BROOKINGS

TechTank

Why hospitals and healthcare organizations need to take cybersecurity more seriously

Emily Skahill and Darrell M. West Monday, August 9, 2021

The fuel shortages and rising gas prices generated by the Colonial Pipeline ransomware attack in May foreshadow the disastrous and far-reaching effects of cyberattacks on critical infrastructure. SolarWinds, JBS, Kaseya, and a torrent of other high-profile cyber incidents have captured the attention of the American public and the highest levels of government, leading to a flurry of federal actions, including the nomination of the first-ever National Cyber Director, formal attribution of the SolarWinds attack to Russia, the release of an executive order imposing new security standards for software on federal procurement lists, and a host of legislative proposals to improve the nation's cybersecurity.

Though these prominent cyber incidents have triggered several cybersecurity initiatives, policymakers have paid relatively little attention to the considerable potential cyber risks in the healthcare sector. The WannaCry ransomware attack which took down the United Kingdom's National Health Service in 2017 served as a wake-up call to healthcare organizations around the world, illuminating the urgent need for proactive investments in cybersecurity. And yet, healthcare organizations in the U.S. remain a vulnerable target, lagging behind other industries on key measures of cyber-readiness.

As the resurgence of COVID-19 cases stretch hospital capacity to the limit, it provides a fresh reminder of just how critical it is for our healthcare infrastructure to be resilient in times of crises. With the sharp uptick in ransomware attacks on healthcare organizations during the pandemic, and the first death attributed to a ransomware attack in 2020, it is clear that that malicious actors are capable of compromising mission-critical healthcare infrastructure, from the automated refrigerators that store blood products for surgeries to the CT scans that are vital for triaging trauma patients.

Indeed, the recent surge in cyberattacks on healthcare organizations prompted the Cybersecurity and Infrastructure Security Agency, the FBI, and the Department of Health and Human Services (HHS) to release a joint advisory warning of "an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." At the same time, many hospitals are once again reaching surge capacity due to the Delta variant, making cybersecurity more important than ever before.

The Poor State of Healthcare Cybersecurity

In 2017, the Health Care Industry Cybersecurity (HCIC) Task Force established by HHS issued a report to Congress in which they claimed that healthcare cybersecurity is in "critical condition." Four years later, the Task Force's assessment still rings true. Since the onset of the COVID-19 pandemic, the rate of ransomware attacks has soared across all industries, and healthcare has been the disproportionate target of such attacks. The 2020 HIMSS Cybersecurity Survey revealed that 70% of hospitals surveyed had experienced a "significant security incident" within the past twelve months, including phishing and ransomware attacks that resulted in the disruption of IT operations (28%) and business functions (25%), as well as data breaches (21%) and financial losses (20%).

Healthcare organizations are an inviting target for financially motivated threat actors because their broad attack surfaces make it relatively easy for cybercriminals to find vulnerabilities and monetize their exploits. The passage of the HITECH Act in 2009 incentivized investments in health information technology to modernize the U.S. healthcare system, leading to unprecedented connectivity and an expansion in the usage of medical devices. Today, Electronic Health Record systems are the heart of the healthcare organization, connecting medical devices with other applications to provide a more wholistic picture of patient well-being. Additionally, the U.S. boasts an average of 10 to 15 networked medical devices per hospital bed, meaning large healthcare organizations face the herculean task of securing tens of thousands of medical devices, many of which are quite easy to hack. The digitization of healthcare infrastructure catalyzed major advancements in patient care, but also created major opportunities for attack. A single vulnerable asset can provide a threat actor with a foothold into the organization and compromise the confidentiality, integrity, and availability of patient data and medical services.

At the same time, protected health information is far more lucrative than credit card information. Criminals can garner anywhere from $10 to $1,000 per stolen medical record, depending on their completeness. This combination of a broad attack surface and strong financial incentives make healthcare organizations an appealing target for threat actors.

To make matters worse, cybersecurity is underprioritized by many healthcare organizations due to competing priorities and finite resources. The 2020 HIMMS Cybersecurity Survey reveals that "cybersecurity professionals may not necessarily have access to the security solutions and other tools they need in order to fully secure the environment" due to tight and stagnant IT budgets. Moreover, researchers have found that the average healthcare organization spends about 5% of its IT budget on cybersecurity, while the rest is devoted to the adoption of new technologies. Alarmingly, this means that organizations are expanding their attack surface despite lacking the tools to adequately defend their digital estate.

Consequently, the healthcare industry has fallen behind many other sectors in its ability to detect, prevent, and mitigate cyberattacks. For example, healthcare organizations take an average of 236 days to detect a data breach and 93 days to mitigate the damage, compared to an industry average of 207 days to identify and 73 days to contain an attack. Due to their failure to proactively invest in cybersecurity, healthcare organizations hit with cyberattacks have paid steep costs to mitigate the threat. IBM's 2021 Cost of a Data Breach Report revealed that the healthcare industry had the highest cost of a data breach for the eleventh year in a row, with an average cost of $9.23 million in 2021. Studies have demonstrated that proactive investments in cybersecurity lead to long-term saving, but cybersecurity spending can be hard for healthcare administrators to justify when faced with other compelling priorities, like staff increases to meet the demands of a once-in-a-century pandemic.

The Path Forward

With an ever-increasing attack surface, compelling financial incentives for attackers, and under-budgeted, substandard cybersecurity operations, the US healthcare system is indeed in critical condition. Public-private partnerships and increased investments in healthcare cybersecurity will be key to shoring up the healthcare industry and safeguarding the nation's critical infrastructure.

Just as handwashing is a foundational element of modern medicine, cyber hygiene must be regarded as a basic and essential component of a functioning medical system. At present, healthcare systems are highly vulnerable to cyberattacks and opportunistic threat actors are increasingly taking advantage of the industry's weak security posture to exfiltrate patient data and disrupt key medical systems. With the confidentiality, integrity, and availability of patient data, medical devices, and entire healthcare systems at stake, healthcare organizations must undergo a paradigm shift, placing greater value on cybersecurity and proactively investing in security protections.

"Just as handwashing is a foundational element of modern medicine, cyber hygiene must be regarded as a basic and essential component of a functioning medical system"

Policymakers can encourage proactivity by providing matching funds to organizations that seek to engage in risk-based planning and bring their practices up to par with state and federal regulations. Additionally, policymakers can simplify and strengthen the regulatory environment for healthcare security to develop a more unified and comprehensive set of standards that healthcare organizations can easily navigate. Federal agencies must also continue to collaborate with healthcare industry partners to develop robust contingency plans to avert catastrophe in the event of a serious cyber incident.

In the end, however, the fate of healthcare security comes down to whether organizations are willing to make significant investments in cybersecurity. If the healthcare sector is to move the needle on cybersecurity, industry leaders must begin to treat digital assets as they would patients. Just as a responsible healthcare professional seeks to identify and treat patients' underlying chronic conditions before they cause a serious medical emergency, so too must responsible healthcare organizations address vulnerabilities in their digital infrastructure to prevent cyberattacks. After all, even computers are not immune to viruses.

IBM is a general, unrestricted donor to the Brookings Institution. The findings, interpretations, and conclusions posted in this piece are solely those of the authors and not influenced by any donation.