From Tech Guru to Business Enabler

Five strategies for CISOs in a time of rapid change

It goes without saying that the threats faced by IT leaders have evolved over the years. It wasn’t so long ago that an antivirus administrator might have been the extent of a company’s IT security team, and viruses were generally sent as email attachments. As threats got more complex, larger teams played defense and focused on protecting the perimeter of the corporate network. Eventually, organizations realized they needed to be more proactive in managing threats, and the CISO became a more common job title. Today, with corporate data residing on everything from mobile devices to social media platforms to cloud-based applications, security is an exponentially more complex undertaking than ever before.

“Some have said that we should now be thinking of threat landscapes in the plural,” observes Scott Crawford, managing research director at Enterprise Management Associates (EMA), a Boulder, Colorado-based research and consulting firm. “At one end of the spectrum are industrialized attacks—highly commoditized malware that’s bought and sold much like legitimate software. At the other end are the micro-targeted attacks that might affect a handful of users after extensive research by the perpetrators.

“It’s much more about risk management these days,” Crawford continues. “The sheer volume means that threats must be prioritized according to the risk they present. This means CISOs and CSOs must be intimately familiar with the business—what is the real impact of various kinds of attacks, versus the resources required to prevent them.” A study by Forrester Consulting came to a similar conclusion last year when it found that 50 percent of IT governance professionals expected business decision makers to exert more influence on “deciding how much security and privacy risk is acceptable.”

To get a sense of how these changes play out in real life, CIO Digest checked in with three IT security leaders serving in highly regulated industries. Their challenges are as diverse as their organizations themselves, but all agree that the role of the CISO has changed dramatically in the past few years. The following are a few tips that these leaders offer to their peers to help keep their heads above water:

“Security management is a dynamic process that changes with each new piece of information we obtain.”

— Sharon Finney, Corporate Data Security Officer, Adventist Health System

Rather than the singular, it goes without saying that the threats faced by IT leaders have evolved over the years. It wasn’t so long ago that an antivirus administrator might have been the extent of a company’s IT security team, and viruses were generally sent as email attachments. As threats got more complex, larger teams played defense and focused on protecting the perimeter of the corporate network. Eventually, organizations realized they needed to be more proactive in managing threats, and the CISO became a more common job title. Today, with corporate data residing on everything from mobile devices to social media platforms to cloud-based applications, security is an exponentially more complex undertaking than ever before.

“Some have said that we should now be thinking of threat landscapes in the plural,” observes Scott Crawford, managing research director at Enterprise Management Associates (EMA), a Boulder, Colorado-based research and consulting firm. “At one end of the spectrum are industrialized attacks—highly commoditized malware that’s bought and sold much like legitimate software. At the other end are the micro-targeted attacks that might affect a handful of users after extensive research by the perpetrators.

“It’s much more about risk management these days,” Crawford continues. “The sheer volume means that threats must be prioritized according to the risk they present. This means CISOs and CSOs must be intimately familiar with the business—what is the real impact of various kinds of attacks, versus the resources required to prevent them.” A study by Forrester Consulting came to a similar conclusion last year when it found that 50 percent of IT governance professionals expected business decision makers to exert more influence on “deciding how much security and privacy risk is acceptable.”

To get a sense of how these changes play out in real life, CIO Digest checked in with three IT security leaders serving in highly regulated industries. Their challenges are as diverse as their organizations themselves, but all agree that the role of the CISO has changed dramatically in the past few years. The following are a few tips that these leaders offer to their peers to help keep their heads above water:

“Security management is a dynamic process that changes with each new piece of information we obtain.”

— Sharon Finney, Corporate Data Security Officer, Adventist Health System
#1: Take a risk management perspective

A few years ago, the CISO could be reasonably content in the IT silo, managing security within the closed environment of the corporate network. Today, it’s necessary to take a broader view. IT risks are a subset of an organization’s overall risk landscape, and the key is minimizing risk without impeding the business. “It boils down to one question: what is the real impact to the enterprise?” says EMA’s Crawford. “With the complexity and sheer number of threats, that’s a harder question than it used to be.”

Sharon Finney, corporate data security officer at Adventist Health System, found this transition easier than some. “Hospitals and healthcare as a whole have been leaders in risk management for years,” she asserts. “What I try to do is plug into that existing process.” Governance at this multi-state network of hospitals and long-term care facilities is led by a Compliance Board, consisting of business unit leaders, IT leaders, and external representatives specializing in law and compliance.

Although they report to the CIO, Finney’s team is tightly integrated with the company’s compliance team. “I have a dotted line report to our vice president of Compliance,” she says. “My team is involved in all of the technical change control discussions. We’re constantly evaluating risks against what we’re trying to accomplish as an organization.”

At FBL Financial Group, an Iowa-based firm whose primary operating subsidiary and managed companies offer life insurance, investment, and property-casualty insurance products across the West and Midwest, the Risk Governance Board reports directly to the organization’s board of directors. “My team reports quarterly metrics to our Enterprise Risk Management dashboard, for further analysis by senior management,” explains Darwin Larrison, FBL Financial Group’s director of Enterprise Information Protection. “The areas that are green, yellow, or red aren’t
the same every quarter. Things fluctuate according to the amount of new information we’re dealing with as it relates to weaknesses or improvements with new protections and controls.”

In early 2010, Sudhakar Gumma-di, corporate information security official at Molina Healthcare, Inc., had enterprise risk management added to his team’s charter. The Fortune 500 firm owns primary care clinics and administers health plans and Medicaid Management Information Systems (MMIS) in 15 states and is faced with a number of regulations.

“With the passage of HITECH [the Health Information Technology for Economic and Clinical Health Act] in 2009, executive management wanted someone specific to ensure that risk controls were at an acceptable level,” Gummadri recalls. His team is now responsible for making sure all patient and business data is protected.

“Healthcare is in huge transition in the United States, and this makes risk management a moving target,” Gummadri asserts.

“But it’s especially important for us since we administer Medicare and Medicaid programs for state governments, and are thus under greater scrutiny.”

#2: Focus on strategy

Yesterday’s CISO focused on demonstrating compliance and automating compliance reporting. This remains a crucial part of the risk management endeavor, but it’s only the beginning. “Measurements are important, but some of the data points we’ve historically used are open to question themselves,” asserts EMA’s Crawford.

“Enterprises today have such a huge volume of risk-related information—logs from multiple security systems, legal and compliance data, business plans—that the CISO today often needs to use some of the methodologies of the field of business intelligence to make sense of it all.” And the analysis needs to align with the goals of the business.

At Molina Healthcare, Gummadri’s team always produced compliance reports, but his risk management team has been empowered to be more strategic. “We now have an ongoing process of compliance reporting, penetration vulnerability testing, and assessments at the application and database layers,” he explains. “From that information, we work with our business units, legal department, and executive management to evaluate risks and devise physical and technical controls and other strategies to mitigate them.”

Gummadri’s team partners with Symantec in several key parts of this process. Symantec Control Compliance Suite, in use since 2010, is deployed across the enterprise.

“Our compliance reporting is now fully automated, and the Policy and Standards Managers in the product help us create and enforce these enterprise-wide procedures, which saves my team a lot of time,” Gummadri explains. He adds that he’s looking forward to deploying...
the product’s new Risk Manager. “Being able to define business security objectives, and apply controls based on those objectives, is just what my risk management team needs,” he asserts.

Symantec Endpoint Protection enables the team to customize policies for different employee groups according to business needs, and Symantec Security Information Manager correlates log data from Molina Healthcare’s entire security infrastructure, helping to distill it into actionable reports and alerts. In addition, to protect confidential data in motion and at rest, Gummadi’s team is in the process of deploying Symantec Data Loss Prevention.

At Adventist Health System, Finney’s team also uses Symantec Endpoint Protection and Symantec Control Compliance Suite to support the organization’s risk management initiatives. “Endpoint Protection was already in place when I arrived in 2008, but I also had a relationship with Symantec from prior roles,” she recalls. “Early on in my tenure, we decided to add Control Compliance Suite to automate a lot of reporting that had previously been done manually.” The team is currently deploying Control Compliance Suite’s Policy Manager, using some of the product’s standard templates while custom designing others to fit their unique needs.

Adventist Health System also has a subscription to Symantec DeepSight Security Intelligence. “We use this tool daily to keep our finger on the pulse of emerging threats and the security landscape throughout the world,” Finney explains. “It is another tool we have to keep us better informed so that we can make smarter choices about where we apply resources and ad-hoc risk assessments. Security management is a dynamic process that changes with each new piece of information we obtain.”

#3: Communicate up and down
CISOs have always had needed to communicate results to to management and disseminate IT policies to end users. If anything, clear and concise communication is even more important in an era of tight budgets and limited human resources. “CISOs are often called to defend themselves from both ends of the spectrum,” says EMA’s Crawford. “Business executives would rather put your budget request toward building the business, so they’re asking which risks are really worth throwing resources at. And end users complain that security procedures keep them from getting work done. You’ve got to speak both languages.”

At FBL Financial Group, Larsson doesn’t need to work hard to get executive management’s attention on security issues. “Our internal audit department does much of that for us,” he says. As an employer and a publicly-traded financial services firm, FBL is subject to Sarbanes-Oxley (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Model Audit Rule (MAR), and many state-level regulations. “Audits definitely help to point out your weaknesses, but not so much your strengths,” he notes. “That’s why I make sure to call out the progress we’ve made as well as the good things we do in meetings, in a special section in my report to senior management, in occasional emails to the user community, and with our CIO.”

For Adventist Health System’s Finney, the key is to get everyone involved. “Our security program is not highly centralized,” she explains. “People ask me, ‘How do you do security?’ Well, I don’t do security. I try to get 55,000 other people to do it because I cannot singlehandedly make it happen.”

“I don’t do security. I try to get 55,000 other people to do it because I cannot singlehandedly make it happen.”

– Sharon Finney, Chief Data Security Officer, Adventist Health System


Paul Proctor of Gartner discusses the changing role of the CISO with Sam Pierre-Louis of MD Anderson Cancer Center at go.symantec.com/ciso-webcast.
Molina Healthcare all have more than half of their servers virtualized, with new VMs being added continually. They’re all looking to implement a bring your own device (BYOD) policy in the near future, at least for some users, and all have deployed applications in the cloud. “‘No’ can no longer be the default answer when a new technology is requested,” says EMA’s Crawford.

When FBL Financial Group’s Larrison was promoted to his current position in 2011, he noted that his new team was appropriately cautious about the security implications of new initiatives, but recognized the importance of thinking outside the box to help protect the company and enable the business at the same time. “Given today’s technology environment, it’s critical that we continue to reinvent ourselves for better agility,” he explains.

Offsetting the potential risk associated with the loss of key personnel with deep knowledge of in-house systems, Larrison determined that engaging managed service providers for selected functions would not only prevent such a crisis, but also reduce cost and complexity while improving security. “We were innovative,” he remembers, “and we wound up with a much more workable solution.”

One of those providers is Symantec Managed Security Services, which provides log analysis, alerting, and management of the company’s intrusion detection system.
“With the passage of HITECH in 2009, executive management wanted someone specific to ensure that risk controls were at an acceptable level.”

— Sudhakar Gummadi, Corporate Information Security Official, Molina Healthcare, Inc.

and prevention systems and other security infrastructure—all provided from Symantec’s Security Operations Center, delivering 24×7 protection.

Adventist Health System is constructing a new building for its IT department, complete with a state-of-the-art green data center. When the team moves in next spring, the data center will be more than 80 percent virtualized. “When I had a physical server, if things got bad enough, I could walk over and push a button and turn it off,” Finney relates. “So as we deployed VMware across our data center environment, we had to adjust our incident response plan. All of that had to change as we walked into that new world. And we have had to adapt quickly to other new technologies as well—electronic medical records, IP-enabled medical devices, mobile devices for providers, and cloud-based services."

Gummadi reports that Molina Healthcare’s data centers are now around 70 percent virtualized with VMware, and the organization is looking to deploy a new virtual desktop infrastructure (VDI) system. “Virtualization has worked great with our servers, and we expect a centralized desktop environment to drive efficiency and reduce costs as well,” Gummadi explains. “And with all the data in the data center rather than scattered everywhere, it will improve security.”

**#5: Simplify**

CISOs a few years ago were awash in complexity—heterogeneous server environments, multiple tools for multiple systems, a proliferation of physical servers. Today, the concept of simplicity may seem counterintuitive while adapting the new technologies and trends discussed earlier. But a strategic, risk management-oriented perspective will likely result in simplified operations, even as hardware and software tools keep pace with more complex threats. “We have been growing rapidly in recent years,” notes Molina Healthcare’s Gummadi. “The only way we can keep up is to have tools and processes that aren’t unnecessarily complex. In our case, virtualization helps us accomplish this, as does minimizing the number of vendors we deal with by working with companies like Symantec who offer broad solutions.”

“As a hospital, simplicity, or lack thereof, can make a life or death difference,” asserts Adventist Health System’s Finney. “Although adding new endpoints may seem complex at first, the ability for a nurse to carry a lightweight tablet in a hospital environment will have a huge impact on how we care for patients. My team needs to have flexible processes in place so that these technologies can be deployed.”

Says FBL Financial Group’s Larri-son: “Our IT team’s vision is ‘Simple. Modern. Fast.’ Our move to managed services helped us deliver all three of those objectives.”

Mark Mullins is a managing editor of CIO Digest and senior manager of Symantec’s SMB and Channel Publishing Programs’ team.

---


---

**COMPANY PROFILES**

**ADVENTIST HEALTH SYSTEM**

Founded: 1973
Headquarters: Altamonte Springs, Florida
Community Impact: 55,000 employees and 7,700 licensed beds
Territory: 10 states in the Southern, Midwestern, and Rocky Mountain regions
Website: www.adventisthealthsystem.com

**FBL FINANCIAL GROUP**

Founded: 1945 (primary operating subsidiary, Farm Bureau Life Insurance Company); 1939 (Farm Bureau Property Casualty Group, operated by FBL)
Headquarters: West Des Moines, Iowa
Assurance for Families: FBL’s underwriting companies protect 548,000+ households
Territory: 14 Western and Midwestern states
Website: www.fblfinancial.com

**MOLINA HEALTHCARE, INC.**

Founded: 1980
Headquarters: Long Beach, California
Lives Affected: 4.3 million individuals and families on government-funded health programs
Territory: 15 states, coast to coast
Website: www.molinahealthcare.com