FORTINET

REPORT

State of Physical Security and Its Convergence with Cybersecurity in Healthcare

Executive Overview

Fortinet recently conducted a survey of leaders from the College of Healthcare Information Management Executives (CHIME) to get a clearer sense of how the convergence of physical and digital security is currently being addressed within organizations around the world.

The collective responses show several current trends regarding security perceptions and preparations in healthcare:

Convergence of Physical Security and Cybersecurity

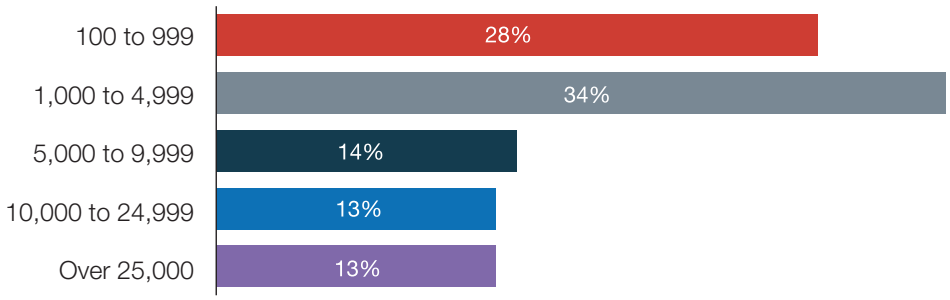
- **Physical-cyber security integration** ranks as a critical or important topic for **75%** of the healthcare IT leaders.
- **Protecting IoMT devices** tops the list of priorities for 2019 at **more than 60%** of organizations.
- **Almost three-quarters** of organizations are still implementing **segmentation** to control IoT/IoMT risks.
- Data from **physical access controls** is not being collected, analyzed, or correlated with network security at a majority (75%) of organizations.
- **Only 8% of organizations are currently using facial and object recognition** for things like identity and access management. Over **half** of respondents think they have a business case for the investment, while others cite budgetary constraints or lack of staff/skills as reasons for not adopting the technology.
- **C-suite-level involvement in physical security issues** is reported at only **31%** of the organizations.

Methodology for This Study

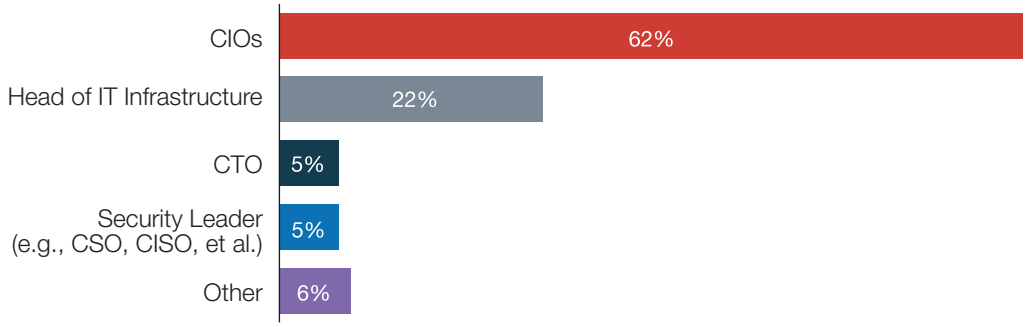
At the end of 2018, Fortinet sent a brief survey to CHIME's membership of global healthcare IT professionals concerning the current state of their organization's cybersecurity initiatives—specifically related to physical security and its convergence with cybersecurity.

Demographic details on the survey participants include:

Organization size. About one-third of the respondents represent midsize organizations with 1,000 to 4,999 employees. More than one-quarter come from large organizations employing 10,000 or more total staff members.



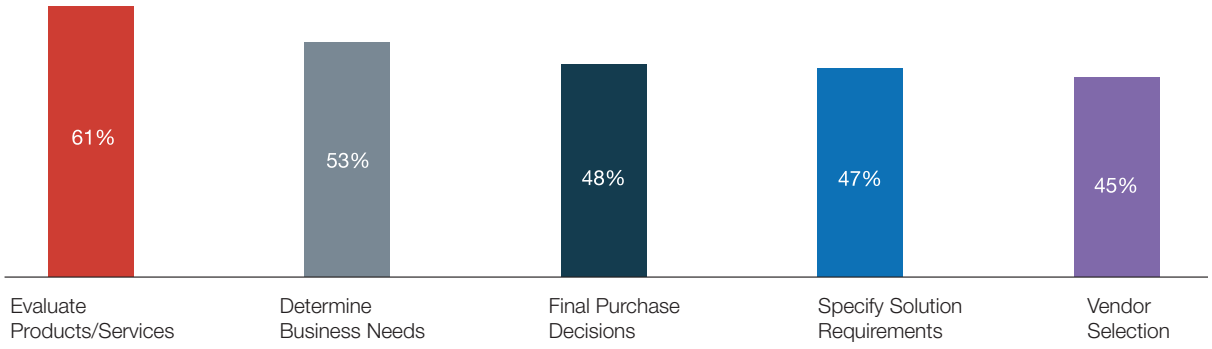
Survey Responses Organization Size



Role and Title of Survey Respondents

Role. CIOs comprise a majority of the respondents. 22% are IT infrastructure leaders. Only 5% hold titles that are specific to the security function.

Responsibilities. A majority of the leaders surveyed report being involved with evaluating products and services for physical security of their operations. More than half are involved with determining business needs and getting internal buy-in beyond the IT team. Making final purchase decisions, specifying solution requirements, and vendor selection also received high rates of response.



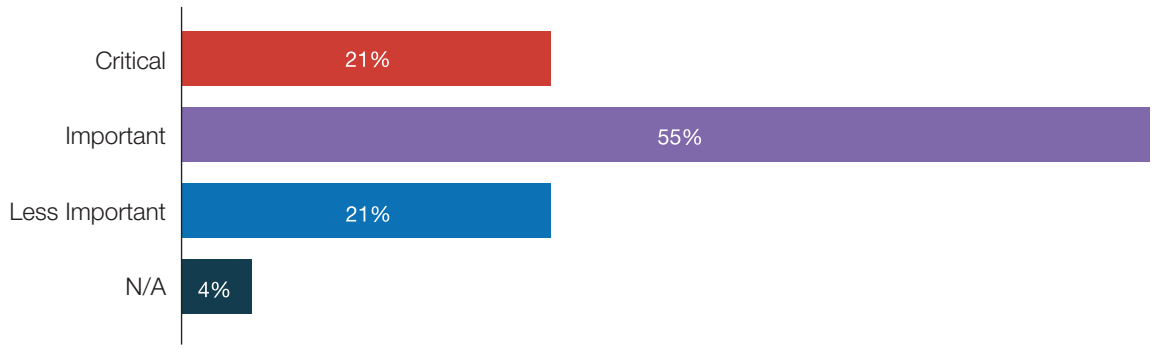
Level of Involvement in Physical Security Solutions

Healthcare Security Trends

Trend: A Strong Desire for Physical-Cyber Security Integration

To combat data theft, physical objects that contain or control patient information must be protected—even if that information is kept offline. Physical security in healthcare includes protection of medical devices, machines, and even paper documents. And there are benefits to connecting physical security (and correlating data) with the network-based systems in charge of cybersecurity.

When it comes to integrating physical security with digital protection via network controls or NGFW security, **three-quarters** of healthcare IT leaders rank this as a "critical" or "important" priority for their organization. Convergence of physical and digital security is seen as "less important" by a minority (21%) and "not applicable" to only 4%.



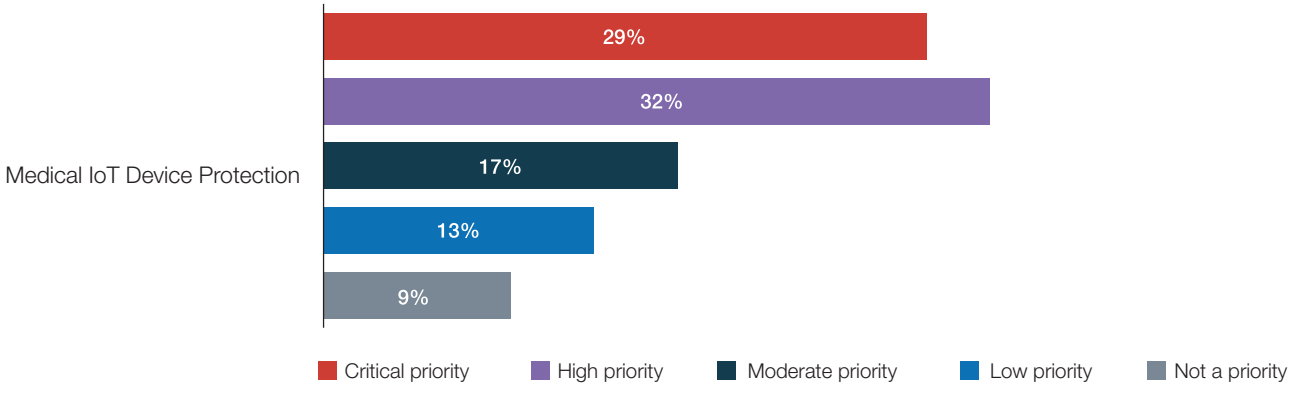
Importance of Integrating Physical Security with Cybersecurity

Trend: Growing IoMT Exposure and Incomplete Segmentation

IoMT devices are rapidly proliferating; an estimated **20 to 30 billion devices** will be online by 2020.[1] Many of these products are designed to travel beyond hospitals—where either physical or digital tampering can occur without any direct oversight of hospital staff. These "headless" devices typically do not have any robust built-in cybersecurity capabilities of their own.

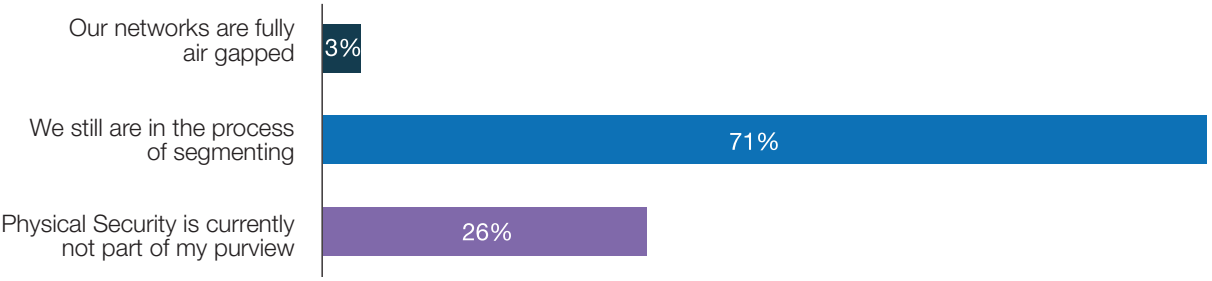
Network segmentation gives healthcare IT teams a comprehensive view of internal traffic, allowing them to detect anomalous activity that might indicate a breach or compromised IoMT device. This visibility allows security to see when devices, data, or malware move laterally into different network segments. **Internal segmentation firewalls (ISFWs)** are designed to detect and stop malicious code from crossing from one segment of the network to another.[2]

Prioritization of security initiatives reveals **IoMT device protection** at the top of the list, with more than 60% of survey respondents ranking it as a "critical" or "high" priority.



Importance of IoMT Device Security for Your Organization

The days of "air gapping" physical security are past: **fewer than 3%** of respondents report having networks that were fully air gapped for physical security protection of IoT endpoints. And a clear majority (71%) indicate they are still segmenting their network to protect against IoT/IoMT-based threats. Perhaps even more troubling, another one-quarter were unable to answer the question of whether or not these devices are secure because they fall under the category of "physical security"—which is beyond their purview.

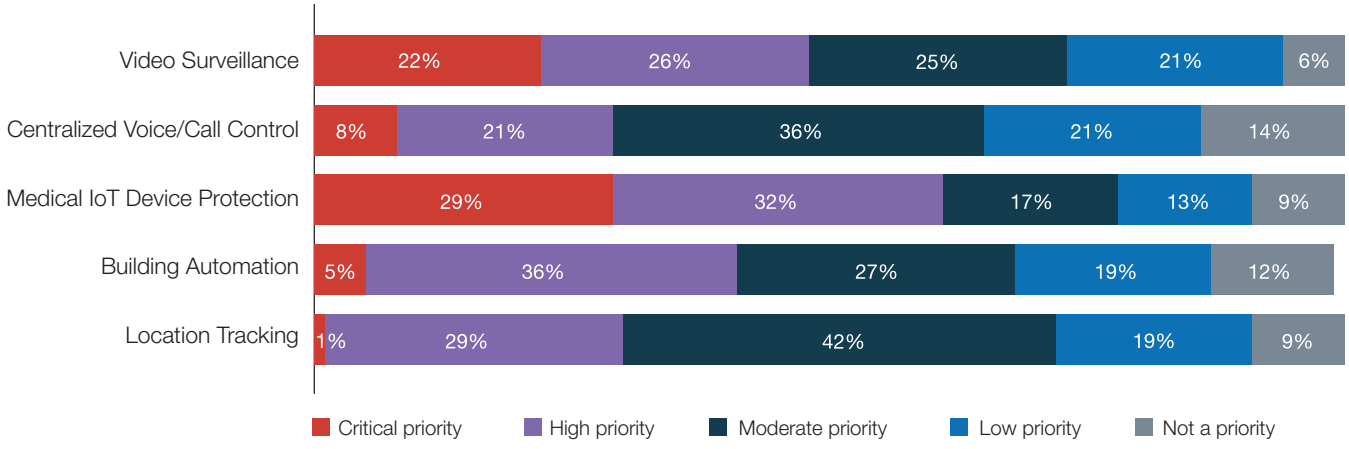


Current Status of Physical Security IoT

The rapidly growing number of IoMT devices, combined with the easy opportunities they provide for cybercriminal exploits and incomplete network segmentation, present an especially troubling risk exposure for most healthcare organizations.

Trend: A Need for Advanced Video Surveillance

Healthcare facilities are vulnerable to physical risks that include theft and robberies, incidents involving police and hospital security, false legal claims, and vandalism. Maintaining a safe and secure environment is part of an organization's reputation and their responsibility to staff, patients, and visitors. Advanced video surveillance solutions offer built-in capabilities such as 24/7 monitoring, intelligent analytics, and real-time alerts. In rating the level of priority of different security initiatives at their organization, nearly half of survey participants list video surveillance as a "critical" or "high" need for securing their organization.



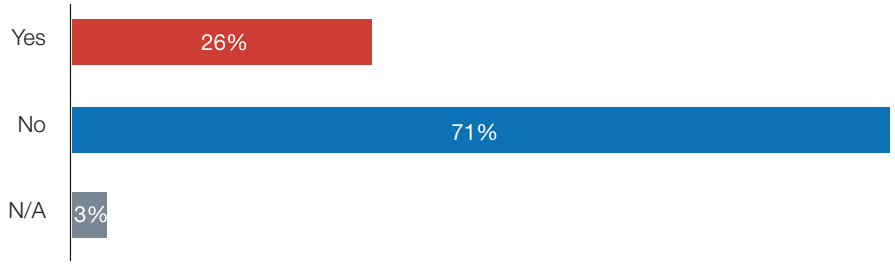
Prioritization of Physical Security Issues

Advanced video systems use network connectivity to deliver many of their critical capabilities. And like IoMT devices, these systems typically do not include their own built-in cybersecurity defenses. In 2016, the Mirai botnet attack took advantage of this exact vulnerability to amass an army of compromised closed-circuit TV cameras and routers. Mirai then launched a massive distributed denial-of-service (DDoS) attack that left much of the internet inaccessible on the U.S. east coast.[3] To address this exposure, networked video surveillance systems must be protected by the organization's cybersecurity architecture.

Trend: Data from Physical Access Controls Is Not Being Shared

The vast majority of the physical access controls (e.g., keycard swipes, door opening) that are currently in place across healthcare-operated environments are not capable of collecting or analyzing data in conjunction with cybersecurity systems. Only about 25% of the organizations represented currently use any type of data correlation between physical controls and cybersecurity systems.

In Verizon's **2018 Data Breach Investigations Report**, 56% of cyber incidents within the healthcare industry were attributed to internal threats. The most common cause of these cyberattacks was human error (35%) followed by intentional misuse (24%).[4] Closing the gap between physical and network security controls could help reduce some of these risks. Sharing threat intelligence between physical access controls with digital tools like user and entity behavior analytics (user-based controls) or network access controls (device-based controls) can improve detection of potential problems while enabling automated, policy-based responses for fast alerts, containment, and remediation.



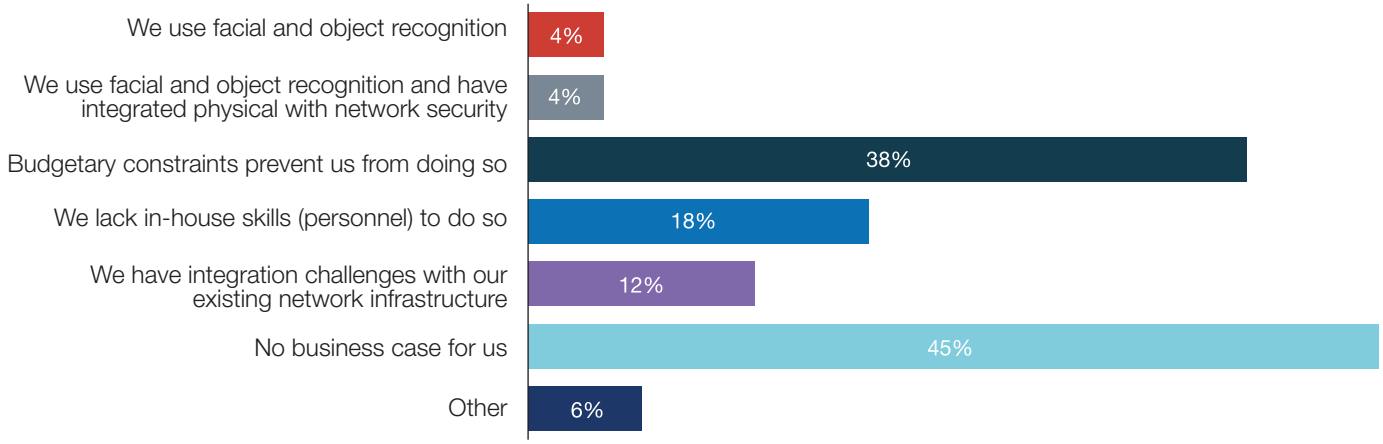
Organizations Correlating Physical Security and Cybersecurity Data

Trend: Facial and Object Recognition Shows Potential, but Adoption Remains Low

Facial recognition in healthcare has the potential to revolutionize identity management for staff as well as patients, making healthcare safer and more efficient. Once a patient has validated their identity and entered into the system, they could potentially "register" by presenting themselves to a kiosk, log into the system using facial recognition, and then sign forms without human intervention. Patients can also use facial recognition to verify they are taking their medication as prescribed by remotely logging into the system via a mobile device that records the patient's face, the medication, and the patient taking the medication.[5]

In terms of physical security controls that apply advanced digital technologies for facial and object recognition, almost half indicate their organization did not have a business case for investing in this type of solution. More than one-third showed interest, but budgetary constraints rendered purchase and deployment of this sort of solution prohibitive. Another 18% report lacking the necessary staff or skills for a successful adoption.

Only 8% of those surveyed reported current use of facial and object recognition technologies in their health organizations—and only half of that total had these physical controls integrated with broader network security.

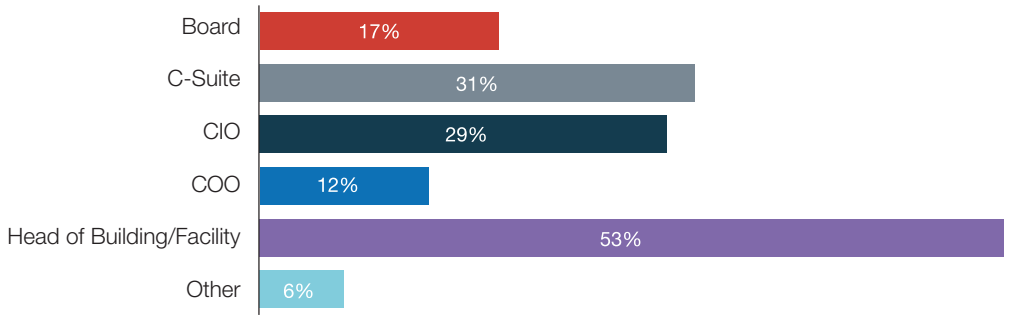


Current Status of Facial and Object Recognition for Physical Security

Lack of Prioritization of Physical Security

The cumulative costs of a major breach (e.g., operational downtime, lost revenue, damaged reputation with consumers, network infrastructure repairs, lost data and IP, lawsuits, and compliance penalties) can amount to a lethal blow for almost any organization. Security should now be a line-of-business concern with the direct involvement of C-suite executive leadership or even the board of directors.[6]

Unfortunately, the survey uncovers a serious gap when it comes to physical security and the levels of engagement at many organizations. For example, only 17% of boards of directors track and measure physical security. Fewer than one-third of organizations track and report physical security at the CEO level. Instead, for more than half of survey participants, physical security is tracked and reported no further than the leaders of the building and maintenance teams.



The Organizational Level at Which Physical Security Is Tracked and Reported

Takeaways

In order to prioritize physical security while integrating it into existing cybersecurity infrastructure, healthcare organizations should heed the following recommendations:

01 Leverage **an integrated network security architecture** that enables physical-cyber convergence

02 Tap integration for **unlocking automation** of physical security workflows and threat-intelligence sharing

03 Prioritize **network segmentation** to secure sensitive data

04 Gain complete device **visibility** and **control** with network access control

05 Implement **automated containment responses** in the event of a policy violation

06 Keep an **eye on the edge**—from wireless access points to software-defined wide-area networks (SD-WAN)

Forward-thinking healthcare executives see digital technology as a tool that can support value-based care to provide better patient outcomes at lower cost. As the healthcare industry continues to merge on-premises care with digital tools like IoMT devices and patient remote services, the separation between physical and digital security systems must also be addressed.

In response, business and security leaders must work together to establish immediate priorities for protecting vulnerable data and reduce critical risk exposures. And as a key best practice, an integrated security architecture offers a foundation for connecting the physical and cyber worlds through intelligence sharing, visibility, control, and automation.

[1] Amy Young, "What Internet of Medical Things (IoMT) Devices Mean for Healthcare Cybersecurity," HealthTech, April 18, 2018.

[2] Jonathan Nguyen-Duy, "Healthcare's Secret Weapon for Securing the IoMT," CSO, February 1, 2018.

[3] Josh Fruhlinger, "The Mirai botnet explained," CSO, March 9. 2018

[4] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[5] Clarice Smith, "Facial Recognition Enters into Healthcare," Journal of AHIMA, September 4, 2018.

[6] Marc Wilczek, "Lack of C-suite collaboration hampering cybersecurity, report finds," CIO, October 9, 2018.

February 11, 2019 11:21 AM

347692-0-0-EN

Mac:Users:susiehwang:Desktop:Egnyte:Egnyte:Shared:Creative Services:Team:Susie-Hwang:Egnyte:Shared:CREATIVE SERVICES:Team:Susie-Hwang:2019:Brochure-Healthcare-CHIMES-survey:brochure-healthcare-chimes-survey