IS YOUR BUSINESS THE NEXT TARGET OF RANSOMWARE?

envisionet

5 Things You Can Do To Keep Your Business Safe

Security & Compliance Are Business Leader Responsibilities

By Damon Clements

As a business leader, you are responsible for a great many things but often business owners do not put enough emphasis on security. Instead, many leaders attempt to play the odds and bet that problems will not come their way. As a leader you have two options when it comes to security. You can either address security and compliance now, invest the appropriate amount of time and resources into securing your organization or you can deal with it after you have been breached and explain to an angry public why such a security incident occurred under your watch.

Security and compliance need to be executive-level priorities and have support and adequate financial support from the top. After all, if you find yourself in the midst of a security incident, who else in your organization do you think will be dealing with the media, board of directors, investors, patients, lawyers, and insurance companies?

In the November-December 2015 of the Journal of Health Care Compliance, Art Weiss, chief compliance and ethics officer for TAMKO Building Products, noted a recent Department of Justice memo which indicated that the DOJ will be prosecuting more people in leadership roles for security breaches.

Who do you think will be held liable for a breach?

Ransomware on the rise

We should all be paying close attention and take stock from all of the recent ransomware attacks. This type of threat is on the rise and it's getting more difficult to prevent or recover from. In one recent event, a California-based hospital was subject to this type of attack and had to transfer patients and were soon put in the national media spotlight. Healthcareinfosecurity.com made a point to say that no organization is immune from outbreaks of malware, which is designed to forcibly encrypt all data residing on personal computers, mapped drives, servers, or even cloud folders. In fact, the Hollywood Presbyterian Medical Center, based out of Los Angeles, found this out the hard way when they became victim to such an attached and had to declare an "internal emergency". In this event, the hackers demanded 9,000 bitcoins to decrypt their data, which is currently worth about $3.6 million.

In this particular incident, the crisis went on for 10 days. A lifetime in the healthcare industry. The hospital tried to downplay the incident, stating that "this incident did not affect the delivery and quality of the excellent patient care you expect and receive from Hollywood

-rian Medical Center. Patient care has not been compromised in any way." While this is meant to be a statement of reassurance and comfort, the damage had already been done. After a national embarrassment highlighting a hospital that did not have access to medical records and medical devices controlled by computers, there are serious questions the hospital faces. How did this impact patients? Will there be lawsuits for malpractice? Will patients die?

What's just as frightening is how easy it is for this type of threat to enter into any business environment. When we consider nearly every other major data breach and hacker attack, the root cause was most likely a simple click of the mouse on a link within a phishing email.
Who do you think will be held liable after an investigation that will undoubtedly reveal that the attack may have been prevented and resolved with little-to-no impact had the hospital followed basic security principles and best practices?

These types of events can be avoided or heavily mitigated. In another similar incident, a doctor in a medical practice clicked a link in a phishing email and in short order received a ransom note indicating that all data had been encrypted and would not be restored until a large ransom was paid. However, in this case, the doctor had a good backup and disaster recovery process in place. They were able to call their IT support provider and in short order, had their data restored from a recent backup. They had to re-enter a few patient records but otherwise were not impacted.

So what are some things you can do within your organization and as a responsible business leader to ensure your organization or healthcare practice does not end up in the national spotlight or written about in blogs and articles like this one? The following 5 recommendations could mean all the difference.

Get a second opinion

Even if you have a team of technology engineers working for you or a capable consultant you trust, a second opinion should be used to evaluate your security and compliance with regulations such as HIPAA and PCI with raw data and reports that go directly to you, the business leader. Typically, independent security assessments will always find holes and sometimes these holes are very large, needing immediate attention. By and large, this is due to the fact that many internal IT departments and even outsourced IT service providers are made up of terrific desktop computer and network specialists but not specialists who have knowledge of the unique threats, liabilities, compliance, and security concerns within the healthcare industry.

If you as a business owner, hear the words, "we have it handled" it is most likely time for an outside expert's opinion to evaluate your security and offer you advice from experienced compliance experts that can explain the security concerns, and remediation steps in terms you can understand, instead of the usual technical jargon.

Know where your data is

A simple concept but surprisingly organizations are often not able to identify all of the locations where sensitive data lies. If you cannot pinpoint where the data lives and what kind of data lives there, there is really no way to ensure that data is safe or properly backed up. Additionally, under HIPAA, healthcare organizations are required to lock down sensitive patient data and prevent unnecessary access to this data. If there is data sitting on an unprotected thumb drive, or in a network folder that anyone and everyone has access to, then you are not in compliance.

Ensure backups will actually work when you need them

When is the last time you tested your backups? How often are your backups performed? Where are your backups being stored? Do you know whether your backups have been completing successfully each time? These questions are critical for business owners and decision-makers to understand have some level of visibility in to. Often, this is all entrusted with IT and business leaders have little-to-no understanding or any assurance that their critical data is adequately redundant. Additionally, if the proper investment is not made, you may wind up with a backup solution that is inexpensive and looks good on paper but find in the heat of the moment, that it takes days to restore or that the process fails entirely.

As a business leader, you should take the time to estimate just how much it would cost you if your systems were to be down. Some smaller medical practices and firms have found this cost to exceed $60,000 per day. If your backup strategy keeps you down for several days, can your business survive that expense? Are your backups being stored off-site? If not, what would happen if a fire took out your entire facility? Could you get your business back on its feet without ANY of your historical data? While monthly fees may seem like a costly expense, these expenses will pay for themselves many times over when you are able to quickly recover or avoid the high costs and the damage to your reputation that a disaster will cause.

Do not ignore your vendors

While you focus your attention on your internal compliance do not lose sight of the compliance obligations you have with your vendors and subsequently, their vendors!

HIPAA mandates that you must notify your patients and can be held liable if any of your vendors cause a breach. These fines can range anywhere from $100 to $50,000 per incident and up to $1.5 million annually. This is a little-known fact for many medical professionals and one that could prove devastating financially, if not taken seriously. The reason this isn't clear for many, is that it wasn't always this way. In fact, it wasn't until the passing of the HIPAA Omnibus Final Rule in 2013 that this became a requirement. In essence, it says that business associates (vendors) must also comply with the HIPAA security rule and that a business associate agreement alone, is not enough to comply. If faced with the reality of a HIPAA audit, you and your business associates will be included in that audit.

Be firm with your business partners and vendors and be willing to walk away from them if they are not willing to adhere to their compliance obligations. You do not want to end up on the receiving end of a breach caused by one of these partners due to ignorance or inadequate compliance efforts.

Fund the security you really need

We are all familiar with security practices and techniques such as anti-virus and firewalls but it takes much more than this to properly secure your environment and mitigate your risk to an acceptable level. The first problem with these technologies is that they are often installed with default configurations that really aren't protecting you from most known threats and vulnerabilities. Investing in an effective security program, one that is ongoing, and thorough, is your best strategy for lowing your risk.
The basics of a good security program starts with a thorough security scan to identify configuration problems and vulnerabilities. These can be prioritized according to level of risk and a plan can then be made to properly address those issues. Typically, this report will provide internal and external vulnerability data and find areas where you are most susceptible to a breach. Internal to your network, there may be sensitive data that is accessible to individuals who should not or do not need that access. There may also be terminated employees who still have access to company networks, with passwords that are set to never expire.

There should be systems in place that continually check and log network activity, detecting anomalies and unauthorized access. Security is not a "set it and forget it" type of strategy. It requires diligence, ongoing analysis, and a trained eye (not just the average "IT specialist") to properly configure and address any incidents.

ENVISIONET
Your vision. Our mission.

www.envisionetllc.com
envisionetllc | envisionetllc