Optimizing Best Practices Through Risk Analysis

As a participant in the Health and Public Health Sector Coordinating Council's Joint Cybersecurity Work Group, Clearwater fully supports the 405(d) Task Group's "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)" recommendations.

Even in the most mature organizations, these best practices and tools are often not implemented for every system or device across the enterprise. Furthermore, different systems and their components may require different security controls based on their unique attributes. In today's complex IT environment, with too few available resources and dollars for cybersecurity, how does an information security leader decide what to address first and how best to reduce risk?

Foundational to a good security program is an enterprise-wide, information system-based security risk analysis. A risk analysis will identify and evaluate the applicable vulnerabilities and threats for each system based on its profile, as well as which controls are in place to address these scenarios.

Leading healthcare organizations following a best practices approach are utilizing cyber risk management software as a service to facilitate a comprehensive enterprise-wide risk analysis and risk response process. As a result, they are identifying their highest risks, optimizing deployment of security controls, and measuring progress, resulting in greater risk reduction at lower costs.

Steven R. Cagle
CEO
Clearwater - IRM|Pro®
steve.cagle@clearwatercompliance.com

How Aligned Are Provider Organizations with the Health Industry Cybersecurity Practices (HICP) Guidelines?

A KLAS-CHIME WHITE PAPER

The 405(d) Task Group—convened by HHS following the Cybersecurity Act of 2015—recently released "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients" (HICP), a document containing recommendations for provider organizations on how they can reduce and mitigate their cybersecurity risks.

CHIME HealthCare's most wired™

KLAS®

CLEARWATER

HICP identifies 10 overarching cybersecurity practices that organizations of all sizes should focus on. For each practice, subpractices based on organization size are also outlined. The 10 overarching cybersecurity practices are:

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

Where do provider organizations stand today in their adoption of these best practices? To answer this question, KLAS and CHIME analyzed responses from the 600+ healthcare organizations that participated in the 2018 Healthcare's Most Wired survey. Though that survey and the HICP guidelines do not overlap in every regard, this white paper explores adoption of those HICP guidelines that were measured by the Most Wired survey. This analysis was augmented by provider commentary and data collected by KLAS via other research efforts.

Key Findings

Regardless of size, **most organizations have deployed email and endpoint protection systems**, establishing an initial layer of defense against internal and external threats.

Many **organizations are transitioning from homegrown identity and access management (IAM) solutions to commercial solutions** to support their identity policies. Multifactor authentication (MFA) remains a gap for half of small organizations.

Data-loss prevention (DLP) solutions have been widely adopted, though **deployment of on-premises DLP solutions has slowed as organizations have transitioned to the cloud.** Organizations are more likely to back up data in a physical location than to use cloud backup services.

Today's security requirements are challenging historical asset management practices, making it increasingly necessary for organizations to establish clear policies that align their IT, information security, healthcare technology management, and procurement teams.

Most organizations have network access control (NAC) solutions to monitor devices that connect to their networks; however, **less than half of small organizations are using network segmentation** to control the spread of infections.

Large organizations report more sophisticated and more frequent vulnerability scanning and application testing. **Small organizations more frequently turn to penetration testing** to identify vulnerabilities.

Most organizations have an incident-response plan in place and participate in an information sharing and analysis organization (ISAO); **only half of organizations conduct an annual enterprise-wide exercise** to test their plan.

Medical device security remains a top concern for organizations as they weigh patient-safety risks. Their medical-device-security programs are often supported by strong cybersecurity practices in other areas.

Small organizations are less likely to utilize cybersecurity policies such as a dedicated chief information security officer (CISO), board-level committees and governance, risk management, and compliance (GRC) committees, and bring-your-own-device (BYOD) management.

Author
Dan Czech
dan.czech@KLASresearch.com

To view the full report, visit
www.klasresearch.com/reports

1 Email Protection Systems

Email Protection System Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
1.S.A Email system configuration	1.M.A Basic email protection controls	1.L.A Advanced and next-generation tooling
1.S.B Education	1.M.B Multifactor authentication for remote email access	1.L.B Digital signatures
1.S.C Phishing simulation	1.M.C Email encryption	1.L.C Analytics-driven education
	1.M.D Workforce education	

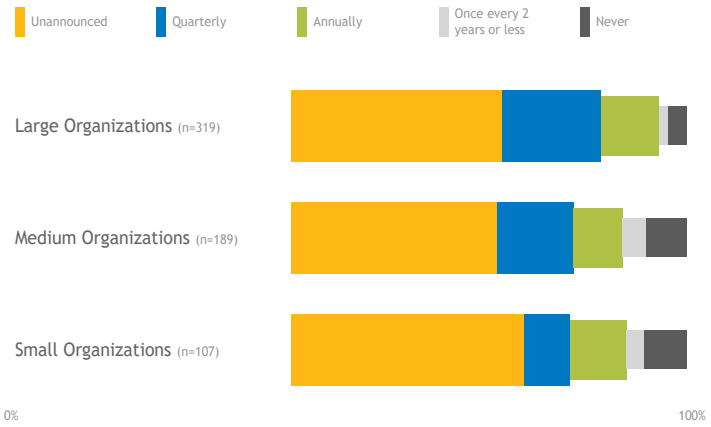
Email is the most common attack vector through which healthcare organizations are put at risk. Email protection systems provide filtering and encryption to minimize external threats, like phishing or ransomware attacks, and mitigate internal risks, whether malicious or unintentional. Every organization needs email protection from either their default email provider, such as Microsoft Office 365, or from external email protection tools, such as Proofpoint, Mimecast, and Zix.

Since email is a necessary, but high-risk, form of communication, email-security strategies are considered table stakes at most healthcare organizations. Therefore, the Most Wired survey does not collect in-depth data on email security. However, some data is collected that applies to the Task Group recommendations regarding workforce education and the use of digital signatures.

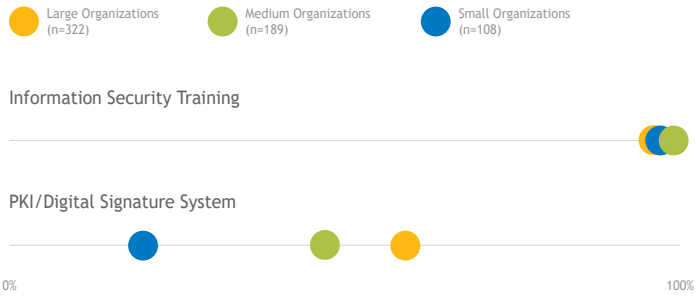
The Task Group recommends that organizations conduct monthly phishing simulations, which often include on-the-spot workforce training. Over 70% of organizations that participated in the Most Wired survey conduct such simulations at least quarterly, with many doing it more frequently. However, there is room for industry improvement since about 16% of small and midsize organizations do not conduct phishing simulations at all or do them less than once a year. The Most Wired survey also measured the use of digital signatures, which allow users to verify that emails come from trusted sources and have not been manipulated in transmission. Large organizations are three times more likely to have adopted this technology than their smaller counterparts.

"We are using [our vendor's] complete service to remove spam and malicious email out of the environment. The service works extremely well. The level of spam that is entering our users' mailboxes is extremely low. The speed at which [our vendor] evolves around spam campaigns is tremendous. The technical completeness of the service is really amazing. [Our vendor] has helped us implement encryption in such a way that we get minimal pushback from users. If a user is being forced to come back to the portal to pull an email, the interface is still very good. The user experience is positive, so people don't hate [our vendor] like they hate other email security products. ***The main outcome we have seen is the reduction in spam and malicious email.*** *" - Manager, IT Security, Large Organization*

Frequency of Phishing Exercises



Adoption of Email Protection Technologies/Policies



2 Endpoint Protection Systems

Endpoint Protection System Subpractices—by Organization Size

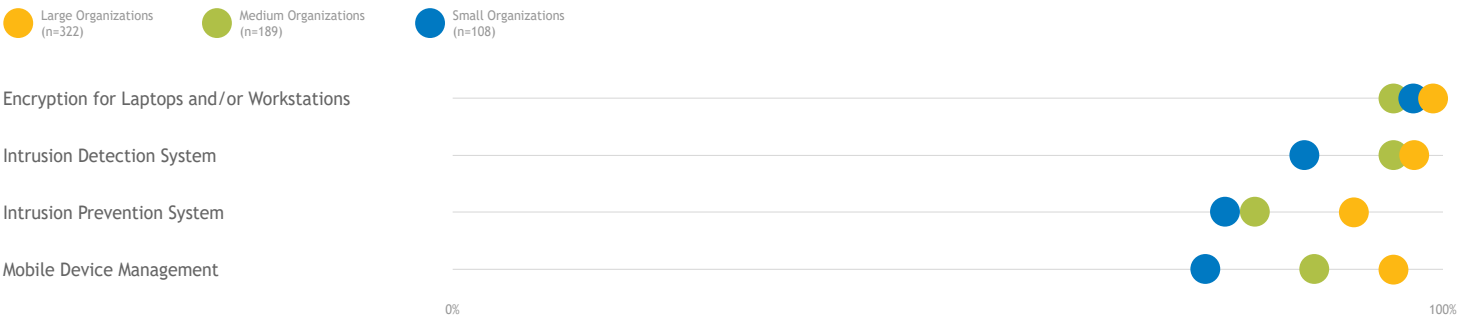
Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
2.S.A Basic endpoint protection	2.M.A Basic endpoint protection controls	2.L.A Automate the provisioning of endpoints 2.L.B Mobile device management 2.L.C Host-based intrusion detection/ prevention systems 2.L.D Endpoint detection and response 2.L.E Application whitelisting 2.L.F Microsegmentation/ virtualization strategies

While email remains the top attack vector, the increasing mobility of the workforce makes endpoints just as critical for healthcare organizations to secure against client-side ransomware attacks or the theft/loss of equipment, PHI, and other sensitive data. The use of antivirus software is one of the most basic ways to protect endpoints, but the Most Wired survey didn't ask about this method due to its ubiquitous deployment.

Nearly all surveyed organizations report that they currently use endpoint encryption, a simple and relatively inexpensive protection method. While most organizations have implemented intrusion-detection and -prevention systems, about 20% of small organizations have not implemented this first line of defense. The majority of surveyed organizations have implemented mobile device management to secure both hospital-owned and BYOD smartphones and tablets, though the opportunity remains for additional organizations to implement this software. Doing so ensures that PHI remains containered on devices and that organizations have the ability to wipe a device—or a portion of a device—should it become lost or even become disconnected from a secured hospital network.

"[Our vendor] has been an extremely good MDM solution for our hospital. The container functionality makes it easy to manage our hospital-owned devices, and the SMS requirements are rock solid. We are also using [our vendor] with BYOD. We have to ask our BYOD users to jump a few hurdles, but the product does a good job with separating personal data from hospital data and forcing strong passwords. The separation of data gives us some ability to wipe a mobile device if it is lost or stolen. With [our vendor], we are doing all we can do to contain the mobile devices that are being used in our hospital."—CISO, Large Organization

Adoption of Endpoint Protection Technologies



3 Access Management

Access Management Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
3.S.A Basic access management	3.M.A Identity 3.M.B Provisioning, transfers, and deprovisioning procedures 3.M.C Authentication 3.M.D Multifactor authentication for remote access	3.L.A Federated identity management 3.L.B Authorization 3.L.C Access governance 3.L.D Single sign-on

Identity and access management (IAM) technology is becoming increasingly important for healthcare organizations as they attempt to balance security needs with end users' desires for quick system access. 83% of surveyed organizations have implemented single sign-on (SSO) solutions, which enable quick and easy access to multiple systems with a single login. Healthcare IAM is made even more complex by the fact that a single user may have different roles and need to be provisioned with different levels of access at different times.

While there is some opportunity for smaller organizations to increase adoption of strong password requirements, most organizations report adoption of thorough basic access management policies. Many organizations are making the transition from homegrown IAM technologies to third-party tools, with large organizations significantly more likely to have implemented identity management and provisioning tools. Organizations that did not clearly establish and document which IAM policies they wished to support with these tools report having more challenging implementations.

Phishing scams are proving more successful at compromising users' credentials, increasing the need for multifactor authentication (MFA) so that stolen credentials can't be used to access PHI. Less than half of smaller organizations have an MFA solution in place today. Regardless of size, organizations report little adoption of adaptive/risk-based authentication, which requires additional verification based on the risk level of the action being attempted.

Adoption of IAM Technologies/Policies

"The strengths of [our product] are the integration to other applications and the analytics and compliance pieces that allow us to see who has accessed different systems in order to recertify them. We brought in [our vendor] and kicked off our IAM project so that we could ensure that the right people have the right access at the right time. We don't want to overprovision or allow people to retain access if their roles change. It will take us some time to get to that point. ***We are changing our culture, and [our product] is an incredible engine, but most companies can't use it fully because they have to change their culture****. Those organizations would be very disappointed if they thought the solution would solve all their problems. We used a third party that really knew how to reengineer our processes."—Cybersecurity Program Manager, Large Organization*

4 Data Protection and Loss Prevention

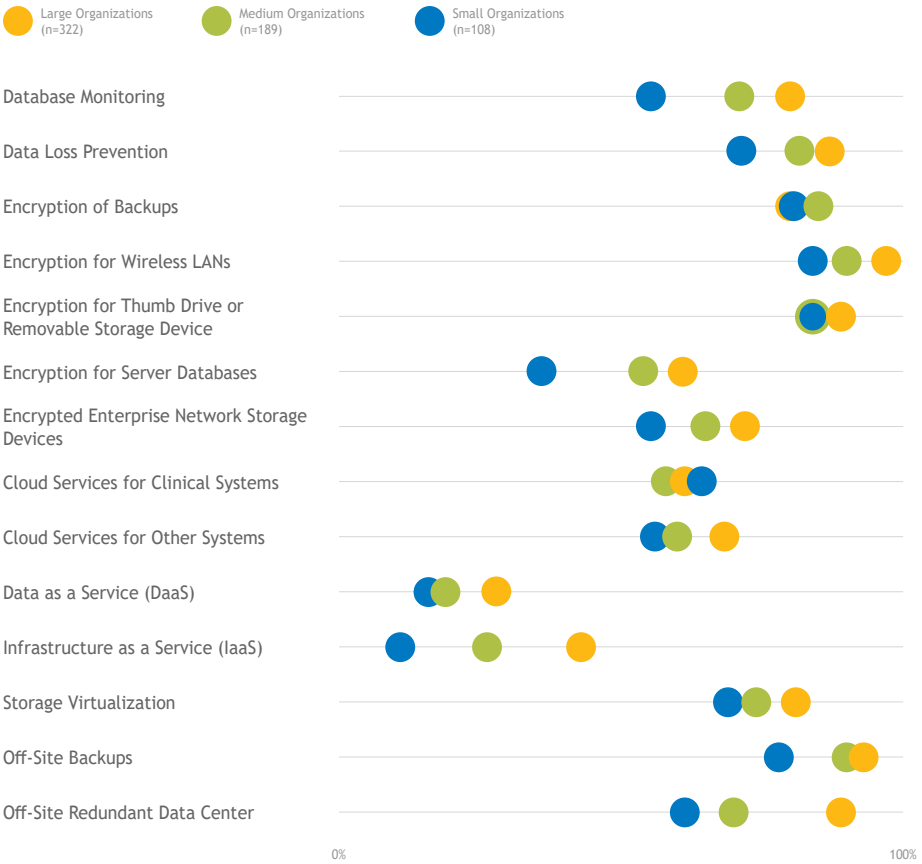
Data Protection and Loss Prevention Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
4.S.A Policy	4.M.A Classification of data	4.L.A Advanced data loss prevention
4.S.B Procedures	4.M.B Data use procedures	4.L.B Mapping of data flows
4.S.C Education	4.M.C Data security	
	4.M.D Backup strategies	
	4.M.E Data loss prevention	

As the healthcare industry moves toward increased interoperability, it is becoming increasingly important for organizations to make sure patient data is shared in a safe and secure way. Policies and procedures for protecting data at rest, data in use, and data in motion form the basic foundation for data-loss prevention (DLP), and technology solutions are then used to support these policies. While the Task Group characterized DLP tools as a subpractice for medium and large organizations, the majority of surveyed organizations, including over 70% of small organizations, report having a DLP tool in place, though small organizations' DLP implementations are more likely to be limited in scope. Organizations' whose DLP deployments include exact data matching or fingerprinting are more likely to be satisfied with their tools and to report low levels of false positives. As data and applications continue to move to the cloud, some organizations express hesitation to further deploy on-premises DLP solutions.

The majority of organizations encrypt data in multiple ways, though the encryption of server databases and enterprise network storage devices is less common, especially in small organizations. All surveyed organizations report backing up their data; off-site backup strategies and redundant data centers are more commonly employed than cloud backup services. Very few small organizations report using Data or Infrastructure as a Service; while medium and large organizations are more likely to use these services, adoption is still limited.

Adoption of DLP, Encryption, and Data Backup Technologies/Policies



"We have used [our vendor's] software for a long time, so we are mature users. Their exact data match feature is unique among vendors, and we have long believed that [our vendor] is our only option for DLP. Some vendors just can't fulfill their promises for exact data matching. ***We adopted that functionality a long time ago because of the PHI in our environment, and it helps us to be much more accurate with our alarms and triggers****. If something triggers an alarm for bad encryption or a DLP event, we can investigate it and block it. The system makes our decisions much more accurate."*
—CISO, Large Organization

5 Asset Management

Asset Management Subpractices—by Organization Size

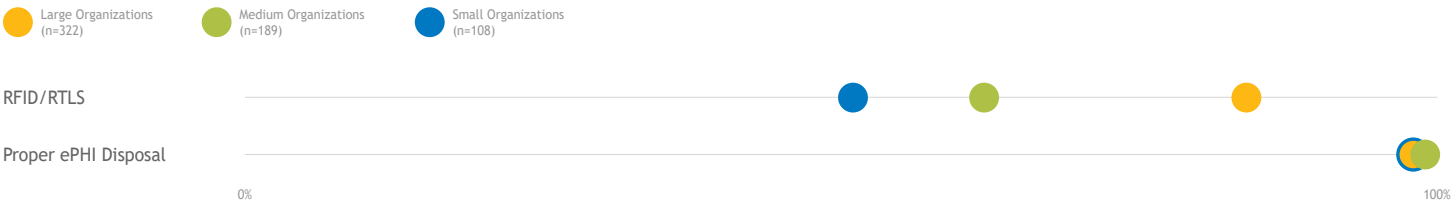
Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
5.S.A Inventory	5.M.A Inventory of endpoints and servers	5.L.A Automated discovery and maintenance
5.S.B Procurement	5.M.B Procurement	5.L.B Integration with network access control
5.S.C Decommissioning	5.M.C Secure storage for inactive devices	
	5.M.D Decommissioning assets	

Historic asset management practices (i.e., practices that include simply tracking purchased devices) are insufficient for today's security environment. Organizations must have insight into devices' operating systems, MAC and IP addresses, recent users, locations, patching information, and much more. And in order for organizations to blend security best practices into their IT asset management, the IT, information security, healthcare technology management, and procurement teams need to all be on the same page and working toward the same common goals.

While the Most Wired survey collected relatively little information about organizations' asset-management practices, nearly all organizations report proper disposal of PHI-containing assets. There is room for improvement when it comes to having real-time device-location data—only 50% of small organizations and 60% of midsize organizations use RFID/RTLS technology to identify and track assets. (Additional context regarding asset management struggles is included in section 9 on medical device security.)

"We mainly use [our vendor] for tracking assets when a piece of equipment is due for maintenance or when we have a recall or an upgrade. Our department is responsible for most of the portable medical equipment that we give out to customers. It should be very simple to get that equipment back and get it reprocessed, but customers hold on to things, and they don't send them back. We were sending people out at 2 a.m. when everyone was gone to go open every door and every drawer to find equipment. We don't have to do that anymore. Today, we go to the RFID system and look for specific pieces of equipment, and then we send somebody out to find it. ***We are now able to meet our deadlines nearly all of the time, compared to 50% of the time before we got [our vendor].*** *If I have a piece of equipment worth three million dollars, I will get my money's worth from [our vendor] just on that one piece."*
—Director of Biomedical Engineering, Medium Organization

Adoption of Asset Management Technologies/Policies



6 Network Management

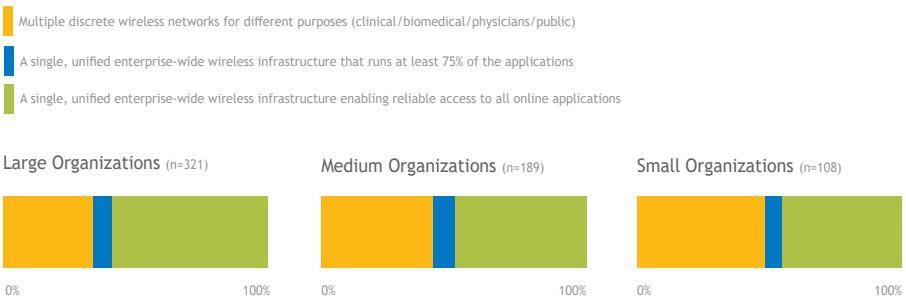
Network Management Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
6.S.A Network segmentation	6.M.A Network profiles and firewalls	6.L.A Additional network segmentation
6.S.B Physical security and guest access	6.M.B Network segmentation	6.L.B Command and control monitoring of perimeter
6.S.C Intrusion prevention	6.M.C Intrusion prevention systems	6.L.C Anomalous network monitoring and analytics
	6.M.D Web proxy protection	6.L.D Network-based sandboxing/malware execution
	6.M.E Physical security of network devices	6.L.E Network access control

Networks support connections and the movement of data between systems, but if not properly deployed and managed, they can also enable cyberattacks to spread and gain access to many sources of PHI. Large organizations are more likely to have a single, enterprise-wide wireless infrastructure, while small and midsize organizations are more likely to have multiple discrete networks deployed for different purposes. Regardless of the number of networks deployed, it is critical for organizations to implement proper segmentation to keep the impact of an attack isolated to specific portions of the network.

The Task Group prioritizes network segmentation for small organizations, yet less than half report segmenting their networks today. Use of firewalls and physical device security is widespread across all organization sizes. Network access control (NAC) systems—which automatically profile new assets that connect to the network—help ensure that proper security controls are applied prior to a device being granted access. Across all sizes, the majority of surveyed organizations have implemented the Task Group's suggested focus for large organizations on anomalous-behavior detection to catch and quarantine abnormal events.

Wireless Infrastructure Setups in Use



> *"We have a strategy around devices that can't be patched. We are doing network segmentation through [our vendor's] product for those devices. Devices that meet requirements are okay and have lower risk assessments, so those can move forward.* ***In general, if devices don't meet our requirements, they don't go on the network****. We just segment them through [our vendor's] product."* —Information Security Systems Director, Large Organization

Adoption of Network Management Technologies/Policies

7 Vulnerability Management

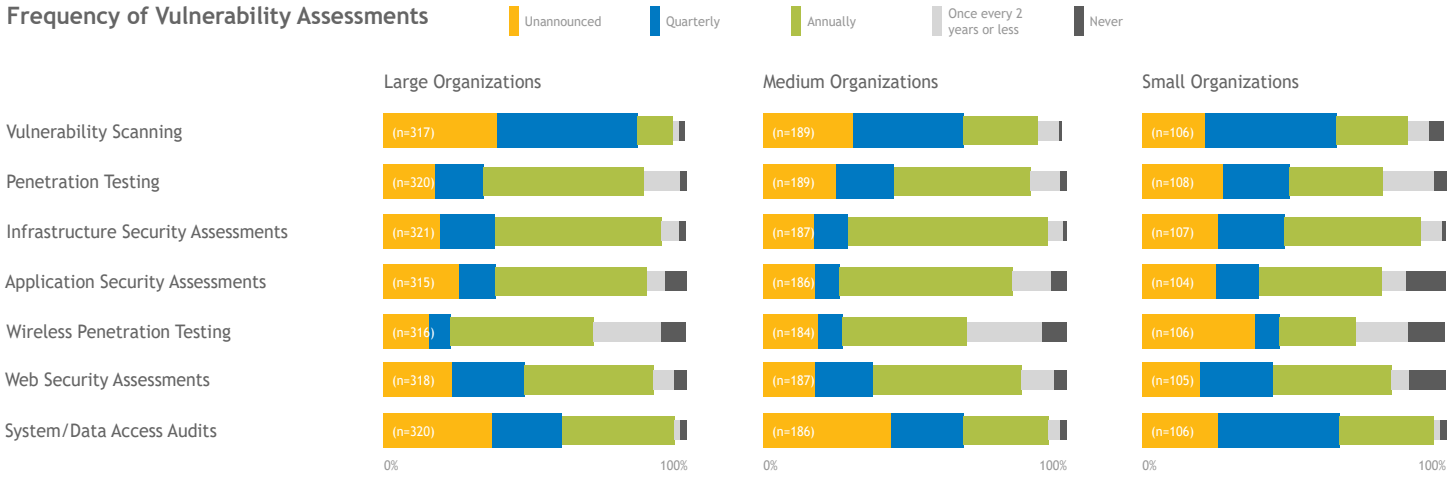
Vulnerability Management Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
7.S.A Vulnerability management	7.M.A Host/server-based scanning 7.M.B Web application scanning 7.M.C System placement and data classification 7.M.D Patch management, configuration management, and change management	7.L.A Penetration testing 7.L.B Remediation planning

Vulnerability management includes scanning for and identifying potential vulnerabilities as well as establishing policies for how to prioritize and remediate vulnerabilities once discovered. About 90% of large organizations run vulnerability scans at least quarterly; 60% of small and midsize organizations do so. Few organizations conduct web-security, infrastructure-security, or application-security assessments more than once a year. Augmenting a robust vulnerability-scanning program with penetration testing by internal or external teams can help organizations look deeper for vulnerabilities. Though the Task Group recommends penetration testing as a practice for large organizations, small organizations are the most likely to perform general penetration tests or wireless penetration tests at least once a quarter. Once vulnerability assessments have been performed, nearly all organizations report their progress and remaining gaps to leadership. Resource constraints keep some small organizations from involving multiple business units in their remediation work once the gaps have been identified.

> *"We are leveraging [our product] for vulnerability scans across the health system. We are also using it as an internal scanner, and we are forwarding all the logs to our analytics platform so that we have more information to review and analyze to do better threat hunting. Every log goes into [our product], and then it gets forwarded to the analytics platform for further review. When things are highly critical, we forward them to the analytics platform to make sure we have the data we need to hunt threats and see lateral movement."* —Vice President, Information Security/HIPAA Security Officer, Large Organization

Frequency of Vulnerability Assessments



Vulnerability Assessment Follow-Up Plans

8 Incident Response

Incident Response Subpractices—by Organization Size

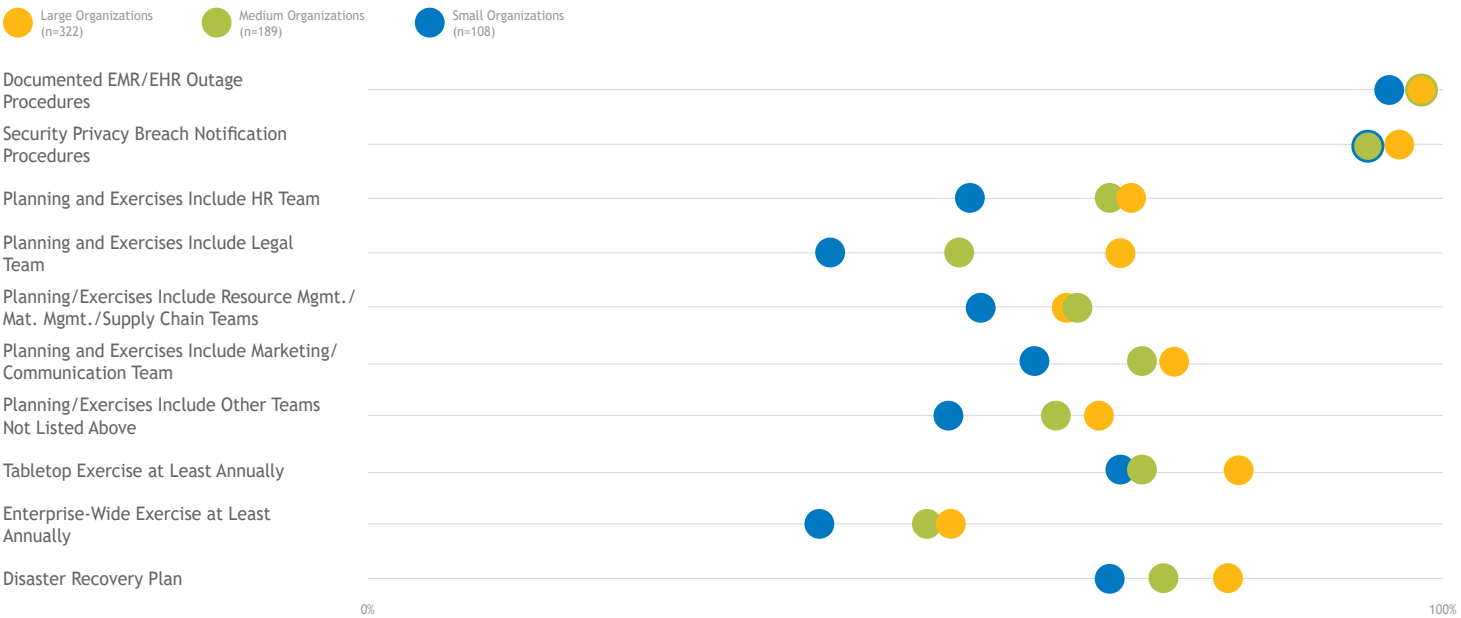
Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
8.S.A Incident response	8.M.A Security operations center	8.L.A Advanced security operations centers
8.S.B ISAC/ISAO participation	8.M.B Incident response	8.L.B Advanced information sharing
	8.M.C Information sharing/ISACs/ISAOs	8.L.C Incident response orchestration
		8.L.D Baseline network traffic
		8.L.E User behavior analytics
		8.L.F Deception technologies

Organizations of all sizes should have an incident-response plan outlining policies and practices for quickly and efficiently isolating and mitigating adverse security events. These plans should involve all applicable hospital departments and should include guidelines for proper notification should a breach occur. Most organizations have a plan in place and conduct annual tabletop exercises to practice and refine their plans. Only about half of organizations conduct an annual enterprise-wide test. Nearly all organizations participate in an information sharing and analysis organization (ISAO) that helps organizations escalate known threats and share best practices for protection. Large organizations are most likely to participate with the Health Information Sharing and Analysis Center (H-ISAC); small organizations are more likely to look to nearby HIE partners rather than national ISAOs.

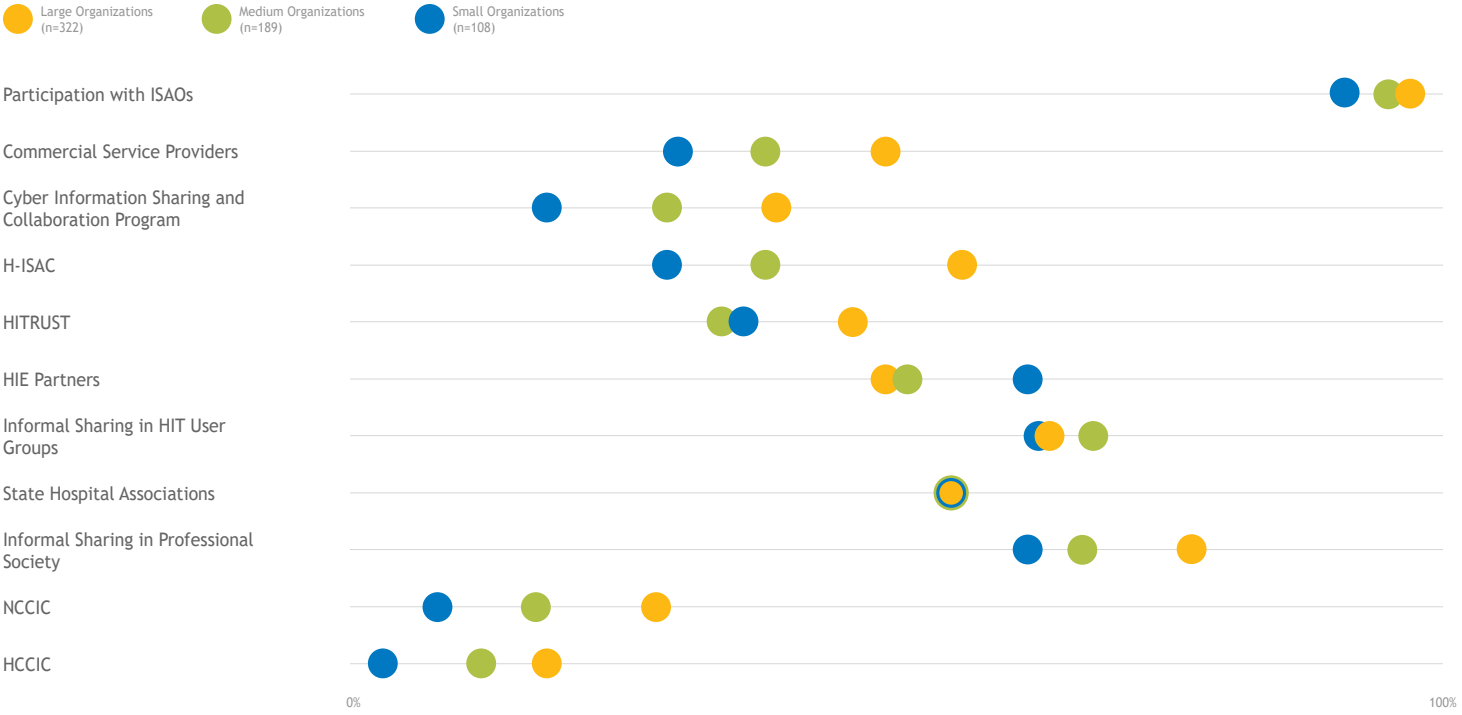
While the Most Wired survey didn't ask about participation in a security operations center (SOC)—insourced, outsourced, or hybrid—it did ask organizations about their adoption of security information and event management (SIEM) tools and user-behavior analytics (UBA) for providing analytics to their SOC. While most organizations have SIEM tools in place, adoption of UBA tools is still early; large organizations are more likely to have adopted this technology, but less than half have it in place today.

***"The ability to detect and respond to incidents is the biggest outcome we achieve using [our SIEM product]**. Whether we find the most important things depends on the content we write. We use a third party to manage [our product] because they deliver a lot of our content. The product does a very good job of correlating alerts very quickly based on the content we have developed. [Our product] works extremely well."* —Manager, IT Security, Large Organization

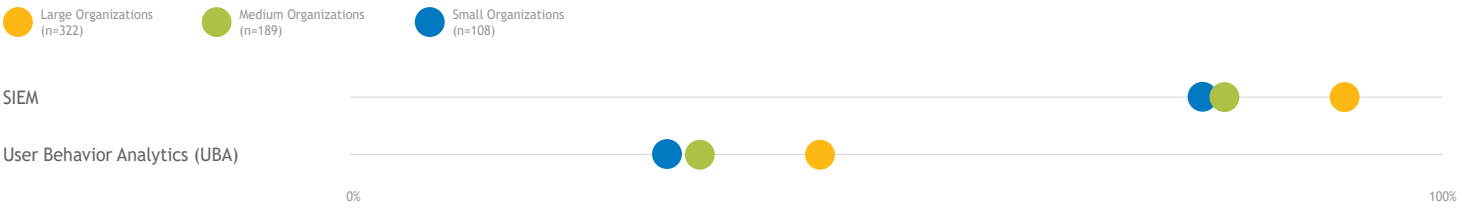
Adoption of Incident Response Plan Components



ISAO Participation



Adoption of Analysis Tools



9 Medical Device Security

Medical Device Security Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
9.S.A Medical device security	9.M.A Medical device management 9.M.B Endpoint protections 9.M.C Identity and access management 9.M.D Asset management 9.M.E Network management	9.L.A Vulnerability management 9.L.B Security operations and incident response 9.L.C Procurement and security evaluations 9.L.D Contacting the FDA

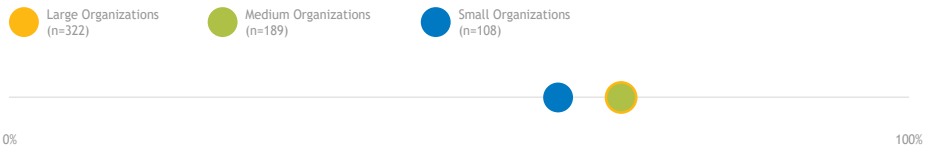
While the Most Wired survey asked relatively few direct questions about medical device security, it is a top concern for organizations due to the inherent security challenges presented by FDA-approved devices and the potential for device breaches to affect patient safety.

The Task Group's recommendations for securing medical devices include specific applications of technologies already mentioned, such as endpoint protection, IAM, asset management, network management, and vulnerability management. While medical devices may present a few unique security challenges given their lengthy life cycle, organizations that properly apply security technologies and policies for their medical devices gain confidence in their ability to protect patient safety.

Across organization sizes, the top medical-device-security struggles reported include (1) out-of-date operating systems that organizations cannot patch and (2) a lack of asset and inventory visibility due to insufficient tools and the large number of devices that must be secured. Additionally, many organizations haven't formalized internal ownership of medical device security and are just beginning to bring security into the medical-device procurement process, including pre-purchase risk assessments, MDS2 forms, software bills of materials, and patching provisions.

Large organizations are more likely to have invested in technology to support their medical device security programs, while small organizations report a high level of confidence in their ability to protect patient safety and secure devices due to lower device volumes and strong internal policies.

Medical Device Password/Access Controls Usage



"The biggest issue is inventory management. Even when I feel good about the inventory, I always ask the team whether things are current. We are always worried about missing a category of devices. The devices can be infested with all kinds of vulnerabilities or other problems, ***but I am confident that if I know about something and where it is, I can take care of it. The things I don't know about are what worry me."*** —CISO, Large Organization

10 Cybersecurity Policies

Cybersecurity Policies Subpractices—by Organization Size

Small Organizations 1-50 beds	Medium Organizations 51-300 beds	Large Organizations >300 beds
10.S.A Policies	10.M.A Policies	10.L.A N/A*

*The Task Group did not offer specific subpractices for large organizations different from those recommended for small and medium organizations.

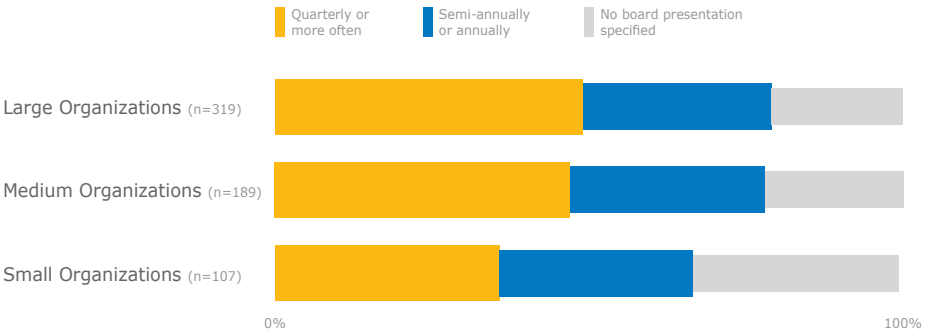
Successful cybersecurity programs are not based on technology alone—rather, they are based on policy and supported by strong technology. While various policies underly each of the previous nine cybersecurity practices, organizations' overall security policies should include the following elements: proper classification of data; definition of roles and responsibilities within the organization (including proper governance); employee education; definition of acceptable data and tool usage; definition of proper use of personal and employer-provided devices; and creation of a cyberattack response plan.

Small and medium organizations are nearly four times as likely to lack a CISO at their organization compared to large organizations. Nearly half of medium and large organizations have cybersecurity as a topic at board meetings at least quarterly. While most organizations have a governance, risk, and compliance (GRC) committee in place, less than half of organizations (and fewer than one in five small organizations) have a board-level committee overseeing their cybersecurity program.

Small organizations are far less likely than medium or large organizations to have implemented a BYOD program at their organization, though the majority do have an MDM program in place.

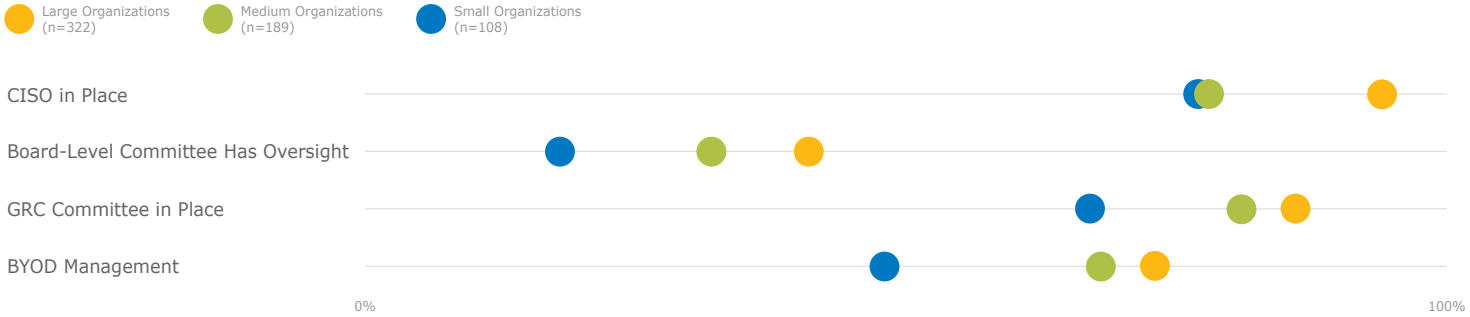
When selecting a framework to support their policies, organizations predominately turn to the NIST Cybersecurity Framework as the industry standard. However, other frameworks (such as the HITRUST CSF) are in use, and several organizations use a combination of industry standards to develop their programs. About one in five small and medium-sized organizations use self-developed frameworks.

How Often Is Security an Agenda Item at Board Meetings?

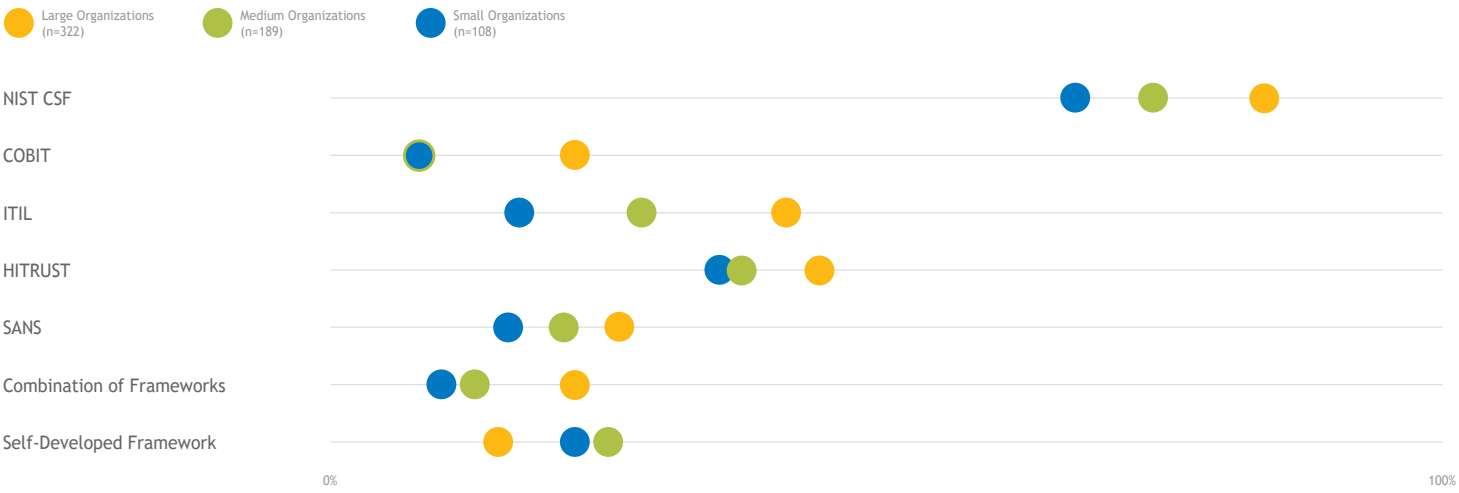


"[Our product] has been fine. We don't have complaints about it, and we have pretty good user adoption. The support has also been good. I would score [our vendor] pretty well on all of their functionality. ***They leverage the appropriate framework****, and we are able to leverage the tool to install other applications.* ***We can support our policies across the array of devices out there.****"* —Senior Director of HIM/Information Privacy & Security Officer, Large Organization

Adoption of Cybersecurity Leadership and Policies



Adoption of Security Frameworks



Conclusion

The HHS Task Group's cybersecurity practices provide a strong, comprehensive foundation from which organizations can build cybersecurity programs and policies and then augment those policies with technology. For many practices, industry adoption aligns with the Task Group's recommendations. However, opportunities for improvement exist, especially among smaller organizations, where budget constraints and a lack of qualified talent are more likely to hinder progress.

CHIME HealthCare's most wired™

The College of Healthcare Information Management Executives (CHIME) is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,700 members in 51 countries and over 150 healthcare IT business partners and professional services firms, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of information management to improve the health and healthcare in the communities they serve. For more information, please visit chimecentral.org.

KLAS®

Using the voice of healthcare software and services customers, KLAS has measured healthcare IT vendor performance since 1997. Today, KLAS collects and publishes customer feedback on over 800 products and services. Roughly 30,000 providers work with KLAS each year. Since healthcare IT is often a nuanced and complex discussion subject, over 98% of KLAS research is collected in live conversations over the phone, to ensure accuracy and clarity. All interviews are strictly anonymous, and participants are granted broad access to the feedback of other participants. Vendor access to KLAS' findings is available through subscription and individual report purchases.

CLEARWATER

Clearwater is the leading provider of Enterprise Cyber Risk Management and Compliance Solutions for healthcare providers and their partners. Clearwater earned 2018 Best in KLAS Award for Cybersecurity Advisory Services and the 2017, 2018, and 2019 Black Book Award as the #1 client-rated provider of Cyber Risk Management Services in healthcare. Clearwater delivers solutions to hundreds of health systems, health partner organizations, medical device manufacturers, and federal institutions nation-wide. Our complete enterprise cyber risk management solution begins with the most comprehensive, industry-proven risk analysis available, as demonstrated by a 100% OCR acceptance rate.