JTaylor™

Healthcare Consulting | Valuation

Partner Insight Series:

Cybersecurity Risks:
Are You Protected?

August 1, 2024

Cybersecurity Risks: Are You Protected?

Think back to your first job twenty years ago –when the rolodex was your lifeline, fax machines were used daily, and paper files were neatly organized in one filing cabinet after the next. If you ever pause and think, "What happened to this place?" you're not alone. Like it or not, the digital world has taken over. Some aspects of your first office may make you nostalgic, while others make you incredibly grateful for technology and the time it saves you compared to the time you spent on monotonous tasks you performed back then. However, with these positive technological changes come new risks. Businesses can now operate more efficiently, but must be cognizant of cybersecurity threats. As hackers get smarter and the risks escalate, business executives can't help but wonder: How do you truly know if your business is secure?

Cybersecurity Risks

Every business is a target of cyber criminals. The pertinent data may differ and potential uses by bad actors vary, but no one is immune. Healthcare entities are subject to heighted risk, with protected data being at the center of cybersecurity breaches. The Health Insurance Portability and Accountability Act (HIPAA) requires healthcare entities to maintain the confidentiality of protected health information (PHI) and protect it from being disclosed without a patient's consent. HIPAA guidelines require stringent data security measures. However, even when following applicable HIPAA guidelines, healthcare entities can still be a victim of a cybersecurity breach.

Beyond the scope of protecting data in the normal course of operations, healthcare entities are particularly concerned with cybersecurity risk when considering a merger with another entity. While the potential for growth, synergy, and financial gain may exist, decision makers want to know what liabilities and risks they may be taking on from the target entity. How thorough are their data protection measures, and how will their data security system and mesh with ours? More to the point, can you trust the other company's leadership? Hackers have so many opportunities to access information, and if you don't start thinking like a hacker to identify the areas where your business is vulnerable, then your risk may be higher than you'd think.

Avenues for Data Infiltration

For organizations to appropriately assess their risk, they must first consider the various avenues for data infiltration. User error is a common way outsiders gain entry into a company's information system. Password hacking is a deceptively simple process – rather than typing in potential passwords, hackers use automated scripts to quickly gain access. This can happen in a matter of seconds, depending on the simplicity of the password employed. Therefore, it is recommended that companies educate their employees on creating strong passwords or passphrases and changing them frequently, and the importance of not using the same passwords across multiple websites or software applications.

"Phishing" is another way hackers can penetrate a business's information systems. While we may feel that we are smart enough to recognize suspicious emails or links, hackers are getting increasingly sophisticated. Cybercriminals design phishing emails and links that are sometimes indiscernible from those used by legitimate companies, so employees don't always recognize

them as dangerous. The best way to avoid phishing breaches is by educating employees about common phishing tactics so that they know what to look out for. They should also be trained to verify the legitimacy of an email by face-to-face communication or a direct phone call to the sender before clicking on unexpected links or downloading attachments. Being aware, being smart, and being careful goes a long way.

Vulnerabilities within the organization also create opportunities for outsiders to access company data. There are a lot of misconceptions that a network firewall offers sufficient protection, but what it ultimately comes down to is everyone within the organization and the measures each person is taking. Each organization has different weaknesses, and hackers know to look for those holes in an organization's cybersecurity environment. The best way to combat this issue is to do internal checks within your company, keep hardware and software up to date, and make sure the environment is as secure as possible.

Dark Web

The "dark web" is one of those mystic terms frequently thrown around, but a lot of people don't understand what it is or how it works. Ultimately, the dark web is just a subset of internet content that utilizes a different browser. While most of us think of the dark web as sinister, there are certain applications available on it that are used by legitimate businesses or governmental agencies. The scary part is that the possibilities for illicit activity on the dark web are endless and often anonymous, so once a company's data ends up there, they no longer have control over what happens to it.

This raises the question, "What do users of the dark web want with my company's data?" Information that may seem innocuous to employees of an organization – such as names, phone numbers, insurance information, and more – can be extremely valuable to certain bad actors. The act of acquiring the data itself can prove to be rather lucrative, with a single record often generating hundreds of dollars. Given the tremendous volume of records within, for example, a health system's database of billing and electronic health records, it's not surprising that some may see this as a gold mine. One reason the data is so valuable to those who intend to misuse it is that – especially when paired with artificial intelligence – the information can be utilized to commit fraud, mimic identities, or for other negative purposes like targeting other individuals or organizations. The bottom line is that dealing in data can be profitable activity for those intent on using it for their own gain. Therefore, a company's cybersecurity measures are critically important.

Prevention and Risk Management

Having preventative measures in place can be extraordinarily beneficial when it comes to managing cybersecurity threats. There are too many incidents where businesses don't adequately invest in security measures. However, when they inevitably experience an incident, it usually results in substantial monetary losses that far exceed what they might have spent on trainings, protective software, cybersecurity consultants, and other preventative measures. Costs incurred when responding to a breach include lost revenue due to business interruption, costs to recover compromised data, professional fees for legal counsel and information technology consultants to determine specifically what data was compromised, costs to comply with breach notification and reporting requirements, and more – sometimes even ransom payments to regain access to critical data or systems.

According to IBM's 2024 *Cost of a Data Breach* report[i], the average cost of a data breach globally increased to almost $4.9 million in 2023 –a 10% increase from the previous year. One reason the costs are so high is that, according to the report, it takes an average of almost 260 days to identify and contain a data breach – which allows a significant amount of data to be accessed and misused. The United States holds the unenviable spot of having the highest average data breach cost worldwide, at over $9 million. The healthcare industry leads the way, with an average cost of close to $9.8 million per data breach. Unfortunately, healthcare has incurred the highest cost per breach for over ten years. This is influenced by a variety of factors that make healthcare entities an attractive target, including the immense amount of data housed by such entities, a plethora of electronic devices that contain security weaknesses allowing hackers to gain access, and the extreme impact of disruption which makes them vulnerable to ransomware attacks.

One of the most positive ways you can encourage preventative action is by having regular open discussions within the executive leadership of your organization about whether security enhancements are needed. Failure to comply with HIPAA requirements may result in both civil and criminal penalties, so Chief Information Security Officers (CISOs) and other executives have a tremendous responsibility to ensure they have appropriately security measures in place. The best course of action is to have a predetermined strategy in place for addressing a data breach if (or more likely, when) it does occur. Do not cover it up. Instead, have an incident response plan in place that can be readily deployed. This plan should address how the organization can maintain operations without access to key technology, such as electronic medical records, for a period of time, as well as roles specific individuals will play in investigating and responding to the breach.

Outside companies can help with an organization develop a cybersecurity plan, but there are also several ways that companies can build up and invest in their security measures internally. Conducting employee training and awareness sessions routinely, investing in Advanced Threat Detection and Anti-Malware software systems that have the capability to identify and respond to potential threats, enabling Multi-Factor Authentication (MFA) across systems, and conducting incident response simulations and planning sessions regularly are a few ways that businesses can start protecting themselves from potential threats. There are a multitude of options available to protect your organization from cybersecurity threats, but it takes thoughtful planning and consideration to find what works best for your situation. Do not wait until it is too late to start building up an armor of security measures and an action plan.

Final Thoughts

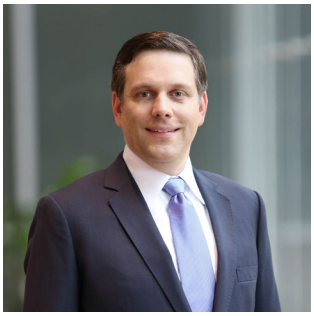
It can be challenging to find the optimal balance between maximizing technology to keep work operations efficient and employing stringent security measures. But isn't that sense of friction positive? If you don't feel some level of inconvenience, you may not be doing enough to protect your data. Investing in data security is simply a cost of doing business in the 21st century, and it's more critical than ever before as hackers are getting more and more sophisticated. Healthcare entities in particular are frequent targets, so it is imperative that these organizations rise to the occasion and address the risks head-on. Investing time and money up front is far better than dealing with the aftermath of a cyber-attack.

*For a deep dive on cybersecurity within the healthcare industry and more information on how you can help protect your business from cyber threats, listen to the **JTaylor Healthcare Podcast,** Season 4 Episode 5: Cybersecurity Insights within Julian Ratnayeke, available on streaming platforms and jtaylor.com.*

Kyle W. Kirkpatrick, FACHE

Partner | Director of Consulting Services
817.502.7731 | kkirkpatrick@jtaylor.com

Kyle has over 25 years of consulting and operational experience working in healthcare and life sciences with public and private organizations across the U.S. He is a former hospital CEO with experience running groups of hospitals, managing joint ventures, implementing new strategies, driving EBITDA enhancements, and creating positive organizational cultures. He has worked as a consultant within Big 4 firms focused on strategic planning, M&A, and operational improvements. His strategy experience includes facilitation, visioning, strategy and operating model development. He has strong project management experience to coordinate complex initiatives across multiple stakeholder groups.



Herd A. Midkiff, CVA

Partner – Consulting Services
817.546.7036 | hmidkiff@jtaylor.com

Herd has over 20 years of experience serving clients in the healthcare, non-profit, and investor-owned sectors. He has extensive experience in strategic planning, including joint ventures, business acquisition, due diligence services, and managed care contracting support. He also draws upon his healthcare and finance background to provide business enterprise and compensation valuation services. His clients include large multi-hospital health systems, physician-owned hospitals, entrepreneurs, and attorneys.

[i] IBM. (July 2024.) *Cost of a Data Breach Report: 2024*. https://www.ibm/com/downloads/cas/1KZ3XE9D