The 21st Century CISO

As the technology environment continues to evolve, many people believe we're moving toward a future in which organizations outsource much of the delivery of IT services, which will shift the organization away from IT implementation to procurement and management of suppliers and services, nonetheless requiring a CISO – Chief Information Security Officer – to set direction and establishing an overall IT architecture. To communicate this shift, the CISO must have the ability to address these subjects at different levels so that all members of the organization have a clear understanding of the group's direction.

Storytelling can be a powerful tool for communicating with diverse people across the organization. Framed as security issues, stories and images that people can understand allow them to relate better to the issues even if they lack a background in technology. However, stories based on fear are generally unsuccessful in realizing this goal. The ability to reframe an issue in a story that focuses on the opportunities and identifies benefits that outweigh the risks is going to be the hallmarks of a successful CISO. If people feel they belong and they matter, they will tackle any challenge.

We cannot influence people unless we communicate with them. And as the scope of information risk expands, we need to communicate with a wider range of people across the organization.

Communicating with people isn't always easy, as most of us have discovered. If we start relaying technology details to non-technologists, we won't capture their interest, and in fact, we run the risk of doing the opposite.

To communicate, a CISO – Chief Information Security Officer - must become chameleon-like, with the ability to blend into a variety of environments. We need enough knowledge of each business domain to be able to communicate with different groups using language they understand. And we need to discuss these subjects at different levels. A Chief Financial Officer - CFO - may only want to hear a high-level summary expressed in terms of financial impact and return, which is often not easy when discussing security investments targeting hard-to-quantify threats. Product group managers want to hear security issues expressed in terms that relate to sales, marketing, and operational efficiency.

I've found storytelling to be a powerful tool for communicating with diverse people across the organization. When I frame security issues as stories and images that people can understand, they relate better to the issues even if they lack a background in technology.

I like to tell stories using metaphors and analogies. They are easily remembered, and they translate complex subjects into simple terms everyone can understand. To paraphrase Benjamin Zander, the conductor and visionary, the power of an orchestra's conductor comes from awakening possibility in others (Zander and Zander 2000). In the same way,

I believe the power of the CISO comes from awakening the awareness of risk among people across the organization. I use stories based on metaphors to create that awareness.

For example, employees often find it hard to understand the dangers of stealthy threats. This is because the threats are unobtrusive, concealing themselves so they can steal information over the long term. Users are usually not even aware that a problem exists on their system. They still associate malware with obvious, annoying symptoms such as screen messages and system crashes. So when we tell them we've detected dangerous software on their machine, they have a hard time believing that it matters.

To communicate the danger, I sometimes use the analogy of ants and termites. "Malware used to be like food-eating ants in the kitchen," I explain. "You'd know when you had an infestation because you'd see ants crawling over the countertops and walls. Once you knew about them, you'd spray or set traps to eliminate them.

"But today, threats are more like the termites that can live in your walls. You can't see them, and you may not even know they are there. But they're doing much more damage than ants ever did. In fact, they may be destroying the structural integrity of your house."

I've found using analogies helps quickly drive home messages. People immediately understand that these invisible threats can undermine the structure of the computing environment, just as termites undermine houses. This makes them more likely to accept the next step, which is that we have to perform the digital equivalent of tenting their computer to eradicate the vermin.

Fear is Junk Food

Just as building trusted relationships is essential to influencing the organization, I also think we need to transcend the doom-and-gloom that can pervade discussions of security topics.

The security industry has a tendency to use fear to sell products. Internally, as security professionals, we sometimes share this tendency. Of course, security really is about scary things: threats, vulnerabilities, and risk. But focusing on fear as the primary motivator is like living on a diet of junk food. It may provide immediate gratification, and it's somewhat addictive, but ultimately it's not healthy for either the CISO or the rest of the organization.

In the short term, fear can scare people into action and help drive funding for security projects. However, relying on fear alone can only work for so long. Eventually, it has the opposite effect. It causes the CISO to lose credibility. In fact, I think relying on fear may even contribute to the high rate of job turnover among CISOs. Those who rely too much on selling fear are snacking on an unhealthy diet, and eventually the organization realizes this and rejects them.

Ultimately, fear doesn't work for other reasons too. Most people don't want to listen to a continuous stream of negativity. If we are always seen as the source of negativity, we will lose our audience. If we are continually viewed as the group that says no, we will be ignored. People will bypass security restrictions in order to meet their business needs.

Even within the security organization, fear can become a gravitational force—a black hole—drawing ever-increasing attention to the negative side of security issues and draining energy that should be directed to enabling the business.

Accentuating the Positive

So how do we take a more positive approach? We must focus on our mission at Intel—Protect to Enable. This mission shifts the emphasis from the negative to the positive: how we can help the business achieve its goals by solving security problems. It puts hope and optimism before the challenge.

This mission is aligned with the business. Rather than being antagonistic, it is based on common values. It sets an optimistic tone, and, in the long term, optimism is a far better motivator than pessimism. Threats may be frightening, but our goal is to see past the threats and identify the opportunities. To paraphrase the noted Stanford University behavioral scientist Chip Heath, there's no problem that cannot be solved without a new framework. Therefore, if we can't see a solution, we have the wrong framework. Protect to Enable provides this new framework. It helps us focus on finding solutions.

Imagine you're invited to attend a meeting to discuss whether the company should start using a specific cloud-based business application from a new supplier. Clearly, this product introduces risks: it comes from an unfamiliar supplier, it's accessed over the Internet, and it means sensitive data will be stored outside the enterprise.

A narrow security view might focus solely on minimizing the risk. However, this narrow view can lead to a Catch-22 situation, as discussed in Clayton Christensen's book *The Innovator's Dilemma* (Christensen 1997). Typically, it goes something like this. To minimize the risk, the organization initially restricts the use of a new technology. For example, the technology can only be used for low-risk data, or by a narrow segment of employees. The problem with this approach is that it also reduces the business benefit to the point that the benefit of the technology cannot justify the expense and effort of adopting it. So we reach an impasse. To make the technology a viable proposition, we need to be able to show a business benefit—but we can't show a business benefit because we won't allow viable use of the technology.

Protect to Enable provides the new framework that frees us from the innovator's dilemma. It allows us to focus on the opportunity and identify benefits that outweigh the risks. For example, introducing a new supplier increases competition for our existing suppliers—leading to future savings for our organization. This benefit aligns with the business and is one that everyone in the organization understands. Perhaps less intuitive, but equally important, the savings can be used to fund security controls to mitigate the risk of using the technology more widely. Now our benefit/risk equation has a positive result rather than a negative one. By enabling the technology to be used more widely, we realize bigger business benefits that outweigh the additional cost of controls. This example also underlines the need for CISOs to build business acumen that enables us to see the opportunity and how it can be used to overcome the challenge of funding security initiatives.

Demonstrating the Reality of Risk

Of course, the security organizations' role still centers on managing risk, which includes discussing the negative consequences of people's actions. If we frame this discussion carefully, I believe we can inform without fear-mongering. By describing possible outcomes and solutions without using emotional language, in terms listeners can understand, we create a context in which the organization can make the decisions that are best for the business.

Even when we have to highlight unpleasant outcomes, we're not fear-mongering if our information is based clearly on reality. Here's another example from our experiences at Intel. As our customers' use of the Internet expanded, Intel's marketing groups naturally wanted to expand their external online presence by creating new websites. So we, as Intel's information security group, began assessing the risks and the security controls required. Some of our marketing teams didn't find this an appealing prospect. They needed to move quickly, with the freedom to communicate however they thought best, and they viewed security procedures as bureaucracy that slowed them down and hindered their ability to communicate with customers and partners.

What happened next was far more persuasive than any of our initial efforts to forestall potential problems. A few websites were launched without rigorous quality control. Hackers found the weaknesses in these sites, but they didn't crash the sites or steal information. Instead, they inserted links to porn sites.

When this unfortunate fact was discovered, it provided the leverage we needed to improve security procedures. I realized this was a case where a picture spoke a thousand words. So, to illustrate the impact, I simply showed the links to people within Intel. This wasn't fear-mongering. It was simply demonstrating the real consequences of their actions on the Intel brand. Everyone could understand the implied question: Do we want our brand to look like this? This ended, once and for all, any discussion about whether we needed to apply rigorous quality control to external websites.

The CISO's Sixth Sense

In the book, *Blink*: *The Power of Thinking Without Thinking* , author Malcolm Gladwell describes an interesting experiment. Researchers asked subjects to play a game in which they could maximize their winnings by turning over cards from either of two decks. What the subjects didn't know was that the decks were subtly stacked. They could win by selecting from one of the decks, but selecting from the other deck would ultimately lead to disaster. After about 80 cards, the subjects could explain the difference between the decks. But they had a hunch something was wrong much sooner, after only 50 cards. And they began showing signs of stress and changing their behavior even sooner, after only about 10 cards, long before they cognitively understood a difference existed.

As CISOs, we develop a sixth sense about security issues. Often, my instincts suggest a need to act or begin investigating a specific direction long before our group is able to fully understand or explain what is happening. This sixth sense is particularly relevant in the security realm, where our information is almost always imperfect or incomplete. When a threat strikes, we do not have time to conduct extensive research or wait for

evidence to accumulate. Therefore, we need to act decisively based on imperfect information.

I think we develop this sixth sense from the diverse experiences and skills we've acquired during our careers. We can also foster this sixth sense by being aware. Some security professionals tend to be inwardly focused, looking only at the data and systems they need to protect. At Intel we try to be more open and outward-looking, sharing information, and seeking input from a variety of sources, including peers across our company and at other organizations. This can help CISOs spot early warning signals and correlate information to quickly identify threats. Like secret service agents scanning a crowd, our experience helps us spot anomalies, to see the signals and ignore the noise.

By intercepting threats early, we may be able to minimize or entirely eliminate the impact. We may also reduce the effort needed to deal with the threat. Early action may avoid the need for emergency response and a potentially major cleanup effort.

Taking Action at the Speed of Trust

A sixth sense is only of value if the organization can act on it quickly. This requires two things. First, we need the courage to take a leap of faith based on what we believe. This courage is rooted in attributes such as being centered and credible, with a clear sense of our mission.

The second requirement is that the organization responds quickly when we inform them about a security issue. This rapid response is only possible if we have established trusted relationships with people across the organization. Because of these relationships, the organization can act at the *Speed of Trust*, as Stephen M. R. Covey describes it in his book of that name (2008). Faster, frictionless decisions are possible because people know, from experience, that our information is reliable and that our focus is on enabling rather than spreading fear.

The CISO as a Leader

Above all, 21st century CISOs must become effective leaders who can inspire their teams to enable and protect the organization.

Over the years, I've identified three essential themes I try to instill in my team and constantly reinforce in our day-to-day interactions. Our security team members must believe in our mission; feel they belong to our Intel IT security group and Intel as a whole; and feel they matter.

If I can make people feel they believe, they belong, and they matter, they will tackle any challenge. If people understand the greater goal, it helps establish an emotional connection and guide their everyday actions. This is a key reason that I have thought so much about defining our mission, and that I spend so much time helping our team see how their jobs are connected to the business's objectives and concerns.

For example, a typical operational goal might be to patch all systems within a week of a new software release. This goal is more meaningful if we establish the links to the business using I believe, I belong, and I matter. I believe in the mission of Protect to Enable. If I'm not protecting to enable, the other employees at the organization I belong

to cannot do their jobs effectively. The company doesn't achieve its results, and the company doesn't execute its vision. Patching systems quickly matters because it helps our users do their jobs, which in turn helps the business achieve its goals.

Looking to the Future

As the technology environment continues to evolve, many people believe we're moving toward a future in which organizations outsource much of the delivery of IT services. If this trend continues, what does it mean for the CISO?

In this view of the future, the organization shifts away from IT implementation to procurement and management of suppliers and services, while setting direction and establishing an overall IT architecture.

In addition to this, the organization will need to retain the core competency of the security group, the management of information risk. Essentially, organizations cannot outsource risk. We can hire companies to deliver our business systems, but we're still responsible for compliance with SOX. And if a breach results in theft or leakage of personal information, we're still responsible for reporting it. Furthermore, we still suffer the damage to our brand, even if the breach was due a failure of the supplier's systems. As regulations proliferate and more and more personal information is stored in business systems, the risks can only increase.

Therefore the CISO's abilities will remain essential, even if the job title changes. The organization must retain the management of information risk as a core competency. As CISOs, we are poised to continue providing that core competency as long as we can effectively work within this new environment by developing the abilities I've described in this article and throughout my book *"Managing Risk and Information Security"*. These abilities enable us to work with others to support the Protect to Enable mission.

==========

This article is based on material found in the book "Managing Risk and Information Security" by Malcolm Harkins. Visit the Intel Press web site to learn more about this:

http://noggin.intel.com/intelpress/categories/books/protect-enable

Also see our Recommended Reading List for similar topics:
www.intel.com/technology/rr

About the Author

Malcolm Harkins is vice president of the Information Technology Group, and Chief Information Security Officer (CISO) and general manager of Information Risk and Security. The group is responsible for managing the risk, controls, privacy, security, and other related compliance activities for all of Intel[1]s information assets.

Before becoming Intel[1]s first CISO, Harkins held roles in Finance, Procurement and Operations. He has managed IT benchmarking efforts and Sarbanes Oxley systems compliance efforts. Before moving into IT, Harkins acted as the profit and loss manager

for the Flash Product Group at Intel; was the general manager of Enterprise Capabilities, responsible for the delivery and support of Intel¹s Finance and HR systems; and worked in an Intel business venture focusing on e-commerce hosting.

Harkins previously taught at the CIO institute at the UCLA Anderson School of Business and was an adjunct faculty member at Susquehanna University in 2009. In 2010, he received the excellence in the field of security award at the RSA conference. He was also recently recognized by Computerworld magazine as one of the top 100 Information Technology Leaders for 2012.

Harkins received his bachelor¹s degree in economics from the University of California at Irvine and an MBA in finance and accounting from the University of California at Davis.

==========