UNDERSTANDING THE FIGHT AGAINST TARGETED CYBER THREATS

"There are only two types of companies: those that have been hacked and those that don't know they have been hacked." - Former Cisco CEO John Chambers.

Healthcare businesses are not taking cyber security seriously. For those responsible for budgeting decisions, duties to clients and patients, and ensuring the long-term viability of a business, protecting your internet-connected and networked software and data is as necessary as finding customers and generating revenue. Despite the reality that bad actors work continually to undermine your security and illicitly access your system, companies fail to address basic IT security issues. Business leaders, it appears, either do not fully understand their vulnerabilities or choose to do nothing to address them. Moreover, companies that employ security measures such as firewalls, security cameras, and monitoring procedures view cybersecurity as a finite problem that they can solve rather than an ongoing battle against would-be intruders targeting you, your business, your bank account, and your customers. Common positions include:

"My IT people take care of that."

"Security is an expensive cost, makes me no money, and I see no value in it."

"I have not had a security breach, so what is not broken does not need to be fixed."

The reality is that thieves never stop, and their attacks are increasingly more sophisticated. Ransomware[1] attacks on businesses occur every eleven seconds, and 54% of all ransomware attacks are successful. Although ransomware attacks have decreased in overall volume since 2019, they have become increasingly more effective. In 2020, complex system intrusion attacks designed to deploy ransomware spiked in response to the pandemic and increased by more than 200% through the end of 2021[2]. Hackers also continue to prey on

[1] Ransomware comes in two forms, the most common being a cryptor, a program that encrypts data and demands money in return for a promise to restore the data. Blockers do not affect the data but instead prevent access. Aleksandar Kochovski, *Ransomware Statistics, Trends and Facts for 2022 and Beyond,* Cloudwards (March 22, 2022).

[2] *Data Breach Investigations Report,* Verizon Wireless (2022).

unaware system users through social engineering—psychological strategies that leverage a user's behavior resulting in an action that breaches confidentiality or compromises system access credentials. Thieves feast on your habits, tendencies, and complacency.

A breach can be devastating to a small or medium-sized business. Fines often reach seven figures. For example, a Tennessee-based business associate reached a settlement agreement in September of 2020 with the Department of Health and Human Services to resolve potential violations of the Health Insurance Portability and Accountability Act (HIPAA). The business associate, which provides various services, including health information management services to hospitals and clinics, agreed to pay $2.3 million to HHS and comply with an extensive two-year corrective action plan after a hacker stole protected health information comprising over six million individuals[3]. In addition to fines and damages, companies—particularly healthcare companies—victimized by cybercrime experience severe damage to their reputations. In an industry where privacy and confidentiality are paramount, what health care provider is willing to work with a company that experienced a breach?

The healthcare industry has changed, and many stakeholders have transitioned at least parts of their support structures to overseas resources out of necessity, creating a truly global industry. Others rushed to reorganize and accommodate a remote workforce during the pandemic. Cybersecurity is an ongoing effort. We must strive to remain on pace with attackers and ensure that our infrastructure remains as secure as possible. Unfortunately, bad actors see the pandemic as an opportunity. Total cybercrime increased by 600% during the pandemic[4]. The most significant contributing incentive for pandemic-related cybercrime is remote workers. Every user in your process who works outside your secure corporate network and beyond your security controls creates new vulnerabilities that constitute risks for you, your business, your customers, and their patients. The reality is that opportunistic thieves know this, and your healthcare company with access to medical records is a high-value target[5].

With that in mind, leaders must remain mindful of cyber threats and relentlessly defend their data systems. This article highlights the present dangers and hacker strategies that have emerged in the wake of the pandemic. I also outline risk mitigation strategies, the U.S. Government's efforts to protect patients, and how those efforts affect healthcare organizations.

Flashback to 2020

It was March 18, 2020. The Centers for Disease Control had confirmed the first U.S. Coronavirus case almost two months prior and restricted global air travel. The U.S. declared a public health emergency in February, followed by the WHO's declaration that COVID-19 was a

---

[3] *HIPAA Business Associate Pays $2.3 Million to Settle Breach Affecting Protected Health Information of Over 6 million Individuals,* U.S. Department of Health and Human Services, Press Release (September 23, 2020).
[4] Max Pitchkites, *Top Cyber Security Statistics, Facts & Trends in 2022,* Cloudwards (March 22, 2022).
[5] The black-market value of medical records is estimated to be $250 each and up to $1,000. Credit cards sell for around $4 each, and Social Security numbers are available in bulk for as little as $.01 each.

pandemic and President Trump's national emergency declaration. The healthcare industry faced unprecedented crises as illnesses, hospitalizations, and deaths soared. As a result, hospitals struggled amidst bed, personnel, supplies, and equipment shortages while state and federal agencies began circulating guidance for care rationing.

In a stunning display of humanity, the Maze Team—an infamous group well-known for their high-profile attacks to exfiltrate sensitive files using ransomware—published a press release declaring that the group would "stop all activity versus all kinds of medical organizations until the stabilization of the situation with [the] virus."[6] Following the Maze announcement, additional groups promised a ceasefire with healthcare organizations. While attacks on healthcare organizations did not stop altogether, the commitment seemed promising—for a little while.

Fast forward to October 2020, and all hope that bad actors would keep those promises was long gone. During the Fall of 2020, reports of ransomware attacks against hospitals, medical practices, and every type of business associate that might have access to protected health information were rampant. The increase in activity was so significant that the Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, and the Department of Health and Human Services co-authored an October alert warning of ransomware activity targeting the healthcare and public health sector.[7]

The pandemic suddenly forced millions of people to remain at home while our businesses struggled to sustain operations. Once secure transactions that took place within the virtual confines of network security, monitoring tools, encryption, vulnerability scanning, penetration testing, antivirus software, intrusion detection, packet analyzers, and firewalls transitioned to the porous and untested data pathways of personal home computers, unsecured home Wi-Fi networks, and unencrypted file sharing. The temptation was too much, with a black-market value of $20 for health insurance credentials and between $250 and $1,000 for medical records[8].

Increased Threats and Hacking Strategies

The shift in healthcare to remote work did not result in hackers innovating with new strategies to compromise your data. Instead, for every unprepared sector of the workforce, it was as though we punched holes in our barricades, laid down our arms, and hung welcome signs inviting bad actors into our transactions. Studies demonstrate that hackers and thieves deployed their tried-and-true tactics to worm their way into our systems, workflows, and transactions. That same tactic remains the most significant cybersecurity threat to your organization today: social engineering.

---

[6] *Ransomware Groups Say They Won't Attack Hospitals,* Virsec (March 24, 2020).
[7] *Ransomware Activity Targeting the Healthcare and Public Health Sector,* CISA (October 28, 2020).
[8] *The Value of Date: A Cheap Commodity or a Priceless Asset?,* Trustwave (2017).

Hackers use social engineering or some form of "hacking the human" in 82% of data breaches, and 60% of those breaches involve email deception.[9]

Why are email phishing attacks still considered the most significant threat? You might be familiar with the old saying, "People rob banks because that is where the money is." Phishing works. Recall the September 2020 breach settlement by the Tennessee-based business associate. That breach resulted from a cyberhacking group discovering a worker's credentials through an email phishing attack and accessing the business associate's Virtual Private Network. The business associate, ironically providers of compliance and information technology services, remained unaware of the breach for eight days until the Federal Bureau of Investigation notified them of the intrusion.

You know phishing attacks have become sophisticated when we have names for nineteen variations. These variations include spear phishing, vishing, email phishing, HTTPS phishing, pharming, pop-up phishing, evil twin phishing, watering hole phishing, whaling, cloning, deceptive phishing, social engineering, angler phishing, smishing, man-in-the-middle attacks, website spoofing, domain spoofing, image phishing, and search engine phishing.

Phishing

Phishing is a form of social engineering. Attackers use human interaction, learned social skills, and routine to obtain or compromise information. Typically, an attacker will craft a phishing email to create a sense of urgency, curiosity, or fear in their would-be victims. For example, a common strategy is to spoof a Microsoft email, inform the reader that their password is about to expire, and instruct them to act quickly to avoid disruption. Of course, the reader may click on a link in the email that directs them to a fake Microsoft website, where they may enter their email username and password to reset their password. Immediately upon entering their access credentials, the thief will use them to access the victim's email account. There the attacker will remain hidden for as long as possible to collect information from emails sent and received until discovering something of value.

Another typical example is an emailed notification that the reader has received a fax, voicemail, or a receipt from a recent payment requiring verification. The intent is to raise the victim's curiosity about the communication or fear regarding a charge they do not recall. The attached item does not open the fax, voicemail, or receipt. Instead, it directs the victim to another spoofed webpage asking for login credentials.

Spear Phishing

Software and mail servers with access to threat-sharing platforms can often detect and block phishing attacks because attackers send identical, or nearly identical, messages to hundreds or thousands of users. Spear phishing, on the other hand, is a more selective approach

---

[9] *Data Breach Investigations Report, Verizon Wireless* (2022).

in which the attacker identifies and targets specific individuals. They customize the messaging by using specific characteristics about victims, job positions, companies, and the victim's contacts. Often, the attacker impersonates a close contact of the victim.

For example, the phishing email may appear to come from an executive or a manager in IT to a worker. The email may look and read just as emails from the executive normally do. The deception triggers a feeling of trust in the victim that the message is authentic. Spear phishing requires much more effort by the attacker, and success rates are much higher.

Brute-Force Attacks

The rapid transition to a remote workforce required many businesses to give their employees remote access to secure networks using remote desktop protocol servers, or "RDP" servers. Companies deployed many of these RDP servers—a proprietary Microsoft tool used to access Windows servers and desktops remotely—without the most up-to-date software installed, which left them vulnerable. As a result, hackers attacked these remote access servers using brute-force attacks. The cybersecurity firm Kaspersky recorded over 3.3 billion brute-force RDP attacks worldwide in the first eleven months of 2020, compared to 969 million during the same period in 2019.[10]

A brute-force attack is a strategy by which a hacker uses a program to guess a password or encryption key by systematically attempting every possible combination of characters. Dangers posed by brute-force attacks are why password policies are so important. For example, the practice of using a word or combination of words found in a dictionary is much more susceptible to a brute-force attack than using a random assortment of letters, numbers, and non-alphanumeric characters. Words and numbers associated with you, your family, or your business, including your date of birth, your address, your age, your phone number, your children's names, or a pet's name, are information that a hacker can quickly discover and use when attempting to crack your password.

Today's Risk Mitigation Strategies

A discussion of specific cybersecurity risk mitigation strategies can fill a book. In fact, many books are available on the subject. At a minimum, there are three principles that decision-makers should embrace.

1. Find an expert that you can trust.
2. Learn enough to ensure that your trusted expert works diligently to protect your infrastructure and your data.
3. Be agile.

Finding an Expert

[10] https://securelist.com/the-story-of-the-year-remote-work/99720/

Not all information technology professionals are alike.

Some describe themselves as hardware people, others as network people. First, you must identify a person or organization that understands security in both domains. Your IT support should understand network setup, maintenance, security, and workstation controls such as access, use, encryption, and transport. For healthcare organizations, IT professionals must know regulations specific to healthcare security, including physical, technical, and administrative safeguard requirements contained in the HIPAA Security Rule. Second, your IT professionals must have the resources and tools to monitor your cyber environment efficiently and effectively. Lastly, you should require regular evidence-based reporting that demonstrates the effectiveness of your security controls.

Learn Cybersecurity Basics

You do not have to become a cybersecurity expert. However, you should become familiar with the body of regulations, rules, and guidance that will equip you to make decisions. Many organizations and professional associations offer basic cybersecurity courses for business leaders. Additionally, many federal agencies provide guidance to businesses.[11] Your cybersecurity experts should design your cybersecurity controls according to these regulations, rules, and guidance.

The National Institute of Standards and Technology, a division of the U.S. Department of Commerce, publishes the NIST Cybersecurity Framework as part of the federal government's "recognized security practices" intended to reduce cyber risks cost-effectively. The agency promotes standards, guidelines, best practices, methodologies, procedures, and processes recognized as the most current model for security practices.[12]

Be Agile

A recent trend, particularly regarding the transition to remote workers, is to take a more agile approach to cybersecurity. The threat landscape changes rapidly; therefore, you must equip your business to respond quickly without becoming paralyzed by the process. Frontline security professionals must have the authorization and resources to identify and respond to a threat instantly. Such a posture requires ongoing risk management efforts and continuous, real-time monitoring. Correcting errors and deploying security controls require careful planning, resources, and approvals. However, securing a vulnerability and cutting off an attacker's access to your network should be immediate in response to a threat or a breach.

---

[11] Link to C*ybersecurity for Small Business: Cybersecurity Basics* published jointly by the Federal Trade Commission, U.S. Department of Homeland Security, National Institute of Standards and Technology (NIST), and U.S. Small Business Association: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf

[12] Authorized under 15 U.S.C. § 272(c)(15) and 6 U.S.C. § 1533(d).

Recent Legislative Developments

A 2021 amendment to the Health Information Technology for Economic and Clinical Health Act (HITECH ACT) requires the Department of Health and Human Services (HHS), as part of the agency's enforcement of HIPAA, to consider whether covered entities and business associates have implemented and applied "recognized security practices"—including those regarding cybersecurity.[13] If a covered entity or business associate that suffered a security breach can demonstrate that it implemented those "recognized security practices," the amendment provides for reduced penalties if the breach resulted from a violation of HIPAA's Privacy or Security Rules. The amendment further provides for early and favorable termination of a compliance audit when the covered entity or business associate provides evidence of implementation.

The amendment does not authorize HHS to increase penalties or expand the length, scope, or number of audits based on noncompliance with recognized security practices. Moreover, the legislation does not subject covered entities or business associates to liability for choosing not to adopt and apply recognized security practices. On the other hand, the legislation does not restrict HHS's authority to enforce the HIPAA Security Rule. The good news is that this legislation offers healthcare organizations some credit for efforts to mitigate risk when—despite implementing robust cybersecurity measures and safeguards—they nevertheless become victims of sophisticated cyberattacks.

In April of 2022, HHS published a Request for Information (RFI)[14] to help the agency understand how covered entities and business associates voluntarily implement recognized security practices defined in the 2021 amendment. The RFI further clarified the agency's intentions by indicating that HHS considers a covered entity to have recognized security practices in place for the prior twelve months if the entity fully implemented those practices. However, HHS does not consider the establishment and documentation of the initial adoption of recognized security practices adequate. Instead, you must show that recognized security practices were actively and consistently used.

Final Thoughts

The most important takeaways from reading this article are to recognize that cybersecurity is an ongoing battle, you need experts to fight the battle, and you must equip yourself to lead the battle. No organization, network, or system is ever hackproof. Make a concerted effort to learn about cybersecurity threats and discover how to deploy safeguards within your environment. A robust cyber defense can encourage attackers to move on to easier prey. Your data, your customers' data, and their patients' data depend on it.

---

[13] H.R. 7898; See NIST Cybersecurity Framework.

[14] 87 Fed. Reg. 19833 (Apr. 6, 2022).