Innovation and its Implications for Security

CSOs do their part to minimize risk and bring innovation to fruition

CSO Custom Solutions Group

cisco

Executive Summary

Companies today remain competitive through innovation. For CSOs, innovation frequently includes risk, so security must be a consideration in developing and executing innovation strategies—like it was at Cisco when the company rolled out handheld wireless devices to its employees.

Today, innovation isn't just a "nice to have"; it's a compulsory way of life for virtually any enterprise. And, given the competitive nature and pace of business, it's here to stay.

But, like anything new, innovation does present some risk. "Innovation absolutely must be tempered with security considerations," says Brad Boston, senior vice president, Global Government Solutions Group, and former CIO for Cisco.

Rest assured, security doesn't have to stunt creative spirit. And for those companies that are doing it well, security doesn't even necessarily have to change for innovation to flourish.

A Competitive Edge

Innovation is about originality, inventiveness and even individuality. It's about new products and services, and better ways of doing things. However, it's not always

Getting Innovation Right

Our experts from Cisco offer some learned advice for embracing innovation in a secure and thoughtful manner:

- Don't try to hold back the tide. It's a waste of energy to reject innovations because of the security vulnerabilities they pose. So make them happen in a secure manner.
- Make education a priority. Innovation success often boils down to the individual's understanding of the risks. So preach the positives and teach the potential negatives.
- Be innovative yourself. Be one of the first to embrace innovations and use your own experience to set an example.
- Learn from each other. There's never enough time to reinvent the wheel. Cisco, for example, hosts a program that allows users to share the what, why, and how of new technologies and processes.
- Be prepared to make mistakes. Mistakes will happen, at both company and individual levels. Anticipate them, accept them, learn from them—and move on.

particularly "fancy," says Boston; some of the best innovations come in more basic forms.

Innovation means change, hopefully resulting in tangible, sustainable business value. And in these competitive times, it's innovation that will help enterprises to remain agile, open and responsive to evolving market demands and emerging business opportunities.

Take, for example, the iPod. Apple's invention exemplifies innovation—not just in the features that have taken it so many steps beyond the Sony Walkman, but in the monumental way that it's changing how people acquire music. Boston also points to Southwest Airlines as an innovator that has shown remarkable ingenuity in its operations. Though its process changes have been fundamental, the impact on the airline industry has been wide-reaching.

Of course, some companies are better at innovation than others, and that success often stems from company culture. As corporate attitudes become more innovative, explains Boston, creative cultures are emerging that foster new and better ways of doing business. True innovators don't rest on their laurels; they want to win, and so they go out of their way to reward creativity and recognize individuals who think outside the box. These are the companies that are realizing the true value of innovation in many profitable ways—and performing well against the competition.

A Risky Proposition

"Innovation and collaboration technology are doing an absolutely outstanding job of flattening the world and accelerating productivity," says John Stewart, vice president and CSO for Cisco.

But for all its positives, innovation does obviously assume a certain amount of risk, which begs an important question: How does innovation impact enterprise security and vice-versa?

Innovation introduces newness—new technology, new processes and even new levels of collaboration. "Like almost anything invented in history, what we don't know, we just don't know," says Stewart. And therein lies the challenge. Any innovation that touches the business introduces some level of vulnerability. For example, as companies adopt new technology for collaboration, inexperienced individuals may not know how to share their presentations. Doing whatever it takes to make a meeting happen, they may display their entire desktops and inadvertently expose sensitive e-mail communications.

This newfound spirit of collaboration also results in the sharing of more information than ever before. "That's the net good and the net bad of collaboration," says Stewart. It's important to share the right information, but not necessarily all information. This challenge is highlighted, he says, by the rising tide of "co-opetition," to which Cisco is no stranger. Many businesses must work closely with competitors to be successful, for instance, when hammering out industry standards. That means enterprises have to find ways to openly share—without leaving

Innovation Basics

Upgrading the Network for Better Security

The enterprise network has become a critical lifeline in any business. Enterprises rely on it for voice, video and data. What's more, with all business systems "on-net" and providing 24x7 customer service, downtime is simply not an option.

"Unfortunately, we've discovered that the same amount of care is not given to maintain the network as compared to computers and applications," says John Stewart, vice president and CSO for Cisco, "even when the upgrades are freely included in the software support." Computers are frequently the primary focus for security investment, and applications are reasonably well maintained, he says. "But we're terrible at upgrading our networks, even when there's so much to be gained and so much at risk."

Interestingly, that gap occurs despite the fact that next-generation networks can significantly improve an enterprise's ability to respond to competitive pressures and market demands to innovate. Take, for example, service-oriented network architectures that function as services delivery platforms. "We rely on our networks and the services they provide; there is no doubt in my mind that more services will be provided via networking," says Stewart. "As a result, we need the kind of network that supports new and evolving IT strategies, including Web services and the virtualization of applications such as voice, video, and telepresence."

As a result, Stewart explains, enterprises can see valuable business outcomes like increased productivity and efficiency with reduced costs; enhanced resiliency and business agility; improved customer relationships; increased revenue; and maximum business opportunities.

And aren't those the driving forces behind any worthwhile innovation?

the doors to their inner sanctums wide open.

What's more, enterprises are often taken aback by the speed of innovation. "It is incredibly difficult to keep up with what's going on because innovation occurs at such a fast clip," says Stewart. So it's not always easy to look at innovation from a security perspective, especially at the individual user level.

Recognizing and Mitigating Risks

That said, business leaders must take risks; it's what sets the business apart from the competition. But taking undue risks can put the business in jeopardy. It's the CSO's job to help mitigate risk and build consensus on the management of the overall risk threshold, says Robert Bragdon, publisher of CSO magazine. Ultimately, the CSO can enable business leaders to do more—to innovate more—by making it more comfortable to take risks.

Of course, when applied unilaterally, security is a barrier and potentially an inhibitor to innovation. For example, the government has strict rules around encryption. In some cases, these rules have become so daunting that the people who are supposed to be following them throw them out altogether, endangering the company's position.

CSOs need to take due care that security does not stunt innovation. But does innovation mandate radical changes in security strategy? Not according to Stewart: "Innovation doesn't change the security strategy that all companies must already have in place today." But it does mean that security has to be top of mind when figuring out how to bring innovation to life. Businesses must temper innovation with security considerations, asking important questions like: How does a new product potentially expose our enterprise? How can collaboration be done more securely? How do we select the most secure solutions?

Cisco realized this all too well a few years ago, when the company adopted an innovative new business tool: wireless handhelds. Cisco wanted to hold off on officially rolling out the technology to its user base until handheld wireless devices matured and presented less of a security risk. "At the time," Boston explains, "wireless was the single biggest nightmare for CIOs." But Cisco employees had their own

ideas, and when Stewart audited the user base, he found that 9,000 PDAs of different makes and models were already in use.

Indeed, the technology was making a business case for itself, truly revolutionizing the Cisco workforce. In some cases employees were synching their PDAs with their computers—for e-mails, contact lists, and calendars, among other things—which allowed for new levels of productivity and collaboration. But because they were unsanctioned business tools, Stewart had no control over their security. What's more, users were left to their own devices. If they lost their PDAs, IT simply couldn't help them—or secure their data.

Stewart says that the company needed to embrace the innovation, but with an eye towards risk management, and that meant taking a more regimented approach. Cisco approved and standardized on a single handheld solution that best fit the needs of its employees and the security requirements of the organization. This approach addressed those requirements technologically, meaning users had to accept security as part of the innovation. In the end, standardization proved to be a fair balance between offering a fundamental new way to do business and protecting the company, Stewart says. Now, Cisco is offering multiple choices for handheld devices to its employees, all with embedded security.

In addition to e-mail, scheduling and other basic functions, users have access to a full range of corporate applications via their wireless handheld devices, bringing the innovation to a whole new level.

"What's interesting is that we're seeing people, for example in the sales organization, stop using computers because everything they need is on their handhelds," says Stewart. "So in some respects, this innovation has actually increased security in that computers are not at risk and users are not connecting to other networks."

Embracing Innovation

Indeed, it's every CSO's duty to wholeheartedly embrace innovation. To do that, they must possess a deep understanding of the business. "In fact, CSOs are being hired today without IT or security experience," reports Bragdon. "But a keen understanding of the business and the ability to communicate effectively is a must."

CSOs who don't have strong business acumen can be perceived as holding the enterprise back, and can lead their business units to be regarded as cost centers rather than business enablers. "Of course, one of the biggest challenges that CSOs face is aligning security with the needs of the business and making sure that all investments clearly support company strategy," says Bragdon. In other words, are you providing the right tools to execute on the strategy directly, through features that enable innovation—or indirectly, by helping other groups to execute on innovation?

It's important to partner with business leaders. "Work together and the value of the security organization increases; work against them and that value plummets," says Stewart. Of equal importance is that CSOs are able to communicate security messages to the masses, as risk often lies in the hands of the individual. "Educate, educate, educate… and then educate some more," Stewart says. "Let users know that you want them to use new technology, but to consider the security risks along the way."

In the end, innovation is somewhere CSOs must go… so go there safely and smartly.

Visit www.csoonline.com/webcasts/cisco for a thought-provoking webcast in which three CSOs discuss innovation.

Info Security Takes Center Stage

IT plays two important roles in innovation, says Brad Boston, senior vice president, Global Government Solutions Group, and former CIO for Cisco. First, the IT organization itself must innovate, by finding creative new ways to deliver services. Second, IT needs to provide the tools to facilitate innovation in the company as a whole, particularly around collaboration.

To do this, IT must fully understand the inhibitions of innovation and take steps to eliminate them. For example, Cisco product innovation is driven by departments scattered around the globe. The company has had to embrace collaboration to make innovation happen in a virtual workspace, and IT was instrumental in creating that environment.

However, it's important to understand that the security organization isn't responsible for making decisions on what protection is necessary, says Boston. Its job is to understand the risks, costs, and alternatives—and then help business leaders decide what risks to take.