OPERATOR INSIGHTS

presented by ENSEMBLE HEALTH PARTNERS

Cybercrime: *A Troublesome Consequence of a Continuing Pandemic*

Cybercrime is flourishing during the COVID-19 public health crisis. According to the Federal Bureau of Investigation (FBI), daily digital crime rose 75% from the start of stay-at-home restrictions until June. And the increasing activity shows no signs of slowing. Three elements have come together to form a perfect storm, enabling the rise in nefarious activity. First, there is greater opportunity—a key driver for theft. With the federal government sending out stimulus checks, extending unemployment benefits, and offering small business loans in response to the pandemic, it has rapidly made money available without many of the typical checks and balances. This has created easier access to a significant amount of funds and opened up the opportunity for fraud and abuse.

At the same time, people are more vulnerable due to the uncertainty and confusion surrounding the virus. They are simultaneously worried and isolated, making them more susceptible to information that appears to provide clarity, insight, and reassurance. Mounting worry is causing the public to click on links they shouldn't, open emails they normally wouldn't, and unwittingly share personal information like credit cards and social security numbers with scammers.

Completing this perfect storm is the mass uptick in Internet use. With a good portion of the U.S. workforce performing their jobs remotely, there is a lot more virtual interactions, including Zoom meetings, emails, instant messaging, and so on. In addition, shopping has moved online with a greater number of people buying things off their computers versus going to the store. The increased Internet traffic is providing fertile ground for cybercriminals to wreak havoc.

Phishing: A chronic problem for healthcare organizations

Even prior to COVID-19, hospitals and health systems were targets for cyber criminals because of the wealth of sensitive, confidential, and comprehensive data these entities collect, store, and use. While healthcare organizations are at risk for many kinds of data breaches, one of the biggest threats is phishing—where scammers use email or text messages to trick people into giving out their confidential information, such as passwords, credit card numbers, social security numbers, and so on. The challenge with phishing is that an organization's vulnerability rests with its staff. If employees don't know how to recognize and avoid these communications, they can inadvertently share information they shouldn't. Even worse, they can click on links that introduce malware into the hospital's IT system, which can lead to more serious cybercrimes, such as ransomware.

Another difficulty with phishing is that it plays on people's fears, which is why it's so insidious in the current climate. For example, there was a recent phishing scam where emails appearing to be from the World Health Organization detailed COVID-19 preventive measures. The wording of the emails was designed to trick people into clicking on malicious links and opening attachments to reveal their username and password. This allowed scammers to steal money and sensitive information.

When phishing emails seem to come from an authority, they can be hard to ignore. Consider the example of an email that was sent out from the "Johns Hopkins Center," which included an Excel attachment that claimed to include U.S. COVID-19 cases. If a staff person opened the Excel file, it downloaded a hostile macro and remote support tool that could be used for nefarious purposes. The university's Center for Systems Science and Engineering has maintained a widely respected COVID-19 tracker to which many healthcare organizations send data. By using a similar, yet slightly different name, the scammers were able to fool several healthcare organization employees into thinking they were sending data to Johns Hopkins, causing them to unknowingly share confidential information.

Stepping up cybersecurity strategies has never been more important

Given the precipitous rise in cyber incidents coupled with the fact that healthcare organizations are prime targets for this type of crime, hospitals and health systems would be wise to take a closer look at their current cybersecurity program and make sure it is robust enough to avert mounting risks. A solid strategy requires a two-pronged approach in which organizations marry technology safeguards with behavioral changes. First, organizations need to examine what they are doing from an IT security perspective to build impenetrable "walls" around sensitive personal, financial, and health information. Entities should follow industry best practice to not only prevent unauthorized access but also quickly respond to any data breaches that do occur, keeping them contained and limiting damage.

Second, organizations must look at how they are training their employees to recognize and avoid potential threats. Regular communication and reminders are key; however, organizations must maintain a delicate balance between providing the latest information and bombarding staff with constant communications that are easy to ignore. Using real-world examples can cut through the noise and help underscore the importance of cybercrime awareness and prevention. In addition to training staff on the risks, organizations should test whether the training is effective or if there are any gaps that remain. This may involve sending simulated phishing emails that reveal what staff is still clicking on, highlighting potential risk points to address.

Another strategy for mitigating risk is to develop a solid business continuity plan. If the pandemic has taught healthcare organizations anything it is that the unexpected can and does happen. Having a business continuity plan can ensure the organization will continue functioning even amid a crisis or unforeseen event. When creating a business continuity plan, first consider what critical processes must keep running no matter what. Then, look at how IT supports those processes and what proactive measures need to be in place in case something happens. For example, what if an organization loses its primary site or, as is the case for many companies right now, what if its entire workforce has left the primary site and is now working remotely, using their own personal networks. How is the organization safeguarding data? By having a plan upfront, the entity can quickly move operations to maintain continuity and be confident it has the appropriate protocols in place. One of the difficulties early on in the pandemic was that people were shifting to remote work on the fly, which opened up opportunities for cybercrime that may not have been there if organizations had more well-developed business continuity plans.

> **"HAVING A BUSINESS CONTINUITY PLAN CAN ENSURE THE ORGANIZATION WILL CONTINUE FUNCTIONING EVEN AMID A CRISIS OR UNFORESEEN EVENT.**

When reviewing cybersecurity measures and business continuity plans, be sure to check with vendors and other business partners about their strategies and programs. Not only is this important in terms of protecting sensitive patient and business information, but it is critical from a compliance standpoint as well. HIPAA holds healthcare organizations accountable for data breaches, even when they occur in a vendor or business associates' systems. Before contracting with a vendor, ask about and agree on necessary security measures, including the need for a designated IT security representative who makes sure the appropriate IT and staff training protocols are in place. Don't forget to document any and all security measures in the vendor's business agreement.

Unlike the pandemic, cybercrime is here to stay

Cybercrime will continue to thrive as long as the factors fueling its growth remain present. However, healthcare organizations that are proactive about putting safeguards in place and are committed to regularly reviewing and updating those strategies, can mitigate cybersecurity risks and keep their patient and company data private and secure.

Matt Tormey, Chief Compliance Officer, Ensemble Health Partners

Blaine Kerr, Sr. Director, Privacy and Security, Ensemble Health Partners

ENSEMBLE®
HEALTH PARTNERS

Solutions born from experience, not theory.
Contact us to learn more at Solutions@EnsembleHP.com or 704-765-3715.