ARMIS®

WHITE PAPER

SECURITY & OPERATIONAL EFFICIENCY - IT BEGINS WITH VISIBILITY.

Table of contents

INTRODUCTION

Medical device security is a mainstay of security strategies in healthcare organizations. It has quickly become the foundational starting point for understanding the pivotal role these devices play in the resilience posture throughout the delicate process of care delivery. An important result from all the industry's efforts in dealing with this issue has led to the realization that the healthcare device ecosystem is much bigger than just medical devices. This facilitates the need to account for all elements of infrastructure and their role in securing a patient's journey through the health system.

In 2021, Armis conducted research related to how the National Health Service (NHS) in the United Kingdom (UK) is approaching this issue and the effectiveness of its strategy across its member trusts. This paper will offer guidance and best practices while offering a view into the results of the research in an effort to help healthcare providers plan for the next chapter in this evolving area of information security and organizational resilience.

TRANSFORMING REGULATORY REQUIREMENTS
INTO STRATEGIC PRIORITIES

Regardless of the type and location of healthcare providers, regulatory burden is common. There are often two to seven legal regulations and technology standards that apply to health IT and Information Security with overlapping requirements, certification criteria, compliance schedules, and penalties for non-compliance. In the case of the NHS, over 70 trusts in the research pool had requirements ranging from Networks & Information Systems (NIS) Directive, Cyber Essentials, ISO 27001, and ranging participation in the Data Security & Protection Toolkit (DSPT) as a self-attestation tool.

Now, there are parallels that can be drawn between these and regulations like HIPAA and HITECH in the United States of America (USA), Data protection rules issued by the French Data Protection Authority, GDPR's coverage across the European Union (EU) and Health Data Law covering healthcare entities operating in United Arab Emirates (UAE). Broad-spectrum alignment to basic tenets of information security can be found in each one of these. Specifically relating to:

- Continuous Risk Management
- Organizational context of security risk to patient safety
- Focus on privacy and security of confidential information related to clinical and demographic data related to the patients
- Requirements to demonstrate operational proficiency
- Establishing standards-based data sharing for security intelligence and incident response

These requirements evolve each year in response to the changing threat landscape and as innovation in Healthcare IT and its reliance on healthcare applications and integrated data from medical devices used to support the clinical decision support process. There is a convergence happening for health systems and hospitals, bringing together information security risk management as a function of enterprise risk management together with clinical quality, safety, and risk improvement.

Basics of Risk

Healthcare organizations today have a dual approach to risk management. One is compliance-based and often governs the information security strategy, while the other is focused on clinical outcomes and patient safety. Additionally, clinical safety is aligned to efforts of departments such as Biomed or clinical engineering, which are tasked with maintaining and servicing the medical devices.

We can see this difference in the research data when asked about how the risk is quantified. In some cases, risk was articulated in terms of maintenance of software on medical devices, while others articulated based on segmentation and deployed security controls. However, almost all organizations had varying levels of compliance with regulations that were driving the adoption of security technology.

A key element that all risk management programs try to improve is prioritizing identified risks with probabilities and likelihood of occurrence combined with organizational tolerance and resources to manage the impact. In this case, since we are talking about IT and Information security-induced risk to the system, appropriate data flows need to be analyzed that help distinguish the impact between nuances of care delivery and reliance on facility infrastructure that has only recently "found" its digital self.

TRANSFORMING REGULATORY REQUIREMENTS
INTO STRATEGIC PRIORITIES cont

Understanding that healthcare is a highly-regulated industry with multiple workflows required for different types of risk assessments and appropriate regulations, it is important to leverage standardization for risk and threat related data sets before using those as inputs to scenarios for emergency management and business continuity planning. This data standard needs to account for:

- Security risk contextualized by treatment area or specialty
- Threat models taking into account IT hygiene and privilege management
- Baseline utilization context for clinical and building management systems
- Clinical or ancillary application dependency and/or data interoperability use cases
- Workflow context for departments such as Biomed/Clinical Engineering and Facilities management

Efforts like the DSPT in the NHS's case are a welcome step in the right direction.

Utilizing overlapping regulations

As onerous as this sounds, overlapping requirements in regulations can simultaneously approach multiple facets of a security program strategy and spread out costs through multiple funding sources. Consider the following example. In a healthcare environment, there will be security requirements that stem from the following:

- National / Federal laws and regulations
- State / Provincial / Territorial laws and regulations
- Information security standards related to
- Financial transactions
- Clinical research and data collaboration
- Collaboration with defense and intelligence agencies

In each case, a crosswalk approach can be designed that helps organizations prioritize leveraging appropriate standards to drive technological architectures and utilize operational data derived to satisfy regulatory requirements. For example, using security requirements specified in PCI-DSS to produce segmentation in the environment that can then be leveraged to manage healthcare data.

In another use case, standards requiring technical approaches to vulnerability management, and risk prioritization driven through clinical research data collaboration, can be used to improve security operations workflows whose data can serve as evidence of capability for compliance with regulations at the state and national level.

These ideas are meant to facilitate process designs that are not just tied to "checking the box" for compliance, they can be used to align activities that need to be performed so appropriate alignment of enterprise risk can happen with clinical workflow resilience. Appropriate time spent on this can help organizations bolster their response to incidents that impact care delivery.

Realities of "real-time" data

When addressing the requirements of continuous monitoring of organizational risk, there is an effort that requires rethinking of processes used to determine vulnerability and impact data and its scope aligned with the healthcare device ecosystem. Data from our research indicates that while most organizations had top-level support from executives relating to these activities, the translation at the operational level, often manifested as just focussing on information security data, rather than the totality of the clinical workflow impact of medical devices.

Looking at the device ecosystem, not all medical devices are equal in their risk profiles. Consider the following examples:

- Devices used directly to provide patient care (e.g., infusion pumps, patient monitors)
- Ancillary devices used to support care (e.g., lab, radiology, sterile processing)
- Operating technologies with critical impact (e.g., pneumatic tube systems, water and oxygen management, HVAC)
- Control systems with high impact to operations (e.g., physical security, alarms, elevator control systems)

All of these are an essential part of "securing the patient journey." Yet, as organizations look at vulnerability management and their approaches to manage the risk associated with these in terms of clinical workflow, the approaches are still point in time. They need to pivot to processes that support real-time analysis of vulnerability data and its impact on operational workflows.

In order to transition from the legacy approach to a continuous monitoring style methodology of vulnerability management, organizations can take advantage of the capabilities that exist in legacy platforms and add innovations with new approaches that take into account:

- Network behavior
- Communication methodology (peer to peer/airspace, e.g., Bluetooth, Z-Wave)
- Real-time passive event-based vs. scheduled scanning
- Utilization data
- Baselined device behavioral telemetry

Utilizing these approaches allows for creating an architecture that takes into account not only the technology footprint but also the workflow impacts in an operational setting. This is critical for healthcare organizations, as operational environments such as Biomed / clinical engineering often consist of devices ranging from 30-year-old lab monitoring equipment all the way to the latest imaging modalities. As the next step, when operations teams account for the role that Operating Technologies (OT) play in a healthcare environment, it becomes clear that vulnerability management is no longer just a security tool kit, but an essential component of continuity of operations.

IDEAS ON DEALING WITH RESOURCE CONSTRAINTS

Efforts re-architecting existing security programs and operational practices do require investment. This was evident from research data from the NHS showcasing the progress made in implementing security controls for device identification and segmentation. Yet, the efficacy still needs to be proven, demonstrating operational capability challenges. Investment doesn't always need to be financial. In the case of programs related to the security of healthcare device ecosystems, a significant amount of training needs to occur to account for the introduction of data and processes that are foreign to traditional security teams. Proper scope for implementing strategy can help narrow down the goals and success criteria that will be classified as demonstrable artifacts for compliance and showcase ROI in terms of organizational resilience.

People & Money

Over the last decade, medical device security initiatives have been instantiated through IT due to their characteristics as an edge computing device. As a result, healthcare organizations have had to take some time to understand the operational implications of applying traditional security methodologies when mitigating threats that may impact care delivery and patient safety. While this approach has yielded innovations in technology, we still need to account for context from clinical and operational workflows.

Why the separation between clinical and operational? With the former being focussed on care delivery while the latter on providing the "plumbing" that the former needs to be successful, this minute difference has a big impact on how organizations need to adjust strategy while embarking on a medical device or OT or Industrial control system (ICS) security initiative.

While planning for funding, understanding the scope is vital as that creates initial alignment for the purpose of launching the program. This may be for patient safety or to manage risk during significant growth, or for preparation for a merger or acquisition event. In each case, it is appropriate to draw from funding sources that closely align with the outcomes of the "why" instead of the "how" (in this case the tech).

From a staffing perspective, an approach should be designed that can leverage existing mechanisms for risk management and leadership buy-in. There will be a need for some investment in FTEs, whether organically or from a partnership with a managed service provider. This will need to be augmented from expertise from clinical, operational, and risk departments so that appropriate data reporting and use case functionality can be designed before technology is purchased and that alignment to clinical and operational use cases can be realized.

Finally, considering human factors and workflow, appropriate training in the following areas can significantly impact the capability of the information security and clinical operations teams. Appropriate testing methodologies need to be implemented that encompass:

- Alignment of security incident response to emergency response and clinical workflow frameworks
- Baselining business continuity metrics for organizational thresholds for data loss and duration of systems downtime
- Understanding time thresholds for personnel workflows (e.g., time for a Biomed technician to replace a pump, time for an IT technician to replace a viewing station for CT scanner, how long it takes to provision a handheld scanner for medication dispensing, etc.)

Most importantly, including security scenarios such as ransomware and supply chain attacks as part of emergency management drills results in the proper development of muscle memory for IT and information security responders and helps baseline true time estimates for incident response and recovery.

SHINING A LIGHT ON VISIBILITY. NOW WHAT?

The visibility into the totality of the healthcare device ecosystem is vital to the success of any medical device security strategy. It is also the foundational element of effective threat modeling. It provides security teams with the most realistic view of the attack surface when analyzing security intelligence in terms of impact on operations.

Prioritizing vulnerabilities and leveraging modeling

Threat models are an essential part of security strategy as they provide the following telemetry for efficiency of response:

- Dynamic view of the attack surface
- Vulnerability and Safety exposure across the ecosystem
- Identification of threat actors
- View of attack vectors
- Enumerating hospital assets (operations) vs. patient assets (clinical)
- SecOps capability
- Metrics to bridge operational reality with academic data of perceived risk

These models not only allow security teams to design and test appropriate workflows for incident response, they also become a data feed for emergency management to test contingency processes and simulate operations in the event of an incident. While there has been significant progress within many organizations to do this, investment is still needed to design and implement proper testing infrastructure such that actual metrics can be used to determine operational risk instead of data derived from tabletop exercises.

A key element of threat modeling is understanding the role that vulnerability management plays not only for identifying security exposure, but also for potential safety and operational impacts in a healthcare environment. Advancements in security technology such as Armis, now provide the ability for healthcare organizations to be able to articulate not only what the threat profile is for a particular device that is present in the environment, it also provides:

- View into upstream and downstream data flows
- Context for transient devices that don't connect to the enterprise network
- Device telemetry when utilizing airspace technologies
- View into customized healthcare data protocols as part of behavioral mapping

These pieces are important as they often translate to important workflow and clinical context needed when prioritizing incidents as they help to articulate risk to patient safety, device availability, and the ability to deliver the right care at the right time. Another tangible effect this approach has is on operational efficiency. As the data involved in the risk prioritization has already been contextualized with the appropriate relevance in terms of organizational nuances (both from technology and workflow perspectives), the confidence of identified priorities is high, and that leads to a significant decrease in incident response times and efficiencies in cost management in terms of device and asset inventories.

Driving utilization context to drive response and recovery processes

From a clinical point of view, the next iteration of ROI of a medical device security strategy will need to expand the view from the traditional hypothesis of just securing connected medical devices in an inpatient setting. Clinical risk management includes the following aspects:

- Monitoring clinical workflows in line with quality and safety standards and directives
- Analyzing device utilization to minimize impact to patient satisfaction (e.g., wait times)
- The efficiency of clinical procedures (e.g., reductions in overuse of a specific type of medication)
- Assuring the integrity of data flows used for clinical decision support
- Doing all the above in any type of care setting - inpatient, ambulatory, remote, etc.

Practically, it is complicated to account for these when looking holistically at the totality of services provided by a care provider. To help, organizations can limit the scope by specialty, market alignment, strategic clinical/compliance initiatives etc., to minimize alert fatigue and help the risk governance process grow organically and at a manageable cost level.

Focusing efforts for real-time reporting and integrations with IT operations can help with reduction in help desk response times and increased efficiency of analyst workflows to provide operational cost savings. From a Biomed and facilities context, these integrations can help streamline cross-facility maintenance workflows and help baseline costs for third-party health services contracts. Data interoperability is critical as it establishes the bidirectional data path between the security architecture and existing investments in governance and risk management platforms leading to additional operating cost savings.

CONCLUSION

Risk frameworks, response tactics, threat models are only marginally effective in absence of an actual testing methodology. To reduce the impact of these attacks and improve response effectiveness, there is no substitute for actual simulations and testing of workflow disruptions or system outages. Healthcare organizations that prioritize these efforts as part of normal business operations can weigh their risk telemetry and take into account data such as how long it took systems to be recovered, what was the user impact to “degraded performance,” and did the partnerships for resources and technology work as intended. Practiced over time, the muscle memory and lessons learned from these drills and tests can serve as the bedrock upon which organizational resiliency transcends any attack on their environment.

Armis is committed to helping our healthcare customers realize the vision where risk management and continuity of operations can exist symbiotically, and with proper investment combined with a deliberate sense of urgency, we can make information security an organic extension of the clinical risk management process.

About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

1.888.452.4011