EBOOK

How to establish a strong information security program.

MatrixCare® by ResMed

Data breaches have become increasingly common. Even large organizations with solid security programs in place have been hacked, compromising the accounts of millions of users. Social media platforms, large financial organizations, and global hotel chains have all been breached. The simple fact is that no one is immune.

Long-term care organizations have a special responsibility to protect patient and resident information. As more health information becomes digitized, and more systems move toward interoperability, establishing robust information security programs will be vital for organizations of all sizes.

Hear from three healthcare IT professionals about the necessity of a strong information security (also called "info sec") program, and our steps and considerations for building one.

The importance of a robust security program

"I don't think it's ever been more important to have a solid information security program, especially in healthcare," said Todd Friedman, chief information security officer at ResMed. "Healthcare is heavily regulated, so we already have a lot of controls in place. But because patient safety is involved, it takes on a whole new level of importance."

"It's important to remember that adversaries are improving all the time and info sec work must stay ahead of them," Friedman said. "An important success factor is having support from all stakeholders—from the CEO on down, info sec should be part of your organization's DNA." Friedman also noted that companies operating internationally need to be aware of the EU's General Data Protection Regulation and other laws that apply outside of the U.S. "Focusing on the right risks and setting the right priorities has never been more important for healthcare," he added.

Building blocks of a great program

1

Step one: Governance

Establishing a sound governance structure is a good first step, according to Brian Tolkkinen, director of information security at MatrixCare. Governance, he explained, is a framework that ultimately ensures business assets—and by extension, an organization's mission--are protected. "It sets the tone for how we operate internally and externally and established our approach toward risk, including our risk appetite," he said.

A security program cannot be effective without buy-in from all levels of leadership, Tolkkinen said, including the board of directors, senior leadership, and upper-level management. "Buy-in from the highest levels, including the board of directors and senior management, is crucial," he said. "These leaders should conduct regular risk assessments to identify any risks—such as a pandemic or natural disaster—that can prevent reaching business objectives," he said.

In addition, leaders should establish a program to ensure compliance with regulatory and industry requirements, as well as with any specific mandates included in company policy. And the final building block of a governance structure is independent audits to verify the effectiveness of the safeguards that have been put in place. "It's important to verify that you're doing what you say you'll do in policies and procedures, and also to verify that risks you've identified are being adequately addressed."

2

Step two: Vulnerability management

The next step in developing an info sec program is vulnerability management: identifying areas where threat actors can expose a gap in protection, or worse, take malicious action. “There are also accidental vulnerabilities, such as misconfiguration that allows someone to open a port that shouldn’t be opened,” said Stephen Squires, director of information security at Brightree. “They key thing is to know your environment by conducting vulnerability scans.”

These scans offer an idea of what ports and services may be exposed so they can be protected against attacks. Squires said most vulnerabilities that are exposed are three to four years old. “They are tried, tested, true vulnerabilities that have been out there forever,” Squires said. “Cyber criminals are banking on the fact that our patching regimes are lax or non-existent, which makes it easier for them,” he said. “We hear about a lot of nasty exploits out there and it’s because people don’t patch. So all externally-facing systems need to be looked at to determine whether there are vulnerabilities.”

3

Step three: Risk management

Risk management is another key step to identify risks that could prevent a business from reaching its objectives, said Tolkkinen. Compliance requirements for some organizations, as well as the Sarbanes-Oxley bill, require formal risk management. “This includes maintaining an inventory with system and data classification and continually working to identify, track, and treat any known risks.”

He said companies may opt to work with a third-party security firm for an annual risk assessment. In these cases, a best practice is to make results available on request to customers and other partners via an attestation letter provided by the third-party firm. Working with a third-party firm can help build credibility with customers, business partners, and others, Tolkkinen said. "It can also provide helpful trending to track and communicate progress with management."

Another facet of risk management is business continuity planning. "This is the process of creating a prevention or recovery system to respond to threats such as a cyber attack or natural disaster," Tolkkinen said. "All of these efforts are intended to protect our people and our assets, so we lump impact assessment and continuity planning into our annual risk management program."

4

Step four: Monitoring

One part of an info sec program where technology can play a key role is in monitoring, said Squires. "Again, it's about knowing your environment. You should centrally collect logs from your different systems, but it takes technology like machine learning to look at all of those logs and find anomalies that may indicate compromise."

One of the first things malicious hackers will do once they're inside a system, Squires said, is eliminate the "breadcrumbs" that show how they got in. Because of this, "Having all of your logs centrally stored somewhere off the server helps protect information." Establishing this as a norm is one way of "knowing your environment" that allows alerts to be created for things that deviate from the norm.

An example many multi-national organizations are familiar with is log-ins from a specific geographic domain. "If you have someone who normally logs in from New York simultaneously log in from another location—Australia, for example—that should set off some alarms. It helps you see that something is going on," he said. He added that machine learning or artificial intelligence also helps organizations react more quickly because they can implement learnings from past incidents.

5

Step five: Incident response

Friedman said most information security professionals have come to terms with the fact that "it's not if we'll be breached, it's when." Taking time to develop an incident response plan can not only help protect your business, but also help mitigate the worst effects for your employees and your customers.

One practice Friedman recommends is developing a high-level umbrella plan, and then creating "runbooks" that include specific information for different work groups. "For example, different subsidiaries of a larger corporation might have specific runbooks, or they might be split up by different kinds of attacks, such as ransomware," he said. "The books are very tactical."

One of the main functions of a runbook is to define roles and responsibilities, he said. "When something bad happens, people want to know what they need to do and what success looks like. We want to make that as simple as possible, so having a documented plan with good contact information is critical." The runbooks also answer key questions about involving an organization's legal department, notifying third-party vendors, bringing in law enforcement when appropriate, and enlisting the support of third-party vendors such as a forensics expert.

Friedman said conducting tabletop exercises that bring key players together to work through a hacking scenario is a great way to test your plans. "It's a lot of fun, and I've never been in one where I didn't learn something we could use to continually improve our plans," he said. "If you start off with a small plan and test, then improve, your plan can evolve quickly into something that's robust and actionable."

For many organizations, information security is a function that operates in the background of day-to-day business activities. Most employees don't think about all that goes into ensuring the data and infrastructure they rely on to do their jobs are secure. But in a healthcare organization, information security translates into being able to give providers and clients the confidence that we're watching things that are critically important to them and their residents and patients.

MatrixCare® by ResMed

Learn more about our security program at matrixcare.com/security-program, or call 866-469-3766.