Compliance Today - July 2021
How simplifying your IT environment can bolster security

By Gerry Blass and Jason Tahaney

Gerry Blass (gerry@complyassistant.com) is President and CEO at ComplyAssistant in Iselin, New Jersey, and **Jason Tahaney** (jason.tahaney@comop.org) is Director of Technology at Community Options Inc.

- linkedin.com/in/gerry-blass-917a482/
- linkedin.com/in/jason-tahaney-91653618/

In today's healthcare technology landscape, there is a greater need than ever before for everyone within the organization to be an active participant in cybersecurity. No longer is this simply the role of the health information management (HIM) team or information technology (IT) department. According to Pew Research Center, 71% of workers are doing their job from home all or most of the time.[1] This translates to an increased number of people sharing highly secure information online from home. For healthcare workers, the risk of threats such as phishing or malware attacks against valuable patient data is a real concern.

A simplified, streamlined IT environment is not only a more efficient way to work, but it can pay great dividends in boosting your organization's approach to cybersecurity. Multiple electronic health records systems, patient portals, and networked patient care technologies contribute to a complex infrastructure that can leave room for vulnerabilities, but with some strategic planning, you can ensure your environment reduces risk of breach. This article outlines practical guidance to ensure leaders at all levels within your organization are compliant and mitigate cybersecurity threats.

The power of the cloud

Oftentimes when it comes to simplifying the IT infrastructure within an organization, it's hard to know where to start. One of the first steps that leaders can take is to consider a cloud-based solution. By relying on cloud first, and on-premises solutions as a last resort, health leaders can save their organization countless resources, including time, money, and disaster recovery. Cloud solutions that are compliant with the Health Insurance Portability and Accountability Act provide assurance on a host of levels, with the ultimate goal of protecting patients and their private information. The recent uptick of cyberattacks in healthcare[2] is a telling reminder that corners can't be cut, and with cloud solutions, the chances of security breaches and compromise of proprietary patient data decrease significantly.

With cloud-based solutions, an organization is able to encrypt the data at risk. While some organizations have an easier time with this than others, it is essentially a way to deter malicious or negligent parties from getting access to sensitive data. Data encryption is a key line of defense in a cybersecurity framework, ensuring that the intercepted data are as difficult to decrypt as possible.[3]

While there are other steps that leaders can take to simplify their IT environment and in turn bolster security across the organization, which will be outlined later in this article, ensuring a proper cloud-based solution is one of the best ways to start. With cloud, you're guaranteed that there is already a service in place, and a continuity plan designed to drive your business forward safely and securely. It takes the guesswork out of the equation and

lightens the load for IT professionals, with the goal of simplifying things across the board.

Staying secure in a pandemic world

COVID-19 has caused an approximate 118.7 million cases globally and more than 2.6 million related deaths,[4] and in its wake has left an increasing number of cybersecurity threats. According to FBI statistics, since March of last year, there has been a 400% increase in cyberattack complaints.[5] This is largely driven by the rise in telehealth and more healthcare staff working remotely.

It's no secret that IT departments and HIM professionals in organizations across the country are spread thin and facing new challenges by the day. One of the biggest challenges these leaders face is the lack of parameters in the IT environment. There is a much larger footprint and far less control, especially when so many employees are working from home. Standard procedures that would normally be taken to control the environment are no longer as easy to implement.

To add to the complexity, rolling out a remote access solution requires more management and care than most IT staff are equipped to handle. There are significantly fewer resources to keep the systems running and far less ability to turn on a dime when incidents arise. As we have seen over the course of the last year, policies change almost overnight, and workers could be in the office today and working remotely tomorrow depending on regulations.

Today's IT professionals are working extensively to combat these barriers and mitigate risks as they come. At Community Options, a nationally based nonprofit that seeks to provide housing and employment opportunities for people with disabilities, the IT department has taken creative approaches to mitigating risk across the organization.

To protect against credential theft, one of the methods the organization has implemented is to incorporate the Community Options logo on email authentication screens and other IT system login screens. This allows for easier identification of those credential theft attacks that attempt to spoof user login screens, or to trick the user into logging in with their company credentials. Microsoft Office 365 offers great tools for enforcing these checkpoints, as opposed to a generic Microsoft sign-in page.

To take it a step further, the organization is also using adaptive authentication and leveraging geolocation as well as IP address reputation to identify any potential malicious log-ins to Office 365. This is in place, along with other metrics used to identify emails that could be used to steal credentials.

Barriers to security and how to overcome them

At a high level, the combination of risk complexity and lack of appropriate resources remains the biggest barrier for organizations when it comes to cybersecurity. Small organizations especially struggle to have the team and tools in place to meet the demands of keeping their system safe 24/7, which is what the job requires.

While the COVID-19 pandemic has certainly amplified these challenges, one of the best ways to fight them head-on is through education. It's important for everyone in the organization, from the C-suite to the frontline workers, to understand the responsibility and role they play in keeping patient data and information secure. Cybersecurity training for leaders at all levels of the organizational hierarchy reinforces that everyone is held accountable, not just people within the IT department.

Another wise strategy for any organization, regardless of size, is to look to industry leaders for insight. The U.S. Department of Health & Human Services in partnership with the Section 405(d) Task Group released a list of five

common threats that small, medium, and large organizations can face, which include:[6]

1. Email phishing attack;
2. Ransomware attack;
3. Loss or theft of equipment or data;
4. Insider, accidental, or intentional data loss; and
5. Attacks against connected medical devices that may affect patient safety.

In conjunction with the five threats, the U.S. Department of Health & Human Services also charged the Task Group with identifying 10 best practices or controls to mitigate these threats. The goal is to provide organizations with an industry standard that can be implemented over a 12-month period. It is voluntary and incentive-based but can pay substantial dividends for organizations looking to minimize risk and the resulting downtime.

Lastly, organizations should work to create an internal task force designed to combat these issues collectively. While this is certainly easier for larger organizations, it's important to have people from various departments who have a pulse of what threats are most pertinent for the organization at any given moment and know what steps the team is taking to address them. By having a recurring meeting on the calendar, it becomes easier to keep these issues top-of-mind and approach them head-on.

Compliance for everyone—not just your IT team

It bears repeating that best practices in maintaining security should not solely fall on the shoulders of your IT team. It is crucially important that senior leadership is involved, and while it should be obvious why, many organizations fail to incorporate C-suite level executives.

While you can't build Rome in a day, you can start small. Quarterly huddles with senior-level leadership are a great way to provide updates on how the organization is growing, what threats are most evident at the moment, whether there is potential for a threat, and if a program is being executed in a home or somewhere that involves IT. It also is a great way to answer each and every question that comes up. For chief financial officers, board members, and other key stakeholders, the world of cybersecurity is not their day job, so they rely on the IT staff's insight to give them the answers they need with the business in mind. At the end of the day, it's about arming them with best practices so they can make good business decisions.

In addition to meeting with senior leaders regularly, organizations have found success with mapping out potential threats and assigning controls to respective threats on a risk registry. It's a great visual and documentation tool to see where your organization stands with compliance and trace the likelihood of a threat occurring. It also can easily be viewed by leaders and stakeholders across the organization—not just the IT team.

Steps for HIM teams and beyond

Ready for your team to take the first step in mitigating risk and moving your organization down the path toward a safer IT environment? Here is a quick recap of steps you can take to get started.

- **Ensure your application is cloud-based.** Cloud-based architecture is a great way to ensure your organization follows best practices and mitigates risk.
- **Provide education across the organization.** Cybersecurity education is a great way to protect your organization and employees, but general computer training is also key for reminding them what

applications are frequently used that can open the organization up to risk.

- **Consider a risk registry.** Risk registers are effective tools for documenting and visualizing which threats are most pressing for your organization. They also are helpful when it comes to enabling controls that can help combat threats regardless of organization size.
- **Create a risk management committee.** This committee is a great way to hold your organization accountable and make sure leaders (especially those in the C-suite) are taking a holistic approach to risk management on a consistent basis.
- **Avoid complacency!** Persistence is critical when it comes to cybersecurity for your business, and it's also the hardest thing for organizations to do. There are always going to be operational requirements for the company, such as keeping the lights on, but security is arguably more or equally important.

Takeaways

- Discover new ways to simplify the cybersecurity infrastructure at your organization regardless of company size.
- Learn about the biggest information technology security risks organizations face today and actionable solutions for mitigating them in the pandemic environment.
- Define barriers that organizations face when it comes to risk and simple solutions to effectively combat them.
- Receive guidance for ensuring that everyone within the organization is compliant with cybersecurity risk management, from the C-suite level to the frontline workers.
- Get steps that your health information management team can take to help ensure your organization's information technology environment is as safe as possible from risk.

1 Kim Parker, Juliana Menasce Horowitz, and Rachel Minkin, "How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work," Pew Research Center, December 9, 2020, https://pewrsr.ch/3fsNnua.
2 Hannah Mitchell, "Pandemic drove uptick in cyberattacks: 3 report findings," *Becker's Hospital Review*, February 23, 2021, https://bit.ly/3tZP6fB.
3 "Cyber Edu: What is Data Encryption? Data Encryption Defined, Explained, and Explored," Forcepoint, accessed May 18, 2021, https://bit.ly/3vcxOx6.
4 Maria Cohut, "Global impact of the COVID-19 pandemic: 1 year on," Medical News Today, March 12, 2021, https://bit.ly/3fvjA44.
5 Maggie Miller, "FBI sees spike in cyber crime reports during coronavirus pandemic," *The Hill*, April 16, 2020, https://bit.ly/2QsVkXG.
6 U.S. Department of Health & Human Services and Healthcare & Public Health Sector Coordinating Councils, "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients," accessed May 18, 2021, https://bit.ly/3fs9IrB.