Securing Digital Health and Care Communities

Addressing 10 common security challenges

Introduction and purpose

A more connected world offers many advantages in terms of information sharing and communication.

But by its very nature, being more connected introduces new threats, as organisational boundaries become blurred. At the same time, the tools used by attackers have become more sophisticated but also easier to use.

This change in the threat domain is a constant challenge for all sectors, not least those operating in the areas of health and care. 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 now, with the next generation of the Internet, a new wave of connected devices and 'things' is extending that threat landscape. The Internet of Things (IoT) is connecting billions of elements, from trees to cars and buildings. Despite the many benefits this connectivity brings, it will also introduce new 'back doors' that must be considered as much a part of the security domain as any IT system.

Health and care organisations are equally susceptible when it comes to IoT. Outside of care facilities, consideration should be given to the telehealth and care environment, including devices, wearables, telemetry equipment and the new breed of health apps. Inside the hospital or clinic, consider connected medical devices and third-party equipment and systems, as well as the built environment.

In July 2016, Dame Fiona Caldicott issued the most recent review of security and information governance in the NHS,[1] which called for tougher penalties and better controls of data and information. The recommendations included a modernised Information Governance Toolkit (ITK), improved cybersecurity controls, data protection enhancements and harsher penalties for malicious data breaches. These proposals have all now been accepted by the Department of Health, as outlined in its formal response.[2]

What is abundantly clear is that traditional approaches to information governance and security are now inadequate. For example, it is fair to say that NHS organisations have concentrated on perimeter and endpoint security, with the added notion that the national network offered a barrier, being one step removed from major threats. Evidently, this view is changing as threat vectors have evolved to include email, web, social, mobile, and malware. Where priority was previously given to preventing attacks, a much more holistic and pragmatic view is needed.

[1] Review of Data Security, Consent and Opt-Outs: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF.
[2] Your Data: Better Security, Better Choice, Better Care https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf.

Contents

In this document, we set out 10 common security challenges facing health and care organisations. In response to the Caldicott review and its acceptance by government, we propose that security should be treated as a system and blended into an architectural approach that more directly aligns business needs with the technology domain. And finally, we demonstrate solutions that help to create that security system, offering the best possible mitigation.

10 common security challenges for health and care organisations

The evolution of the threat domain has seen an increase in the number of new vectors, along with the ever-present threats that exist, most of which are typically procedural (such as patching) or human behaviour related. Here we identify 10 such threats that are common to all health and care organisations, along with suggestions for mitigating these challenges.

1. Availability

Now more than ever, networks and other IT infrastructure can be considered as critical to how our health and care system functions. From entrance to exit and at every step along the patient pathway, reliable access to information is pivotal to patient outcomes and operational excellence.

While networks and systems are increasingly designed for high availability and ease of accessibility, the underpinning fabric and control plane of the devices involved can often be ignored.

Yet they too can be the subject of denial-of-service attacks that can have devastating consequences. It is therefore most important to consider control-plane protection, including the use of policing techniques such as classification and rate limiting of traffic.

2. Malware

Malware represents one of the greatest cyber threats to health and care organisations. The near exponential rate at which new malware variants are released, alongside the inherent limitations of the current signature-based defences, result in a high risk of infection.

Ransomware is one form of malware that has seen a significant increase in popularity and has been responsible for a number of high-profile incidents. As demonstrated by the 2017 WannaCry malware breach, the number of ransomware attacks continues to grow, as it remains an easy route for criminals to extort significant sums of money from their victims.

Contents

In additional to the financial implications, WannaCry showed that a ransomware infection can have a significant operational impact within the health and care setting, especially if critical clinical machines are infected. This is because they are rendered unusable until they can be recovered.

In light of this, a robust backup and recovery procedure remains one of the primary lines of defence against ransomware. However, in many cases the risk of initial infection can also be reduced through a combination of improved user education and the deployment of defensive controls that don't simply rely on signatures alone.

3. Legacy application support

One of the most fundamental security controls is that of software patching. Patching reduces the exposure to malicious software and can make it very difficult for an attacker to gain a foothold in the network. Effective patching can be difficult to achieve in practice and is becoming harder as the number and diversity of network-connected devices increases. Patching can also be problematic when dealing with legacy systems where patches are either not available, or where patching renders the system unsupported by the vendor. The latter is a particular problem for health and care organisations, where software changes may affect a medical device's regulatory status.

Where patches cannot be applied, additional compensating controls can help reduce the exposure. Network segmentation can provide one such control, as can increased monitoring to provide early identification of potentially malicious behaviour. Both these controls rely on a full understanding of the network landscape and the devices that are connected, so that they can be effectively deployed.

4. Internet of Things

Health and care organisations have for many years adopted the use of network-connected medical devices, especially within radiology, where PACS deployments enabled the digitisation of medical imaging as far back as the late 1990s.

Today, the Internet of Things (IoT) revolution is in full swing, not only in the consumer space but also in the clinical setting, with many examples of network-connected medical devices in use such as infusion pumps, patient monitoring systems, and even wirelessly connected medical implants. While these devices have clear clinical benefits, they can suffer from a range of security issues that are due in part to the lack of mature secure software development practices within the device manufacturers. These devices also amplify the network attack surface, as they fall outside established security management practices and are not actively purchased or managed by the IT teams.

Contents

In addition to the quantity and diversity of new devices, there is also the issue of mobility. In the past, large radiology modalities were, by their very nature, static. This meant that they could be easily identified and segregated from the rest of the hospital network. With the adoption of smaller, more mobile clinical devices, it is no longer possible to rely solely on static network segmentation approaches. Instead the network must be able to identify devices as they are connected, and apply security polices dynamically.

5. From healthcare to health and care

The landscape of health and care in England is changing rapidly. Sustainability and Transformation Plans (STPs) will indicate a move to more regional approaches and consideration of the whole system to improve the continuum of care. In parallel, the impending move from N3 (the national network) to HSCN (the Health and Social Care Network) will almost certainly see a shift to regionalised networks that underpin STPs. In many ways, this mirrors the Health Board approach of Scotland and Wales, though they too are likely to see further erosion of boundaries with, for example, partners in social care and the third sector.

While the intention is to bring benefits to both patient outcomes and operational efficiencies, this transition opens up a new range of threat vectors for health and care organisations to consider. The organisational boundary will no longer be as rigid or so easily managed, while visibility and control of what is happening in each organisation's domain will be challenged.

Many organisations are already planning for this shift with information-sharing agreements. Other considerations should be both policy -based, for example co-location working practices, and practical, such as using network awareness tools to identify anomalies.

6. The built environment

Most health and care organisations operate public buildings, whether they are hospitals, clinics, or GP surgeries. It is very difficult to track the whereabouts of every individual within the premises. Whereas much emphasis is often placed on securing the wireless environment, it can be the wired network that is the most exposed, due to accidental or malicious access to live network connections. Several approaches can be employed to address the issue, from physical security where scaling challenges may exist, to authentication, authorisation, and posturing at the network edge.

Multi-tenancy of public sector buildings is becoming more popular, especially with the advent of the One Public Estate programme. Here, the need for 'hot desking' facilities and the potential for reciprocal wireless access can ensure that any user is assigned the correct access privileges, based on a set of user credentials.

Contents

And finally, increasing numbers of converged building management systems are incorporated into the fabric of the organisation's network. These should be considered as IoT systems, as described earlier.

7. Threats closer to home

The National Data Guardian review called out the fact that many security breaches across the health and care environment were not actually caused by malicious external attackers. Instead they were a result of actions by internal employees who were motivated to get their job done but were working with ineffective technology or processes.

This evidence points clearly to the fact that security is not being considered as an integral part of the development of business and clinical systems, but is instead being added as a 'bolt-on'. This approach results in a poor user experience that forces staff to seek alternative approaches to get their job done, even if that means bypassing security controls.

The solutions here are both policy based and practical. Rather than being seen as a barrier, security must form an integrated part of systems development and should support the business or clinical workflow, not hinder it.

In other words, having the right security controls in place allows staff to work freely, but safely.

8. Cultural challenges

Culture was also highlighted by the National Data Guardian review. It found that health and care staff were culturally motivated to provide the best possible care to their patients and, when faced with poorly designed systems that hindered this goal, would find workarounds or alternative approaches to achieve a given outcome.

These workarounds may inadvertently lead to insecure behaviours such as the use of so-called shadow IT, such as the use of unsupported and unsanctioned applications which are often cloud based. There are many examples of staff adopting unauthorised cloud-based email or file-sharing applications. This activity often goes unnoticed, leading to risk of infection from malware, loss of data, and potentially even breaches of data protection legislation. Others include the use of well-known consumer messaging and video-conferencing applications.

Rather than blocking behaviour, it is important to understand which business need isn't being fulfilled by current solutions, and to develop a secure and sanctioned method for achieving the desired outcome. Furthermore, it is important to foster a culture of security within the organisation. This must extend beyond annual training and should introduce security champions – perhaps reporting to the Caldicott Guardian – who can act as local points of escalation and sources of best security practices.

Contents

9. Skills and capability

There is global recognition of the lack of skilled security professionals available to meet the growing demand. This issue is so critical that it formed a core objective within the Government's National Cyber Security Strategy 2016 to 2021[3] and will likely continue into the next iteration.

While Chief Information Security Officers (CISOs) are becoming more common in large companies, UK health and care organisations rarely have the resources to assign such a role. In fact, the Caldicott Guardian is often a function assigned to an executive officer with another primary role. Meanwhile, the practical security function is generally confined to the IT team and is rarely handled by dedicated personnel. This very often results in a reactive rather than proactive response by employees who have to perform this role in addition to their main job specification. It is also unusual for security to be truly operational. Therefore, while numerous security controls are deployed, this lack of dedicated security specialists can mean that incidents are handled in an isolated and highly reactive fashion.

Investment in people, processes, and education is the primary means of addressing skills shortages, but these can also be mitigated by deploying a more integrated security architecture. Closer integration between discrete components can deliver a degree of automated response in the face of security incidents, and can also help identify the most critical events that require operational intervention.

10. Executive leadership

Lack of executive leadership is a recurring theme in the cybersecurity world and, like some of the other challenges above, was also raised as part of the National Data Guardian report and accepted by the Department of Health as an issue that requires addressing. The NHS does maintain strong executive leadership for information governance in the form of Caldicott Guardians, but this role is often not broad enough to incorporate the wider information security and cybersecurity challenges. Overall executive leadership is critical to ensuring that a comprehensive cybersecurity strategy can be developed and implemented, but all too often security is quickly delegated to the IT department.

It is essential for executive leadership to offer clear guidance to the IT team, indicating the most critical clinical and business applications. In turn, appropriate controls can be put in place to help ensure the best possible risk mitigation.

Executive teams must therefore have a clear understanding of the impact resulting from a cybersecurity breach. Such an incident could result in the loss of confidentiality, integrity, or availability of critical clinical or business systems, leading to damage to reputation and public trust and, in extreme cases, increased risk to patients. To support executive understanding, IT teams need to improve their ability to articulate risk in a nontechnical way and seek strong business guidance to prioritise investment.

[3] The UK Cyber Security Strategy - https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

Contents

Adopting an architectural approach to security

We have identified 10 key considerations for organisations to consider as communities develop and transition to new models of care. Each one can, of course, be addressed in isolation, but the most complete and effective approach is to consider security needs as a whole system, supporting the health and care economy to work freely and more efficiently to deliver better patient outcomes.

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 and at the same time be capable of sharing vital contextual and threat information to deliver 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 question of if a security breach will occur, but when.
- Security controls must transcend the traditional ‘block’ approach and instead focus on improving detection and remediation times.
- Security should be developed as a system; that is, distinct components should not operate in isolation and should instead integrate to provide more accurate threat detection and reduce management complexity.

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

Compromise in this sense should be considered across all three aspects of information security: confidentiality, integrity, and availability. This is an important shift, given that all too often emphasis is placed on the loss of confidentiality, when in fact a loss of 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 important to consider the threat.

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

In other words, security is an enabler for the business.

Contents

How can Cisco help?

Cisco has developed a broad security capability over a number of years and is uniquely positioned to deliver security as an integral part of the network fabric, as well as through dedicated physical and virtual appliances.

To aid the development of a robust security architecture, it is helpful to consider the progression of a cyber attack as a continuum containing a number of phases. Cisco has developed a simple mnemonic: BDA, which represents the phases of before, during, and after an attack.

Before

This phase represents the area where most security investment takes place and includes the deployment of defensive capabilities such as firewalls and anti-malware. It is vital to understand that defensive controls, while important, will be breached, and so investment should be spread more evenly across the remaining phases.

During

Controls deployed in this phase of the continuum focus on improved visibility, so that an attack can be rapidly identified and mitigated. Network segmentation also helps manage an attack in the 'during' phase since, when implemented properly, it can contain an attack to a smaller subset of the network and IT estate.

After

The final phase of the continuum is concerned with rapid remediation. It also includes forensic controls that can help identify how an attack occurred as well as which systems may have been affected.

Following the BDA model, it is important to consider the deployment of capabilities that span the entire attack continuum. The focus must go beyond defensive technologies and include essential elements that support rapid identification, containment, and remediation in the face of a security incident.

Being the very fabric of interconnectivity, the network is uniquely positioned to deliver the increased visibility and control required in most health and care organisations. Technologies such as Cisco® NetFlow – a capability that is built into most Cisco network devices – provides real-time network telemetry revealing who is talking to whom, over what protocol, and for how long. Through careful analysis of this telemetry, unusual patterns of activity can quickly be identified and investigated. Such patterns include excessive one-way data transfer, which could be evidence of data being stolen, or data being transmitted between health and care systems and Internet-based machines that are located in unexpected places.

Contents

Segmentation is another important capability that is delivered by the network. Its importance is always increasing, especially in the face of the need to connect a wider range of devices and user communities to a common network infrastructure. Segmentation has, however, remained challenging, with many environments still relying on static segmentation, based simply upon physical location. Furthermore, the segmentation that is in place is often not used to enforce security controls, and traffic is allowed to flow freely across the entire network.

Importantly, each distinct component is able to operate in conjunction with others, forming a tightly integrated security system that can share threat and context data. The overall result is a system that is more responsive to threat and can quickly identify issues as they emerge, allowing for rapid remediation and recovery.

Addressing the challenges covered in this paper requires a top-down approach to the development of a cybersecurity strategy. Cisco Security Advisory services can support health and care organisations in achieving this goal by:

- Identifying key risks to the organisation based on analysis of the information and business impact if breach or loss were to occur.
- Performing a gap analysis to identify areas of weakness between the required level of control versus the current state.
- Highlighting strategic areas for security investment across the organisational, policy, and technology domains to support the secure delivery of front-line services.

Digital transformation within the health and care setting could have a potentially profound impact. However, the ever-increasing reliance on technology requires a comprehensive security architecture that is driven from the top down, and Cisco is uniquely positioned to support our customers in developing this vital capability.

Cisco TrustSec® encompasses a range of capabilities that enable software-defined network segmentation. This is the ability to dynamically apply a segmentation policy as a user or device connects to the network, either wired or wirelessly.

Contents

Cisco TrustSec can capture details about the connected endpoint to inform policy decision making. These details can range from simple user identifiers to device types, installed software, and compliance with software policies (such as whether the device has the latest patches installed). By gathering this information, the system is able to make an informed decision and enforce a predefined security policy, helping ensure that the device is given the access it needs and no more. For example, this information could be used to enforce dynamic segmentation between NHS and social care staff members, ensuring that both communities are provided the access they need to perform their function and limiting access to all other systems.

Cisco NetFlow and TrustSec represent just two of the many innovations that Cisco has developed to embed security into the fabric of the network. As the wider security system is considered, the Cisco portfolio also includes a full suite of capabilities ranging from perimeter access control and intrusion prevention to advanced network and endpoint anti-malware solutions.

Contact us

Cisco has a dedicated team supporting our UK health and care and local government customers. The team's extensive industry knowledge means that they can identify the right Cisco solution for your needs. Contact us for further information.

Authors

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

https://cisco.co.uk/healthcare

C07-740497-00 05/18