FORTRA

Cyber Security in Healthcare: Frontline Defenses for Critical Data

CYBER SECURITY IN HEALTHCARE: FRONTLINE DEFENSES FOR CRITICAL DATA

Modern Medicine: Cyber Security in Healthcare

Technological advancements are dramatically reshaping how healthcare institutions treat patients. From digitalized records enhancing information access to telemedicine broadening the reach of care, these innovations are setting new standards in efficiency and patient engagement.

Yet, amidst these exciting developments, a critical component demands our attention. In this high-pressure environment, where healthcare workers often juggle multiple roles, cyber security can sometimes take a backseat.

This concern is highlighted by the Gone Phishing Tournament 2023 results, where more than 10% of healthcare employees clicked on a phishing link, and over 66% of those entered their passwords.[1]

[1] Source: https://www.terranovasecurity.com/resources/guides/gone-phishing-report-2023

The sector deals with highly sensitive personal data, encompassing patients' personal, medical, and financial information. This data is particularly attractive to criminals because medical information remains relevant and valuable for identity theft over long periods, unlike banking details or passwords that can be changed after a breach.

Fortra's Terranova Security's report, "From Data Protection to Cyber Culture," reveals that 78% of employees see cyber security as solely the IT department's responsibility.[2] This mindset can lead to risky behaviors, and in healthcare, the stakes are especially high.

Given the reliance on technology for critical functions like diagnosis and patient care, healthcare organizations are ideal targets for ransomware attacks. The urgency to regain system access, crucial for patient safety, often forces these institutions into meeting ransom demands quickly.

[2] Source: https://terranovasecurity.com/from-data-protection-to-cyber-culture/

In this interconnected and ever-evolving digital healthcare landscape, remaining vigilant against cyber threats is a lifeline.

Let's define healthcare cyber security training, learn from real-life examples of cyber threats in the medical field, understand why training is needed, and read up on guidelines on what should be included in it.

CHAPTER 1

Defining Healthcare Cyber Security Training

Due to the critical and personal information in medical records, the repercussions of a data breach are profound.

The significant sensitivity of data in healthcare presents unique cyber security challenges. Hospitals and clinics face:

- ☑ **The handling of sensitive patient data.**
- ☑ **A continuous influx of new patients and emergencies.**
- ☑ **The complexity of managing these 'revolving doors' of scenarios.**

This environment demands specialized cyber security measures distinct from standard IT protocols.

Additionally, as technology becomes ever more entwined with healthcare, the rulebook for cyber safety is being rewritten. What works in everyday life won't necessarily be effective in a hospital or clinic. This difference means that even if a medical employee has good habits in their day-to-day life, they will require specific training for the workplace.

Cyber security is fundamental to patient care, legal compliance, operational integrity, and maintaining public trust. The cost of not adequately funding cyber security can be much higher than the investment required to maintain a robust defense against cyber threats.

Healthcare organizations are bound by stringent regulations such as:

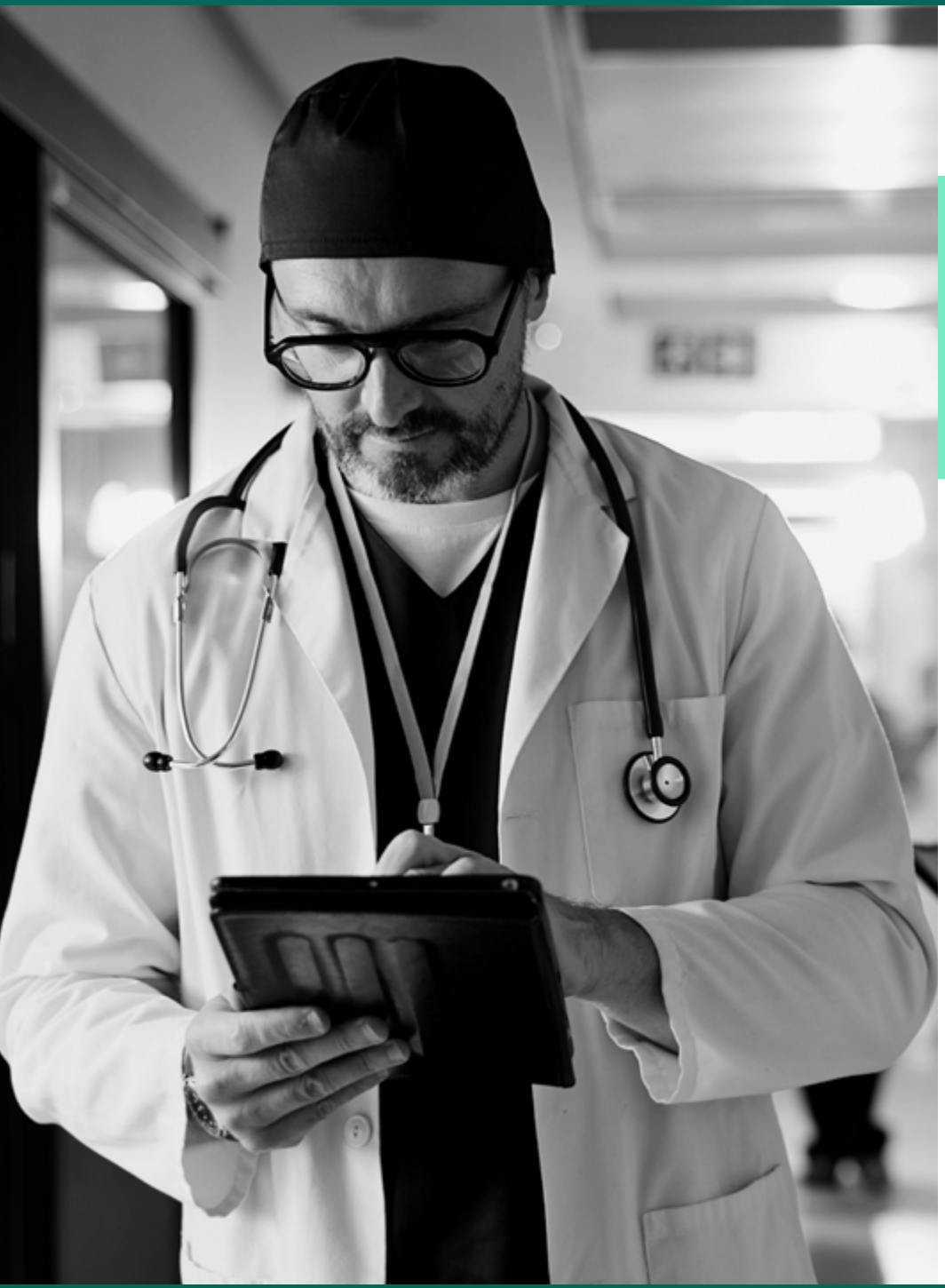
- **Health Insurance Portability and Accountability Act (HIPAA) in the US**
- **The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada**
- **Data Protection Act in the UK**

Non-compliance due to poor cyber security can lead to severe legal repercussions and reputational damage. Patient trust is paramount, and a cyber security breach can irreparably harm this trust, compelling patients to seek care elsewhere.

Cyber threats are constantly evolving, becoming more sophisticated over time. The healthcare sector must keep pace with these changes to protect against emerging threats and inform all its employees of the role they play.

CHAPTER 2

Cyber Security and Attacks in Statistics



In the ever-changing landscape of cyber threats, the healthcare industry stands at a precarious crossroads.

With a 22% increase in attacks from the previous year, reaching 1,684 weekly in the first quarter of 2023, healthcare institutions find themselves third on the list of most targeted sectors, just behind education and the military.[3] This uptick in cyber incidents reflects the valuable and sensitive nature of the data these institutions hold, making them attractive targets for cyber criminals.

The financial repercussions of these attacks are profound, as highlighted by a HIMSS survey.[4] It reveals a sector grappling with significant losses, where 17% of healthcare cyber security professionals report monetary damages from cyber attacks. More than the financial impact, half of these professionals expressed doubts about their organization's ability to recover from the reputational damage inflicted by such attacks.

[3] Source: https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust

[4] Source: https://www.safetydetectives.com/blog/healthcare-cybersecurity-statistics

This fear is not unfounded, considering the dramatic surge in ransom demands from cyber criminals. The average ransom payment in the healthcare sector, which was around $5,000 in 2022, skyrocketed by 29,900% to approximately $1.5 million in 2023, reflecting both the severity and the growing profitability of these cyber attacks for the attackers.[5]

Compounding the issue is the alarming lack of cyber security awareness among healthcare professionals. With 50% of doctors categorized as high-risk for causing data breaches due to insufficient training, the vulnerability is clear.[6]

This vulnerability is further exacerbated by the prevalence of lookalike domain attacks, where 67% of healthcare organizations have been deceived, demonstrating the cunning strategies employed by attackers.[7]

These developments vividly depict a sector under siege, underscoring the urgency for fortified cyber security defenses and comprehensive awareness training. The healthcare industry's struggle against cyber threats is not just about safeguarding data but also about protecting its integrity, reputation, and the trust of those it serves.

[5] Source: https://www.hipaajournal.com/2023-healthcare-ransomware-attacks

[6] Source: https://humanize.security/blog/news/25-healthcare-cybersecurity-statistics-for-2023

[7] Source: https://www.hipaajournal.com/healthcare-email-fraud-attacks-have-increased-473-in-2-years/

CHAPTER 3

Cyber Security Concerns in the Healthcare Sector

Cyber security incidents in healthcare often start with a simple error: an uninformed employee clicks on a malicious email link, triggering costly consequences.

The expenses related to rectifying breaches, legal fines, and loss of revenue due to operational downtime are substantial. Proactive investment in cyber security is often far less expensive than the cost of remediation after an attack.

It's crucial to understand the diverse and complex nature of these risks, so let's look at the specific threats faced by the healthcare sector, according to Theo Zafirakos, CISO at Terranova Security.

Phishing

Hospitals and clinics are often the perfect storm for phishing since employees focused on patient care are bound to neglect proper verifications before clicking on a link or downloading an attachment.

Cyber criminals rely on stressful elements in an employee's job, such as asking for urgent information near the end of the workday or impersonating their boss or other trusted entity.

In this attack, bad actors use social engineering techniques in a message to convince their victims to take urgent action. Stolen passwords or personal information are then sold or used to commit identity theft or other cyber crimes.

Regular training on phishing detection and response, including advanced spear-phishing, is essential in this high-stakes field.

Insider Threats (Lack of Awareness)

Accidental security incidents, often stemming from ignorance or non-compliance with policies, are a significant risk in healthcare. Simple actions like visiting a malicious website or connecting an infected personal device can introduce dangerous malware into the system.

Implementing a stringent role-based hierarchy for data and system access is crucial. Wherever possible, anonymizing sensitive information can make it far less valuable to potential thieves.

It's also vital for healthcare facilities to establish clear policies and guidelines on Bring Your Own Device (BYOD) practices and any physical connections to network systems.

Creating separate network zones for user interfaces and server systems is an effective strategy to isolate and contain incidents within specific network segments. This approach ensures that any breach or issue is confined, minimizing overall system risk.

Ultimately, the root of many security lapses lies in unawareness. Regularly informing and training healthcare employees raises their awareness and equips them with the knowledge to recognize and avoid potential cyber threats.

Data breach (Patient Health Information)

Healthcare organizations handle a vast amount of sensitive patient data, including medical histories, personal identification information, and financial details. Patient health data can be compromised through various means, posing a significant risk to both the patients and the healthcare providers.

The most common way for a data breach is via unauthorized access to healthcare systems, often through hacking or exploiting system vulnerabilities. This attack exposes sensitive patient information like medical records, financial information, and personal identification details.

The risk of data breaches also increases due to insecure data transfer processes and incidents involving lost or stolen devices, which can lead to unauthorized access to sensitive information.

Additionally, healthcare organizations often suffer from internal data breaches (see point 2). These breaches might occur intentionally, driven by personal gain or malicious intent, or unintentionally, due to negligence or a lack of cyber security awareness.

DDoS

Distributed denial-of-service (DDoS) attacks involve flooding a server or application with requests, causing crashes and extended periods of unavailability.

While DDoS attacks are often deployed against websites as a form of protest or to create disruption, they can also serve as a smokescreen for more sinister activities like data breaches. While IT staff are focused on resolving the DDoS attack, cyber criminals may exploit this distraction to initiate other cyber attacks, such as installing malware or stealing sensitive data.

This attack can be devastating for hospitals, capable of bringing critical healthcare services to a standstill, directly endangering patient care, and potentially leading to life-threatening situations if access to essential medical records or life-support systems gets cut off.

The consequences of a DDoS attack are especially alarming when they target mission-critical services in hospitals. An hour of interrupted computer service in healthcare situations can lead to disastrous results. In some cases, internet access may be affected, restricting access to email or other interconnected systems.

In a DDoS attack, IT departments are responsible for implementing effective technological defenses. Strategies like extra on-demand bandwidth to mitigate crashes and content delivery network (CDN) services to filter malicious requests can be crucial. Several modern servers also have hardware protection against this type of attack.

Ransomware

Ransomware attacks typically use malware, like a Trojan worm, to infiltrate and encrypt all the data on a computer. Upon infection, attackers demand a ransom, often through a message on the compromised device, to decrypt the data.

Recent studies, including insights from CISA's COVID-19 Task Force, have highlighted a grim reality in healthcare cyber security: ransomware attacks can potentially lead to patient deaths.[8]

While direct attribution of deaths to these attacks is challenging, the disruption caused by ransomware, such as in the cases of Springhill Medical Center and Düsseldorf University Hospital, shows the indirect but critical impact on patient care.

These viruses are most commonly distributed through phishing attacks that lure users into clicking malicious links or downloading infected files. Remind your users never to click on a link or download a file from a source they don't know.

Checking the URL to make sure it's legitimate is a crucial practice. Even seemingly harmless files, such as documents with .docx or .xlsx formats, can be dangerous if they contain enabled macros designed to execute malicious code.

[8] Source: https://www.cisa.gov/sites/default/files/publications/Insights_MedicalCare_FINAL-v2_0.pdf

IoT (Medical Devices and Equipment)

The cyber security of IoT (Internet of Things) devices in healthcare is increasingly critical, given their wide range, from wearable health monitors to advanced hospital machinery.

These devices are integral to healthcare networks, offering essential data and services. However, their growing interconnectedness also renders them vulnerable to cyber attacks, especially since many weren't originally designed with robust cyber security in mind.

The stakes are high in terms of patient safety. IoT devices play crucial roles in critical care and monitoring. Compromise of these devices can lead to erroneous diagnoses, incorrect treatment decisions, or even direct harm to patients.

Moreover, as they handle sensitive health information, data privacy breaches are a significant concern. Unauthorized access to this data can have serious implications, including the exploitation of personal health information.

The motivation behind attacking IoT devices in healthcare varies. Some attackers aim to disrupt healthcare services for ideological reasons, as a form of protest, or even as an act of cyber terrorism.

Compromised IoT devices not only disrupt services but can also provide cyber criminals with gateways into broader healthcare networks. This access enables them to navigate the system, potentially reaching and exploiting more critical data and systems.

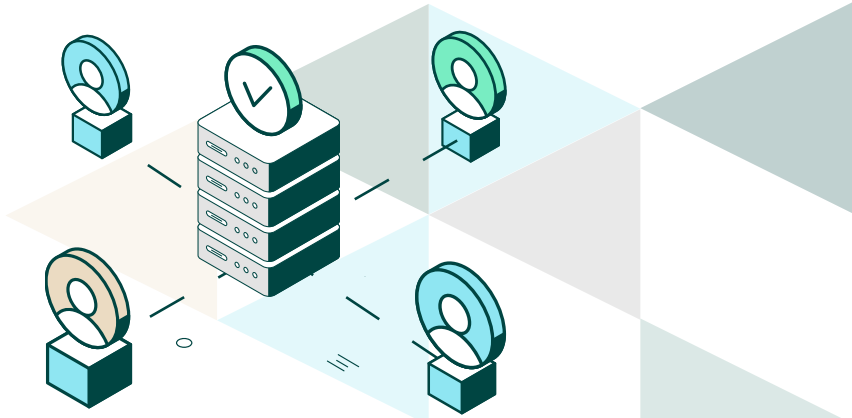
Supply chain risks

Healthcare providers are often connected to and dependent on suppliers, manufacturers, and other healthcare providers. This supply chain, encompassing everything from patient care services and pharmaceuticals to medical and IoT devices, is a complex and interconnected system.

A breach in any segment of this chain can lead to severe repercussions. Compromises within the supply chain could result in the distribution of tampered or counterfeit medical products and services, posing significant risks to patient treatment and safety.

Breaches often occur due to vulnerabilities in a supplier's cyber security measures or lapses in employee awareness. Attackers exploit these weaknesses to gain access to the healthcare provider's network by manipulating system vulnerabilities or through social engineering and phishing attacks targeting supplier employees.

Attackers strategically target the more vulnerable points in the supply chain as gateways into the more secure systems of healthcare providers. This method allows them to penetrate deeper into the network, potentially accessing sensitive patient data or disrupting critical healthcare services. The need for robust cyber security practices and vigilant employee training across the entire healthcare supply chain is thus paramount to safeguard against these risks.



CHAPTER 4

Why Healthcare Organizations Need Cyber Security Awareness Training

Healthcare is a hectic environment with intense workloads and elevated stress levels, significantly increasing the likelihood of human error. Additionally, unlike typical office workers, healthcare employees aren't typically trained in cyber security practices like office workers. This knowledge gap is compounded by the frequent need to leave computers and other devices unattended in emergencies.

Medical workers rely on portable devices, from cell phones to pagers and laptops, VoIP, and other wireless communications means, all of which may be exposed to vulnerabilities when used to transmit sensitive data. The combination of all these factors leads to the situations below:

SENTARA HEALTHCARE (2019)

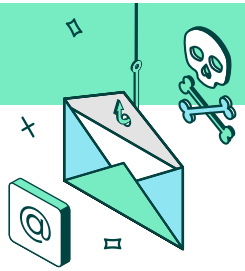
This incident involved mishandling patient information. An employee error led to emails with the protected health information of 577 patients being sent to an incorrect address, including patient names and medical service details.[9]

ORLANDO FAMILY PHYSICIANS (2021)

An unauthorized individual gained access to several employee email accounts due to employees falling victim to phishing attacks. This breach potentially exposed sensitive patient information, including names, Social Security numbers, and medical information. This incident was attributed to inadequate training in recognizing phishing attempts.[10]

[9] Source: https://www.hipaajournal.com/2-175-hipaa-settlement-agreed-with-sentara-hospitals-for-breach-notification-rule-and-baa-failures/

[10] Source: https://www.hipaajournal.com/more-than-447k-patients-affected-by-phishing-attack-on-orlando-family-physicians/



MOFFITT CANCER CENTER (2020)

A data breach occurred when an employee fell for a phishing scam, compromising the email accounts containing patient names, dates of birth, and medical record numbers. The breach highlighted the need for enhanced employee training in cyber security awareness.[11]

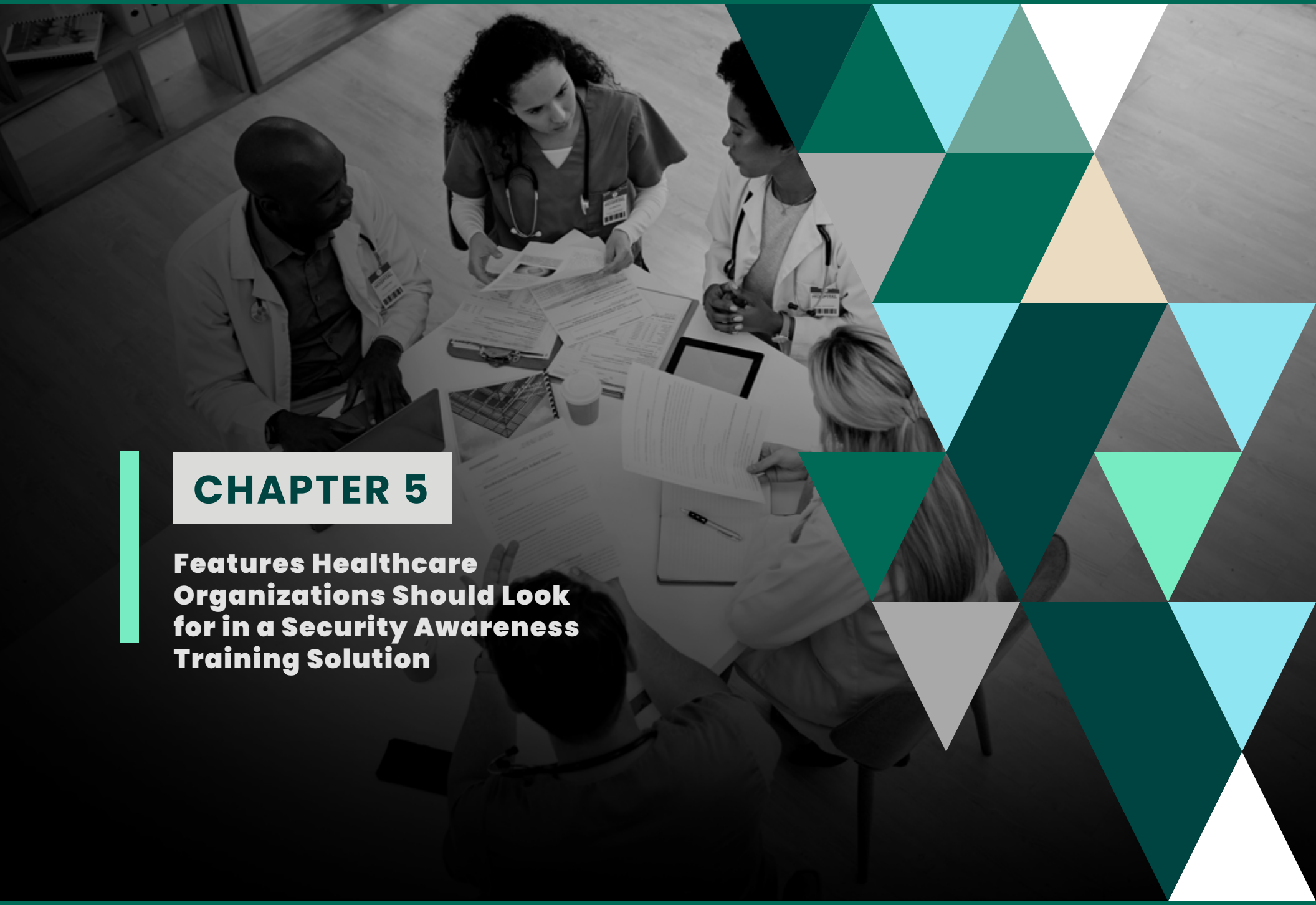
UNIVERSITY OF ROCHESTER MEDICAL CENTER (URMC) (2019)

URMC was fined $3 million for failing to encrypt mobile devices. The breach occurred when an unencrypted flash drive and laptop were lost, potentially exposing patient information. This incident resulted from insufficient attention to encrypting devices containing patient data.[12]

These incidents underscore the critical need for comprehensive cyber security awareness training in healthcare settings. Ensuring all staff are well-equipped to recognize and respond to potential threats is essential for safeguarding sensitive patient data.

[11] Source: https://www.tampabay.com/news/health/2020/09/11/moffitt-stolen-briefcase-exposed-data-of-4000-cancer-patients/

[12] Source: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html



CHAPTER 5

Features Healthcare Organizations Should Look for in a Security Awareness Training Solution

The market for cyber security awareness training solutions is constantly growing, and the options can be overwhelming. Effective awareness training for this industry requires a tailored approach, addressing specific challenges faced by healthcare professionals.

Content tailored to healthcare industry challenges

Cyber security in healthcare isn't a one-size-fits-all matter. Distinct from typical corporate settings, healthcare institutions face unique challenges, requiring specialized training.

Essential modules in healthcare Security Awareness Training (SAT) include:

- ☑ HIPAA and any other laws related to healthcare or personal records
- ☑ Ransomware threats and the signs to detect them
- ☑ Password management and the dangers of password sharing
- ☑ Mobile device security, particularly cellphones and laptops
- ☑ Phishing and social engineering
- ☑ Exchange and disposal of sensitive data

Injecting life into training modules

Your security awareness training must go beyond the mundane. It's about captivating your healthcare employees, not just ticking a box. To achieve this, blend in diverse media types like videos, infographics, and quizzes. These elements maintain interest and accommodate different learning styles.

Gamification is the game-changer, transforming training into an interactive, enjoyable experience. Think leaderboards, interactive cyber security challenges, and more – turning learning into an active and enjoyable journey.

Staying ahead with current content

Your SAT content needs to keep pace in the fast-evolving world of cyber threats. It's not just about knowing the threats; it's about staying a step ahead. Threats like phishing and social engineering evolve so rapidly that new versions of these cyber threats pop up seemingly every month.

Regular updates in your training ensure that your team is always prepared for the latest phishing scams and social engineering tricks. Keeping the content fresh and relevant is key to building a resilient and aware healthcare workforce.

Using analytics to gauge employee comprehension and progress

Analytics capabilities are essential for an effective SAT platform. While it's crucial to detect problem users who create higher risks than others, tracking and reporting should primarily focus on more significant trends to allow you to create better content.

But it's not just about finding the weak spots. Reporting is also crucial to convince executives to continue investing in cyber security awareness training. Graphics and numbers are the best way to do this, whether to reveal a high number of problem users or to demonstrate an improvement over time.

Scalability and customizability in deployment

Healthcare is diverse, and your SAT should be, too. With recent cyber threat statistics showing new threats every month, SAT programs must be adaptable and scalable to keep up with new hacks and viruses.

Tailor it to fit the unique contours of your organization. Whether you're a small clinic or a large hospital, your SAT solution should adapt and scale with your needs. As new threats emerge, ensure your platform can evolve, keeping your defense robust and responsive.

Proactive vs reactive: A dual strategy

All healthcare organizations need detailed reactive cyber security strategies since cyber threats are almost impossible to avoid in this sector. However, there has been an increasing focus on proactive strategies as they can prevent a lot of breaches and minimize their impact if they do happen.

Here is a list of examples for each:

Proactive strategies	Reactive strategies
• Risk assessment • Secure SDLC • Employee cyber security awareness training • Continuous network and system monitoring • Regular software updates and patch management • Data encryption • Phishing simulations	• Incident response plan • System isolation • System alerts • Drive recovery and restoration • Breach analysis and reporting • Disaster recovery • Public relations and reputation management

Transforming your SAT from a routine drill to an engaging, adaptive, and proactive program is not just beneficial—it's essential for safeguarding the sensitive world of healthcare.

CHAPTER 6

Making Cyber Security a Pillar of Your Organizational Culture

Transform cyber security awareness from a checkbox exercise to a dynamic part of your healthcare organization's DNA. Dive in with a plan that breaks down this formidable task into manageable, engaging steps, turning what could be a chore into an empowering journey for your team.

Starting point: Assess, then address

Kick-off with a thorough assessment of your current cyber security culture. Start by evaluating and surveying your employees to determine their current cyber security knowledge. In the healthcare sector, the knowledge level is often lower than in other industries.

Once you have this employee data, determine your objectives, the skill and knowledge gaps you'd like to fill, and the program's scope. Determine the departments, processes, and technologies included in the training.

Engaging leadership and fostering a security-first mindset

Garnering robust support from the top is more than beneficial—it's essential. Healthcare's layered management needs a unified front on cyber security. Interviewing stakeholders on their objectives, concerns, priorities, and capacities can provide valuable insight when you prepare your awareness program plan.

Engage leaders with compelling case studies and pressing cyber threat scenarios.[13] Cultivate a top-down, security-first mindset that resonates throughout your organization.

[13] Source: https://terranovasecurity.com/customer-success-stories/

The training mix: Consistency meets intensity

Balance is key—blend comprehensive annual or quarterly sessions with snappy monthly updates on emerging threats. They're less time and money-intensive than regular training sessions, but they can leave gaps since the cyber threats evolve faster than the sessions progress.

The answer often lies in a blended approach, including larger yearly or quarterly training sessions to set the tone while also having monthly check-ins to educate employees on recent cyber threats.[14] This solution gives you the best protection while having a manageable impact on employee work time.

Incorporating real-world simulations

Healthcare institutions face a bigger cyber security challenge since they don't have a relatively controlled environment like a typical office setting. Doctors and nurses have hectic work schedules, and it can be challenging to integrate cyber security into their daily activities.

Good healthcare cyber security training must include real-world scenarios to contextualize the cyber threats. Examples include:

- ☑ Phishing simulations
- ☑ Roleplaying typical cyber threat scenarios
- ☑ Patient data security scenarios
- ☑ Medical device security training, especially the ones connected to the Internet.

Make it immersive, make it real, and watch the engagement soar.

[14] Source: https://terranovasecurity.com/blog/blog/security-awareness-training-frequency/

Continuous feedback and improvement loops

Continuous feedback is your compass for success. Instead of focusing the program only on finding problem employees, try to use it to find larger trends that the workplace environment or resources might cause.

For example, it's a good idea to have a few different ways to collect feedback about the training from your employees. You might find out that the knowledge gap is caused by issues with your training instead of laxity about the content.

Encourage staff feedback—sometimes, the key to unlocking engagement lies in their insights. And don't forget to celebrate progress. Introduce gamified elements like leaderboards to visualize achievements and foster a spirit of healthy competition in cyber security learning.

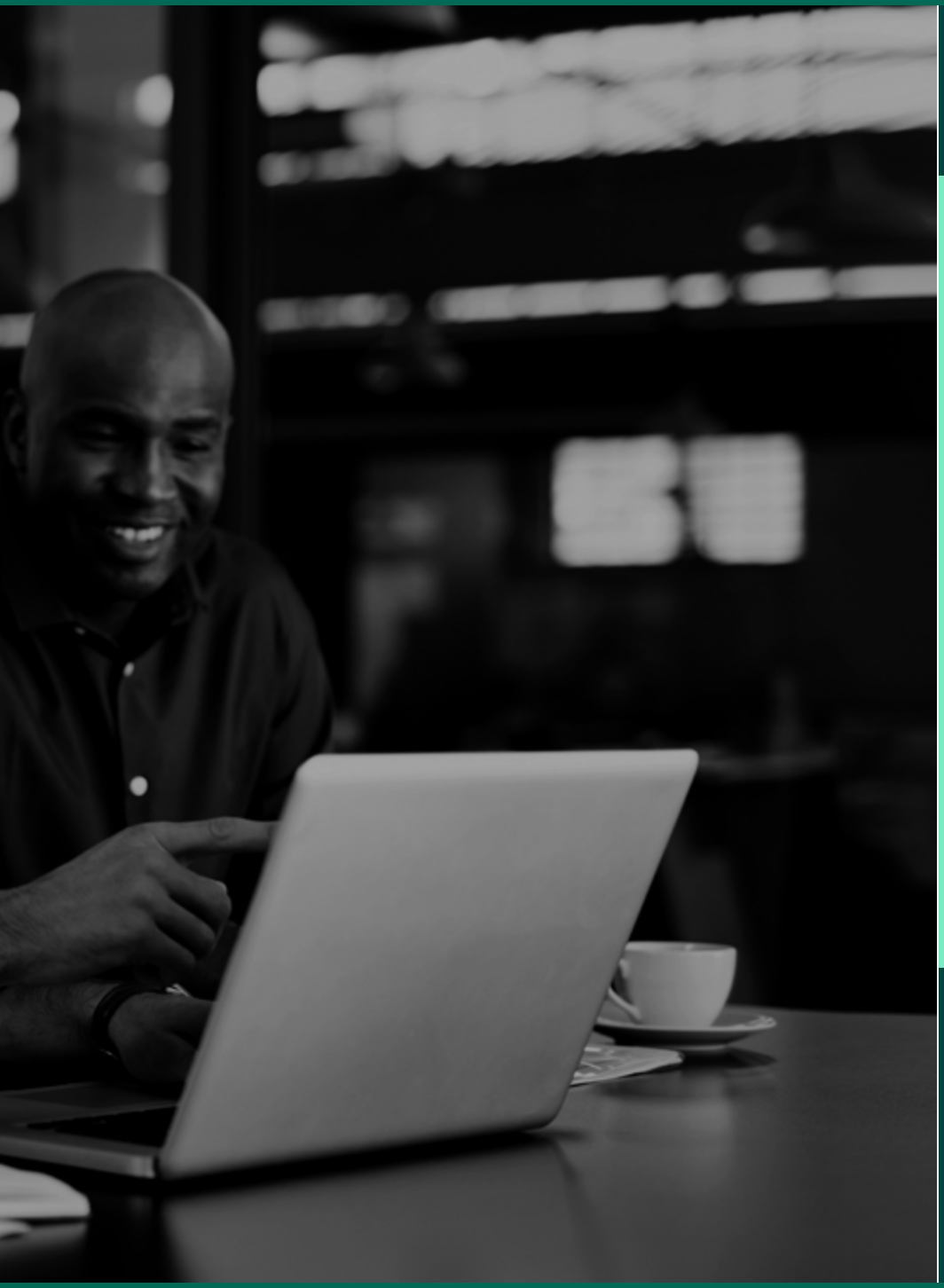
In essence, elevating cyber security training in healthcare is about making it a living, breathing part of your organizational ethos.

Embracing the Cyber Security Challenge in Healthcare

Cyber security awareness is crucial in healthcare, where the stakes are constantly rising due to regulatory demands, the proliferation of telemedicine, and growing ransomware threats.

Terranova Security, a proud member of Fortra's comprehensive cyber security portfolio, offers risk-based campaigns with top-tier training content and realistic phishing simulations in multiple languages, catering to the diverse needs of healthcare professionals.

Terranova Security stands out with its flexibility and customization. Our mobile-friendly platform accommodates the hectic schedules of healthcare workers and includes healthcare-specific issues like PII, PHI, and HIPAA compliance. This ensures that your team is equipped with the right tools to be effective in cyber security.



It's time to empower your team and stay ahead of advancing cyber threats. Take the first step towards a more secure healthcare environment with Terranova Security.

Request a demo today and discover how our tailored solutions can fortify your defenses against the evolving digital landscape. Your journey towards robust cyber security begins here.

REQUEST A DEMO

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

 | tns-ebook-healthcare-0724