention, continuous monitoring, malware detection and removal through:

- Continually receiving intelligence from Cisco Talos. It then correlates files, telemetry data, and file behaviour against this knowledge base to proactively defend against known and emerging threats.
- Anti-virus detection engines, one-to-one signature matching, machine learning and fuzzy fingerprinting to analyse files at the point of entry in order to catch known and unknown malware. This provides faster time to detection and automatic protection.
- Continuing to watch, analyse and record the activity of files entering your network regardless of the file's disposition. Should malicious behaviour be spotted later, AMP sends your security team a retrospective alert telling them where the malware originated and its activity. In a few clicks, the malware can be contained and remediated.

Contents

4.4 Endpoint Protection

As the boundaries of health and care delivery become more fluid, we have seen a move towards work being 'a thing you do', rather than a 'place you go to'. This has resulted in the need for mobile devices and working from environments that were previously considered too risky, or simply didn't have the required access. Now that health and care staff are adopting these new ways of working, it is crucial that the endpoints they use have appropriate levels of security that enables access to information, rather than hindering it.

Cisco provides a range of endpoint security solutions, including AMP capabilities, which:

- Empower employees to work from anywhere with their device of choice. Cisco AnyConnect is a unified security endpoint agent that delivers multiple security services to protect users and organisations. It provides a wide range of security services including remote access, posture enforcement, web security features and roaming protection.
- Offer the ability to protect endpoints when they are no longer connected via virtual private network. Cisco Umbrella provides visibility into internet activity across all devices, over all ports, even when users are off the organisation's network. Umbrella also uses the internet's infrastructure to block malicious destinations before a connection is ever established.
- Specifically for Apple iOS devices, Cisco and Apple have partnered to provide deep visibility and control. Clicking on a phishing link or simply mistyping can take users to malicious sites with unintended consequences. Cisco Security Connector prevents this from occurring, while also gathering all network traffic generated by iOS devices and apps so that network security teams can scope an incident rapidly, with precision and ease.

4.5 Other Solutions

In addition to the solutions already discussed, Cisco's extensive portfolio of products also addresses the following security needs:

- Next Generation Firewalls
- Intrusion Prevention Systems
- Web Security
- Cloud Security
- Router Security
- Email security
- And a range of Security Management solutions.

More information is available at cisco.com/go/security

Whilst the breadth of our portfolio is significant, the most important thing is to understand your own environment, both at an organisational and regional level. You also need to think about the implications of cloud connectivity and remote access.

Why not contact us to help with your security assessment.
http://www.cisco.com/uk/healthcare

Contents

4.6 Incident Response

How should your organisation deal with a breach, in terms of time to react, ensuring effective communications and minimising impacts on workflow and patient care?

Cisco's Incident Response Service helps organisations prepare for, manage and recover from network attacks and data breaches. It includes three principle offerings:

- Emergency response – quickly address the most pressing concerns in the case of incidents such as a data breaches or ransomware. Build a plan to identify the attacker; scope and contain the situation; identify the root cause; design strategies to remedy the underlying issues.
- Retainer – Cisco support is available before an incident arises, with proactive services to strengthen security posture. When emergency assistance is required, virtual Cisco responders begin work within hours, before travelling to site.
- Proactive threat hunting – identify vulnerabilities before they impact the organisation. Cisco responders will work in partnership to hunt for and address existing adversaries in the network.

Contents

5. Conclusion

Security begins with policy

Strong executive leadership helps ensure that policy is understood and acted upon through new processes and behaviours.

Understanding the threat domain as a whole supports an architectural approach and helps identify the required security capabilities.

In terms of building the system, we have also highlighted a number of security domains that organisations need to consider. Some will be more important that others, depending on the individual organisation, but it is essential that these solutions work together in a systematic way to provide the best possible protection.

With advanced threat intelligence, we possess the broadest range of security capability in the industry. Working alongside our partners, we stand ready to help health and care organisations to mitigate risk – at a local, regional and national level.

6. About Cisco in Health and Local Government

For 20 years, Cisco's dedicated Healthcare and Local Government teams have provided personalised consultative advice and regularly issued guidance papers into the marketplace, advising on a business-led approach to technology investment for both business and technical audiences.

In 2016, we united our Healthcare and Local Government teams, predominantly in response to market moves toward the integration of healthcare and social care, whether through devolution, Integrated Care Systems (ICS) or the implementation of Sustainability and Transformation Partnerships (STP).

Contact our experts:

Mike Badham Senior Solutions Architect – UK Health and Care and Local Government:
020 8824 4138
Mark Jackson Principal Information Assurance Architect – UK Public Sector:
020 8824 8535

Find out more at:

https://cisco.com/uk/healthcare/security

http://www.cisco.com/uk/healthcare

http://www.cisco.com/uk/localgovernment

7. References

Securing Digital Health and Care Communities: Addressing 10 common security challenges

National Data Guardian – Review of Data Security, Consent and Opt-Outs

Lessons Learned Review of the Wannacry Ransomware Attack

Care Quality Commission – Safe Data, Safe Care

Local Government Association Cybersecurity Funding

Cisco Talos Threat Intelligence Group

Cisco Network Visibility and Segmentation

Cisco Advanced Malware Protection

Cisco Endpoint Security

Cisco Incident Response Service