WHITE PAPER

November 8, 2024

Unveiling the Layers of Cyber Threats in Healthcare

Written by:
Anupriya Ghatge, Victor Leke, Akshara Rajesh, Aniya Stanford,
Mikinzi Strykul and Julie Tu

RELI Group

RELI Group

Unveiling the Layers of Cyber Threats in Healthcare

The healthcare industry has experienced a significant increase in cyber attacks over the past decade. The frequency and severity of cyber attacks targeting healthcare organizations has risen steadily, making it one of the most targeted sectors. In 2024, healthcare was the third-most targeted sector, accounting for 15% of all incidents. According to the Department of Health & Human Services, there were more than 630 ransomware incidents against healthcare organizations in 2023. This white paper highlights significant cyber threats that U.S. healthcare users face, including data breaches and social engineering tactics.

The threat of data breaches in the healthcare industry presents multifaceted challenges and risks. According to IBM's annual Cost of a Data Breach report, the average cost of a healthcare data breach is estimated to be about $10.9 million, the highest among all industries surveyed. With the digitalization of patient records and the integration of advanced medical technologies, healthcare organizations have become prime targets for cybercriminals seeking to exploit sensitive and personal information such as Personally Identifiable Information (PII) and Protected Health Information (PHI). These breaches can lead to severe consequences, including compromised patient privacy, identity theft, financial fraud, and reputational damage for healthcare providers.

Moreover, the interconnected nature of healthcare systems and the increasing reliance on third-party vendors amplifies the vulnerability landscape, creating potential entry points for hackers. In 2023, on average, 1.99 data breaches of 500 or more healthcare records were reported daily in the healthcare sector.

In 2023, on average, 1.99 data breaches of 500 or more healthcare records were reported daily in the healthcare sector.

In the past, threat actors used social engineering techniques such as phishing attacks related to COVID-19 to target the healthcare sector. Palo Alto researchers found an 189% increase in phishing attacks relating to or targeting pharmacies and hospitals between December 2020 and February 2021. Vaccine-related phishing attacks soared 530% over the same period. Social engineering tactics like these can easily manipulate patients, medical staff or other personnel by appealing to the crisis of the moment.

In Senator Mark R. Warner's white paper, "Cybersecurity is Patient Safety," he calls for additional initiatives to tackle cybersecurity concerns in healthcare. Senator Warner underscores the connection between cybersecurity and patient safety, advocating for a shift where cybersecurity is integral to every organization's business model. He addresses specific cybersecurity issues that have prevailed in the healthcare industry, including legacy systems and the Health Insurance Portability and Accountability Act (HIPAA). Cybersecurity

Unveiling the Layers of Cyber Threats in Healthcare

policies must start upstream, influence equipment design, and permeate through regulations and government actions. This approach empowers healthcare providers to benefit from advancements while maintaining a baseline of cyber hygiene to protect all stakeholders.

After several years of the COVID-19 pandemic, healthcare providers have suffered from the drastic rise in cyber threat attacks, contributing to detrimental losses in several domains. Senator Warner and his staff initiated the conversation to enforce cybersecurity legislation. They have called cybersecurity researchers, advocacy groups, business leaders and trade associations to provide input to address today's pressing cybersecurity challenges. These endeavors aim to ensure patient safety is protected on a national scale.

Cyber Threats Identified in the Healthcare Industry

Legacy Systems and the Internet of Things

The continued use of legacy systems in the healthcare sector is a persistent cybersecurity concern. Due to limited budgets, many healthcare providers cannot replace outdated medical equipment. Unfortunately, legacy equipment can expose medical devices and networks to severe vulnerabilities because patches or updates are unavailable. These vulnerabilities could cause critical issues and potentially life-threatening situations.

According to a study by the CyberPeace Institute, the average cyber attack on a healthcare system leads to 19 days of disruptions that prevent patients from receiving care.

The healthcare industry faces multiple cyber threats due to outdated medical equipment still in use. The software integrated into these machines no longer receives the necessary updates and patches, leaving legacy networks vulnerable to cyber attacks. To make matters worse, the constant expansion and innovation around the Internet of Things (IoT) only increases the risk of cyber attacks. Specifically, IoT devices widen the attack surface for ransomware. Security misconfigurations like unpatched systems or unauthorized access control must be remediated by finding and implementing industry standards like CIS Benchmarks or OWASP Top 10, which can expose sensitive data and outdated components. Attackers can exploit these vulnerabilities by purchasing tools from illegal sources and scanning for and exploiting these weaknesses.

The integration of IoT in healthcare has introduced vulnerabilities in medical devices and software, posing risks to patient safety and system integrity. According to a study by the CyberPeace Institute, the average cyber attack on a healthcare system leads to 19 days of disruptions that prevent patients from receiving care.

The most vulnerable components of the Internet of Medical Things (IoMT) include electronic health records, wireless infusion pumps, endoscopy cameras and radiology information systems. Cynerio's research found that 53% of connected medical devices and other IoMT devices have at least one unaddressed critical vulnerability, which can be exploited to gain access to sensitive data and affect the availability of the devices. The most common risk is insecure credentials, with 21% of IoT and IoMT devices found to have default or weak credentials. Effectively segmenting networks, utilizing secure credentials, implementing proper

Unveiling the Layers of Cyber Threats in Healthcare

access control, and adopting a Secure Software Development Life Cycle are critical to mitigate these vulnerabilities.

HIPAA Limitations

Enforcing HIPAA for covered entities to protect PHI for privacy purposes is essential. The HIPAA Privacy Rule sets standards to safeguard the confidentiality of PHI and dictates how covered entities and business associates handle PHI to ensure an individual's medical information remains private.

However, HIPAA has security limitations as it fails to address emerging data integrity and availability threats, such as ransomware attacks. HIPAA also excludes non-covered entities like software and hardware providers and research organizations who are not required to adhere to HIPAA despite having access to PHI through software, medical equipment, consumer wearable devices, etc. There are gaps in addressing technological advancements, such as mobile health apps and wearable devices, as well as the emerging development of predictive algorithms through artificial intelligence and machine learning (AI/ML) that require vast amounts of patient data to train these models.

The current framework lacks specific provisions to counteract these evolving cybersecurity challenges, highlighting a gap in addressing broader aspects of information security beyond privacy concerns. HIPPA has a limited scope of enforcement, and many health entities struggle with implementing its security controls. As a result, some covered entities and business associates may not prioritize cybersecurity measures until after a breach occurs, which leaves them vulnerable to cyber threats. These cybersecurity gaps leave entry points for cyber attackers to continue threatening the safety of PHI. In the first few years following the compliance date for the Privacy Rule, many covered entities reportedly violated the Privacy Rules requirement without any consequences, leading many analysts to suggest that HIPAA was "all bark and no bite." Additionally, HIPAA regulations tend not to align and evolve with Federal Trade Commission regulations, such as the Health Breach Notification Rule, creating confusion and increasing the regulatory compliance burden for covered entities.

Some covered entities and business associates may not prioritize cybersecurity measures until after a breach occurs, which leaves them vulnerable to cyber threats.

Concerns with Telehealth

Virtual healthcare services, such as telehealth, are now one of the fastest-growing areas in healthcare. Virtual healthcare introduces new tools that share information across multiple locations, expanding the risk's attack surface. It presents significant challenges in healthcare regarding securing PHI and complying with HIPAA. Three risk factors associated with privacy and security in telehealth include environmental factors (lack of private spaces), technological factors (data security and limited access to secure internet and technology), and operational factors (insurance reimbursement, technology accessibility and training). The use of multifactor authentication and encrypted platforms for communication are some ways to mitigate risks associated with telehealth services.

Concerns with AI

Implementing AI in healthcare brings forth challenges, including protecting the integrity of data transfers and regulatory compliance, as healthcare organizations struggle to integrate AI systems while adhering to privacy and security regulations. Due to competition and proprietary

technology, AI vendors face interoperability issues that further complicate data exchange among healthcare organizations. Working with vast amounts of sensitive patient data poses significant data privacy and security risks, such as privacy breaches, unauthorized access, and compromised patient confidentiality due to storing patient data in vendor data centers.

Training models designed to conduct data analytics may have biased data that perpetuates disparities in healthcare outcomes, such as unequal treatment, misdiagnosis, or underdiagnosis of certain demographic groups. Additionally, navigating complex regulatory frameworks between existing healthcare systems and emerging AI platforms presents regulatory and legal challenges. Ethical concerns, high development costs, overreliance on AI-generated recommendations, data quality issues and cybersecurity risks are additional challenges associated with AI implementation in healthcare.

Healthcare security and privacy experts have already raised concerns about the danger of AI-assisted cyber attacks. In July 2023, the Department of Health & Human Services (HHS) issued a threat brief about how threat actors might use AI to exploit vulnerabilities, overwhelm human defenses and automate attack processes. For example, AI can accelerate brute force password cracking, analyze systems to find vulnerabilities and unprotected databases, manipulate customer service chatbots, bypass CAPTCHA systems, and manage and direct Distributed Denial of Service (DDoS) attacks in real ptime – adjusting tactics based on the target's defenses.

AI can accelerate brute force password cracking, analyze systems to find vulnerabilities and unprotected databases, manipulate customer service chatbots, bypass CAPTCHA systems, and manage and direct DDoS attacks in real time.

Concerns with Cybersecurity Supply Chain Risk Management

Implementing Cybersecurity Supply Chain Risk Management (C-SCRM) within healthcare is critical to mitigating the impact of cyber threats and ensuring the availability, reliability and security of medical resources. Disruptions to the healthcare supply chain can contribute to shortages, stockouts or missing inventory. When clinicians do not have critical medical and surgical supplies to deliver patient care, it can disrupt or delay treatment. Integrating information technology systems, including enterprise resource planning systems, electronic health records (EHRs) and supply chain management software, has revolutionized tracking and managing inventory. Cyber attacks targeting these systems can disrupt inventory tracking and management, leading to inaccuracies in supply levels and potential disruptions in patient care.

Healthcare organizations rely heavily on third-party vendors for many services and products. These dependencies can cause vulnerabilities as cyber attacks that target vendors may cascade down the supply chain and affect multiple organizations. A breach in any part of the supply chain can endanger patient lives, compromise patient confidentiality, and disrupt healthcare services and operations. The absence of C-SCRM makes it easier for malicious actors to manipulate data or introduce counterfeit products into the supply chain, posing significant risks to patient safety. The complex interconnectivity of healthcare software supply chains can make the source of a cyber attack difficult to trace. When multiple vendors and systems are involved in the supply chain, pinpointing the origin of a cyber attack becomes complex. As a result, healthcare organizations face difficulties in effectively managing cybersecurity risks.

Unveiling the Layers of Cyber Threats in Healthcare

Other Cyber Threats from COVID-19

At the pandemic's start, many cyber attacks happened across several healthcare domains, including hospitals, pharmaceutical companies, HHS, the World Health Organization and companies across the healthcare supply chain. COVID-19 spawned more malware cyber attackers who identified and exploited common vulnerabilities. The increased reliance on remote work, decreased mobility, border closures, and high demand for personal protective equipment opened the stage for malicious groups to launch phishing, ransomware and DDoS attacks. The pandemic fast-tracked the usage of eHealth services and interconnected medical devices; however, these mediums were particularly vulnerable as a lack of experience and planning made them extremely vulnerable to cyber attacks. These issues persist today as there are gaps in cyber attack training for medical staff alongside insufficient cybersecurity measures to protect against these vulnerabilities.

Cyber Threat Impacts on Healthcare

Endangering Patient Safety

Threat actors targeting healthcare systems can disrupt critical medical services, compromise medical infrastructure, and manipulate treatment plans. These consequences can cause network shutdowns and connectivity loss, ultimately threatening patients' lives. A study in 2022 found that 20% of hospitals that experienced a cyber attack reported increased patient mortality. From that percentage, 57% reported poorer patient outcomes, and 50% reported increased medical complications due to cyber attacks. The WannaCry attacks in 2017 affected the United Kingdom's National Health Service; thousands of appointments were canceled, and patients experienced delays in medical treatment. Joshua Corman, a cybersecurity expert, stated that it is impossible to deny that people did not die because of these disruptions. Losing lives from cyber threats proves how detrimental cyber attacks are and drives the urgent need for proper cybersecurity measures in the healthcare industry.

A study in 2022 found that 20% of hospitals that experienced a cyber attack reported increased patient mortality.

Business Disruption

Cyber attacks in healthcare profoundly impact business operations, often resulting in significant disruptions. These attacks interrupt essential healthcare services and clinical workflows. Ransomware attacks encrypt critical systems such as EHRs, rendering them inaccessible to healthcare providers. DDoS attacks take facilities offline, disrupting care through longer hospital stays, ineffective patient care, misdiagnoses, and delays in procedures and tests. Additionally, these attacks compromise billing systems, disrupting essential services such as scheduling appointments and processing payments. These outcomes overall can contribute to a decrease in patient volume and revenue.

Financial Burdens

Cybersecurity concerns trigger a substantial rise in healthcare prices, causing the healthcare industry to suffer financial burdens. As hospitals continue to rely on digital systems for patient care and administrative functions, they become vulnerable to malicious cyber incidents, such as ransomware attacks. The aftermath of such attacks often brings significant financial burdens, including the costs associated with restoring compromised systems and enhancing cybersecurity measures and potential fines for regulatory non-compliance. In 2023, healthcare data breaches cost an average of $11 million annually, making it the industry with the

Unveiling the Layers of Cyber Threats in Healthcare

highest recovery costs nationwide. Consequently, healthcare providers are compelled to allocate substantial resources to address these challenges, which leads to an uptick in operating expenses. To recoup these additional costs, healthcare facilities may increase prices, putting financial strain on patients and insurers. This escalation in healthcare prices undermines affordability for individuals and families, and exacerbates the broader economic challenges within the healthcare sector.

Damages to Company Reputation

Data breaches in the healthcare industry pose financial and operational risks, and can have profound implications for an organization's reputation, as illustrated by several high-profile data breaches. For instance, the Anthem data breach in 2015, which exposed the PII of nearly 80 million individuals, including names, Social Security numbers and medical ID numbers, not only resulted in a settlement of $115 million but also dealt a severe blow to Anthem's reputation as a trusted healthcare provider.

Similarly, in 2020, a cyber attack on Universal Health Services, one of the largest hospital and health care services providers in the United States, shut down critical systems, including email and medical records. While patient care continued, services were affected, and patients experienced delays and inconveniences. Patients and stakeholders were concerned about the security of their personal and medical information, and the incident underscored the importance of robust cybersecurity measures to safeguard sensitive data within the healthcare sector.

Data breaches in the healthcare industry pose financial and operational risks, and can have profound implications for an organization's reputation.

The erosion of patient trust following an attack or data breach can have far-reaching consequences for healthcare organizations. Patients may become hesitant to share personal information or engage with healthcare providers, fearing further violations of their privacy and confidentiality. Moreover, the negative publicity surrounding data breaches can damage a healthcare organization's brand image, making it challenging to attract and retain patients in an increasingly competitive landscape.

Cybersecurity Workforce Shortage

The cybersecurity workforce shortage is impacting healthcare industries due to budget limitations, an insufficient cybersecurity curriculum, and a lack of cybersecurity professionals with experience in the healthcare industry. The current cybersecurity workforce is estimated to include 1.4 million individuals in the U.S., but it is estimated that there is a shortfall of 483,000 individuals. A study by ISC2 found that 75% of cybersecurity professionals view the current threat landscape as the most challenging in the past five years, and only 52% believe that their organization has the tools and people to respond to these cybersecurity incidents.

Healthcare technology budgets are rising, with organizations spending at least seven percent or more on average. However, most of these funds go to the annual IT budget, leaving six percent or less for investments in cybersecurity. As one measure to combat the cybersecurity workforce shortage, organizations can reprioritize the cybersecurity budget to fall under risk management, instead of IT operations.

A lack of comprehensive and consistent cybersecurity curricula in schools and universities also contributes to the shortage. Many educational institutions have not kept pace with the evolving

Unveiling the Layers of Cyber Threats in Healthcare

cybersecurity landscape, leading to a gap in qualified graduates. Due to this lack of consistent curricula, students may pay more for specialized training through another certification authority. 92% of cybersecurity professionals say their organization suffers from skills gaps in one or more areas. These skills range from technical skills like penetration testing and Zero Trust implementation to non-technical skills like communication.

Because there's a correlation between healthcare cybersecurity and patient safety, robust cybersecurity practices must be in place to comply with laws and regulations. The fast-paced and complex environment makes it difficult for non-experienced cybersecurity individuals to keep up. Enhancing educational programs and curricula is essential; this can be achieved through collaboration with industry partners to develop and update cybersecurity courses that align with industry needs. Offering scholarships, grants and other funds to students pursuing cybersecurity degrees and certifications encourages employees to pursue the necessary training.

Additionally, according to an article by Health IT Security, investing in entry-level talent, leveraging automated technology and reducing burnout are also key to addressing the shortage of cybersecurity professionals. By hiring entry-level candidates and providing them with training, these individuals can advance their careers and envision a future in cybersecurity. At RELI, we address these issues by including cybersecurity interns on our team and providing them with on-the-job training, even with limited experience.

Loss, theft and disclosure of sensitive healthcare data amounted to $96.7 million in 2023, more than tripling the number of breaches from 2022.

However, even with this approach, the challenge of handling multiple urgent cyber threats can strain cybersecurity teams. Leveraging automated technology, artificial intelligence and machine learning can help bridge the workforce gaps. Automated technology can continuously monitor systems, process large volumes of data, and quickly detect threats. Integrating an organization's architecture is crucial for mitigating risk and reducing the workload.

Due to the heightened security workloads and staff turnover, burnout is prevalent in cybersecurity. Integrating security into the initial design of endpoints and systems alleviates the burden on the cybersecurity team and promotes smooth operations. In addition, providing an environment where employees can pursue their passions offers an opportunity to enhance their skills and foster enduring improvements within the company. Policies promoting healthy work/life balance, such as flexible hours, mental health support, and resources for stress management and burnout prevention can help retain professionals in the field.

Physical and Digital Data Loss

There are many advantages to the IoMT, with its easy sharing and facilitation capabilities between patients and networks through real-time monitoring and wearable devices. Still, it is highly sensitive as it handles large amounts of patient information. With an invaluable price tag associated with PHI on the dark web, it is a target for insider attacks. Loss, theft and disclosure of sensitive healthcare data amounted to $96.7 million in 2023, more than tripling the number of breaches from 2022. Healthcare-specific data breaches of 500 or more records were reported on an average of 364,571 records daily. According to IBM, the average cost per breach is $4.45 million, which has skyrocketed since the pandemic.

RELI Group

Unveiling the Layers of Cyber Threats in Healthcare

External data breaches caused by malware attacks, ransomware, phishing and other tactics are the most serious concerns for the healthcare data industry. There are also substantial increases in internal data breaches, assistance from internal agents through privilege abuse, unauthorized access, improper disposal of sensitive data, and unintentional sharing of confidential data to unauthorized parties. These techniques are triggered by a lack of security measures and internal negligence, paving the way for the theft of physical devices, including laptops and hard drives, with PHI and criminal infiltrations into healthcare systems.

AI Impacts

The integration of AI into healthcare systems introduces new cybersecurity threats. Adversarial attacks targeting AI models, such as data poisoning and input manipulation, pose serious risks by manipulating algorithms and compromising patient safety. Integrating AI systems makes healthcare organizations more susceptible to ransomware and malware attacks, with AI-supported malware like "BlackMamba" demonstrating the potential to bypass traditional security measures. Threat actors leverage AI to design and execute attacks, resulting in more sophisticated and damaging cyber incidents.

AI is utilized in various malicious activities, including phishing emails, impersonation attacks, rapid exploitation of vulnerabilities, and complex malware code. AI enables deeper target reconnaissance, allowing attackers to gather extensive information about their targets with unprecedented speed and accuracy. Automation of attacks using AI technology overwhelms traditional human defenses, making it increasingly challenging for cybersecurity professionals to detect and mitigate threats effectively. Additionally, AI-powered ransomware attacks have become widespread and evasive, posing significant risks to organizations worldwide. Based on findings from an MIT Technology Review survey conducted in January 2021, it is anticipated that AI will be employed in malicious activities, including impersonation and spear phishing attacks, more efficient execution of ransomware, spreading misinformation and undermining data integrity, targeting remote workers by exploiting vulnerabilities in home networks, and generating deepfakes. The lack of AI cybersecurity expertise among healthcare professionals contributes to misconfigured systems and inadequate protection against emerging threats.

Automation of attacks using AI technology overwhelms traditional human defenses, making it increasingly challenging for cybersecurity professionals to detect and mitigate threats effectively.

Cybersecurity Frameworks

As the healthcare industry faces growing cyber threats, several aspects are at risk, including company reputation, organizational resilience and patient wellbeing. Healthcare organizations must adopt and adhere to frameworks that strengthen their cybersecurity posture.

The foundational principle of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides an approach to managing and mitigating cybersecurity risks. The Cybersecurity Infrastructure and Security Agency (CISA) Zero Trust Architecture (ZTA) framework emphasizes continuous verification and strict access control in protecting assets and data from threats. The NIST AI Risk Management Framework (RMF) also outlines an approach for securing AI-driven

systems. By examining these frameworks, the healthcare industry can strengthen its cybersecurity posture.

NIST CSF

NIST CSF emphasizes achieving specific cybersecurity outcomes instead of mandating controls and presents an opportunity for healthcare entities to enhance their information security strategies and reliance against cyber attacks. This allows healthcare organizations to tailor their cybersecurity programs to their unique risk profiles while achieving desired outcomes. The healthcare sector is increasingly targeted by cyber threats, making it imperative for organizations to fortify their security measures. Therefore, organizations must implement security programs to minimize the impact of destructive cyber attacks.

NIST CSF emphasizes the "Identify" function, which is crucial for healthcare organizations dealing with numerous connected medical devices, EHRs and other sensitive data. These organizations must implement comprehensive asset inventory, vulnerability management and data classification systems. The framework introduces guidance on managing cybersecurity risks within the supply chain, which is significant for healthcare entities reliant on third-party vendors for services, software and devices. Developing processes to assess vendor cybersecurity postures and ensuring compliance with security standards are vital steps for healthcare organizations. The new "Govern" function of NIST CSF highlights the importance of establishing clear leadership, governance and risk management practices for cybersecurity. Additionally, NIST CSF underscores improved communication and employee cybersecurity awareness. The involvement of HHS in developing NIST CSF suggests a strong alignment with existing healthcare cybersecurity guidance.

A study by Accenture found that 18% of healthcare workers would be willing to sell PII to unauthorized parties if the price was right.

CISA ZTA

CISA ZTA is a critical framework for safeguarding patient data, protecting essential infrastructure and mitigating cyber threats. It offers a proactive approach to healthcare that focuses on preserving resources using the principle of least privilege and "verify before trust."

Healthcare organizations have adopted Zero Trust in their environments, implementing identity verification and authentication before allowing access to medical devices and workstations. With the increasing number of IoMT devices in the healthcare industry, the ZTA approach detects, reports and blocks any abnormal activity before it can increase. The ZTA approach is used for network segmentation to protect networks, devices and patient safety against an expanding threat landscape. Integrating ZTA prevents insider attacks in the healthcare industry; a study by Accenture found that 18% of healthcare workers would be willing to sell PII to unauthorized parties if the price was right. Additionally, employees acting with good intentions and falling victim to external threats may unintentionally expose data.

In a Zero Trust environment, such incidents are minimized because data beyond an employee's role and responsibility is restricted. The ZTA strategy allows more visibility and control over the network. As healthcare stakeholders embrace the Zero Trust strategy, they prioritize continuous verification and validation, fostering a proactive security culture around healthcare.

RELI Group

Unveiling the Layers of Cyber Threats in Healthcare

NIST AI RMF

NIST AI RMF aims to assist organizations involved in various stages of the AI system lifecycle, including design, development, deployment and usage. For healthcare organizations, it provides structured guidance for integrating AI solutions, including identifying, assessing and mitigating risks associated with AI technologies.

NIST AI RMF outlines key definitions, inherent tensions and examples relevant to healthcare. This information can serve as a foundational guide for healthcare organizations looking to implement NIST AI RMF principles in their operations. The NIST AI RMF playbook includes detailed sections on governance, mapping, measurement and management of AI risks. Healthcare organizations can leverage this playbook to develop risk management strategies tailored to their needs and priorities. Integrating NIST AI RMF principles into their risk management frameworks and leveraging resources such as the NIST framework and playbook can enhance AI systems' safety, reliability and ethical integrity in healthcare settings.

RELI Group's Cybersecurity Expertise

As illustrated above, countless cybersecurity threats pose serious healthcare concerns, showcasing that cybersecurity is a daily necessity. Cyber criminals continue to target hospitals and other facilities, a national problem with the potential to impact every citizen.

RELI Group offers comprehensive cybersecurity capabilities tailored specifically for healthcare organizations. These capabilities cover Security Awareness Training, Incident Response, Cloud Security and more. Our focus is on providing maximum security up front, ensuring that healthcare entities are well equipped to defend against a wide swath of threats.

Our focus is on providing maximum security up front, ensuring that healthcare entities are well equipped to defend against a wide swath of threats.

One of RELI's key approaches involves identifying and analyzing Advanced Persistent Threat (APT) groups that target healthcare sectors. Leveraging the open-source repository from MITRE, we pinpoint healthcare-specific APT groups worldwide, understanding their specialties and motivations for cyber attacks. This insight allows us to effectively develop tailored countermeasures to fight against these threat actor groups.

The MITRE ATT&CK framework has been integral to cyber security initiatives and grants RELI access to a comprehensive taxonomy of adversary TTPs. Leveraging this resource allows RELI to identify potential threats more effectively and develop targeted defense strategies to mitigate risks proactively. Continuous improvement is fostered as healthcare organizations refine their cybersecurity strategies using the latest threat intelligence and emerging attack techniques. MITRE's information repository provides healthcare-specific threat actors and potential mitigations. It helps RELI develop an information assurance repository to identify vulnerabilities and determine the best corrective action to remediate them.

As previously highlighted, phishing attacks have multiplied since the pandemic, and healthcare organizations must be prepared to recognize attempts to infiltrate their networks. RELI administers monthly security awareness and training through phishing campaigns to ensure that all clients are equipped to identify key factors of common phishing techniques.

Unveiling the Layers of Cyber Threats in Healthcare

In addition to this expertise, RELI Group also offers a robust internship program to contribute to the future cybersecurity workforce. RELI's Cybersecurity Internship Program is a pivotal initiative to tackle the cybersecurity workforce shortage. This program not only alleviates the industry's talent gap but also enhances the strength of our company by integrating highly motivated interns into our teams. We provide our interns with comprehensive mentorship and training, as well as valuable hands-on experience. Our interns are encouraged to explore and specialize in the areas of cybersecurity that captivate their interests, equipping them with the skills and knowledge needed for a successful career in the field.

RELI's internship program is distinguished by our unwavering commitment to the growth and development of our interns. We recognize and support them as vital contributors to our team, offering extensive resources and training opportunities in essential soft skills such as resume building and professional development. Furthermore, our internship program is designed with flexibility, allowing interns to seamlessly balance their internship responsibilities with college schedules and other commitments. By fostering an environment that values and nurtures our interns, we ensure that they are prepared to enter the cybersecurity workforce and poised to make significant contributions to the industry.

Final Thoughts

Tackling the current shortage in the cybersecurity workforce is vital for upholding security infrastructure, particularly within the healthcare sector. Our proposed solution, alongside our established cybersecurity internship program, directly addresses this challenge by creating a robust pipeline for developing skilled professionals who are ready to enter the industry. This initiative not only ensures a steady supply of qualified cybersecurity experts but also strengthens the overall security framework of healthcare organizations. By investing in and nurturing talent through structured training, mentorship and hands-on experience, we are equipping the next generation with the essential skills needed to safeguard critical systems. Our program serves as a model for addressing workforce shortages, demonstrating a proactive approach to building a resilient cybersecurity workforce. Through these efforts, we are contributing to a more secure future in healthcare and beyond.

RELI is dedicated to advancing cybersecurity initiatives to ensure the highest level of protection for the healthcare industry. We specialize in providing tailored mitigations to meet the unique needs of each organization, supported by continuous monitoring and maintenance throughout the entire system development lifecycle.

Our highly skilled and knowledgeable security team excels in identifying, mitigating, and resolving cyber threats that could compromise healthcare data and systems. Utilizing cutting-edge tools, our team delivers vital support to bolster the cybersecurity posture of healthcare organizations. We remain unwavering in our commitment to safeguarding the confidentiality, integrity and availability of healthcare data and systems.