© Patrick George/Ikon Images/Corbis

WHITE PAPER **BUILDING TRUST**

How Will CIOs Meet Growing Security Threats?

EXECUTIVE SUMMARY

When it comes to protecting enterprise data, CIOs and CSOs are at a crossroads. The complexity and prevalence of security threats continue to grow, bolstered by consumer IT and mobility. The open nature of IT has paved the way for far more sophisticated attacks—beyond conventional credit card data theft to multilevel attacks. Information security executives face perhaps the toughest challenge of their careers.

The business requires and expects total freedom and choice in technology, yet risks come from any number of places: users at their desks, users working from many different mobile devices and unsecured networks, and users downloading applications at will from the Web. Corporate integration with social media sites provides a new path for malware to the network—not to mention privacy risks and even identity theft. Hackers still have many more opportunities to grab enterprise data and are getting smarter by the day. Given the pace of change in our Web-based mobile world, who knows what next month will bring?

EMC²

CIO
Custom Solutions Group

Moving from point solutions to integrated security

Are CIOs and their IT departments prepared? Many companies rely upon point security solutions designed to protect hardware and networks, and deploy broad-based security programs that blanket all applications and users in much the same way. IT's approach to security too often occurs at the last mile, immediately before a new application or suite of services is set to release. This disjointed, retrofit approach has unfortunately resulted in troubling and sometimes disastrous consequences for many well-known companies over the past few years.

It's time to place security front and center of all IT deliverables—in a more proactive, integrated fashion.

It's time to place security front and center of all IT deliverables—in a more proactive, integrated fashion. Take note: this is an opportunity for IT to take the reins of a critical risk factor for the business. Doing this right will enable IT to give business leaders clear avenues to innovate and enter new markets with the help of IT-enhanced services. Instead of being draconian rule-makers, CIOs and CSOs can help their business counterparts do more with less risk.

Given both the opportunities and the threats, CIOs and CSOs must rethink security processes and practices. Moving forward, security ideally becomes an enterprise initiative integrated into all facets of operations and measurable in business terms. CIOs, CSOs, and their teams will do well by adopting a baked-in approach so security isn't a technology wrapper, but integrated across services, processes, user behavior, and technology.

New metrics and business alignment

In the future, CIOs will need to better quantify and justify investments in security technologies and programs to ensure spending is stratified by business risk. IT will need proven methods for evaluating whether a technology is aligned properly with high priority, sensitive business data. What will be the most appropriate risk metrics to track?

The security of the future will be tightly aligned with business goals, shifting to an on-demand service model within the IT-as-a-service infrastructure now under way. IT leaders will work in tandem with the CSO, rather than reacting as the last bastion of defense moments before deployment. As one expert said, this shifts emphasis from the near-impossible task of preventing intrusion to the crucial task of preventing damage.

Understanding the threat landscape

Some CIOs say they are seeing a tenfold increase in the intensity and frequency of attacks on their networks. The Ponemon Institute, in its 2010 Cost of Cyber Crime study, reported that of 47 organizations surveyed, a combined 205 separate and discernible cyber attacks were detected over the course of a four-week data collection period. The average annualized cost of cyber crime for these organizations was $6.2 million.

CIOs and their boards continue to report that security is a top priority. In a poll of more than 800 CIOs in the 2011 State of the CIO survey by *CIO* magazine, respondents cited the increasing importance of security and risk management, driven by the adoption of alternative IT models. Four out of 10 respondents anticipate that improvements to security and risk management will be among their IT organizations' most significant business accomplishments in the year ahead—up from 34 percent in 2010 and 26 percent in 2009.

Security attacks targeted at corporations are complex and multi-layered. Cyber criminals and so-called "hacktivists" are exploiting corporate adoption of social media and cloud services by penetrating corporate networks through technologies such as social engineering. Typically operating in rings, they use stealth and government-agency tactics, such as compromising one company to enable an attack on another. Other methods include sophisticated analytics and intelligence gathering, application layer exploits, and multistaged attacks on sensitive financial, and customer data or intellectual property.

RSA's Executive Chairman Art Coviello speaks with *CSO* magazine publisher Bob Bragdon about the CIO/CSO relationship in today's threat landscape.

IT organizations struggle to stay abreast of these challenges. They must become as agile and as adept at intelligence-gathering as their cyber adversaries. The key to improving organizational defenses is adopting security practices and tools that analyze security risks behind the scenes, comparing activities, and user behaviors against a baseline of "normal" conditions. If high-risk circumstances are detected, IT systems automatically activate additional security measures. For example, if an organization's network detects an employee attempting to log in remotely from an unknown IP address, a challenge question pops up to authenticate user identity, such as: "Of the three names presented here, who have you emailed the most in the past week?"

This is an example of risk-based, contextual, and agile security. For security to achieve this intelligent, automated standard, organizations first need to gain full visibility into what's happening within their IT environments and into the activities of end users. They also need to consider what cyber adversaries are up to and what attack techniques are they using. By employing big data engines and skilled security analysts to process and evaluate these rich sources of internal and external intelligence, organizations develop true "situational awareness," a prerequisite for proactive, predictive security.

As employees push IT to support bring-your-own-device (BYOD) and do-it-my-way computing, more vulnerability appears. CIOs and other senior executives, including CEOs, understand that security must be a top operational initiative.

It used to be a case of not if, but when an organization will be attacked. Today, you must operate with the assumption that you've already been attacked—or even breached.

Building better relationships with the business

For as long as most CIOs can recall, aligning with the business has never been easy or simple. Many CIOs still struggle to overcome the "cost center" moniker, while business leaders want proof that IT is building their applications in the most cost-efficient manner. The business seeks the latest capabilities, and IT leaders work hard to explain what it takes to get there. Now business stakeholders have other, external sources for acquiring what they want. These include IT services traditionally supplied internally—most notably, security.

The problem is, most IT shops and their leaders are not set up to go to market with their services in this new, competitive paradigm. The CIO must communicate the benefits and risks of security in all areas and reinforce notions of simplicity and agility when it comes to security, instead of a process that impedes productivity.

Business understanding of security, with its roots as a highly technical discipline, still has a long way to go. According to the PricewaterhouseCoopers 2012 Global State of Information Security survey, roughly one-third of business executives surveyed are uncertain when it comes to their information security strategies. Only 43 percent of participants believe their organization has an effective information security strategy in place.

In past years, this information gap wasn't as critical, but now CEOs and even boards demand detailed information about security risks. They've seen the headlines about major companies that have been attacked, and they're worried about how a potential breach or data-loss event could have a significant negative impact on revenue, branding, and customer loyalty.

A first step is to change the language IT and security leaders use with business counterparts. Most executives don't relate to terms such as "data protection" and "anti-malware" but instead want an explicit understanding of how IT protects their most sensitive data assets. They may not easily see security as strategic, but at least leaders can understand the risks from financial and business perspectives, and what tools and solutions the CIO needs to minimize those risks.

Security as a market-enabler, not a roadblock

Secondly, CIOs should consider how to present information security as a market enabler, supporting business plans for new technologies such as social collaboration, mobile customer applications, Web 3.0, and the cloud. Too often, security has a negative connotation with businesspeople who've long viewed it as a roadblock to collaboration and customer relationships. It's up to CIOs to show why the opposite is true, and how IT is working to embed security to make it easier and transparent for users.

Many forward-looking organizations are including business stakeholders—along with security and IT leaders—in ad hoc security taskforces or risk committees.

A critical component of communications with stakeholders is framing the message logically in business terms. Many experts suggest centering security discussions around the concept of data tiering and stratification of information—a core security strategy going forward. It's much easier to win internal mindshare by demonstrating how the CIO and CSO assign values to information, and how those values dictate required security levels, rather than issuing mandates with limited or faulty reasoning.

Security can fit well into the IT-as-a-Service model because it should operate seamlessly, automatically, and on demand—without requiring complex logon procedures and other manual processes. IT and security leaders should discuss how security improves productivity when administered and deployed centrally as a service. Benefits include avoiding unnecessary interruptions when viruses shut down email and other applications, and keeping customer, financial, and IP data safe—all of which tie directly to profits and revenue.

In the near future, CIOs must develop and report metrics that link security to business outcomes. Measures such as continuity of operations, user compliance with security policies, adherence to security standards, security outcomes, security software ROI and more will become part of the regular IT-business conversation.

Forging a CIO-CSO bond

Neither CIOs nor CSOs can stand alone in these efforts. Tightening the relationship between CIOs and CSOs will help at all levels including technology selection, policy definition, business communications, metrics, and strategy refinement. Of course, CIOs and CSOs haven't always been on the same page, which is simply a matter of different perspectives and roles. CSOs have traditionally analyzed projects through the narrow security lens, whereas the CIO must adopt a broader, business-objective viewpoint. This dynamic breaks when the CIO learns from the CSO at the 11th hour that a high-priority, Web-based CRM project isn't ready from a security standpoint, for example. Now, the CIO has to deliver the unexpected bad news to the business—never a happy moment.

Fostering a more integrated relationship—in which security and IT teams are not divided by a wall—means that both parties must change some preconceptions and practices.

The CIO can work to integrate the security evaluation framework into all projects and strategies, while the CSO may need to be more flexible on controls for data and applications that don't fall into top-level security buckets. The two parties will have to negotiate time frames as well. With the movement toward agile software development, security teams may struggle to keep pace with product changes unless they can adapt risk evaluation to an accelerated timeline. Working together, the goal is for CIOs and CSOs to agree upon standards, processes, and policies, which they can then bring to the business with a common voice.

But the CIO and CSO needn't go it alone. Bob Bragdon, publisher of IDG's *CSOonline* magazine, points out that many forward-looking organizations are including business stakeholders—along with security and IT leaders—in ad hoc security taskforces or risk committees. This ensures security is not only baked-in, but that critical business-perspective input is factored into any solution or process.

How do you approach security? And how integrated should IT security be with technology and processes at your organization? See how you compare to your peers in these areas by taking this interactive benchmark survey. Click here to begin.

Sealing the "people perimeter" with risk-based security and education

After building the foundation for healthy discussions between IT, security, and the business, it's time to bring everyone together around a business-friendly security plan. Instead of determining how to support applications and devices as they appear on the network, companies should develop security plans around data categories and their associated risk. Users accessing publicly available data have few, if any, controls—while access to mission-critical data is behind the vault, with access allowed only under certain conditions and by a select group of people.

By instituting data classification, IT can determine trust levels that are more appropriate and easier to manage. For instance, if you're a senior finance manager and logged on from inside the secure corporate network, you can view the company's core financials from your mobile phone while walking between meetings. But once you leave the building and enter an unsecured area such as coffee shop with free Wi-Fi, you lose that special access.

A critical piece of the information security strategy is the understanding that security technology is not perfect, and that your people can pose the greatest risk. This is particularly relevant when talking about social networking, because people unwittingly provide the avenue for attack.

Human behavior is hard to change and mistakes will undoubtedly continue, but companies should place a higher level of accountability on their employees in exchange for more freedom vis-à-vis consumer IT. It all starts with education. Do people in your organization really understand the business risks of security, why some data and applications require more stringent controls than others, and how failing to comply with safe computing practices endangers the business at large?

For a reality check, consider sharing intelligence such as the number of attacks on company data and networks from the last quarter—and how IT addressed them. While some companies require quarterly or annual mandatory training, a more effective approach may be delivering security information more frequently and organically through ad hoc workshops, weekly newsletters and emails—or even signs in the break room and walkabouts by security liaisons. Or better still, target education so it addresses risky behavior.

While IT and security departments need to develop the curriculum, business managers will likely have the strongest influence over their teams when it comes to delivering the message and influencing behavior. As with security discussions between CIOs and senior business leaders, managers can drive positive messages about how company security programs enhance productivity, competitiveness, customer satisfaction, and responsibility.

Yet education won't be enough. Companies need procedures and consequences for business units and/or employees that consistently rebuff policies. IT should be able to frequently measure and report on user behavior. While managers and their employees need to take security seriously, it's also IT's responsibility to ensure security is not a barrier to getting work done. Managers will tell you if controls and authentication processes are overkill.

Down the road, policies and controls must be more transparent and automated for users. For example, user access to data should be adaptive depending on risk profile including role, location, control environment, access history, and network conduct, among other factors.

That's more for the future. For now, consider how IT can simplify security controls at the user level. One way is to build controls such as malware detection and encryption into mobile applications vs. relying on the host operating system.

Akin to this is the need for flexibility when it comes to the cornerstones of consumer IT: online software, mobile devices, and social media. When IT attempts to place controls on new technologies, particularly social media, it often backfires with tech-savvy users

PART 1: *CIO* **Publisher Emeritus Gary Beach's discussion with Sanjay Mirchandani, CIO at EMC, and Dave Martin, CSO at EMC and RSA, on the new security perimeter: people.**

figuring out workarounds to go where they want on the Web and to access corporate data from unsanctioned devices. Instead of blocking access to social media and refusing to support a personal device, return to education, and awareness. That way, users understand the risks of their choices and how to prevent problems from happening.

The overriding philosophy of this new security strategy is a bottom-up approach that incorporates viewpoints from across the business and makes it easier for people to incorporate security into daily work life—and to follow key practices required to protect critical information.

A business-friendly approach to governance

Alongside this user-centric approach to security is the need for a new governance model. When devising a governance strategy, frame your decisions around this mantra: the business owns the data. Typically, the security team delivers reports to a few stakeholders such as the CIO, CFO, or the compliance officer. What's needed is a more functionally-representative process consisting of an executive risk committee of the CIO, CSO, the HR director (who has knowledge about employee privacy), the financial or procurement officers who handle vendor data, and the VP of sales, who's in charge of customer data.

At the next level, risk committees should exist within each business unit, reporting to the executive committee, as *CSOonline's* Bragdon points out. Business risk committees work hand-in-hand with security teams to provide input into security-related decisions and processes. In this model, security and IT managers act as consultants who help gather information about the prioritization and risk of business data, and communicate issues up and down the organizational ladder. By integrating security deeper into the company, CIOs and CSOs spread risk visibility to the department level for more successful buy-in.

Technology vision: contextual, information-centric, and agile

The market for security applications and services has exploded in recent years—and for good reason. There are vulnerabilities at every level of the business and in every corner of the infrastructure. Vendors have determined that they can develop a solution for each and every scenario. But do you need all this technology in your business? Are technology and too many priorities preventing you from being agile, and making security less effective than it could be to protect the business and prevent future attacks?

Pressure on IT to reduce TCO and operate leanly haven't eased up, and no one expects it to in coming years. CIOs and CSOs must closely evaluate risk levels for all applications and data categories, and enable prioritization to dictate exactly where to invest in software and services.

Related to this is a better understanding of who represents the largest threat to your business. What are they after, and what kinds of data are most valuable to them? How should their tactics impact your security strategy? These topics deserve security's highest attention. Data should be easily discoverable based on historically suspicious behavior on corporate networks. Monitoring and analytics systems will be critical to help store and analyze risk and report it to executives.

Designing technology around targeted protections is one pillar of the technology vision. The other revolves around data- and application-centric authentication, control, and monitoring, vs. the more common point-solution approach at the hardware and network levels. This bolt-on approach too often results in applying security technology,

PART 2: Gary Beach's discussion with Sanjay Mirchandani and Dave Martin on the new skills needed for today's security environment.

such as authentication and access control, at the end of the application lifecycle. Once we start adding more and more devices and applications into the cloud infrastructure, this reactive device- and location-centric strategy becomes quite difficult to manage.

Today's concerns include how Executive A logs onto the network from his or her Android phone, while tomorrow's may be Executive B wanting to check financials from the road on his unmanaged iPhone. Because data use is so highly distributed, controls to protect that data should also be distributed. That's where we get to application- and data-centric controls. If data is published with embedded controls, it will follow employees from location to location and from device to device.

The strategy becomes wrapping security containers around data and applications and integrating those data-specific controls with user-based access according to job role. This way, security is integrated at the data and user level and is easier to disseminate among many constantly changing scenarios. In the new world, security is tightly aligned with business risk and is much more agile. And it continues to become faster and easier for IT to enable access from different devices and locations through an automated, app-centric approach. Security is no longer a hindrance, but keeps up with the speed of the business.

So how do you deploy this? Application-level security revolves around the concept of a suite of services delivered at the host and application levels with more consistency. Rather than concentrating defenses in one place, at the access layer for example, security controls such as DLP, malware prevention, encryption, and additional access restrictions are embedded throughout the software and network stack to provide distributed, multilayered protection.

As mentioned earlier, controls depend upon risk. Users accessing publicly available data from a corporate laptop may do so unheeded. However, as the sensitivity and importance of the data increases, various protections, monitoring tools, and authentication scenarios will apply to the user attempting access. Much like a university model, the layered segregation between research and administrative information is separated from the more open campus and dorm networks. It's impossible to control the hardware, location, and network connection of the user, so the controls must exist deeper within the application. Corporate app stores will publish containers of enterprise apps with the same model, building protection into the application itself.

Resolution and investigation of issues is also critical and must be more comprehensive, contextual, and rapid. To prevent the most damaging attacks and analyze attempted or successful breaches soon after they occur, companies will rely on advanced analytics to gather information from across the IT infrastructure.

Fortunately, due to industry advancements including Big Data, IT, and security departments will soon enable better management of this complexity without hiring more staff or consultants. Take cloud computing, for example. Public and private cloud providers will deliver built-in security as well as centralized monitoring, management, compliance, and resolution. Compare that with today's piecemeal approach. Cloud, data center, and SaaS providers will become key partners for CIOs and CSOs in developing and managing security. And savvy senior executives will evaluate and select these vendors with security top of mind.

A roadmap to evolve

Without a wholesale change to the traditional enterprise approach to security, a company's very survival is at stake. With security comes trust. Without this trust, a company will be unable to retain customers or succeed with new product or service lines.

Trust is the foundation of business relationships today.

In closing, here are several key takeaways that will help CIOs, CSOs and their business counterparts meet advanced security challenges:

- CIOs and CSOs must fully partner to present a unified approach to security.
- Security must be totally integrated within the business—not an IT-driven activity.
- Security must adapt to the consumer IT, cloud, and device worlds—instead of the other way around.
- Relationships with business stakeholders at senior- and middle-manager levels will be key differentiators in optimizing security success.
- It's up to the CIO and CSO to figure out how to communicate about security in ways the business will not only understand, but will see as critical in supporting revenue, innovation and viability.
- Business and user accountability is imperative, and will depend upon IT and security leaders focusing on the required people, process, and technology changes.
- Security should focus on protecting data and applications, not hardware and networks.
- Security approaches should be more agile and intelligent, modifying defenses based on risk profiles and other contextual assessments.
- Security leaders should aim to achieve situational awareness—gaining full visibility into internal and external threats—to assess risks reliably and optimize security operations accordingly.
- Developing security strategies and controls based on the level of business risk will prevent ineffective IT investments.
- Users are essential to making security work. So security that's simple, transparent, and easy to use will not only be effective—but will help win the hearts and minds of the business.

For more information, please visit
www.emc.com/cio

EMC²

CIO
Custom Solutions Group