COSMOS
Navigate the Compliance Universe

Compliance Today - December 2023

Lynn M. Barrett (lbarrett@wachler.com) is a Partner at Wachler & Associates PC in Royal Oak, MI.

Daniel D. Ayyash (dayyash@wachler.com, linkedin.com/in/danielayyash/) is a healthcare attorney at Wachler & Associates PC in Royal Oak, MI.

Understanding a growing threat: The importance of cybersecurity in healthcare

by Lynn M. Barrett, Esq., CHC, CCP; and Daniel D. Ayyash, Esq.

Healthcare providers and facilities of every size are increasingly being targeted by cybercriminals and falling victim to ransomware attacks, data breaches, and a host of other potentially crippling cybersecurity incidents. In May 2023, 44-bed Mountain View Hospital and 88-bed Idaho Falls Community Hospital (IFC) and their affiliated clinics—which are in rural areas and share the same campus—were victims of a cybersecurity attack that resulted in the facilities having to take their IT system offline, resorting to using paper records, closing some clinics, and diverting ambulances from IFC's emergency room.[1] It took over two weeks for the hospitals to resume accepting ambulances, and still longer for the hospitals and clinics to resume normal operations. With a population of roughly 68,000, Idaho Falls' residents have endured disproportionate impacts arising from the cyberattack since healthcare resources in rural communities are simply less abundant compared to more developed urban areas.

More recently, in August 2023, Prospect Medical Holdings—a private equity firm that operates 16 hospitals and over 165 other clinical facilities in California, Connecticut, Rhode Island, and Pennsylvania—was the victim of a cyberattack that took out critical computer systems for several weeks. As a result, the multistate system had to close some emergency rooms, divert ambulances, and revert to paper charting, as well as cancel elective surgeries, outpatient appointments, and blood drives.[2]

According to IBM Security's *Cost of a Data Breach Report 2023*, since 2020, healthcare data breach costs have increased 53.3%, with an average cost of USD $10.93 million per breach.[3] In the first six months of 2023, there were 395 data breaches of 500 or more records reported by healthcare providers to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR).[4] In August 2023 alone, OCR initiated 18 investigations into data incidents involving eight healthcare providers and seven health plans.

Cyberattacks can have wide-ranging and severe impacts on healthcare systems, resulting in damage to patient health and privacy, costly disruptions to operations, and demanding regulatory consequences. Cybercriminals target healthcare providers and facilities because of the amount and type of information and data they can access.[5] But what exactly does all this mean, and what steps can be taken to address cyberattack concerns?

This article will review a range of cybersecurity incidents, certain consequences of cybersecurity incidents, what regulatory and other governmental responses have been taken, and what compliance professionals and providers can do to help avoid and mitigate the effects of cyberattacks.

What is cybersecurity?

Cybersecurity is a complex and constantly evolving sector comprised of numerous concepts and endless potential pitfalls. So, what exactly is cybersecurity? As a general definition, cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.[6] In today's society, it seems as if nearly everything relies on or is integrated with computers and the internet. Communication, financial transactions, entertainment, transportation, and healthcare are just a few areas deeply connected to and potentially dependent on computers, the internet, and other connective technologies. Many people would be surprised to learn how much of their sensitive information is not only stored on and accessible by local devices such as smartphones or personal computers but also by public and private servers, databases, and other IT systems. Cyberattacks that seek to obtain or expose this information can take on many different forms and may appear entirely harmless, such as a seemingly innocuous email that appears in your inbox but contains harmful malware. When it comes to cybersecurity, there is no such thing as being too cautious, and being able to identify and comprehend the risks associated with various situations can be crucial to maintaining the security of cyber data.

Hackers and intruders. The first step to recognizing cybersecurity risks to make informed decisions about protecting cyber data is to become familiar with common terminology and situations. Cybercriminals are generally referred to as "hackers," "attackers," or "intruders," and these terms refer to people who seek to exploit weaknesses in an entity's software and/or computer systems. Hackers or intruders usually take advantage of these exploits for their own gain, and their actions typically violate the intended use of the systems they are exploiting. Cyberattackers also generally target more vulnerable computer systems with larger attack surfaces, which is the set of different points where an attacker can try to enter, cause an effect on, or extract data from. If a hacker is successful, the results can range from having to deal with minor pesky viruses (such as annoying pop-ups or unwanted plug-ins) to malicious and destructive activity (such as stealing information or corrupting a computer's data).

Malware, phishing, and spoofing. Cybercriminals often seek to inject computer systems with malicious code to accomplish their nefarious objectives. "Malicious code" or "malware" are unwanted programs or software that can damage or compromise data stored on a computer. Malware can have various characteristics, such as requiring the user to perform some action before it infects your computer. This could be as simple as opening a suspicious email attachment or clicking a link to an unfamiliar website. Some forms of malware spread without user intervention and typically begin by exploiting a particular software vulnerability. Once the victim's computer has been infected, the malware may attempt to infect other computers. Many people likely know of someone who has had their email or social media hacked, where the program sends spam messages without them even knowing.

Further, such spam or infected messages may contain an attachment or link to a website that claims to be one thing while in fact doing something entirely different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder. This technique is referred to as "phishing," where a cybercriminal attempts to acquire sensitive data, such as bank account numbers or patient medical records, through a fraudulent solicitation in an email or on a website. A similar concept is "spoofing," where a cyberattacker pretends to be a trusted entity or device to get the receiver to do something beneficial to the attacker. Generally, spoofing consists of two components. First, there is the spoof, such as a fake email or website that looks real. In addition, there is a social engineering component, where the cyberattacker uses psychological manipulation to convince the recipient to do something, such as reveal a password, send money, or approve a wire transfer. Unfortunately, it seems increasingly easy for cyberattackers to appear as reputable people or legitimate businesses, and in our busy lives, it is just as easy to make one wrong

click.

Ransomware. On a larger scale, malware may take the form of a ransomware attack where a computer system is hijacked and its data encrypted, with users being denied access until the hacker is paid a ransom—usually in cryptocurrency—to decrypt or unlock the system. Since a ransomware attack is typically motivated by money, these types of attackers usually target larger entities with highly sensitive data, such as hospital systems that maintain protected health information (PHI).[7] Healthcare providers and hospitals are uniquely susceptible to ransomware attacks because of the highly sensitive nature and amount of individuals' health data. Additionally, the COVID-19 pandemic forced many healthcare entities to rapidly adopt cloud-based databases and other computer systems to accommodate remote and virtual healthcare needs. Although these implementations were done with pure intentions to improve patient care and save lives, the unintended consequence is a dramatically expanded digital attack surface because a greater volume of data is stored online or hosted by remote third parties. Hospitals and other healthcare providers typically utilize third parties to write code and develop the technology for these computer systems, so it is imperative that this technology is as secure as possible.