THRIVEWELL TECH

ASSESSING YOUR ORGANIZATION'S CYBER-SECURITY RISK

5 Key Areas of Cyber-Risk for Senior Living Operators

Cyberattacks are a nightmare scenario for businesses of all types. For senior living providers with protected health data, cyber-breaches create heightened risk.

And while corporate boards and leadership teams are paying more attention to cybersecurity, they may still not understand just how at risk they are. Start with these questions:

- What would it cost your company to lose access to data or key business operations like EMR and billing systems for even one day?
- Do you know the top cyber-security risks at your organization and have a plan in place to address them?
- Do you have data security policies and processes that are clearly communicated to staff – and do you know the associated liability if not?
- Do you have a disaster recovery data center to keep critical operations running?

Today, the cost of cybercrime is in the billions of dollars and healthcare data breaches jumped more than 50 percent in 2020, according to CPO Magazine. Hacking and IT security issues accounted for 70 percent of those breaches – and it took the average business 236 days to recover from one, according to a Bitglass report.

Addressing cybersecurity risks

So what can your company do to protect itself from cyberattacks?

If you don't have in-house cybersecurity expertise – which is not feasible for many organizations – seek a managed services provider, MSP, that does. Cybersecurity experts are highly skilled individuals who monitor, detect, investigate, analyze, and respond to security events. They should work in concert with the MSP's chief security officer who has helped determine your risk profile, the cost to improve it and make intelligent financial decisions about how to address your risk profile, and build a more robust and safer IT infrastructure.

In this article, ThriveWell Tech cybersecurity specialists outline the greatest areas of cyber-risk for senior living and other health care providers and some key considerations for mitigating those risks. Contact us at ThriveWellTech.com or (617) 777-3822 to get started on a more detailed analysis.

1. Protected Health Information (PHI)
2. Legacy Systems
3. Policies and Procedures for Data Security
4. Identity Management
5. Business Continuity and Disaster Recovery

1 Protected Health Information

Phishing Attack: *An employee receives an email appearing to come from a vendor or high-level executive within the organization. They ask you to click on a link or transfer employee information. Unwittingly, the employee has provided access for a ransomware attack on your network or abetted identity theft. Sharing this news with affected employees and the cost to address the identity theft create long-lasting financial and organizational trust issues.*

Scenarios like this are all too common. Despite ongoing education, PHI and data breaches continue to occur through phishing in the form of malicious and increasingly sophisticated email scams.

In a typical ransomware attack, malicious software penetrates the organization's systems and encrypts accessible data. Hackers then demand a costly ransom to decrypt it – and may also threaten to sell or release your data on the internet. The news is rife with examples, such as the July breach of IT firm Kaseya, where hackers demanded a $70 million ransom.

Top 4 causes of data breaches:

- 57 percent – phishing attacks
- 21 percent – credential harvesting
- 20 percent – malware/ransomware
- 20 percent – social engineering attacks

Data source: Healthcare Information and Management Systems Society

So how do you protect yourself against data breach and loss? When it comes to protecting your organization from cyber-probes, employees are your first line of defense. Identity management is a critical back-up. Here are high-level cyber-security measures that the Thrive Well team addresses after performing a comprehensive organizational security audit:

- Comprehensive and frequent cybersecurity education for staff
- Automated back-ups of critical systems Encryption systems for emails and data in case of device loss or theft
- Implementation of alerts for large or suspicious file or monetary transfers
- Identity management processes for systems access

2 Legacy Systems

Lockout: *Your organization's billing department uses a computer with an operating system that is no longer supported by the developer. The data it holds and sends is not encrypted – and the system cannot be updated to add this critical security layer. If this system is breached, either through phishing or a network hack, your organization faces fines through the Health Insurance Portability and Accountability Act (HIPAA) that increase exponentially with each patient record breached – tens or hundreds of thousands of dollars. Communicating this breach to affected clients and dealing with the aftermath, is a CEO's nightmare – even more so if the breach is made public.*

Legacy operating systems and hardware that carry security risks are an unfortunate fact of life for most organizations. It's extremely costly to keep every piece of hardware and software up to date – especially when balanced against day-to-day operating needs.

Common cyber-risks include operating systems where updates are no longer being provided by the vendor or the hardware can't handle an updated operating system. Additionally, some pieces of

Addressing cyber-risk is not a once-a-year or one-and-done discussion. Leadership, department leaders, and IT should routinely discuss the security risks inherent in the systems they use and have a defined process for addressing them.

technology, kiosks for example, simply may not be able to be updated, meaning you will need to bring in an entirely new system. That's a costly, complicated, and long-term process.

So, how do you address legacy systems risk?

- Identify all legacy systems
- Conduct a vulnerability scan that identifies the risks – and put a process in place to repeat and follow up on findings
- Clearly convey the risk and cost of not investing in fixes to leadership and board
- Establish a POAM (plan of action and milestones) to address vulnerabilities in accordance risk. In some cases, an organization may simply need to assign acceptable risk to a piece of technology for a certain amount of time.

3 Policies and Procedures for Data Security

Compliance Is Key: *In the earlier phishing scenario, we outlined an unintentional action by a well-intentioned employee that led to dire consequences. What could make this even more dire? Leaving yourself open to greater liability – and a liability insurance claim denial – if your organization cannot demonstrate processes and policies around such areas as staff cyber training and online behavior.*

Creating policies addressing data security and online behavior is not an IT safeguard in the same way as blocking someone's ability to download software on their laptop or applying content filtering software. But they can help drive employee behavior in areas of risk – and mitigate organizational liability.

Key policies include requiring cyber-security and HIPAA education in your organization's employee onboarding and compliance programs; setting data encryption standards; and, addressing device sharing and usage standards.

Here are a few key questions:

- What is your policy for taking a device home and the repercussions if someone leaves a device unattended and it is stolen?
- Have you defined a policy for an employee who does not follow your organization's cyber-security procedures and clicks on a phishing email?
- Does your staff know what constitutes a breach of HIPAA through email and social media and your policy for those who unintentionally versus intentionally share protected information?
- Are you providing targeted training for staff who routinely handle PHI, in all departments not just clinical?

4 Identity Management

The Angry Ex or Lost Device: *An employee who has access to online financial accounts or your electronic medical record (EMR) resigns. Their supervisor is out on leave, and your organization has no process that notifies IT that access to these accounts needs to be removed. The employee, who harbors a grudge against your company, logs on and the damage is done. Another common situation loss or theft of a device that is owned by the organization or has access to online business systems. With dual authentification or a formal off-boarding process addressing systems access, your organization substantially reduces this risk.*

Identity management factors into a multitude of areas. Organizations must consider how they are managing passwords, including dual-verification or other technologies that protect against password sharing. Using single sign on technology can help organizations manage password security more effectively and create ease of use for staff who use multiple systems.

Do you know who is logging into your systems and what data they are accessing? If your organization suffered a data breach, would an IT forensics team be able to track backward to identify when, who, and how? With a tight identity management system, the answer will be, "yes!"

Access to online systems – where most systems live these days – such as VPNs, EMRs, financial systems, and websites need to be routinely audited to ensure that former employees do not still have access. Systems access should be baked into an organization's onboarding and, most importantly, off-boarding process.

Finally, do you have a record of log-ins, especially for clinical systems? This becomes critical if an allegation of fraud or a care concern is raised.

5 Business Continuity/Disaster Recovery

Disaster strikes: *Have you calculated the cost to your business if you lost power and your ability to operate key systems for a day? What if a flood or fire damaged your data center? What is the revenue loss over two weeks – or a month? Putting a dollar amount to this scenario is the critical first step to making the case for investing in a back-up data center that would avert such a catastrophic shut-down.*

Like legacy systems, business continuity planning in the event of a disaster is one of those areas that is tempting to push to the back burner – with dire consequences. And while it's not technically a cyber-security issue, it's a key cyber issue.

For complete business continuity an organization would essentially need to budget for a second IT data center in an alternative location that is simultaneously running your operating systems. Understandably, this is cost prohibitive.

But you can ensure that you are backing up data, that your organization has identified the core systems required for short-term, day-to-day operations, and has a temporary worksite and server ready to support those. Then, ensure that the security posture at your temporary site is equal to your permanent location.

Ensure that you are backing up data, that your organization has identified core systems required for short-term operations, and has a temporary worksite and server ready to support those.

For organizations who have planned ahead by establishing an alternate data center, don't fall into the geography trap. Too often, we have seen organizations build data center B too close to their primary operational center. That may be convenient for travel and oversight, but if you are on the same power grid or susceptible to the same fire or weather event, your back-up plan has failed.

Building a Strong Cyber Foundation

As more business operations move to the cloud, the safeguards built into your Wi-Fi network are fundamental to cyber-security. Secure, partitioned networks for various users and operating systems add strength to your chosen Wi-Fi provider's own security safeguards.

This and the other areas outlined in this paper are just some of the many pitfalls that can make arming your organization against cyber-attack a daunting task.

Contact ThriveWell Tech and let us start connecting the dots for your organization. We have a formidable management team, a forward-looking vision, and we are actively developing advanced technologies to better support the emerging needs of senior living and other health care providers.

THRIVEWELL TECH

PHONE | info@thrivewelltech.com

Thrivewelltech.com