Revenue Cycle Advisor

powered by HCPro

Top lessons learned from 2020 breach analysis

May 1, 2021 | Briefings on HIPAA

Top lessons learned from 2020 breach analysis

Protenus, a Baltimore-based healthcare compliance analytics company, has released its annual Breach Barometer. It measured 758 health data breaches reported to the Department of Health and Human Services (HHS), the media, or some other source during 2020.

Protenus found the total number of insider incidents increased for the first time in four years in 2020 (110 to 150), and the number of patient records affected by insider incidents also increased from 3.8 million to 8.5 million year over year.

And human error—or malicious behavior by employees—was much more damaging in 2020 than it was in 2019.

Further, hacking incidents increased substantially for the fifth straight year (330 to 470). Further, 2019 and 2020 saw 68 million patient records affected by hacking incidents, compared to 38 million from 2016 to 2018.

"My number one concern is still the lack of importance organizations put on security," says **Rick Ensenbach, CISSP-ISSMP, CISA, CISM, CCSFP,** director at Wipfli in Eau Claire, Wisconsin. "It is often thought of as an additional responsibility, meaning it is secondary to the assigned individual's primary job. It is also often thought of as an IT responsibility, rather than organizational. Organizations need to recognize that the size and complexity of an organization coupled with the misconception — 'it will never happen to us' — must not determine the level of importance an organization puts on information/cybersecurity."

Basic gaps exist

As the Protenus report cites, COVID-19 has had an impact on how hospitals view security. So much attention has been put on the pandemic, and rightfully so. That doesn't mean security should—and can—be sidelined, according to **Kevin Beaver, CISSP,** independent information security consultant with Atlanta-based Principle Logic, LLC, and author of Hacking For Dummies.

"Based on what I see in hospitals and healthcare in general, there are serious gaps in terms of the basic security controls that make up a reasonable security program," Beaver says. "This includes patching, periodic and consistent vulnerability, and penetration testing and network visibility. It's easy for me to say as an outsider, but I still assert that there's never a good excuse to ignore such basics. Anyone who does is going to have a hard time demonstrating due care and will end up on the wrong side of the defensibility discussion."

Ensenbach says compliance has been sidelined in some cases in the past 15 months, an unfortunate outcome of the pandemic. The pandemic is being used as an excuse to not comply, or rather not doing, what people know they should be doing, he adds.

"I know some people who have said they can't do their risk management activities due to COVID," Ensenbach says. "While that may be true, it also tells me there is another problem: lack of qualified resources/manpower. Security often takes a second seat to everything else because many have a false sense of security."

Work-from-home led to risky security business

When the pandemic hit there was a rush to enable more people to work from home says **Jeff Bell**, chief information security officer, advisory services, at Nashville, Tennessee-based healthcare IT partner CereCore. This meant expanding VPN or other remote access technology, as well as video conferencing.

"In the rush to implement or expand these capabilities organizations may have set aside normal security checks and security practices," he says. "For example, technology changes may have been made without a security assessment. Shortcuts were possibly taken that violated the organization's security policies or security best practices."

Here are some examples Bell cites:

- Using older laptops with unsupported operating systems
- Permitting use of personal devices to access the corporate network
- Loosening security posture requirements for remote connections

"Systems could have been directly exposed to the Internet to allow access without a VPN connection," Bell says. "This possible exposure to vulnerable or insecure remote access protocols, such as Microsoft Remote Desktop Protocol, to attackers, or multifactor authentication requirements, may have been circumvented."

Security teams, he adds, should run vulnerability scans and configuration checks and in general perform a security risk assessment of recent changes to identify and mitigate the increased security risks of such changes.

"Good security practices organizations have adopted to manage cybersecurity risk should not be set aside without careful consideration and authorization," Bell says, "but if that may have happened, any new vulnerabilities or risks should be discovered and corrected as soon as possible."

More breaches overall, fewer patients

From 2019 to 2020, Protenus researchers reported an increase of more than 30% in the number of breaches reported—572 in 2019 compared to 758 in 2020—while the number of patient records affected was slightly lower year over year.

"That could certainly be a good thing but it does beg the question: 'How do you know?'" Beaver asks. "In other words, how do you know that the exposure of patient records decreased? A pervasive security challenge across the healthcare industry is not knowing where PHI is located, much less how it's currently at risk. I suspect that at least part of this decrease is simply a lack of knowledge—not knowing what was compromised because so many IT professionals struggle to understand where all of their information assets are on the network and in the cloud."

Beaver acknowledges he fully understands it isn't easy knowing where everything is located across the network environment.

"Still," he adds, "when performing my vulnerability and penetration tests, I come across an unbelievable amount of open network shares that are fully exposing PHI to literally every user on the network, including to those without a business need to know."

Getting better, but work never ends

It's certainly a good thing when we see fewer of the very large data breaches, Bell says. In terms of the number of healthcare records exposed, he notes, the worst year was 2015 when several large Blue Cross organizations were breached by nation state threat actors. The Anthem breach alone exposed nearly 80 million records. Premera Blue Cross was about 11 million.

Total healthcare records breached in 2015 was over 112 million. Protenus has the total number of breached patient records in 2020 at 40.7 million.

"I see this as evidence that the efforts of healthcare insurers and providers to improve their cybersecurity programs is having some effect," Bell says. "Progress is being made. Many recognize they must do better. They are increasing investments in technology, skilled workers, more mature processes. They are getting involved in the Information Sharing and Analysis Centers to share information and help each other. But progress takes time and money. The work never ends. The criminal organizations and nation states are highly motivated by the opportunity they see to target healthcare data. Their tactics, techniques, and tools continually evolve and improve."

Ransomware leads to largest breach

The largest breach in 2020 was the result of a hacking incident involving ransomware: the Blackbaud ransomware attack and data breach that affected 3 million-plus records.

There is a need for more workforce education targeted at ransomware attack vectors since this is the number one way ransomware infiltrates an organization, according to Ensenbach.

Further, he adds, it's time to rethink malware strategy as humans are not perfect and will continue to fall prey to ransomware attacks. "Endpoint protection solutions continue to evolve so security officers and IT need to continue to evaluate their endpoint security strategy," Ensenbach says.

Organizations must have network architecture and security controls that help minimize the damage, Beaver says.

"Now, in 2021, it's still rare for me to find an organization that has a documented incident response plan," he says. "Just as risky, there's often outdated endpoint protection running on workstations and servers, a real lack of user education, and, of course, tons of missing software updates that the criminals behind the ransomware love to target."

Hacking still at the top

Hacking incidents still represent the largest number of breaches for types of incidents—62%. Insider threats are second at 20%. "For healthcare organizations to get ahead of these hackers, risk assessment and employee training and education are crucial. Organizations need to ensure they are testing to make sure the appropriate security measures are working as intended and that backups are separated from the main network, so an attack cannot spread to the backups as well, the authors of the Protenus report wrote.

Too many people get caught up in the latest and greatest technologies and supporting solutions, like threat hunting, that they end up overlooking the silly stuff that the bad guys know they're going to be able to easily exploit, according to Beaver.

"My recommendation here," Beaver adds, "is the same as it has been over the past two decades, and I'm confident it will remain the same well into the future."

First, know your network, Beaver recommends. Second, understand how it's at risk. And finally, do something about it. Each organization that experiences an incident or breach is deficient in one or more of these areas, he says.

"If you keep doing what you've been doing, you're going to keep getting what you've been getting," Beaver says "Something has to change, and the answer is almost always go back and figure out which of the information security basics you're deficient in and master those as soon as possible."

Ensenbach has seen firsthand that senior leadership or the board/trustees are not engaged, uninformed, and often detached from what is going on, leading to another problem.

Management, leadership, boards, and/or trustees need to be engaged and asking important questions. They must challenge security officers, privacy officers, and IT by requiring them to periodically report the state of security/privacy in the organization, the impact to the business, and bringing to light risks posed by threats/vulnerabilities before they become problems, according to Ensenbach.

Getting a handle on insider threats

Insider threats ticked upward in 2020. One example was a fired employee who accessed records. There are a lot of boxes that need to be checked when someone who had access to PHI leaves an organization.

Minimizing insider related risks starts from the get-go when credentials and privileges are created, Beaver says.

"All too often, people are given greater access than what's needed to do their jobs," he adds. "That often comes at the operating system level but also expands into other areas including specific applications, databases and so on. The same goes for ongoing oversight and monitoring of user behavior. It's unrealistic to expect technical staff to be able to monitor everything. This is where technical controls must be leveraged in order to automate these tasks."

Address your user-centric security controls and behaviors. Otherwise, it can come back to bite you pretty badly and often at the worst possible time when you are least expecting it, Beaver adds.

According to Ensenbach, organizations are not good about helping their employees understand insider threats. It may also be uncomfortable to report a fellow co-worker for something perceived as being a threat.

"Once again, employees need to be taught what to look for and report any suspicious activity by a co-worker," Ensenbach says. "From a termination standpoint, organizations need to be realistic about keeping employees on after submitting their notice to leave. Even the most trusted employee could be the organization's worst nightmare."

BAs involved in 24 million breached records

Business associate (BA)-related breaches remains an issue for healthcare providers. BAs were responsible for 24 million breached records in 2020, according to the Protenus report.

Organizations still believe all they need to do is have a BA sign a business associate agreement (BAA), and all is good. One of the most important changes that came out of the HITECH Act was the requirement that covered entities (CE)—and BAs with their sub-contractors—obtain satisfactory assurances that the BA meets all the same requirements for security and privacy that is required of the CE, according to Ensenbach.

"In short," he says, "this means organizations need to go further than simply having their business partners sign a BAA. They should be asking for a copy of their most recent—no older than one year—security audit/assessment, often referred to as risk assessment, to determine if by doing business with the organization it will introduce unnecessary risk to ePHI/PHI."

The biggest challenge in the context of BAs is the companies signing BAAs promising to take the proper precautions to protect PHI and then not doing so. It's often a half-baked version of what's required, according to Beaver. Minimal security standards, no security oversight, and, perhaps worst of all, no ongoing security testing, he adds.

Many organizations have developed formal vendor risk management programs, according to Bell. These programs create a process and tools to evaluate the level of risk of each vendor before contracting and throughout the life of the contract. The level of risk is a function of what level of access the vendor has to the customer's sensitive data, the criticality of the service being provided and the maturity of the vendor's security program.

"Talk is cheap, and executives will say they're going to do what's necessary and even put their reputations on the line by agreeing to the terms in writing but then they get busy and very little gets done," Beaver says. "The best thing you can do is to trust that they are doing it but also verify that it's actually getting done. At a minimum, ask for a copy of their latest vulnerability and penetration testing report and do that on an annual basis. There's a good chance they won't have one to share or the one they do supply is inadequate and does not meet what would be considered reasonable security standards."