

Living in the Copernican Revolution

Developing a Security Posture that Aligns to the Ever-Changing Threat Landscape



Lynda Fleury,
AVP and CISO, Unum Group

In his famous allegory of the cave, Plato argues that the invisible world is the most intelligible notion of the visible world. This forms the basis of Platonic epistemology, whereby Plato concluded that knowledge can be attained from the world of timeless essences and that opinions are based on the shifting world of sensations.

But what happens when the images in the cave are infinite—always changing as subsequent philosophers concluded? Knowledge becomes subjective and variable. This certainly makes sense in the field of information security, considering that information technology is based on mathematical calculations. Lynda Fleury, the assistant vice president and chief information security officer at Chattanooga, Tennessee-based Unum Group, and her team are finding this premise to be true, as there is no “Alpha and Omega” (“beginning” and “end”) to information security.

By Patrick E. Spencer

Getting what you ask for

Fleury first joined Unum, a FORTUNE 500 leader in disability, group life, long-term care, and voluntary benefits, in 1984 as an IT audit manager. Her transition to information security and compliance was actually by accident. “One day I happened to ask the security manager, who was managing the mainframe environment, what he was planning to do about the security for all of the different file servers that were showing up with the OS/2 operating system loaded on them,” she recalls. “It was soon thereafter that I had the opportunity to serve as the special project lead for building out the company’s first PC-based security program. This was December 1989, and I haven’t turned back since.”

Photos by Michael Brunetto

When asked to cite her biggest accomplishment over her nearly 25-year career at Unum, Fleury indicates it goes back to 2001, when her team consisted of just three IT security professionals. “We had been charged to build out a best-in-class information security program, and we simply couldn’t go to senior management and ask them for 20 or 30 IT resources and millions of dollars in funding,” Fleury says. “It was important to build trust as well as a solid foundation, an effort that spanned a period of years and was ongoing.”

Ingredients of security success

The basis of the success Fleury has achieved she credits to her team’s due diligence, proactive management, and accountability. She oversees a team of 30 IT security professionals who are recognized for their innovation and dedication in pushing initiatives that help drive the business forward. “The fact that we haven’t lost the entire network as a result of a malicious intrusion in more than five years speaks volumes to the hard work and efforts of the entire team,” she remarks.

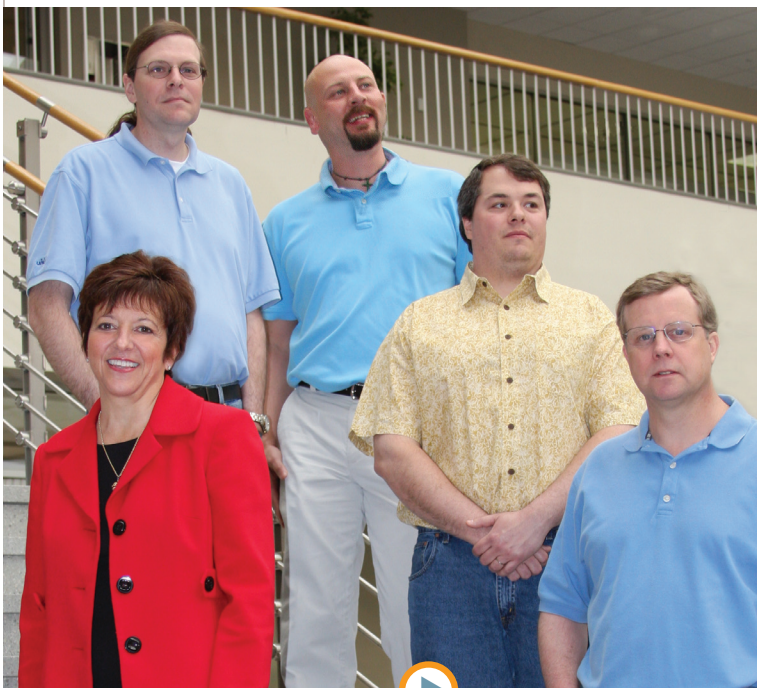
Fleury also cites the support she has received from senior management as a critical factor in building out the security program. “We’re an insurance provider, and one of the measurements includes conducting business with our customers in a secure fashion,” Fleury says. “Our plans start at the top, with the strategic business initiatives of the CeO, and we continually align our security programs to those.”

“The entire senior management team understands the importance of maintaining a comprehensive security and compliance posture,” Fleury adds. “If something goes wrong in our IT infrastructure, we stand to lose the entire network or experience a significant disruption to the business.” This cascades not only to the productivity of Unum’s 10,000 employees but downstream to customers. As a result, Fleury is responsible for reporting on the status of security patches, the threat landscape, and compliance with various regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX) on a business dashboard that goes to senior management each month. These data metrics also include notations around the quality of work performed by her team.

Daily evolution

The virtual explosion in the growth of the threat landscape is something Fleury and her enterprise Information Security & Risk Management (eISRM) team take seriously. “When you look at polymorphism and obfuscation and the almost ridiculous increase in the

variance of malware, this is something that definition-based detection can address only so far,” says Brad Shoop, security architect II. “Behavioral and heuristic detection is going to be critical. But that won’t be enough, end-user awareness is also key. Simply because you think that you live in a safe neighborhood doesn’t mean that you won’t get broken into.”



Lynda Fleury, AVP and CISO (bottom left); Brad Shoop, Security Architect II (top left); Mike Landreth, Systems Manager (top middle); Chris Dupuis, Security Architect II (second to right); and Tom O’Brion, network Security Consultant (bottom right).

Fleury continues: “The good ole’ days of the mainframe and the closed, private network with no connection to the outside world are long past. That simply isn’t reality.” Despite its challenges, however, advances in technology have allowed Unum to become a global FORTUNE 500 company. “Technology moves at a very rapid pace,” Fleury explains, “and security maturation tends to lag behind with the introduction of new technologies.”

“What I’ve tried to communicate to our senior management team is that there is no beginning and end to our information security efforts,” Fleury says. She goes on to explain that a security program must evolve every single day in order to keep pace with the expanding threat vector. “Gone are the days of kids simply wanting to make a name for themselves. It’s



Delivering the Benefits: Unum Group

Founded: 1848
 Headquarters: Chattanooga, Tennessee
 Workforce: Approximately 10,000
 Fortune Ranking (2008): 251
 Customers: Protect 25 million people and serve the needs of 171,000 businesses worldwide, including 42% of the FORTUNE 500
 Business Units: unum u.S., unum u.K., Colonial Life
 Benefits Paid (FY2008): nearly \$6 billion
 Revenue (FY2008): \$10 billion
 IT Organization: 650+ IT professionals, including 30 IT security professionals
 Website: www.unum.com

now criminal activity focused on extracting data and profiting from it.”

The leadership of empowerment

When it comes time to soliciting feedback from several different members of Fleury’s team on what makes her successful, her leadership skills quickly come to the forefront. “The biggest thing for me is her understanding of security, respect for our perspectives, and unwavering focus on the business,” Shoop observes. “She puts a lot of trust in us, allows us to do what we think is necessary, and then backs us up. I am the newest member of the team,

Two-decade Security Career Pays Benefits

With two decades of experience in information security, Lynda Fleury, the AVP and CISO at Unum Group, is recognized as a thought leader in her field. She built the Enterprise Information Security & Risk Management team at Unum from the ground up, inculcating best practices, instituting security standards, instilling an infectious passion across the entire staff, and creating synergies that connect information security with the business.

In addition to the internal loyalty and respect of her 30-member staff of professionals and stalwart support of the senior management team, she has garnered external recognition that includes the 2009 CSO Compass Award from *CSO Magazine* and the 2008 Information Security Executive Southeast Award.

and the thing that has impressed me the most is the appreciation she shows to everyone on the team.”

Yet, at the same time, eISRM Systems Manager Mike Landreth notes that Fleury is willing to serve as a counterweight, pushing the team to look at the broader picture and to consider the impact of actions on the business.

The intertwining of information security and the business is also an important factor: “This was not the case in my prior roles,” Shoop

// There is no beginning or end to information security. It must evolve every day. //

—Lynda Fleury, AVP and CISO, Unum Group

recalls. “It was truly enlightening to join an organization that had already surpassed that hurdle.”

Chris Dupuis, security architect II, possesses a slightly different perspective than Landreth and Shoop on Fleury’s leadership skills. “I’ve worked on other teams during my tenure at Unum, many of which were topnotch,” Dupuis says. “However, Lynda provides a level of empowerment that drives quality and efficiencies attained by few teams and organizations.”

When to outsource?

In order to stay on top of evolving security threats, Fleury and her team work with Symantec on various fronts. In 2004, they opted to outsource security monitoring and management of their network to Symantec Managed Security Services. “Others in my peer group, especially with the current economic challenges in front of them, are looking to in-source network security monitoring and management,” Fleury reports. “However, with the rapid growth in the threat landscape and the corresponding 24x7 requirements, I really think it is impossible to replicate the value we gain from [Symantec] Managed Security Services.” Beyond the reduced security risk and enhanced operational efficiencies, Fleury is able to reallocate up to three IT FTEs who would need to be dedicated to monitoring and managing network security to other tasks.

“It ultimately boiled down to ensuring that I’m allocating my resources to what matters most,” Fleury says. “Rather than culling through piles and piles of data logs,

the team can focus on what is really important—critical alerts, issues important to the business.”

In 2005, Fleury and her network security team opted to outsource mail security to MessageLabs, which Symantec acquired in late 2008. “We previously managed mail security in-house,” Landreth remembers, “and it was a major headache; 24x7 ‘babysitting’ to prevent malware intrusions and spyware and to deal with false positives.” With the Hosted email Security Solution from MessageLabs, Fleury was able to reallocate two IT FTEs to other security-related initiatives. The solution is also saving Unum on storage resources, as the spam is filtered out before it hits the network. In addition, fewer false positives and virtually no spam drive organizational efficiencies—from end users to Fleury’s eISRM staff.

“MessageLabs is a great solution for us,” Landreth says. “We’re able to outsource our mail security infrastructure, yet we are able to maintain email policies based on our business requirements. With the MessageLabs solution, we don’t need to submit a request and wait for hours; rather, we are able to make the change in real time ourselves.”

Getting deeper security insight

About two years ago, the Unum team added Symantec DeepSight Threat Management System on top of Symantec Managed Security Services. “It provides us with virtual real-time information on issues related to IDS, IPS, our Web security gateway, and other pieces of

our IT infrastructure that help us hone in on specific threats to our environment,” Shoop says. “The threat landscape changes daily, and DeepSight helps prioritize our efforts on what is important.”

And as many of these tasks were previously performed manually, the labor cost savings is dramatic—equating to as much as 80 hours of full-time employee (FTE) time each month, depending on the malicious activity that is happening in the wild. Instead of spending valuable time compiling threat reports, the team is now able to focus on initiatives that drive the business forward.

Ensuring compliance with security standards

Fleury and her team manage information security through various industry frameworks. She introduced ISO 27000 and 27001 as a standard in 2001, and the team also adheres to COBIT and COSO (Committee of Sponsoring Organizations). “We’re heavily regulated in the insurance industry—from federal and laws, to privacy and security issues, to annual Sarbanes-Oxley audits,” Fleury explains. “Automating security and compliance reporting is critical for us.”

Symantec Enterprise Security Manager (now part of Symantec Control Compliance Suite) was first introduced into the Unum environment under a prior data center outsourcer (Unum has since re-assumed management of its data center), which had some strict guidelines around standard best practices and configurations. “We initially acquired [Symantec] Enterprise Security Manager in order to maintain well-documented configuration standards,” Fleury says. “We’re now in the process of using that baseline to build our security controls documentation,” Landreth adds. “This will also include a monthly security health check to ensure that we don’t have any gaps or vulnerabilities.”

To streamline endpoint management on its approximately 1,400 data center servers and help ensure their security, the Unum IT team also uses Altiris Server Management Suite. The team provisions a standard configuration across all of the different systems—from UNIX, to Microsoft Windows, to Linux—and maintains a 28-day patch management window using it.

The benefits of email retention and e-discovery

In order to address compliance-related requirements around email retention and discovery, the Unum IT team was an early adopter of Symantec Enterprise Vault, implementing a solution with the help of Symantec Consulting Services that included Discovery Accelerator and Microsoft Exchange Journaling in 2004. With responsibilities for legal discovery, Fleury and her team herald the benefits of the solution. “Prior to the implementation of Enterprise Vault, anytime we needed to perform an email discovery, whether it was in support of the legal department for a litigation matter or from an employment perspective, we were looking at a labor-intensive undertaking,” Fleury remembers. “We either had to grant ourselves access to get into each employee’s mailbox to conduct the search, or we had to perform restores of—often—hundreds of tapes.”

With hundreds of hours of manual retrieval and searches associated with each discovery request, the Unum team has seen a dramatic improvement in IT staff productivity, with as much as one FTE reallocated to other tasks. In terms of email storage, with nearly 20 terabytes today, Unum would be looking at as much as 40 terabytes without the single-instance archiving and data compression capabilities of Enterprise Vault. When this is coupled with the ability to move email archiving from tier-one storage to tier-four stor-

age, the savings extend into the hundreds of thousands of dollars.

Following in the footsteps of Kant

Many believe that Immanuel Kant in his *Critique of Pure Reason* put the “final nail in the Platonic epistemological coffin” when he argued that the mind is only capable of thinking in terms of causality and

thus knowledge is determined by the continuums of space and time. Indeed, the Copernican Revolution had a far-reaching impact across many disciplines that is still felt today.

Fleury and her team at Unum have grasped the implications of the Copernican Revolution for information security. There is no beginning or end to information security, but rather it is a variable that must be addressed daily. And with the right leadership, strategies, and technology partnerships, they are poised to continue taking on the infinite and ever-changing challenges of information security. ■

Patrick E. Spencer (Ph.D.) is the editor in chief for CIO Digest and the author of a book and various articles and reviews published by Continuum Books and Sage Publications, among others.



Podcast

Check out the Executive Spotlight Podcast with Lynda Fleury and other members of her team at go.symantec.com/unum



Ensuring Security and Compliance with Symantec’s Help

- > Symantec Managed Security Services
- > MessageLabs Hosted Email Solution
- > Symantec Enterprise Vault
- > Symantec DeepSight Threat Management System
- > Symantec Enterprise Security Manager
- > Symantec AntiVirus (in the process of migrating to Symantec Endpoint Protection)
- > Altiris Server Management Suite
- > Symantec Consulting Services
- > Symantec Education Services
- > Symantec Essential Support Services