

ARTICLE

Under Attack: Five Practical Steps to Thwart Increased Cyber Threats

<https://www.chartis.com/insights/under-attack-five-practical-steps-thwart-increased-cyber-threats>

While health systems have focused on the immediate health needs caused by COVID-19, cyberattacks have increased as hackers have exploited the outbreak's disruption. The World Health Organization has reportedly seen a fivefold increase in cyberattacks since the onset of COVID-19¹. The threat is ever-mounting given the expanded work-from-home workforce, hastened deployments of teleworking infrastructure and new solutions for virtual care and patient communications, among others. Various governmental organizations including the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA)[2] have reported a growing number of malicious actors—including hackers, hacktivists, and state-sponsored hackers—trying to take advantage of unsecured, vulnerable individuals and organizations.

Health systems need to be ready to protect against attacks. Certainly, big investments in new cybersecurity solutions will be limited given the current financial crisis health systems face, but there are several immediate, no-cost, and low-cost steps organizations can take to protect against increased cyberattacks in the age of COVID-19.

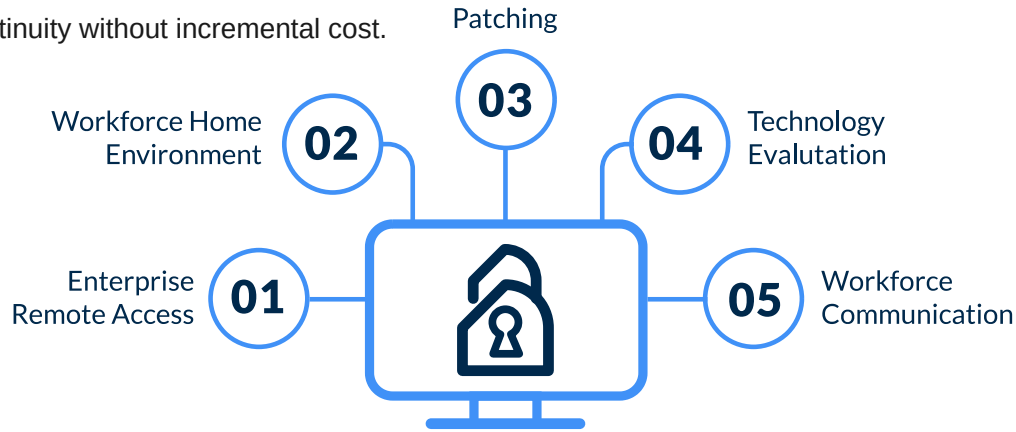
Healthcare and Cyberattacks

The healthcare industry has long been the most popular target industry for cyber actors given its wealth of sensitive data. In fact, the Illinois Public Health Department's website was just recently hacked by ransomware, and the U.S. Department of Health and Human Services' (HHS) computer system has also been under attack. Health systems are also seeing increased threats. For example, while organizations began enabling technologies for their remote workforce, hackers immediately began targeting teleworking infrastructure including remote communications platforms such as Zoom and Microsoft Teams by hijacking online meetings not secured with passwords or unpatched software. Additionally, cyber actors have been attempting to exploit known vulnerabilities affecting VPN products such as Fortinet, Palo Alto and Pulse Secure. The surge in teleworking has also led to an increase in the use of remote desktop applications that utilize Microsoft Remote Desktop Protocol (RDP). Attacks on unsecured devices using RDP have been widely reported. And, given the proliferation of internet-connected devices, we expect the healthcare

industry to see a continuation of phishing- and malware-related incidents using COVID-19 as a lure with ransomware becoming the new norm.

Immediate Priorities for Focus

Below are five immediate key areas for health system focus that can have a positive impact on security and business continuity without incremental cost.



01 – Secure the Enterprise’s Technology That Supports Remote Access.

IT leadership should validate that the primary systems used for remote access have been fully secured. This includes ensuring that remote access systems like VPN technologies are fully patched and system monitoring and alerting is in place to detect abnormal activity. All devices that connect remotely should have properly configured firewalls, anti-malware, and intrusion prevention capabilities in place. Organizations should adequately test remote access solutions for security and capacity, while updating their cyber incident response plans considering the new work environment.

02 – Ensure the Remote Workforce Secures Their Home Environment.

As healthcare organizations continue to roll out teleworking options, policies should be reviewed to ensure organizational use of strong passwords, changed routinely. It is also important to provide guidance on how to best secure their work-from-home environment, including:

- Changing the default password on the home router, enabling WP2 encryption, and using a strong password;
- Encouraging patching of home computing devices that are used to connect to the organization’s network;
- and Securing ePHI or other sensitive data.

03 – Patch, Patch, and Do More Patching.

Many organizations struggle to maintain regular patching cycles for servers and workstations, and malicious actors know this. Operating systems like Windows/Linux and applications like Adobe, Google, and Chrome, among others, need regular patching to address new vulnerabilities. COVID-19 exacerbates the situation as information systems teams are deployed supporting other crisis efforts. Technology leaders should look closely at their vulnerability management programs to ensure this critical process is being properly managed.

04 – Conduct Thorough Technology Evaluations.

The pandemic has prompted organizations to roll out new COVID-19 supporting technologies in compressed timelines. In many cases, new mechanisms have been put in place without proper cybersecurity controls or full assessment of potential risks. One example is the hastened deployment of virtual care to scale with demand, as demonstrated by the [Chartis/Kythera Labs Telehealth Adoption Tracker](#). As a matter of best practice, cybersecurity teams should be routinely engaged to support system selections, design, and rollout. If not already actively participating in these efforts during COVID-19, the chief information security officer (CISO) should closely evaluate any new technology that was recently rolled out to support the crisis to ensure adequate security safeguards and as-needed adjustments have been implemented. Additionally, CISOs should strongly consider evaluating, updating, and testing their Cyber Incident Response Plans, Data Backup Plans, and Business Continuity/Disaster Recovery Plans. Furthermore, a detailed review of the entire security program should be a part of every CISO's roadmap that utilizes existing best practices like the NIST Cybersecurity Framework and Critical Security Controls for Effective Cyber Defense (CIS 20).

05 – Push for More Regular Workforce Communication.

As the situation evolves, healthcare organizations should strongly consider the human factor that contributes to cybersecurity. Most malicious actors rely on basic social engineering methods to convince users to click on a link or download a file or attachment. Many recent phishing emails are disguised to look like a communication from a trustworthy source like from HHS or the local Department of Health with key information regarding the pandemic. Today's crisis requires a strategy that includes ongoing education and reminders to the workforce to exercise caution when handling any email with a COVID-19-related subject line, attachment or hyperlink and to be wary of social media pleas, texts or calls related to COVID-19. It is critical to provide regular training and communications to the workforce on how to spot and report cyber scams, social engineering attacks, phishing and other malicious cyber activity. Regularly reminding employees of the risks and precautions should be part of an overall communication plan.

In this time of unrest, healthcare organizations cannot let their guard down regarding cybersecurity, and there are many impactful activities that technology leaders can be doing now that don't require additional funding. Remaining diligent with cybersecurity efforts should be a priority, even during the COVID-19 crisis. The last thing any health system wants to experience is a cyber incident while responding to this pandemic

or focusing on recovery.

Sources

1 "WHO Reports Fivefold Increase In Cyber Attacks, Urges Vigilance". 2020. Who.Int. <https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance>.

2 HIPAA Privacy And Novel Coronavirus. 2020. Ebook. Office for Civil Rights, U.S. Department of Health and Human Services. <https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf>.

References

"Defending Against COVID-19 Cyber Scams". 2020. Cybersecurity And Infrastructure Security Agency. <https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams>.

Health Care Industry Cybersecurity Task Force. 2017. Ebook. 1st ed. Public Health Emergency. <https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf>.

"Health Sector Council Cyber Working Group" 2020. Health Sector Council. <https://healthsectorcouncil.org...>

"Management Checklist For Teleworking Surge During COVID-19 Response". 2020. Health Sector Council. <https://healthsectorcouncil.org/covid-checklist/>.

"NIST Publishes Multifactor Authentication Practice Guide". 2020. Cybersecurity And Infrastructure Security Agency. <https://www.us-cert.gov/ncas/current-activity/2019/08/01/nist-publishes-multifactor-authentication-practice-guide>.

Our services

[STRATEGIC TRANSFORMATION](#)

[PERFORMANCE TRANSFORMATION](#)

[DIGITAL & TECHNOLOGY TRANSFORMATION](#)

[CHARTIS CENTERS FOR AI & STRATEGIC INTELLIGENCE](#)

[PAYER TRANSFORMATION](#)

[STRATEGIC COMMUNICATIONS & CHANGE MANAGEMENT](#)



Parrish Aharam
Senior Partner



John Petersen
Partner