SECURING THE PATIENT JOURNEY

Operational considerations to drive cyber resilience

Table of contents

A **DOSE** OF REALITY

Do adverse outcomes from Information Security incidents truly, and quantifiably, affect patient safety & clinical risk? This question is the genesis behind a lot of the debate and scrutiny that medical device manufacturers, in addition to most of the healthcare provider industry, have had to grapple with for the last 10 years and counting. While the governance of security programs has been on a positive trajectory, the key systemic issue affecting operational success of this particular focus area is the lack of effective cohesion between information security risk, enterprise risk, and clinical risk management.

Terms like Internet of Things (IoT), Internet of Medical Things (IoMT) and medical device security have dominated the security industry in terms of coverage. However not all medical devices are equal in their risk profiles. Consider the following ecosystems in healthcare delivery organizations (HDOs):

- 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, we as an industry, while making some progress, are still grappling with how to address security from the manufacturing side. For manufacturers, the reality of medical device security is different, as they must take into account security for:

- Specialized devices used during prototyping and clinical research
- Protecting the manufacturing process
- Assuring the supply chain and all the control systems that are part of that network of suppliers
- Once the devices are in “production” environments, security then needs to be managed across decades of product lifecycle intermingled with regulatory certifications.

It is this disconnect between the complexities of two very different approaches to device security that have coalesced in a way that is unprecedented when we look back at 2020 and peak into the next two to three years.

PRIORITIZING WITH PURPOSE

Navigating our way through the pandemic, innovations in clinical care have created use cases where modern medical devices are integrated with native cloud-based platforms to provide high confidence data and clinical workflows. These advancements have altered the threat profiles for organizations by shifting the focus from simply data protection, to now the continuity of operations and assuring the integrity of data flows that are used in clinical decision making. The expanding scope of ransomware-based extortion incidents or supply chain threats further exacerbates the urgency to effectively pivot the current security strategies that are in place for organizations.

Current structures for risk management in HDOs are born out of techniques that were designed more than 30 years ago. As illustrated in the figure below, due to the hierarchy of information flow, there is an organic data filtration process that gets introduced as information is shared across the business units that most times is responsible for creating the fissure between enterprise and clinical risk especially related to information technology and security.

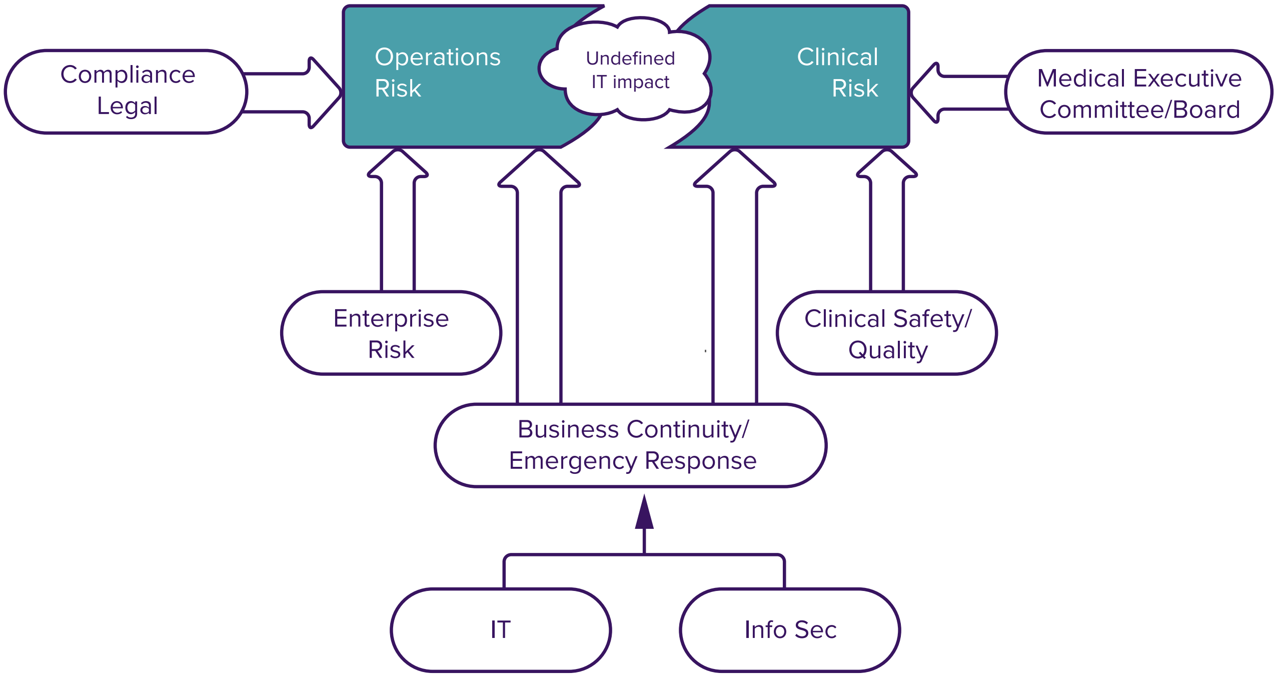


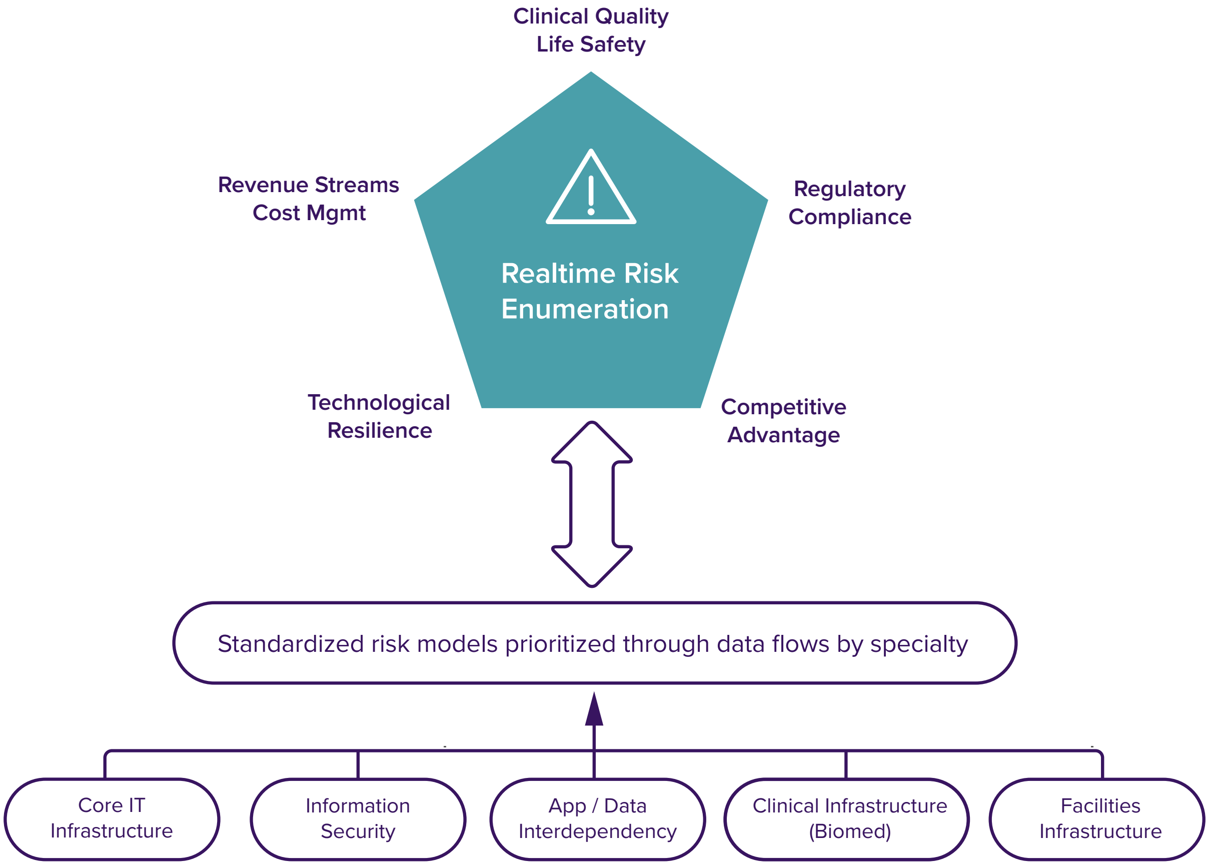
Figure 1: Organic Data Filtration Process

A key element that all risk management programs try to improve is prioritization of 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 impact between nuances of care delivery and reliance on facility infrastructure that has only recently “found” its digital self.

Understanding that healthcare is a highly regulated industry with multiple workflows required for different types of risk assessments based on federal and state 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

Illustrated below, you see an example of how this data can help reduce the siloed approach to risk intelligence and streamline information sharing cross-specialty in the new age of connected healthcare delivery with a focus on continuous monitoring.



Investment in this process, leveraging existing industry frameworks, can help HDOs prioritize actions needed for resilience with clarity towards the patient experience and clinical safety.

CLINICAL VS. **OPERATIONAL**

Medical device security initiatives over the last decade 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 that baselines communications behavior, device configurations, and visibility into specialized network protocols, we still need to account for context from clinical and operational workflows.

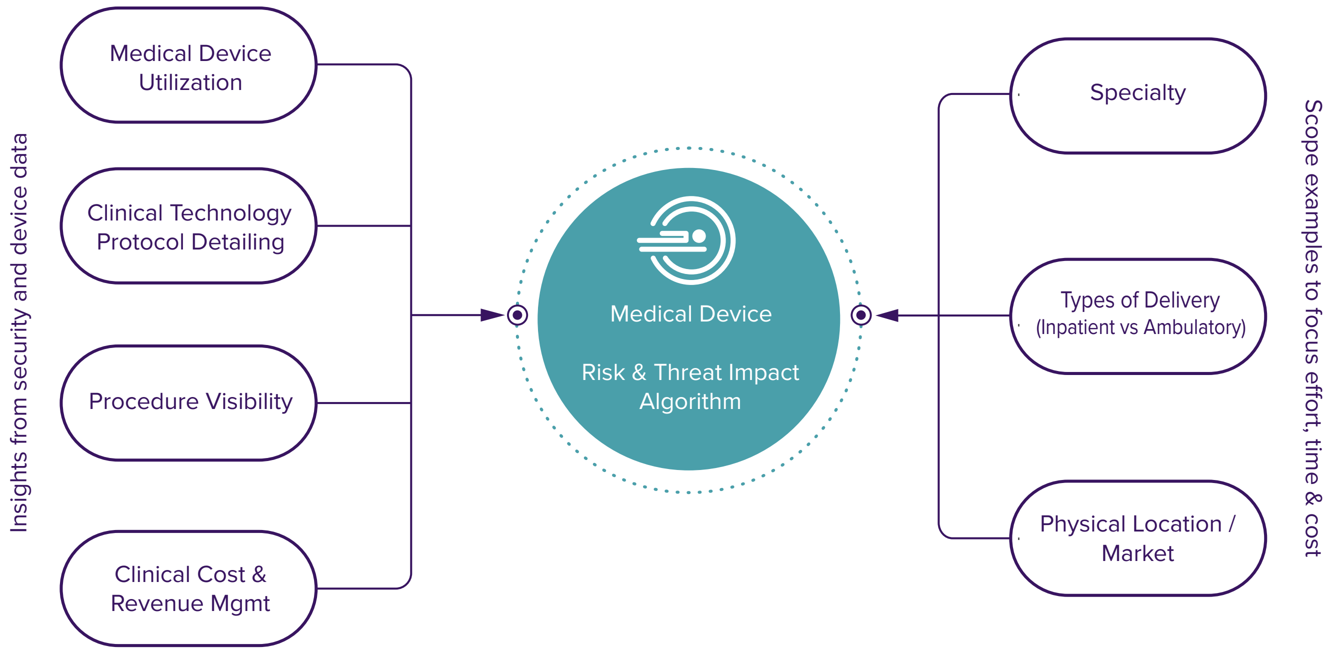
Why the separation between clinical and operational? With the former being focused on care delivery while the latter on providing the “plumbing” that the former needs to be successful, this minute difference has a big impact on how organizations need to adjust strategy while embarking on a medical device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

Clinical context as the bedrock

From a clinical point of view, we need to expand our 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 inline with quality and safety standards and directives
- Analyzing device utilization to minimize impact to patient satisfaction (e.g. wait times)
- Efficiency of clinical procedures (e.g reductions in overuse of a specific type of medication)
- Assuring 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 as shown below to minimize alert fatigue and help the risk governance process grow organically and at a manageable cost level.

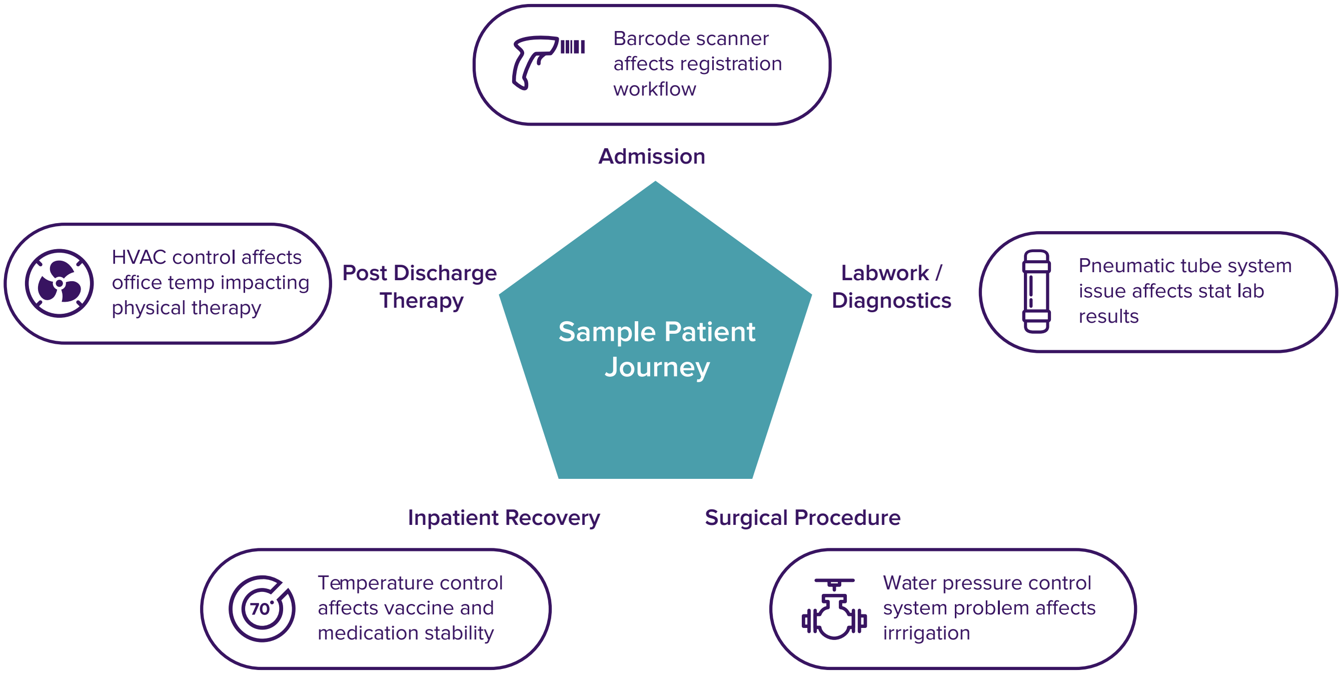

Insights from security and device data
Medical Device Utilization
Clinical Technology Protocol Detailing
Procedure Visibility
Clinical Cost & Revenue Mgmt
Medical Device
Risk & Threat Impact Algorithm
Specialty
Types of Delivery (Inpatient vs Ambulatory)
Physical Location / Market
Scope examples to focus effort, time & cost

Clinical context derived through this process and aligned with the appropriate framework can yield powerful insights for risk management teams that are also analyzing the operational impacts from threats to the healthcare device ecosystem.

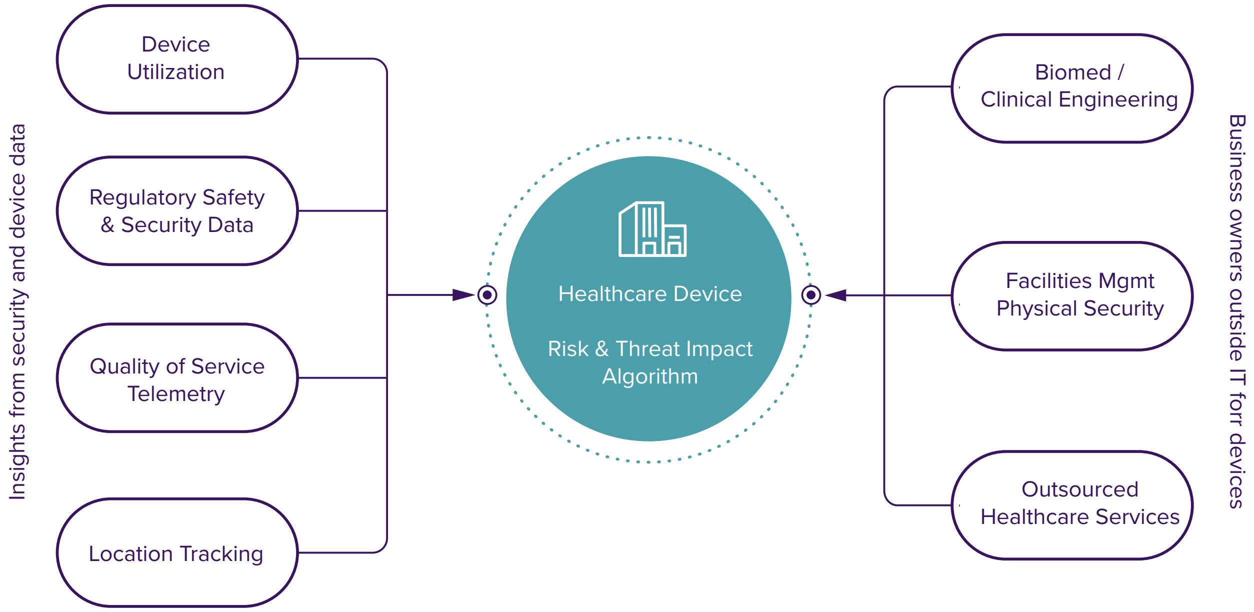
Extending our view to the entirety of the ecosystem

What is the healthcare device ecosystem? The easiest way to grasp it is to visualize all the secondary technology and machines that serve as the infrastructure that powers medical devices. For example, elevator control systems in the context of patient movement, pneumatic tube systems for intra hospital transport of lab specimens, temperature control sensors for vaccine storage, gas control systems for suction and oxygen delivery. This is where the conversation extends past simply IoMT or medical devices to include operating technologies (OT) and industrial control systems (ICS) in healthcare settings. Increasingly, these systems are connecting to the hospital network and even the Internet itself. And with that, comes an expanded attack surface by which an increasing number of vulnerabilities can be exploited by bad actors.

The visibility into this ecosystem is vital to the success of any medical device security strategy. It is also the foundational element of effective threat modeling providing security teams with the most realistic view of the attack surface when analyzing security intelligence in terms of impact to operations. An illustrative example of this ecosystem showcases how an OT infrastructure can have a clinical impact.


Barcode scanner affects registration workflow
Admission
HVAC control affects office temp impacting physical therapy
Post Discharge Therapy
Sample Patient Journey
Labwork / Diagnostics
Pneumatic tube system issue affects stat lab results
Inpatient Recovery
Surgical Procedure
70°
Temperature control affects vaccine and medication stability
Water pressure control system problem affects irrrigation

Most healthcare organizations today possess a mix of OT and ICS devices that range from control systems approaching 30 plus years in age to smart building controllers deployed in the last year or two as part of a facility upgrade initiative. This is in addition to the medical device footprint we discussed earlier that is maintained by the biomedical or clinical engineering departments. At a high level, to make sure you have appropriate visibility into operational workflows, the ecosystem risk architecture needs to be designed as shown:


Insights from security and device data
Device Utilization
Regulatory Safety & Security Data
Quality of Service Telemetry
Location Tracking
Healthcare Device
Risk & Threat Impact Algorithm
Biomed / Clinical Engineering
Facilities Mgmt Physical Security
Outsourced Healthcare Services
Business owners outside IT forr devices

Using this approach to design use cases and data visualization out of the security architecture allows for real time visualization of impact to clinical and facility operations.

PRACTICING THE THEORY

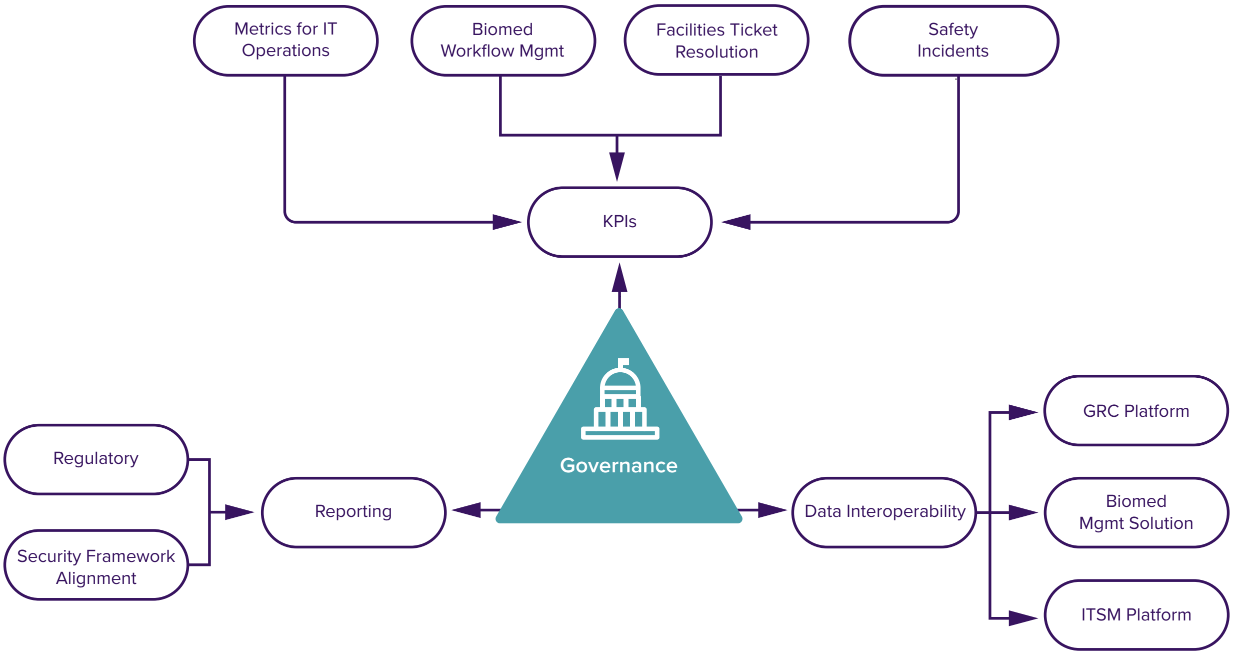
All of the concepts presented thus far are theoretical approaches to classify and analyze risk. To get the most out of and operationalize this process, appropriate testing methodologies need to be implemented that encompass:

- Alignment of security incident response to emergency response frameworks (e.g. H-ICS, NIMS etc)
- Scheduled and ad hoc table top drills walking through response scenarios for security incident-based and operational workflow-induced situations that affect operations
- 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 proper development of muscle memory for IT and information security responders and helps baseline true time estimates for incident response and recovery. Using the emergency response frameworks also standardizes data that can be shared with federal agencies and law enforcement if needed.

Realistic performance management

Strategic programs like medical device security initiatives warrant appropriate governance due to their scope and reach into the organization. To help showcase success and demonstrate elevated capability of the risk management function as it pertains to ROI, three areas of consideration -KPIs, Reporting and Data interoperability are shown below:

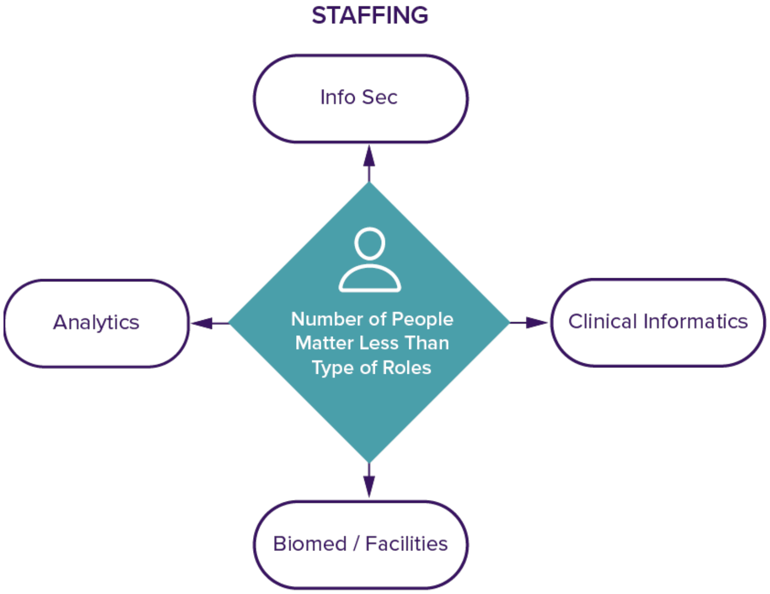


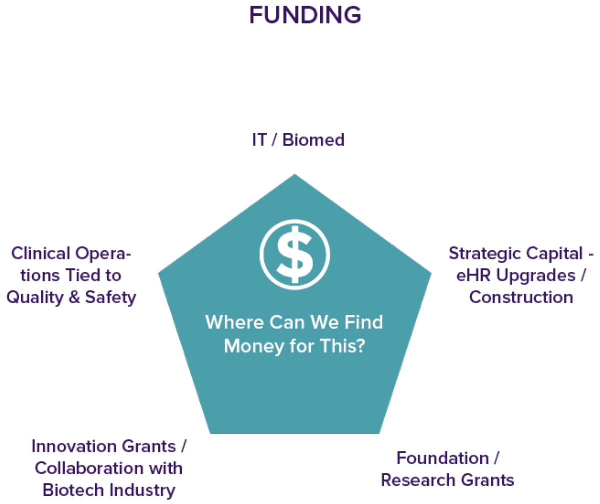
Focusing efforts for real-time reporting and integrations with IT operations can help with reduction in help desk response times and increased efficiency of analyst workflows to provide operational cost savings. From a biomed and facilities context, these integrations can help streamline cross-facility 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 costs savings.

Staying ahead of resource implications

The focus around financing of a medical device security strategy has historically been around the burden of technology. Ironically, that is the one piece of the pie that has the least amount of inertia thanks to innovations in cloud technology, behavioral baselining leveraging advanced models for machine learning, and configuration data for billions of devices that can be accessed in a matter of seconds.

The rest of the program elements are a different story. Let's showcase resourcing best practices and tips and tricks for financing an operational program as opposed to just focusing on the implementation of a tool.




FUNDING
IT / Biomed
Clinical Operations Tied to Quality & Safety
Where Can We Find Money for This?
Strategic Capital - eHR Upgrades / Construction
Innovation Grants / Collaboration with Biotech Industry
Foundation / Research Grants

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 physical 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 FTE's whether organically or from a partnership with a managed service provider. This will need to be augmented from expertise from departments illustrated in the diagram so that appropriate data reporting and use case functionality can be designed before a technology is purchased and that alignment to clinical and operational use cases as showcased in this paper can be realized.

FINAL THOUGHTS

In the near future, to implement realistic and effective medical device security strategies, healthcare organizations will need to account for:

- Appropriate scope that is tied to clinical and operational strategy aligned with revenue targets
- Understanding risk profiles that take into account both legacy debt and innovative approaches to the aforementioned device ecosystems
- Organizationally introspective threat modelling that accounts for nuances within departmental workflows and appetite for change
- Investigation into human factors as they relate to pivoting of security operations functions to support resiliency and deal with the data deluge/alarm fatigue that occurs when you first begin this journey
- Visibility to the expanded attack surface that comes when the elements of the device ecosystem connect directly to hospital networks and the Internet
- Understanding the capabilities that Managed Security Service Providers (MSSP) as well as Managed Detection and Response Providers (MDRP) bring to the table and how it can be used as a catalyst to bridge operational impact scenarios along with information security practice improvements

The IoT and connected device ecosystem will continue to evolve how we leverage these devices within the industry today. Starting with wearable sensors, we are now seeing increased usage of augmented reality, nanotechnology, smart sensors with voice recognition, and robotics. While all of these innovations will yield remarkable improvements to the quality of care, we need to see how the security industry comes to terms with designing appropriate architectures to identify threat models that have not yet been identified.

The term “it takes a village” applies perfectly in this situation as these issues cannot be solved with just HDOs or medical device manufacturers. The good news is that cross-industry workgroups who design these practices have already started to work together including a fair amount of collaboration internationally as well. Where we need to see momentum is on investment. Not only in designing new solutions, but in helping organizations understand that medical device security, at its core, is an exercise for improving resilience, rather than a compliance exercise to protect data.

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

20210729-1