INSIGHTS FROM THE BDO CENTER FOR HEALTHCARE EXCELLENCE & INNOVATION

BRACE FOR THE BREACH — BDO CYBER THREATS INSIGHTS

Two trusted leaders in the field of cybersecurity explain the latest trends in types of cyberattacks and offer case studies and lessons learned in a webinar on Oct. 17, 2018. They revealed the most underrated threats to the health sector, and offered guidance on building a "cybersecurity culture," including suggested policies and procedures.

Understanding the landscape of cybersecurity threats and ways to mitigate those threats can seem daunting. New threats are emerging all the time, as bad actors seek to gain access to the valuable data collected and stored by healthcare organizations, including health systems and hospitals.

"We have to really start with leadership," said Shawn Belovich, a managing director in the technology & business transformation services practice at BDO. "We need to embrace cybersecurity and we need to push it across the board."

In the first half of 2018, U.S. healthcare organizations reported 176 large-scale data breaches. With the widespread adoption of electronic health records (EHRs) and introduction of many other connected technologies in the health setting, hospitals and health systems are vulnerable to cyberattacks. For instance, the number of connected medical devices is estimated at 10 billion, and will reach 50 billion by 2028, according to BDO. Meanwhile the cost of cyber liability insurance continues to climb along with the number and frequency of attacks.

As a result of this threat, healthcare organizations are beginning to re-evaluate operations, Belovich said.

Read more ▶

TYPES OF ATTACKS AND THEIR PREVALENCE IN HEALTHCARE

In order to adequately prepare, healthcare organizations should understand the cyber threat landscape, said John Riggi, senior advisor for cybersecurity and risk at the American Hospital Association (AHA) and former FBI cyber executive. Riggi identified the top seven general categories of attacks as:

- Denial of service attacks
- Business email compromise
- Supply chain attacks
- Internal threats
- Crypto hijacking
- Ransomware
- Computer intrusions

Denial of service attacks make a machine or network resource unavailable to intended users, disrupting their work and processes. Denial of service attacks can sometimes be amplified by criminal services available on the Dark Web, Riggi explained, making them more damaging. Luckily these have not been too prevalent in healthcare. However, a growing category of threat is supply chain attacks, wherein an adversary attempts to compromise a vendor's technology or network connections to penetrate the network of the vendor's customer. Given the large number of vendors and the variety of technology and services moving in and out of hospitals every day, this type of attack may represent a significant vulnerability for hospitals and health systems.

"Before resources are diverted from defending against external threats to defending against internal threats, one has to understand what constitutes an internal threat related incident reported to HHS," Riggi said. These types of data losses include stolen unsecured laptops or, for example, staff mistakenly emailing unencrypted spreadsheets containing protected health information.

Crypto hijacking, on the other hand, is a growing threat that is not well-known in the healthcare sector, Riggi said. This "cryptojacking" malware harnesses an organization's vast computing power, network resources, and energy to illegally mine lucrative digital currency. While the malware itself may not intentionally do harm to a computer system, its energy and computing power drain may disrupt important services that hospitals provide and compromise care delivery or patient safety, Riggi said.

Ransomware continues to be the best-known and perhaps the greatest cyber threat to hospitals. "Although the economic gain by the bad guys is relatively low, the impact to care delivery operations and potentially patient safety may be significant," he said. Belovich also noted that Ransomware services can be purchased on the Dark Web, allowing for the easy entry of new threat actors.

Another major and perhaps the most significant threat to hospitals are computer intrusions originating from external, mainly foreign-based criminal organizations. Based upon a June 2018 study of Federal data published by the American Medical Informatics Association, hacks account for just 15 percent of all cyber incidents in healthcare, but 85 percent of stolen records, Riggi said. The average price on the black market for a lost or stolen health record is $408, compared to $148 for all industry records, showing that patient records are desirable stolen goods.

WHO'S BEHIND THE THREATS?

Hacktivists, criminals and nation-states are the three broad categories of cyber adversaries who are conducting these types of cyberattacks. For hospitals and health systems, criminals are the biggest threat because they tend to go after high-value targets of patient health data to sell on the dark web and monetize through other frauds. Criminals may also deny access to critical information such as patient records by encrypting those records through the deployment of ransomware. However, nation-states are also a significant cyber threat and have increased their targeting of hospitals and health systems.

"They're being targeted by hostile nation-states for theft of intellectual property related to medical research, innovations, cancer studies, population health studies, research for precision medicine and clinical trials, and also potentially for conversion for military use such as biological weapons," explained Belovich and Riggi. "They also could be looking for advancement of healthcare in their own countries or some combination thereof."

Additionally, nation-states may be looking for individual health records of high-value targets such as leaders of our military or government, Riggi explained. He recalled having a conversation with the CEO of a small, rural hospital in the Midwest who felt that his hospital would never be the target of a nation-state.

"When I asked the location, I realized immediately that they were positioned right outside a sensitive government military installation," Riggi said, adding that the personnel with high-level security clearances and their families associated with this base may be treated at the local hospital. "I guaranteed this CEO that his hospital and all his network connections had already been mapped, probably by China and Russia, seeking to gain those health records."

As with this rural hospital CEO, many healthcare leaders underestimate the threat from nation-states. In a survey by the AHA of 475 hospitals, only 7 percent of respondents named nation-states among their top three cyber adversaries. The most cited were external criminal cyber adversary (52%), internal threat (38%) and hacktivist (10%). It's interesting that hacktivists were cited more often than nation-states as a top cyber adversary, but reports show that very few hacktivists target hospitals, Riggi and Belovich said.

Read more ▶

INTERCONNECTEDNESS AND CYBER THREATS

As hospitals become more digitally connected, they increase their risk of attack. The global electronic health market was valued at $23.5 billion in 2016, and is expected to reach more than $33 billion in 2023. The drivers behind this market are adoption of electronic health records (EHRs) and mobile devices as well as the move to cloud-based software solutions for hospital processes and mobile devices.

"The healthcare field is in the early stages of re-evaluating its operations with regard to new cyber threats," Belovich said. "The field has to continually monitor and change its strategy and re-evaluate the strategy to handle our investments in technology."

Just getting a basic accounting of all the devices that are network-connected at a hospital can be a tremendous challenge, Riggi said. There's also a phenomenon of so-called "shadow IT" where clinicians and other staff may attach devices to the network without the knowledge of IT professionals, creating a gap between the inventory of connected devices and the actual number of devices connected throughout a facility, he added.

In the past year, there's been a 126 percent increase in the recall of medical devices as a result of corrupted software, Belovich noted.

KNOWING AND FEARING ORANGE WORM

Orange Worm is a new threat actor that has deployed malware in a campaign targeting the healthcare field and its supply chain across the world. Orange Worm has been observed installing a custom software backdoor across the healthcare field. The major targets, specifically in the supply chain, are pharmaceutical companies, IT companies supporting healthcare organizations and medical device manufacturers. Importantly, Orange Worm can mutate and avoid detection like a biological virus.

"Orange Worm overall has been very patient and well-conceived," said Belovich.

For Riggi, Orange Worm is an example of a well-conceived supply chain attack, along with the intelligence and evolution of cyber adversaries. "Orange Worm to me is very concerning," he said. "There are a couple of reasons why. Although it's been detected, it has been detected lying dormant and the true intention is not known. It is speculated the malware may have been developed for economic espionage reasons. Whenever I see sophisticated malware lying dormant, for me that indicates potential hallmarks of nation-state activity. I'm not stating Orange Worm originated from a nation-state, but, again, its true intent is very suspicious. Infected medical devices, such as MRI machines, can have a tremendous impact on patient safety and care delivery if any malware goes undetected and causes a malfunction in the machine."

FOUR CASE STUDIES OF CYBERATTACKS

Four case studies of recent cyberattacks on health providers—all included in the **BDO Cyber Threat Insights Report for Q2 2018**—focused on the healthcare field and, were presented by Belovich and Riggi, to illustrate the cybersecurity challenges facing the U.S. healthcare field:

1. A non-profit healthcare organization in the Mid-Atlantic breached in spring 2018 in a malware attack affected 500,000 patients, with compromised EHRs, patient registration and billing records.

2. A healthcare practice in the Midwest in spring 2018 was hit by SamSam ransomware, a very strong form of encrypted software, with a Bitcoin ransom demanded.

3. A physician practice on the West Coast in late summer 2018 was hit at all three facilities. The attacker encrypted the EHRs of 85,000 current and former patients, which were stored on the system of a third-party IT vendor.

4. A physician practice in the Midwest in late spring 2018 experienced ransomware that disabled all files, system functions and the system report function. Servers were taken offline for four days with a ransom demanded in Bitcoin.

THE RAMIFICATIONS OF RANSOMWARE

Ransomware attacks don't just affect computer systems – they can also result in ambulance diversions and systems failures that directly affect patient safety, Riggi noted. Long term, the effects can mean possible accreditation issues, fines and reputational harm to the brand, Belovich added.

Some of the actions hospital leaders can take include providing cybersecurity training for all staff members and providers, appropriately assessing the security of third-party vendors, changing and strengthening passwords, educating patients on the issue through multimedia, and designing everything in the hospital system and workflows with security in mind, both experts said.

Metrics can help gain the attention of executives and board members, they added. For instance, the click rate on test "phishing" emails (where the user clicks on a link that provides a way for a virus to enter a computer network) can be as high as 30 percent within an organization. Staff training, frequent reminders and most importantly an organizational culture of cybersecurity can reduce the click rate to under 10 or even 5 percent, said Riggi.

"The challenge is presenting metrics that are not too technical and tactical to the CEO and the board," he said. "Boards and CEOs understand risk and they understand risk reduction." Based upon attendee feedback BDO/AHA cybersecurity webinar on October 17, 2018 was very well received.

Read more ▶

KEY TAKEAWAYS – CYBERSECURITY BEST PRACTICES FOR THE HEALTHCARE FIELD

According to Gregory A. Garrett, BDO's Head of U.S. & International Cybersecurity, the following cybersecurity best practices have been gathered from the education, training, and consulting services which BDO has conducted in the past year in partnership with the American Hospital Association (AHA):

- Understand U.S. hospitals and health systems are high-value targets for cyberattacks, thus, cyber education and training programs are a must!
- Gather threat intelligence in order to understand the threat landscape to help your organization prepare in advance of a cyber data breach.
- Hire an independent firm to conduct email attack threat assessments, network attack threat assessments, vulnerability assessments, and penetration testing on your information system in order to obtain an accurate picture of your organization's real information security posture.
- Realize cyber threats are always changing, evolving and growing in sophistication so it is vital to have an effective Business Continuity Plan and Disaster Recovery plan.
- Ensure your organization has an active monitoring, detection, and incident response capability to rapidly identify cyber intrusions and quickly contain and eradicate malicious software.
- Inform senior leadership and governing board members with relevant but not overly complex cyber threat statistics to help inform them so they can make better business decisions regarding cybersecurity investments.

Don't miss the latest BDO News and insights – subscribe here.

People who know Healthcare, know BDO.

ABOUT THE BDO CENTER FOR HEALTHCARE EXCELLENCE & INNOVATION

The BDO Center for Healthcare Excellence & Innovation unites recognized industry thought leaders to provide sustainable solutions across the full spectrum of healthcare challenges facing organizations, stakeholders and communities. Leveraging deep healthcare experience in financial, clinical, data analytics and regulatory disciplines, we deliver research-based insights, innovative approaches and value-driven services to help guide efficient healthcare transformation to improve the quality and lower the cost of care. For more information, please visit https://www.bdo.com/industries/healthcare/overview

@BDOHealth www.bdo.com/blogs/healthcare

Accountants | Advisors | Doctors
www.bdo.com/healthcare

ABOUT BDO

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 650 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 80,000 people working out of nearly 1,600 offices across 162 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

CONTACT

GREGORY GARRETT
Head of U.S. and International Cybersecurity
703-770-1019 / ggarrett@bdo.com

PATRICK PILCH
Managing Director and National Leader, Healthcare Advisory
212-885-8006 / ppilch@bdo.com

SHAWN BELOVICH
Managing Director, Technology & Business Transformation Services
202-644-5430 / sbelovich@bdo.com