Embedding Information Security into the Organization

Risk and business have always been inseparable, but new information security risks pose unknown challenges. How should firms organize and manage to improve enterprise security? Here, the authors describe how CISOs are working to build secure organizations.

M. Eric Johnson
Center for Digital Strategies, Tuck School of Business at Dartmouth College

Eric Goetz
Institute for Information Infrastructure Protection (I3P) at Dartmouth College

Like a hail storm over a car lot filled with new vehicles, information security failures have steadily dented many shiny corporate reputations, reducing customer trust and eroding shareholder value.[1,2] Risk and business have always been inseparable, but today, new information security risks pose unknown challenges for firms and governments alike. With terrorist groups increasingly using information tools and developing cyber capabilities, foreign governments engaging in large-scale espionage, and criminal syndicates setting up professional cybercrime operations, organizations are facing a new generation of threats that are often difficult to detect, and it's nearly impossible to assess their long-term consequences. Of course, many information risks still arise from mundane sources. Bank of America's (BOA's) Executive for Corporate Information Security and Business Continuity, Doug Smith, lamented, "I worry about paper. Bank of America spends almost a billion dollars a year on copier paper. That is a huge risk."

Many other business trends accentuate information security risks. Outsourcing and off-shoring bring new partners into an extended enterprise, with different technologies, cultures, and sensitivities to information management.[3] Contracting, telecommuting, and mobile workers all contribute new security risks. In such outsourced, extended enterprises, effective risk management is quickly becoming a source of competitive advantage. Consequently, the security management and chief information security officer (CISO) roles are becoming more strategic. Yet, we've found that moving the needle on information security is a team activity, requiring everyone's participation. The technology community has made much progress in the past five years to improve security's technical aspects. However, some of the hardest remaining challenges involve people and organizations.

Throughout 2006, Dartmouth College's Tuck School of Business conducted extensive field research in addition to workshops with IT and security executives in large firms (more than 30 Fortune 500 level companies).[4–7] (Although CISO is a common title for the senior information security person in a large organization, many firms, such as BOA, don't use this title for the head of information security. In this article, we quote executives who, in most cases, represent the CISO for that firm. We omit titles for ease of exposition, although many of these are available at http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/ResearchSecurity.html.) Here, we present the results and examine the security and organizational challenges facing executives of large multinational firms. We believe security executives can make a significant impact in transforming their organizations in three pivotal areas: successfully measuring security and security improvements, inculcating security into a company's organizational culture, and developing models to strategically invest in security. They should also focus on some key imperatives when building security into their companies from the ground up.

The challenges

Managing security risks is a balancing act between maintaining security and not inhibiting the business.[8] IT executives in every sector agree that lasting improvement in information security requires participation from everyone in the organization. We've found that, like the quality-management movement in the 1980s,[9] security is "bolted on" in many organizations, rather than being infused into them. From our field research interviewing security managers, we found that large firms' CISOs struggled with the following pervasive challenges.

Raising the level of understanding within an organization

As security professionals work to elevate the level of security education and knowledge within their companies, one of the first hurdles is to reach a point at which organization members know what questions to ask and how to find the services they need. The ultimate objective is to let the business units share in information security risk management. Phillip Shupe at Eastman Chemical summarized the common concern: "The biggest challenge I face is developing a level of education in the company where we can provide consultancy to all the organizations throughout Eastman. So, when someone requests security that we understand and they understand what they're asking for."

Of course, education must start at the top. The top executives at many large firms really understand the risks. BOA's Smith noted, "The top of BOA, they get it. They clearly get it, and they remind me every day. Our chairman and CEO actually carries a piece of paper in his pocket [with] the eight things he worries about most, and I'm two of the eight, 25 percent." In several cases, we found that the senior management isn't the biggest hindrance to better security. Rather, middle management might represent one of the largest challenges because they impact the organization daily. As the US Army's CIO, General Steven Boutelle pointed out, driving security awareness through all levels of management is key: "The issue really is the mid-level management—those are the people who make the resourcing decisions on a day-to-day basis." Part of raising awareness involves personalizing risks for managers, showing them how vulnerabilities could affect them as individuals. Showing a manager in the banking sector, for example, that his or her personal information (including credit-card information and personal details) is available on a music-sharing network drives home the need to protect customer data. Senior leadership must also ensure that metrics and incentives hold middle management accountable—nothing gets people's attention faster than telling them their pay or bonus is affected. Senior managers can also lead the way by asking security-related questions when their subordinates present progress reports or propose new projects. Such questions send the message that everyone should be prepared on security topics when they interact with senior leadership.

Changing behavior

In many organizations, awareness of security issues among senior executives is growing, but it is often still too reactive. A more proactive stance would help organizations deal more effectively with emerging problems and compliance issues. Awareness is the first step, but as Theresa Jones from Dow Chemical put it, "My biggest challenge is changing behavior. If I could change the behavior of our Dow workforce, then I think I've solved the problem."

One good way to do this is to have line managers (as opposed to corporate staff) take personal responsibility for security and involve company auditors to help enforce security levels. This creates a different level of awareness among line managers; it also helps integrate security into the corporate culture, making it a crucial part of the business process. Cisco's CIO, Brad Boston, gave an example of how to further personalize security for line managers: "The most creative one I heard was [from] a friend of mine at Intel. He was trying to get his line managers to own security for their employees, so they created a vehicle of giving you a speeding ticket or a fine, depending on the severity of your security violation. So, [if] an employee did something … really bad … there's a financial penalty […] So they made the managers pay the fines to incent them to go and talk to the people about not violating the rules."

Dealing with globalization

A growing challenge is establishing and maintaining a strong security program that spans the globe. Even in organizations in which the security group has implemented a strong core program, it's still challenging to get business units worldwide to take ownership of their security risks. As Staples's Chris Dunning noted, "Securing a global retail firm is very challenging. I feel we have good ownership for core infrastructure security within the organization. The big challenge for us now is getting that security ownership out into the business, into those key critical applications that really run the business that are outside the infrastructure."

Protecting data and intellectual property

One of the most frequently cited challenges was the difficulty of protecting an organization's data and intellectual property—information that increasingly makes up the bulk of a company's value—particularly in global organizations in which information resides with multiple divisions and partners. New technologies (including ubiquitous mobile devices) and collaborative cultures within organi-

Part of raising awareness involves personalizing risks for managers, showing them how vulnerabilities could affect them as individuals.

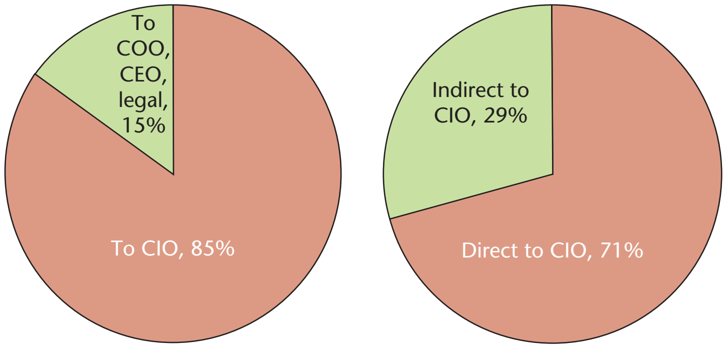

Figure 1. Top security executive reporting relationships. In a recent workshop, we looked at a sample of 20 large firms for a breakdown of who the top security executives reported to.

zations make protecting information an even greater challenge, especially because it's difficult to know when you're losing intellectual property. Eaton's Jack Matejka noted that security extends beyond protecting intellectual property to facilitating its application, "not only to protect […] the intellectual property itself, but also to build stronger, more secure, more highly reliable products."

Strong identity management can help control who gains access to information and with what permissions. However, this becomes both a policy and a technology challenge, as security policies must be realistic and enforceable. As Cisco's Boston noted, "A lot of companies made policy decisions that only a few top executives get Blackberries because of the intellectual property risk. But they don't bother to see whether their employees really do it anyway. And then they don't go and close that risk. So you have to go take a look at, are the things that you think you just said 'no' on actually enforceable? Or are they going to do it anyway?"

Another key component to protecting information is protecting customer and employee privacy. Nancy Wilson at Time Warner Cable said, "My biggest challenge right now is data privacy from the enterprise perspective. Not just from corporate IT, but working with our divisions that are very distributed, and different data just residing everywhere, from the systems side and then from the mobile device side."

Moving from technology to security management

Security used to be more about providing other business groups with the latest security technologies and solutions; senior management now increasingly asks security groups to provide governance, policy development, and consultancy-type functions.

As senior management of Fortune 500 companies raises security awareness, and as customers start to demand better security, this shift in emphasis—viewing security as a critical business function—gives security groups greater authority to enforce security measures. This can go so far as to give the groups veto power over decisions associated with excessive risk, even if this means pushing back a new product or service's launch date. A pivotal part of empowering the security group is leveraging its understanding of the organization. If the security group can help match operational security risks with business objectives, it can show how security measures really protect the firm.

Expanding securely

For growing companies, the greatest challenge is keeping the organization and its critical assets secure in times of rapid expansion. As the size and scope of operations grow, maintaining a consistently high level of security becomes difficult. An added challenge is when expansion includes acquisitions or opens systems to external partners. Companies often make business decisions about expansion without first consulting the security group concerning possible risks introduced via that decision. Cisco's Steve McOwen put it this way: "I guess the main challenge would be, as our company expands through acquisition, through partners, through growth throughout the world, […] how to protect and monitor what's going on and protect our critical assets."

Complying with laws and standards

Many organizations find it challenging to stay in compliance with various government laws and regulations, such as the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA), as well as industry standards, including the Payment Card Industry Data Security Standard (PCI-DSS). International organizations have the additional challenge of complying with laws and regulations in all countries of operation. In particular, European privacy requirements and associated "safe harbor" provisions from the US Department of Commerce, which lets European data flow into the US, are an enormous issue for many firms.

Funding improvement with tight budgets

In industries in which security problems haven't landed on the front page of the business papers, or in which security's added business value isn't immediately apparent, some managers are constantly struggling with security budget cuts—having to do more with less. Limited resources are a problem for large and small companies because there's an abundance of threats but only limited resources to deal with them. In addition, security managers are regularly faced with a difficult question: "How much security is enough?"

Organizing for security

Although security structures within organizations vary

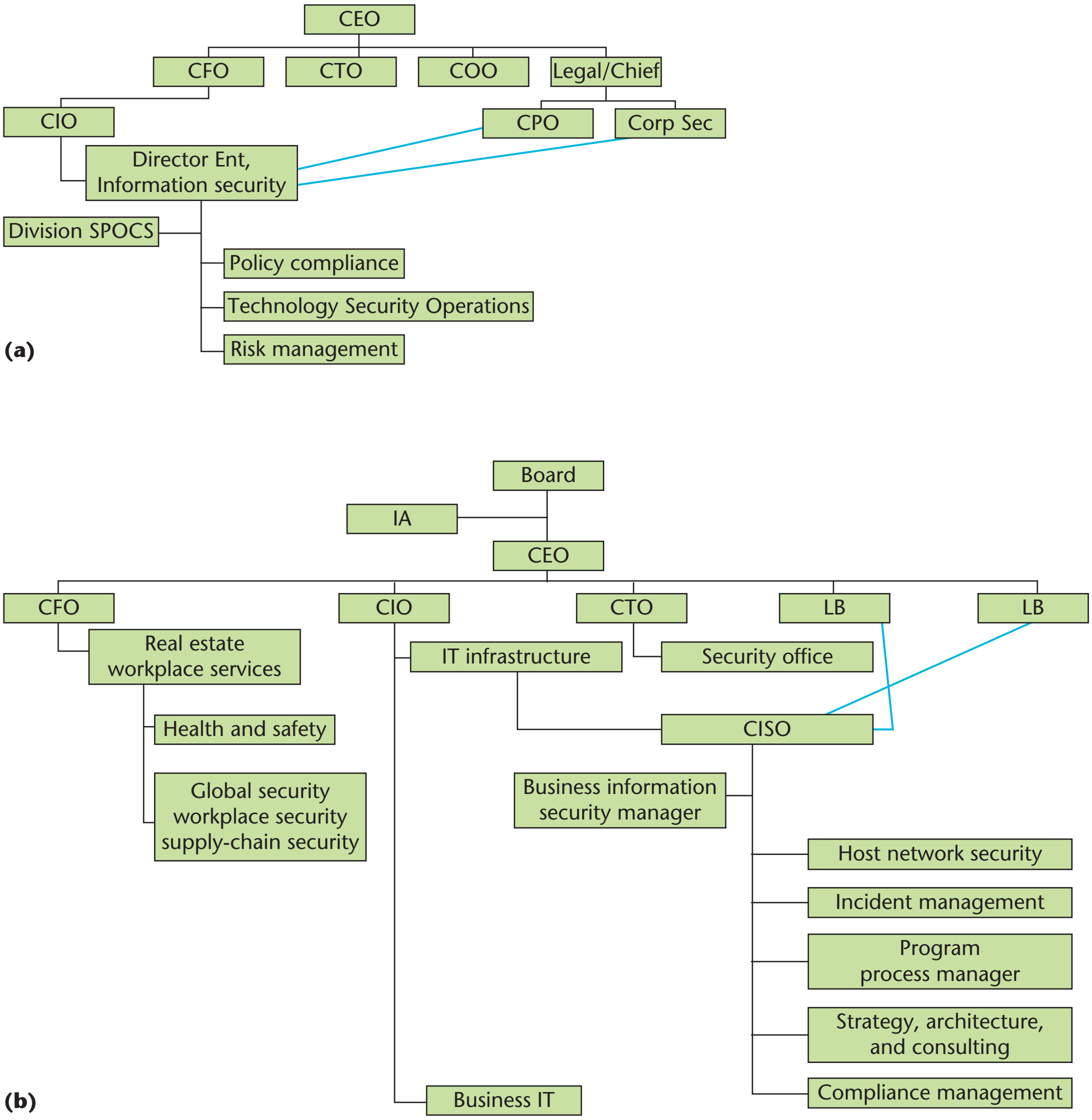

Figure 2. Organizational structure. (a) In some organizations, security management reports directly to the CIO; (b) in others, it reports indirectly to the CIO through other IT executives.

substantially, some key similarities existed between several of the companies we examined. In many cases, security groups are themselves divided into different units, dealing with information security, strategic risk and risk management, business continuity, operational security, network operations, infrastructure, architecture and engineering, policy development, and so on. Reporting relationships also vary between organizations—most security executives report (directly or indirectly) to the organization's CIO, while some report to executive committees of the company's CEO or the company's general counsel. Figure 1 shows the breakdown for 20 large firms (Fortune 500 level) who attended one of our recent workshops. In 85 percent of these firms, the top security executive reports to the CIO; of that number, 71 percent report directly to the CIO, and the remainder report to the CIO through some other IT executive. Figure 2a shows a typical organizational structure in which security management reports directly to the CIO, whereas Figure 2b shows an organizational structure in which it reports indirectly to the CIO through other IT executives.

There are usually also some "dotted-line" reporting relationships to other executives responsible for specific lines of business and various committees (or councils or task forces), including audit, board, risk, compliance, or technology steering committees, and other business units such as the corporate security department. In some cases, a chief risk officer or a chief technology officer is also in the mix. Global organizations might also have some kind of geographic or regional structure of responsibility. Some security organizations also liaise with other company departments such as HR, legal, risk-management, and physical security on issues such as policy development and compliance. In other cases, some of what could be considered security functions, such as privacy, ethics, compliance, policies, or strategy, is done by separate groups within the organization.

Security organizations' funding streams also vary, but for most large firms, the CIO ultimately controls and approves funding. If the security organization reports to the head of an operational unit or other senior executive, that person (or persons) might control the budget as well. In cases in which operational security functions (for example, protecting the organization's infrastructure against viruses or denial-of-service [DoS] attacks) are separated from more strategic or compliance-related security functions, several different sources might control funding. Sometimes, individual business units might provide funding for specific security projects, and, in one case, the audit group had security funds available.

Change is good

For most organizations we examined, the security group's organizational structure is in flux and seems to undergo frequent change. At a recent workshop, more than half of the participants stated that their reporting relationship (that is, the box represented in the figure, not the individual person they report to within the organization) had changed in the past year. A significant number experienced changes in their reporting relationships in the past six months. Only a few organizations haven't had any structural or personnel changes in their reporting relationships in the past year. For almost every organization represented, the security group's internal structure had also changed in the past year, clearly showing that restructuring security functions is an ongoing process.

Reasons for structural changes are manifold. They can be based on changes to a company's operational environment, business goals, and external-risk environment, as well as its need to comply with new regulations. In some instances, operational and tactical imperatives, rather than strategic shifts, have driven structural changes. In others, restructuring occurred to centralize responsibility for IT security; as Donna McJunkin at 3M said, "The CIO we have now wants to have *one* neck to choke, and she decided that's mine."

Best practices for structuring the security group

It's difficult to pinpoint structural best practices because the security landscape changes so rapidly that further structural changes are likely in the coming years. Steve Shirley of Lowe's gave the following example: "I see [our organizational structure] continuing to change for the next several years because of the internal and external factors […] We've actually moved compliance into a separate role that reports to a different group. Compliance is its own program within IT across the enterprise, so that's out of security now […] Consumer privacy now is starting to boil up through security, and probably, over time, I think that will end up leaving security and becoming part of some broader enterprise organization."

Security is about people

It's less important how a security organization is structured and more important that the organization has the right people to implement security successfully, meaning individuals who take ownership of security and build good relationships with others in the organization and external partners. Dell's Jeff Chumbley noted,

> "Organizations come and go, evolve in shape […] I think everybody's company is reorganized all the time. The effectiveness, I think, comes within the ownership of the individuals that are part of that team and having a clear common goal […] And if you want to talk about challenges in the security organization, or compliance, or whatever you are talking about, it's finding the talent […] I need people that have the technical base and the business acumen. It's that tie. I can go hire geek after geek after geek to do penetration testing or application assurance, but if there is no business acumen there, I don't know how much value that provides."

But security professionals who have technical and engineering skills—who understand how to explain the risk-reward trade-off and can sell solutions within the organization—are difficult to find. Align Technology's Jim McMahon related his search for an information security manager: "I have talked to 32 candidates in the last four weeks—some incredibly bright people who can define the very best way to trigger a firewall; people who have the ability to take and meet a virus head-to-head with sword in hand, [but] who couldn't sell me a piece of cake if I was starving." Bose's Terri Curran said, "I would throw out any of the best and brightest technicians that I met for one person that could tell me about a manufacturing line. We don't have any middle ground with people understanding the business. I'm talking about security people. I don't think security people understand business."

Preventing burnout and managing a healthy rate of turnover is a critical organizational issue for security. As Cisco's Stewart put it, "Frankly, the other thing that I would offer up as the number one threat to my team is [waning] morale. Keeping awake and alive and passionate about what is fundamentally feeling like a losing battle. And so a 15 percent refresh in the management and in the technical talent is almost essential to keep the energy as high as it is today." But, IBM's John Moore cautioned, "If you have too much turnover or too much reorganization, you can't make progress on more strategic initiatives."

Security beyond firm boundaries

Managing security beyond a corporation's borders remains a tough issue for most firms. Although many have staff in place responsible specifically for managing external business partnerships, resources are stretched very thin. One problem is that business's pace is so rapid. The security groups are often forced to react to events, but, as Bill Aertz from Medtronic noted, "There are just not enough bodies or time to get it done well."

Many firms have adopted simple fixes, such as adding security clauses to supplier contracts that specify security baselines, adherence to security standards, and best practices, or allow the organization to periodically test the partner's security. However, actually enforcing remediation of security vulnerabilities, especially for partners that are critical to the organization's business, remains difficult. To enforce remediation, the security group ideally needs the support of the business unit that plans to work with the partner. An industry-sanctioned level of security certification would provide more assurance that partners are following best practices.

Cultural differences between companies and potential business partners can also cause difficulties when partners have an incompatible view of security risks or are behind the times on good security practices. Security can also become a new stumbling block between partners that have done business for years. In these cases, partners will sometimes resent being asked about their security arrangements.

Transforming the organization

Through our field studies and workshops, we've identified three major areas in which security executives can make a significant impact in transforming their organizations: finding ways to effectively measure security and quantify if security is improving; creating an organizational culture of security at a company that ensures that security is "ever present" and part of every employee's understanding of risk; and developing security investment models that build security in at the outset as a fundamental part of every project.

Measurement—risk and security

Metrics are a management fundamental, but when it comes to security, many open questions exist: how do you know if security initiatives and awareness are making a difference? How should metrics cascade throughout the organization? How can risk and security metrics be more closely tied to tactical and strategic decision making?

Many companies use checklists (generally comprised of yes-or-no type questions) or scorecards to track security. Scorecards, which measure things like IT operations, system architectures, security measures, and compliance, can provide insight into how changes to architectures, configurations, and settings can affect security. Various facilities can use them to check whether a list of security measures has been implemented (for example, if the antivirus is up-to-date on all the desktops), how many vulnerabilities exist in certain systems, or how many attacks an organization is facing (for instance, the number of hits on the external intrusion detection system). One problem with scorecards—and many other metrics for that matter—is that they often provide some kind of percentage score, but it's hard to really prove their validity. Are the metrics really helping to reduce risk? Will they help save money next year? Will they add business value?

Other organizations use composite metrics to provide insight into security levels. These can contain various elements depending on the type of organization, the business sector, and the organization's goals. Composite metrics aim to provide risk scores so that different groups within the organization can set security targets and help identify acceptable risk levels. This helps senior management determine whether an appropriate amount is being spent on security. Dow's Neil Hershfield argued that "[composite metrics] are something that would be easy to understand, that you could describe to people and recognize you're not going to get 100 percent because of the cost. I like that […] I think that's a good way to talk about managing risk." Good business metrics typically exhibit variability. If everyone gets the same score (pass), there's no room for improvement. Composite metrics that have many different components and result in a wide range of outcomes provide a useful measure for distinguishing organizations.

BOA uses a "compliance effectiveness metric," which correlates security training and testing scores, audit findings, actual security breaches and events, and individuals' security behavior to generate a composite score. According to Smith, "The top 300 executives within Bank of America get scored. Those scores are actually reviewed twice a year by the chairman and CEO, as well as the global chief risk officer for the bank, and as one of those executives, about half of your compensation every year is dependent on your score. So, when you tie up half of

Enforcing remediation of security vulnerabilities, especially for partners that are critical to the organization's business, remains difficult.

some of the executive compensation to compliance, people get it."

BOA also uses two high-level, composite metrics to measure *immunity* and *resiliency*. These metrics comprise various measurements captured at different stages of the information life cycle, from when the company obtains the information until it destroys it. The immunity metric comprises 15 different elements, whereas the resiliency metric has 12. Among the things measured for the immunity metric are percentage of total transmissions printed; percentage of data destroyed compared to the total population data; number of monitoring violations; and number of rogue devices or managed devices on the network. For the resiliency metric, BOA measures things like how quickly the security team stopped the spread of a virus outbreak on the network, or whether there was business downtime due to a DoS attack. BOA bases its security metrics on a technique from the US Centers for Disease Control to measure wellness and health. Using these metrics, BOA uses a percentage metric to make a statement about the level of immunity or resiliency in any organizational unit. BOA also has a metric to calculate the cost of a security breach for every account exposed. This cost includes a monitoring cost, identification cost, loss of reputation, and account flight.

Executives and senior-level management need to be aware of, engaged in, and supportive of security issues, strategies, and policies.

Dow Chemical's senior management and audit committee are interested in security in terms of its Committee of Sponsoring Organizations of the Treadway Commission (COSO) elements, so Dow tries to develop metrics around these five elements to evaluate internal controls and create a controlled environment. The five elements are control environment, risk assessment, control activities, information and communication, and monitoring. The company also measures executive support and security awareness levels.

Some of the biggest challenges with security metrics involve linking them to the business—for example, capturing an incident's business cost in terms of revenue loss. Equally challenging is establishing a metric's validity and building metrics that change over time to incorporate changes in the risk environment while remaining comparable to past measurements.

Benchmarking and certification

Benchmarking within an industry and between different sectors can also help ensure that an organization's security is on a par with its peers. Mike Bilger, a partner within IBM's security consulting organization, noted that "Virtually every report we write, our clients want to see [how they compare to] their peers." However, security benchmarks are still relatively immature, and this is an area that deserves additional attention. Particularly, it would be useful to have some reliable benchmark of what percentage of their IT budgets companies are spending on security.

Some firms adhere to International Standards Organization (ISO) standards, such as ISO 17799 for information security management, or standards from other bodies. ISO 17799 certification does provide a basic level of assurance that an organization has implemented some security measures and checks, but nothing more. Security executives viewed security certification in general with skepticism, saying it doesn't always help reduce risk or improve security, although it can help with compliance.

Culture

Organizational culture is particularly important for security, given that an organization's overall security is the result of each individual's actions. But what does a secure culture mean in a global organization? How do you "inculcate" information security? What role do executives take throughout the organization regarding information security?

One pivotal factor in creating a culture of security is setting the right "tone at the top." Executives and senior-level management need to be aware of, engaged in, and supportive of security issues, strategies, and policies that address them. Employees should hear executives talking about security as a core part of the business. With the constantly evolving security landscape, executive education is very important. Eaton's Jack Matejka emphasized this point: "'Tone at the top' […] was a term brought forth with Sarbanes-Oxley as one of the controls. But tone at the top is executive, senior-level management familiar, aware of, [and] sensitive to the different aspects of security. And it's a moving target. We're continuously improving senior management's understanding of what we're faced with in the galleys."

Senior management involvement is essential because many high-level decisions—outsourcing, joint ventures, and so on—have security implications that senior management often doesn't consider. Executives with a good enough understanding of security risks can make informed, risk-based decisions and actually sign off on accepting the risks a decision brings with it. The security organization must help facilitate the risk discussions and develop business solutions. Lowes' Shirley agreed: "There has to be a business alignment. Rather than tell them what security is doing, *show* them a business problem that you're fixing."

To really create a security culture, however, awareness and buy-in have to permeate throughout all organizational levels. A good way to get people to better understand security is to make clear the value of the information being protected and thereby illuminate the risks and consequences associated with losing or compromising that information. IBM's Linda Betz argued, "Certainly a lot of companies end up doing some kind of a buy-in by employees, that these are all the codes of conduct or whatever it means. We call them business-conduct guidelines. But to some extent, how are you pulling folks into understanding that they're responsible, too?"

Dell's Chumbley argued that this is all about helping the organization understand risk:

> "The whole role of the security organization is to drive risk down in an organization. So if we can figure out how to do that effectively, we can actually become strategic enablers for the corporation by allowing them to make business moves that they wouldn't otherwise have been able to make, either because they couldn't understand the risk or they couldn't manage risk, or they couldn't identify the risk. So I think we can almost move into a strategic planning position in that nature. Can we go do this, or is it too risky? How do we manage it? How do we mitigate it?"

Personalizing security issues for employees, including senior management, also helps. Incentives to promote good security behavior are critical. As Jones from Dow Chemical stated, "You have to reward people when they do security well, when they are practicing a safe computing environment. And you have to have consequences when they're not doing it well [. . .] You have to advertise both."

Investment decisions

Security investment decisions require a shared understanding of risks and benefits. Who needs to be involved in information security investments? What funding models have been the most successful?

Spending on regulatory compliance versus discretionary security efforts varies widely from firm to firm and sector to sector. Among the firms we examined, compliance budgets varied extensively from 1 to 2 percent to 10 to 12 percent. This wide range is partially a result of accounting challenges for security spending. Certainly, compliance and the increased involvement of audit functions have highlighted the importance of security and funding for initiatives. Medtronic's Aertz said, "We have a pretty unconventional approach from our audit group. They are willing to stick their toes in the water and offer some money to help us get stuff done." Compliance issues have raised security's visibility within many firms and led to funding increases. However, many security executives worry that in the long term, this might do more harm because it encourages people to adopt an "if we're compliant, we must be secure" attitude. Staples's Dunning argued that an organization's security strategy should provide an acceptable level of risk to support the company's operations and objectives; it shouldn't simply be a reassurance that the organization complies with existing laws and regulations: "The actual security strategy and implementation is in place because it's the right thing to do for this company in support of the day-to-day business that we have."

In some cases, regulations like the Sarbanes-Oxley Act have enabled security groups to implement things they wanted to do anyway, or learn over time to define projects that they were interested in doing in terms of compliance. But as Terri Curran at Bose put it, "Who's driving the bus here? Is security driving regulation, or is regulation driving security? And you'll hear a lot of the comments and the analysts groups tell you that we're ignoring security for the sake of regulation. And I believe that to be true in a lot of companies."

Likewise, security initiatives come from different places within different organizations and get prioritized and funded in different ways. Staples has an annual process for updating its information security strategy. As part of that process, the IT group and different business units within the organization pitch their security requirements to the director of information security. Requirements at the different organizational layers get weighed and rolled into next year's overall information security strategy. For Staples, the annual strategy drives the security initiatives. The biggest challenge isn't really getting money for security initiatives; it's being able to add security people to the organization.

One way some executives fund security is to bundle it with other initiatives, such as company-wide data-site consolidation, which helps improve security while achieving other objectives. Of course, security executives will quickly agree that building security in from the beginning is cheaper and saves time, compared with having to bolt it on later or having to fix things on the fly. As Hewlett-Packard's Sherry Ryan said, "If you don't build it in from the beginning, guess what? It will delay your project, and it will cost more." Raising awareness of this within the organization—better yet, showing past examples of this within the company—helps drive security investments.

Firms vary greatly when it comes to using explicit business cases for new security initiatives. Some firms don't ever demonstrate a return on investment (ROI) for security,[10] whereas others need to do it for all new initiatives. Some organizations are at least starting to view security as part of an opportunity cost rather than competition for it. In other words, security is a necessary prerequisite that any new (or existing) project must consider. Another driver for security investment is demonstrating security as an "enabler" for the business that measurably saves money by preventing negative things from happening. Security will be particularly valued if it can help improve performance and reliability. This approach can take hold if the security group works with other parts of the organization to build security into business strategies and plans.

Organizing for security is clearly an evolving topic of high concern for IT executives within large enterprises. Based on the findings we present here, we believe security executives should address five key imperatives in building security into their organizations:

- Globalization and outsourcing have increased the challenges of securing extended enterprises. Information flow within and between firms is increasing, with more sensitive information migrating to devices at the network edge. Protecting intellectual property in this environment requires a change in security thinking, from a technology to a behavior focus.
- Customers and business partners are demanding greater levels of security. This is a good trend because it moves the security discussion outside information technology groups and into business units. Security groups should be ready to manage this process.
- Security metrics must be more tightly linked to the business and communicated in simple terms. Although traditional scorecard metrics are useful, a few composite metrics shared across organizations will lead to better decision making.
- Investment in security must move from reactive add-ons to proactive initiatives that are aligned with the company's strategic goals. Helping business partners understand risk is the key to developing aligned initiatives.
- Building a secure culture requires a sustained effort to inculcate the organization. Focused education is helpful, but an ongoing discussion around security must come from the top. Middle management might represent the biggest barrier to transforming the organization.

If security executives keep these imperatives in mind, they will be one step closer to truly embedding information security into their organizations. □

Acknowledgments

This work was produced under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College and supported under award number 2003-TK-TX-0003 from the US Department of Homeland Security (DHS), Science and Technology Directorate. Points of view in this document are those of the authors and do not necessarily represent the official position of the DHS, the Science and Technology Directorate, the I3P, or Dartmouth College.

References

1. K. Campbell et al., "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market," *J. Computer Security,* vol. 11, no. 3, 2003, pp. 431–448.
2. A. Acquisti, A. Friedman, and R. Telang, "Is There a Cost to Privacy Breaches? An Event Study," *Proc 5th Workshop on the Economics of Information Security*, 2006; http://weis2006.econinfosec.org/prog.html.
3. M.E. Johnson, "The Safety of Secrets in Extended Enterprises," *Financial Times*, 18 Aug. 2004, p. A7.
4. E. Goetz and M.E. Johnson, *Embedding Information Security Risk Management into the Extended Enterprise*, I3P tech. report, 2006; http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CIO_RiskManage/Overview.pdf.
5. Center for Digital Strategies, "Information Security and Privacy: At Odds with Speed and Collaboration?" *Thought Leadership Summit on Digital Strategies Overview*, Tuck School of Business at Dartmouth, 2004; http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/SecurityAndPrivacy/Overview2.pdf.
6. J. Shore, "Security Summit," *Network World*, 1 Nov 2004; www.networkworld.com/research/2004/110104summit.html.
7. S. Dynes, H. Brechbühl, and M.E. Johnson, "Information Security in the Extended Enterprise: Some Initial Results from a Field Study of an Industrial Firm," *Proc. 4h Workshop on the Economics of Information Security*, 2005; http://infosecon.net/workshop/index.php.
8. M.E. Johnson, "A Broader Context for Information Security," *Financial Times*, 16 Sept. 2005, p. 4.
9. J.M. Juran and F.M. Gryna, *Quality Planning and Analysis*, 4th ed., McGraw-Hill, 2000.
10. L.A. Gordon and M.P. Loeb, "Return on Information Security Investments: Myths vs. Reality," *Strategic Finance*, Nov. 2002, pp. 26–31.

***M. Eric Johnson** is the director of Tuck's Glassmeyer/McNamee Center for Digital Strategies and a professor of operations management at the Tuck School of Business, Dartmouth College. His teaching and research focuses on the impact of information technology on supply-chain management. Johnson has a PhD in engineering from Stanford University. His research articles have appeared in such journals as* Management Science, Communications of the ACM, *and* CIO. *Contact him at m.eric.johnson@dartmouth.edu.*

***Eric Goetz** is the associate director for research at the Institute for Information Infrastructure Protection (I3P) at Dartmouth College. His research interests include understanding information security and critical infrastructure protection vulnerabilities and threats, and developing business and policy solutions to counter security risks. He is a fellow of the American Assembly's Next Generation project. Contact him at egoetz@thei3p.org.*