TUCK SCHOOL OF BUSINESS AT DARTMOUTH
GLASSMEYER/MCNAMEE CENTER FOR DIGITAL STRATEGIES

www.tuck.dartmouth.edu/digitalstrategies

Institute for Information Infrastructure Protection

Embedding Information Security Risk Management into the Extended Enterprise

An Executive Workshop

Embedding Information Security Risk Management into the Extended Enterprise[1]

An Executive Workshop on Developing a Secure Organization
Hosted by the Institute for Information Infrastructure Protection (I3P) and the Tuck School of Business's Center for Digital Strategies, both at Dartmouth College

A Workshop on Developing a Secure Organization recently convened to discuss how companies are embedding information security risk management into the extended enterprise. In today's outsourced enterprises, effective risk management is quickly becoming a source of competitive advantage. The technology community has made much progress in the past five years improving the technical aspects of security. Yet moving the needle on information security is a team activity, requiring participation by everyone in the corporation. The hardest remaining issues involve people and organizations. In this workshop, CISOs[2] from Fortune 500 firms gathered to debate the challenges of organizing for security. The objective was to go beyond understanding best practice to develop an action plan for the next 12-18 months. This workshop included security leaders from 3M, Align Technology, Bank of America, Bose, BP, Cisco Systems, Colgate, Dell, Dow Chemical, Eastman Chemical, Eaton, Hewlett-Packard, IBM, Lowe's, Medtronic, Staples, Time Warner Cable, and the U.S. Army, along with academics from Dartmouth, MIT, RAND, and the University of Virginia.

Key Insights Discussed in this Article:

---

[1] This overview was written by Eric Goetz of the I3P and Professor M. Eric Johnson of the Tuck School of Business at Dartmouth College. The workshop and research were partially supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate.

[2] CISO (Chief Information Security Officer) is common title for the senior information security person in the organization. Not all firms at the workshop use this title for the head of information security.

Organizational Challenges of Embedding Security

Embedding information security risk management into the organization will require a shift in security thinking. One of the motivators for the workshop was the realization that information security has many similarities with the quality movement of 20 years ago. Like quality in the beginning, security seems to be "bolted on" in many organizations, instead of being infused into the organization. Likewise, firms are struggling to determine how to organize and fund security.

This workshop examined how to embed security into the organization, touching on issues of organizational structure and culture; measurement; and investment. Throughout the day, senior security executives debated risk management and security issues. Education, of course, was a principal topic because security is not just a technology problem, but an organizational and cultural one. Metrics and benchmarking within and between industries were targeted as areas where CISOs could help raise the bar for security and quantify successes. Also intriguing was the question of security as a source of competitive advantage for organizations. Clearly, some firms view security as a key element of their overall business strategy.

Workshop chairman Eric Johnson, from the Tuck School, opened the workshop by drawing the quality analogy and asking participants to identify their major organizational challenges. The following are the most pervasive challenges the group currently face:

- *Changing security posture from being reactive to being proactive*. In many organizations awareness of security issues among senior executives is growing, but awareness is often still too reactive. A more proactive stance would help organizations to deal more effectively with emerging problems and compliance issues.

- *Raising the level of understanding within an organization.* Security professionals are working to elevate the level of security education and knowledge within their companies. One of the first hurdles is to reach the point where members of the organization have the awareness to know what security questions to ask and how to find the security services they need. The ultimate objective is to enable the business units to share in information security risk management. Eastman Chemical's Phillip Shupe 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."

- *Changing behavior*. As security is about people as well as technology, many organizations are struggling with changing how employees and partners view security issues. Raising awareness of security problems and good security practices would go a long way to protecting organizations and their vital assets. As Theresa Jones from the Dow Chemical Company 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."

- *Dealing with globalization.* A growing challenge is establishing and maintaining a strong security program that reaches across the globe. Even in organizations where the security group has implemented a strong core security program, it is still a challenge to get business units around the world to take ownership of their security risks. This includes protecting key applications that really run a business, but are outside the core infrastructure. As Staples' 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 intellectual property, data*. One of the most frequently cited challenges was the difficulty of protecting an organization's intellectual property and data, particularly in global organizations where information resides with multiple divisions and partners. The use of new technologies, including ubiquitous mobile devices, and collaborative cultures within organizations make protecting information an even greater challenge, especially as it can be difficult to assess when intellectual property is being lost. Eaton's Jack Matejka's worries extend beyond protecting property to facilitating its application, "not only to protect it, the intellectual property itself, but also to build, stronger, more secure, more highly reliable products." A key component to protecting information is the need to protect customer and employee privacy as well. Nancy Wilson of 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."

- *Not just delivering security technologies.* The changing role of security groups is both a welcome opportunity and a challenge. Security used to be more about providing other business groups with the latest security technologies and solutions; security groups are now increasingly asked to provide governance, policy development, and consultancy type functions. Dartmouth's Martin Wybourne emphasized that his biggest challenge was "moving from being technology driven to risk management driven."

- *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 grows, or as an organization expands its operations to new countries or markets, it becomes difficult to maintain a consistently high level of security. An added challenge is when expansion includes acquisitions or opening up systems to external partners. Steve McOwen from Cisco Systems 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."

- *Meeting compliance with laws, regulations, and standards.* Many organizations find staying 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), a significant challenge. For international organizations, compliance with laws and regulations in all countries of operation is another added challenge.

- *Responding to cuts or changes to the security budget.* In firms within industries where security problems have not landed on the front page of the business papers, some participants were struggling with security budget cuts—having to do more with less. Limited resources are a problem for large and small companies because there is an abundance of threats, but only limited resources and manpower to deal with them.

Business Drivers for Security

A senior executive panel, made up of Brad Boston, SVP and CIO of Cisco Systems Inc., Steven Boutelle, LTG and CIO of the U.S. Army, and Doug Smith, Executive for Corporate Information Security and Business Continuity at Bank of America, discussed what drives security in their organizations. The panel, moderated by John Gallant, Editorial Director and President of *Network World*, also focused on how security can be embedded into organizations; how security issues can best be communicated to senior executives; whether security is becoming part of business strategy, or remains an 'add-on'; what organizational barriers still exist that stifle security improvements; and how different groups within an organization interact to arrive at a rational risk management process.

Gallant opened the discussion by noting, "At *Network World* we survey our senior IT readers many times throughout the year, and interestingly, security has always been the top concern. But what's changed over the past three or four years is that security has become the very active concern. Before, it was sort of—yeah, I think I need to say security is a top concern. Now people are really worried about it."

"You don't know what you don't know." Protecting against new threats. At the same time that business, government, and military operations are becoming ever-more networked and reliant on IT, cyber threats are increasing. According to the Army's Steven Boutelle, "this is probably the first time in the history of man that we've seen our threat to the nation, to the corporate world, to industry, and obviously the military, move from physical space to cyber space." With terrorist groups increasingly using information tools, foreign governments engaging in large-scale espionage, and criminal syndicates setting up professional cybercrime operations, organizations are faced with a new generation of threats. These new threats are difficult to detect, and it is near impossible to determine the long-term consequences of some attacks. It is hard to plan and resource for threats that are difficult to define. Bank of America's Doug Smith reminded the group that there are many old risks that simply seem to grow: "I worry about paper. I mean, Bank of America spends almost a billion dollars a year on copier paper. Now I don't know about you, but to me that is a huge risk."

***Balancing collaboration and risk*.** Organizations use information systems to collaborate and share information. Innovative companies build value through new online processes and transactions, and the free exchange of ideas. At the same time, intellectual property—the information that increasingly makes up the bulk of the value of a company—needs to be protected and business risks minimized. Strong identity management can help control who gains access to information and with what permissions. This becomes both a policy and a technology challenge, as security policies also need to be realistic and enforceable. Cisco's Boston noted that many strict security polices are not enforceable: "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?"

***Protecting reputation*.** In an era where stories abound of companies losing customer information and hackers making off with databases and back-up tapes, preventing a loss of company reputation has become an important driver for security for many organizations. Preventing high-profile security breaches has become particularly crucial for organizations that market themselves as security companies, or that strongly rely on customer trust.

Cisco's Boston remarked, "We have become a security company. And the worst thing that can happen to a security company is for you to have a big security breach in a very public way. And when

[Cisco CEO] John Chambers made that strategic decision a few years ago at his planning meeting, I made it clear that the entire organization was going to have to really understand their role in helping us with executing security. Because the whole business proposition goes down if we have a major, major security violation."

Getting management involved. The panel all felt that they had buy-in for security from their senior management, and that senior management generally understood security issues. Bank of America's Smith underlined the importance of top-management support. "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 many cases, senior management isn't the biggest hindrance to better security. Boutelle pointed out that 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." What the U.S. Army and various large businesses are doing is providing training and awareness courses for senior and mid-level managers to better understand current threats and possible consequences of not securing systems and data. This should help mid-level managers make more informed decisions when it comes to balancing the need for maintaining operational efficiencies and providing security. Part of raising security awareness also involves personalizing security risks for managers, showing them how vulnerabilities could affect them as individuals. For example, showing a manager in the banking sector that her personal data (including credit card information and personal details) can be found on an internet chat room really drives home the need to protect customer data.

Boutelle argued that one of the greatest barriers is a generational disconnect: the difference between the "digital natives," people who grew up with computers and IT, and who often have an inherent understanding of IT security issues, and the "digital immigrants," the people who grew up before computers were a common household appliance, and who often find it harder to understand the impact of these issues. As time goes by, more and more "digital natives" will reach mid-level management positions, hopefully improving the situation.

Measuring improvements in security education and awareness. Many organizations have ongoing security education and awareness programs, but how do they measure whether these programs are effective? The panelists suggested several methods to check effectiveness. One technique is to monitor whether the programs actually lead to improved security practices. For instance, Cisco has developed tools that warn employees that what they are about to do may be bad from a security standpoint; the employee then gets to choose whether to proceed or not. Another option is to monitor security violations and publicize these violations within the company. This can have the effect of further raising security awareness by offering real-world examples of what can go wrong. The public embarrassment of the offender can also act as a good deterrent to others in the company.

The U.S. Army takes a similar approach of measuring the effectiveness of education, continuing to explain and demonstrate the reasons for security policies, while taking action against serious violations. For instance, soldiers used to post potentially dangerous digital pictures or classified information (e.g., showing their defensive installations) on their websites or blogs. The Army now monitors these sites and keeps track of detailed statistics by quarter. They also provide training to recruits on why posting such information endangers troops.

At BOA there are different types of mandatory security training courses for everyone in the organization. Employees are tested on the training they take and monitoring tools are used to check compliance with security policies. In addition, BOA also uses a "compliance effectiveness metric", which correlates security training and testing scores, audit findings, actual security breaches and

events, and security behavior of individuals, to come up with 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 some of the executive compensation to compliance, people get it."

***Listening to customer demands for greater security*.** Customers are increasingly asking their potential partners questions about their levels of security. In many cases, potential business partners are asked to conduct vulnerability assessments on their systems, or have to verify that they adhere to certain industry best practices or standards. In fact, with regards to requests for quotes in BOA's treasury business for treasury cash management services, questions are more frequently asked about information security and business continuity than about pricing or availability; security issues are also weighted higher in scoring mechanisms, clearly showing the growing importance of security for customers, especially in certain sectors like finance.

As more and more businesses provide services via the internet, consumer confidence in e-commerce and electronic transactions has become an important issue. As media reports of security breaches multiply, customer confidence in electronic transactions may be waning. For organizations that have embraced e-commerce as part of their business model, customers' anxieties about cyber security should act as a strong driver for better security. However, a real difficulty is not knowing what the consequences of a security breach would be for an organization. For instance, what really happens if a company exposes the private information of 100,000 customers? How many of them would move their business to a competitor? More information on quantifying such consequences could help make the case for stronger security.

***Empowering the security group*.** As Fortune 500 companies, particularly its senior management, raise security awareness throughout the organizations, and as customers start to demand better security, this shift in emphasis—viewing security as a critical business function—provides the security group with greater authority to enforce security measures. This can go so far as to give the security group "veto" power over decisions that are associated with excessive risk, even if this means pushing back the launch date of a new product or service. A pivotal part of empowering the security group is understanding one's own organization. If the security group can help match operational security risks with business objectives, they can show how security measures really protect the "jewels of the kingdom".

***Sharing ownership of security*.** Members of the panel agreed that, in order to really raise the level of security throughout the organization, the various business units of the organization need to take ownership of security in their area. One good way to do this is to have line managers take personal responsibility for security, and involve company auditors to help enforce security levels. Involving auditors in the process 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, rather than having it bolted on at the end.

Cisco's 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 be more aware and own security for their employees, and 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 dumb, or did something really bad, you got a different level fine, *and* there's a financial penalty that the offender's manager had to pay. So they made the managers pay the fines to incent them to go and talk to the people about not violating the rules."

***Guarding against short-sighted legislation*.** In an environment where cyber security issues are in the mainstream of public consciousness, lawmakers increasingly feel obliged to regulate on issues like protecting user information, phishing, authentication, etc. Many of these issues are highly complex, contextual, change rapidly over time, or are independent of specific technologies. Unfortunately, in some cases, members of Congress are proposing bills (and members of the Congressional staff are influencing legislation) on complex issues that have not been fully explored. This can lead to legislation and regulations that are short-sighted or counterproductive.

Doug Smith provided an example, "In October of 2005, the FFIEC, which is a group of federal regulators … issued guidance on authentication for internet-based applications and phone-based applications for financial services companies. And they did it with the intent to stop phishing and identity theft. And the guidelines, the guidance itself, does nothing to stop phishing or identity theft, yet financial institutions, who are already well on their way in implementing multi-layer, multi-tier authentication capabilities, now have to stop and go back and review everything they've done. And we have a deadline at the end of this year to do that. At Bank of America, we have 419 internet-based applications. We have 30 different IBR systems that customers can dial into. And so you can imagine the huge shift in resources and investments that we had to make to be able to cover that guidance, [but] that really does nothing at the end of the day to stop phishing or stop identity theft."

Organizing for Security

In a moderated roundtable format, participants explained how their security organizations were structured, how they were funded, and who they had reporting or other relationships with. The group focused on the following issues: What are the biggest security concerns for the next 12-18 months? How are these concerns reflected in current or planned security organizations? What elements of organizational structure really matter: reporting relationships, sponsorship, funding, or responsibility (governance vs. deployment)? How are business risks stemming from partner organizations managed?

***Organizational structure and funding*.** While the structure of security organizations varied substantially, there were some key similarities between many of the companies represented.

In many cases, security organizations are themselves divided into different units, dealing with things like information security, strategic risk and risk management, business continuity, operational security, network operations, infrastructure, architecture and engineering, policy development, etc. Reporting relationships also vary somewhat between organizations. Most of the security executives report (directly or indirectly) to the CIO of the organization, while some report to executive committees of the company's CEO, or the company's general counsel (see Appendix for examples of organizational structure).

There are usually also some reporting relationships to various committees (or councils or task forces), including audit committees, board committees, risk committees, compliance committees, or technology steering committees, and other business units or departments like the corporate security department. In some cases, a chief risk officer or a chief technology officer is also in the mix. For global organizations some kind of geographic or regional structure of responsibility may also exist for security. Some security organizations also liaise with other company departments like HR, legal, risk management, and physical security on issues like policy development and compliance. In other cases, some of what could be considered security functions, such as privacy, ethics, compliance, policies or strategy, are housed outside the security organization.

Funding streams for the security organization also vary, but, for most participants, funding is ultimately controlled and approved by the organization's CIO. If the security organization reports to the head of an operational unit or other senior executive, that person (or persons) may control the budget as well. In cases where operational security functions (i.e., protecting the organization's infrastructure against viruses, denial of service attacks, etc.) are separated from more strategic or compliance-related security functions, funding may also come from, and be controlled by, several different sources. A few participants noted that funding for specific security projects may be provided by individual business units, and in one case, the audit group had funds available for security.

Change is good. For a large majority of the organizations represented, the organizational structure of the security group is in flux and seems to be subject to frequent change. For more than half of the participants, their reporting relationship (i.e., the box—not the individual person—within the organization that they report to) had changed within the past year. A significant number have experienced changes in their reporting relationships within the past six months. Only a few organizations have not had any structural or personnel changes in their reporting relationships within the past year. For almost every organization represented, the internal structure of the security organization had also changed within the past year, clearly showing that restructuring of 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, the external risk environment, as well as needing to comply with new regulations. In some instances, structural changes have been driven more by operational and tactical imperatives, rather than strategic shifts. In other cases, restructuring was done to centralize responsibility for IT security; in the words of 3M's Donna McJunkin: "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? The group felt that it is difficult to pinpoint structural best practices because the security landscape continues to change so rapidly that further structural changes are likely in the coming years in order to keep the security organization aligned with other changes in the business or the external environment.

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. But we've had business incidents that are putting more focus on monitoring and vulnerability assessments and things that we used to, and the 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 also."

The general sentiment seemed to be that it is 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, and sure everybody thinks their company is unique and reorganized all the time, but 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, *and* who understand how to explain the risk-reward trade-off *and* can sell solutions within the organizations are difficult to find. "I've been seeking to hire an information security manager," said Align Technology's Jim McMahon. "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 meet a virus head-to-head with sword in hand, [but] who couldn't sell me a piece of cake if I was starving." Echoed Bose's Terri Curran, "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 reducing unplanned turnover is a critical organizational issue for security. As John Stewart from Cisco Systems 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% 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."

Managing security beyond the borders of a corporation remains a very tough issue for most firms. The extended enterprise, including customers and external partners, poses many risks. Although many firms have staff in place specifically responsible for managing external business partnerships, the resources are stretched very thin. One problem is that the pace of business is so rapid. Companies often make business decisions about partnerships without prior consultation with the security group concerning possible risks introduced through that partnership. Then, the security groups have to react, but, in the words of Bill Aertz from Medtronic Corporation, "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, best practices, or allow the organization to periodically test the partner's security. However, actually enforcing mediation of security vulnerabilities, especially for partners that are critical to the organization's business, remains difficult. To enforce remediation of a partner's vulnerabilities, 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 a totally 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 been doing business for years. In these cases, partners can sometimes feel resentment when asked about their security arrangements.

Transforming the Organization

Measurement—risk and security. Metrics are a management fundamental, but when it comes to security, there are many open questions: 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? What types of metrics should CISOs champion?

Many companies are using checklists (generally comprised of binary questions, i.e., yes-or-no type) and/or scorecards to keep track of security. Scorecards measure things like IT operations, system architectures, security measures, and compliance. Scorecards can provide insight into what effects changes to architectures, configurations, and settings can have on security. Scorecards can be used at various facilities to check whether a list of security measures has been implemented or not (e.g., has a certain patch been installed on all the machines in this environment? Is the anti-virus up-to-date on all the desktops?), how many vulnerabilities exist in certain systems, or how many attacks an organization is facing (e.g., the number of hits on the external IDS). One problem with scorecards, and many other metrics for that matter, is that they may often provide some kind of percentage score, but it is 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 levels of security. These can contain a variety of elements depending on the type of organization, the business sector, and the goals of the organization. Composite metrics aim to provide risk scores so that different groups within the organization can set security targets and help identify levels of acceptable risk. This helps senior management get a sense of 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% because of the cost.… I think that's a good way to talk about managing risk right there." Tuck's Johnson pointed out that "good metrics exhibit variability. If everyone gets the same score (pass), there is no room for improvement."

Composite metrics that have many different components and that result in a wide range of outcomes provide a useful measure to distinguish organizations.

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 of IBM noted, "Virtually every report we write our clients want to see [how they compare to] their peers. Not by name, but how do we compare to peers in our industry?" However, security benchmarks are still relatively immature and this is an area that is worth additional attention. Particularly some form of reliable benchmark of what percentage of their IT budgets companies are spending on security would be useful.

Some participants' firms adhere to International Standards Organization (ISO) standards, such as ISO 17799 for information security management, or standards from other bodies. But the general feeling was that ISO 17799 certification provides a basic level of assurance that an organization has implemented some security measures and checks, but nothing more. Security certification in general was viewed with skepticism as not always helping to actually reduce risk or improve security, although it can help in the area of compliance.

IBM uses metrics to see specifically if the company has reduced security risks. IBM-developed tools, such as GSRisk, analyze risks and threats to the company. This analysis is then mapped against security investments from the previous year to show whether the investments led to a tangible reduction of risk. IBM also uses a risk tool and process to measure the potential severity of pending situations. This tool takes into consideration things like probability of occurrence, visibility impact, and rates, pending situations along a scale of Alpha (business as usual) to Delta (extremely serious event). IBM also has a dashboard that has five security elements, but also includes compliance, financial, and general IT elements.

Cisco measures the effectiveness of its security awareness program by checking if people know about the awareness program and are applying the knowledge gained as expected. In fact, whether someone has taken the awareness training now affects their bonus. Another example of measurement at Cisco

was the development of a business case on displacing work in certain technology centers. The company made an investment to free up the IT team from having to clean up "janitorial messes of worms, viruses", etc. This freed up so much of their time that the investment provided a return in just nine months, much sooner than had been anticipated. The Cisco security group also measures customer satisfaction among the people within the company for whom they provide services, with that customer satisfaction rating affecting the engineer's bonus. This helps the security group to better understand that even if they have to say 'no' to something, they need to explain the reasons why.

Bank of America has two high-level, composite metrics to measure immunity and resiliency. These metrics are made of a variety of measurements captured at various stages of the information lifecycle, from when the information is obtained until it is destroyed. The immunity metric is made up of 15 different elements, while the resiliency metric has 12 elements. Among the things being measured for the immunity metric are percentage of total transmissions being printed; percentage of data destroyed compared to the total population data; how many monitoring violations were there; how many rogue devices or managed devices are there on the network; is the patch remediation process being executed effectively, etc. For the resiliency metric, BOA measures things like how quickly was the spread of a virus outbreak on the network stopped, or was there business downtime due to a denial of service attack? BOA based its security metrics on a technique used by the Center 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 unit of the organization. BOA also has a metric to calculate the cost of a security breach for every account exposed. This cost is made up of elements including a monitoring cost, identification cost, loss of reputation and account flight.

As senior management and the audit committee are interested in security in terms of the COSO elements, Dow Chemical tries to develop metrics to fit within the framework. Dow builds its security metrics around the five Committee of Sponsoring Organizations of the Treadway Commission (COSO) elements for evaluating internal controls with the goal of creating a controlled environment. The five elements of COSO are: control environment; risk assessment; control activities; information and communication; and monitoring. The company also measures the level of executive support and awareness of security.

Hewlett-Packard collects data on the response and clean-up costs for every security incident by using labor rate costs, which are updated annually. The costs of these incidents are reported monthly on security scorecards and tracked over time to see if costs go down. Cisco is doing something similar, monitoring the personnel costs to clean up after very severe incidents.

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

Culture. Organizational culture is particularly important for security, as 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 is the role of executives 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 within an organization need to be aware of, engaged in, and supportive of security issues and strategies and policies to address them. Executives should be heard 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, 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 within the galleys."

Senior management involvement is essential because many high-level decisions—outsourcing, joint ventures, etc.—have security implications that often aren't considered. Executives with a good enough understanding of security risks can make informed, risk-based decisions, and actually sign off on accepting the security risk that a decision brings with it. The security organization must help facilitate the risk discussions and help develop business solutions. IBM's Moore noted, "I was just emphasizing the importance of the solution because all too often security is known as the 'no shop'." Lowe's 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 through all the levels of the organization. A good way to get people to better understand security is to make clear to them the value of the information that is being protected, and thereby the risk and consequences associated with losing or having the information compromised. IBM's Linda Betz argued, "I mean, 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?"

The way security issues are communicated is also crucial. Security needs to become a part of the discourse of an organization, part of the organization's core values and business processes, so that people understand that "double-clicking on Britney Spears" can have consequences for them and the organization in the same way that "carry[ing] an open gallon container of sulfuric acid" would not be a good idea. Part of this may be to "piggy-back" security on something for which a strong corporate culture already exists at an organization, such as safety, customer trust, etc. However, companies should recognize that creating a secure culture also requires making a clear commitment to security—providing additional resources, taking into consideration certain inconveniences, or simply revising existing business processes and practices. In the words of Neil Hershfield from Dow Chemical, companies need to be "willing to take on what it's going to take to be secure."

Another aspect of creating a secure culture is giving employees tools to help them implement security. For instance, one company has developed workstation security tools that highlight vulnerabilities on individual users' workstations and provide information on how to fix a problem. Using such tools prevents well-meaning employees from having to become security experts. An organization reaches the desired state of a secure culture when security has become part of its everyday business practices.

Personalizing security issues for employees, including senior management, can also help build a secure culture. Incentives, a system of rewards and punishments to promote good security behavior, are critical. Dow Chemical's Theresa Jones said: "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. And you have to advertise. You have to advertise both." However, RAND's Shari Pfleeger noted, that rewards themselves depend on the corporate culture, "Some corporate cultures prefer giving you recognition by your peers to giving you money. And in cultures like that, you have an all-hands meeting and you give somebody a security award."

On the punitive side, it is difficult for some companies to explicitly say that a certain person was fired for information security violations. However, this kind of information usually travels through the organization unofficially, or a company can mention aggregated data on terminations due to security violations as part of its awareness training. The company could also re-send its security policy to employees on the same day that certain people are fired without explaining the reasons for the dismissals. On the positive side, companies can give out and announce security awards or other types of rewards for good security behavior. Security successes could be highlighted in company newsletters or on an organization's website. At BOA, half of an executive's bonus is tied to their security performance—this is another good way to penalize poor security and reward good security, while clearly incorporating security into the organizational culture.

Using examples of publicized security breaches at other organizations in formal security awareness training and as part of the less formal company discourse can bring home the reality of security risks to management and employees. Getting part of the security message into training that is provided by other departments, such as HR training, or training by the engineering group or the ethics department, can also help make security a mainstream company issue and embed it firmly within the corporate culture. Security training should be regular or ongoing, not just a one-time thing. One company is using a behavioral-based performance process—having peers observe the behavior of their colleagues in the work environment—to observe actions from a safe computing perspective. Tuck's Hans Brechbühl noted that the ultimate indicator of a secure culture is "when it's essentially happening naturally; it's kind of a part of everybody's business practices. It's a part of what they do."

A major hurdle to creating a single, unified culture around security is that we are in an age of global corporations, outsourcing, mergers and acquisitions and networks of partnerships. A company might have a presence in a country or region that has no history of information security awareness, or the company is working with a partner that is wholly uninterested or unaware of the imperative of good security. Even harder may be changing an existing corporate culture to embrace security in the case of an acquisition. In any case, an organization needs to be patient when building a corporate culture as creating a significant impact can take years.

Investment Decisions. Security investment decisions require a shared understanding of the risks and benefits. Who needs to be involved in information security investments? What funding models have been most successful? What drives investment—business case, compliance, or fear? Tuck's Scott Dynes asked, "If there were no laws, do you think we would have the same security spending?"

Security spending on regulatory compliance versus discretionary security efforts varies widely from firm to firm and sector to sector. Among the participants, compliance budgets varied extensively from 1-2% to 10-12%. Certainly compliance and the increased involvement of audit functions have highlighted the importance of security and funding for initiatives. Medtronic's Aertz noted, "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 the visibility of security within many firms and led to funding increases. However, many participants worried that, in the long term, this may be doing more harm than good as it can encourage attitudes such as 'if we're compliant, we must be secure'. Chris Dunning of Staples 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 is in compliance 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 allowed the security group to implement things that they wanted to do anyway, because they were required under the regulation, or the security group learned over time to define projects that they are interested in doing in terms of compliance. But as Terri Curran of 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—I really do."

Likewise, security initiatives come from many different places within different organizations, and get prioritized and funded in different ways. Staples has an annual process to update the strategy for information security. As part of that process, IT and business owners of security within the organization pitch their security requirements to the director of information security. All of these requirements at the different layers of the organizations get weighed up and rolled into the overall information security strategy for the coming year. For Staples, the annual strategy drives all the new security initiatives. The biggest challenge isn't really getting money for security initiatives, it's being able to add security people to the organization.

At Cisco, the security group pushes some security products and initiatives itself. Being a technology company that develops some security products, this probably happens more often at Cisco than in other organizations. For other security initiatives, business units approach the security group with services they want provided, such as digital certificates. In other cases, business units request applications or other types of functionality through the IT department, but the security group gets involved whenever the functionality or service has security implications. What initiatives ultimately get funded depends on measurements of how security is doing in certain areas, as well as on the current risk environment.

In general, the current risk and threat environment plays a major part in getting funding for new security initiatives. New initiatives will often be approved by senior management if it can be shown that they mitigate risks or current threats, such as spyware or the loss of intellectual property. Security groups are also starting to work with internal auditors and risk management groups to articulate high-level threats to the business in a type of integrated risk/threat assessment. One company examines extreme risks (which could be cyber or not)—risks that could affect the bottom line of the company by a billion dollars during a year—and develops security initiatives to counter those. However, with this approach high-profile, visible events like the latest worm sometimes receive more attention than other less obvious threats, such as insiders.

For a growing number of firms, there has been progress in moving security from an add-on to an integral part of the business. For some firms, security has become viewed as a value-adding component of their business, a selling point that gives the company an edge over competitors (e.g., the company has the ability to protect its customers' intellectual property).

Barry Horowitz of the University of Virgina observed that many firms package "security on top of other initiatives as a way to get something done." Several participants agreed, mentioning that they have been successful in building in security from the outset for new, big company initiatives and projects, such as company-wide data-site consolidation or offshoring development work to China. There was a consensus that building security in from the beginning is actually 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 quipped, "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.

In other companies, security is at least starting to be viewed as part of the opportunity cost, not as competing with opportunity cost. Or, in other words, security is a necessary prerequisite that has to be taken into consideration for any new (or existing) project. Another driver of 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 is working with other parts of the organization to build security into business strategies and plans.

Participants varied on whether they needed to make an explicit business case for new security initiatives. Some participants don't need to demonstrate a return of investment (ROI) for security, while others need to do it for all new initiatives. Mostly, existing security initiatives are considered as "flow through" and don't require a new ROI calculation every year.

One problem that was raised was the issue of security as the "bottomless pit". The security group is sometimes viewed as insatiable, as asking for money year after year, and often for intangible things that may or may not happen. Senior management could be tempted to ask, "how much is enough?" In a situation like that, how do you measure progress? A good approach to counter this mindset may be to be able to tell stories about, and provide evidence of, security success where the security group prevented an attack and saved the company from costs or other negative impacts.

Conclusion—Imperatives to Building a Secure Organization

At the end of the workshop, the group ranked the top security imperatives based on the discussion and listed the following as the most important imperatives for CISOs for the next 12-18 months:

Metrics:

- Develop composite metrics that are simple to understand and clearly linked to the business.
- Increase benchmarking activities both within and across industries.

Investment:

- Align information security initiatives with the company's strategic goals.
- Help business partners understand the risk and business case for security as an integrated part of the extended enterprise.

Culture:

- Inculcate information security into the DNA of the organization.
- Develop and find security talent that can understand the business and communicate the business case for security.

Of the imperatives, metrics was the clear winner among workshop participants. Reflecting on the list, Eastman's Shupe summarized the comments expressed by many participants, "The trump card is proactive metrics—aligned with the company's strategic goals."

Panelists, Participants, and Research Team
Executive Workshop on Developing a Secure Organization
March 1, 2006

Bill Aerts	Director of Information Protection Medtronic Corporation
Linda Betz	Director, IT Policy & Information Security Global Infrastructure IBM
Mike Bilger	Director, Security and Privacy Services IBM Corporation
Brad Boston	SVP & CIO Cisco Systems, Inc.
Steven W. Boutelle	Lieutenant General Chief Information Officer/G-6 Office of the Secretary of the Army U.S. Army
Hans Brechbühl	Executive Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Jeff Chumbley	Director, Global Information Security & Compliance Dell
Terri Curran	Director, Corporate Information Security Services Bose Corporation
Chris Dunning	Director IS Enterprise Information Security Officer Staples Incorporated
Scott Dynes	Senior Research Fellow Center for Digital Strategies Tuck School of Business, Dartmouth College
John Gallant (moderator)	Editorial Director & President Network World
Eric Goetz	Assistant Director, Research and Analysis I3P, Dartmouth College
Ian Henderson	Security Advisor BP p.l.c.

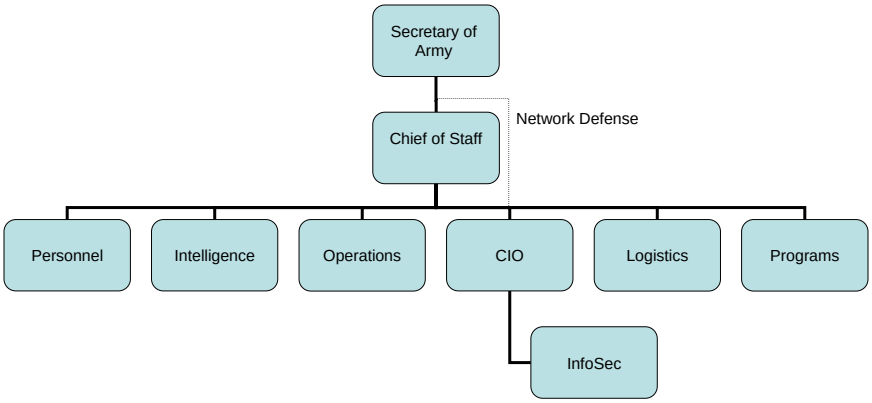
Neil Hershfield	Director, Chemical Sector Cyber Security Program The Dow Chemical Company
Barry M. Horowitz	Professor of Systems and Information Engineering University of Virginia
M. Eric Johnson	Professor of Operations Management Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Theresa Jones	Director of Information Security, Compliance, & Risk Management The Dow Chemical Company
Dave Margulius	Analyst and Founder Enterprise Insight
Jack Matejka	Director, IT Security Eaton Corporation
Donna McJunkin	Manager IT Security and Integrity 3M Corporation
Jim McMahon	Senior Director, Chief Security Officer Align Technology, Inc.
Steve McOwen	Senior Manager, Audit, Incident Response and Security Services Cisco Systems, Inc.
Jeff Mitchell	Director of IT Security & Architecture Lowe's
John Moore	Director, Business Continuity, Disaster Recovery, and Security IBM
Andy Ozment	Researcher MIT Lincoln Laboratory
Shari Lawrence Pfleeger	Senior Information Scientist RAND Corporation
Rich Quinney	Manager of Communication Services The Pep Boys
Sherry Ryan	Chief Information Security Officer Hewlett-Packard

Steve Shirley	VP of IT Security & Strategy Lowe's
Phillip D. Shupe	Manager, Systems Integrity & Administration Eastman Chemical Company
Doug Smith	Corporate Information Security and Business Continuity Executive Bank of America
John Stewart	VP and Chief Security Officer Corporate Security Programs Organization Cisco Systems, Inc.
Terri Tuya	Director, Information Risk Management Global Information Technology Colgate-Palmolive
Sondra Walker	Associate Director I3P, Dartmouth College
Nancy Wilson	Director, Enterprise Information Security Time Warner Cable Corporate
Martin Wybourne	Vice Provost for Research I3P, Dartmouth College

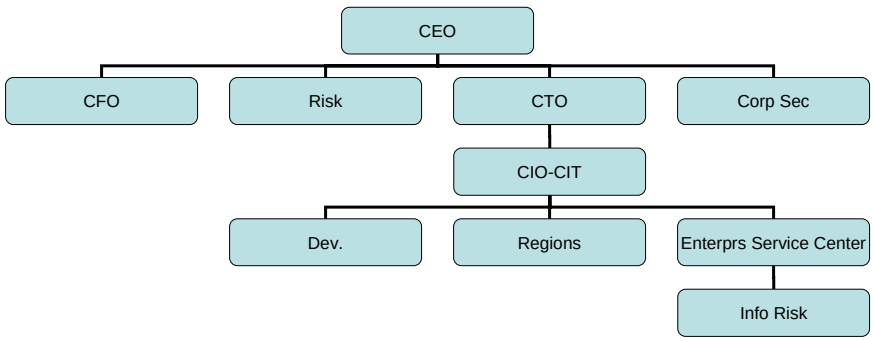
APPENDIX

Examples of organizational structure

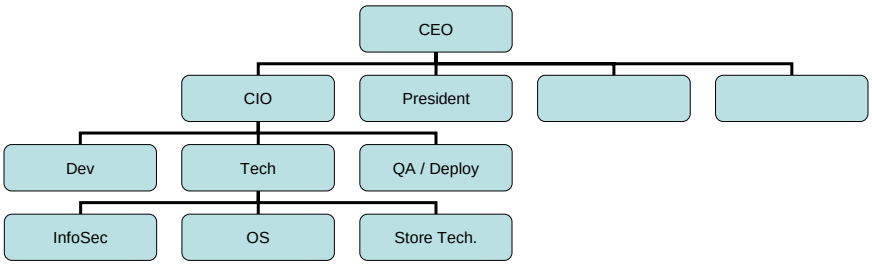
US Army



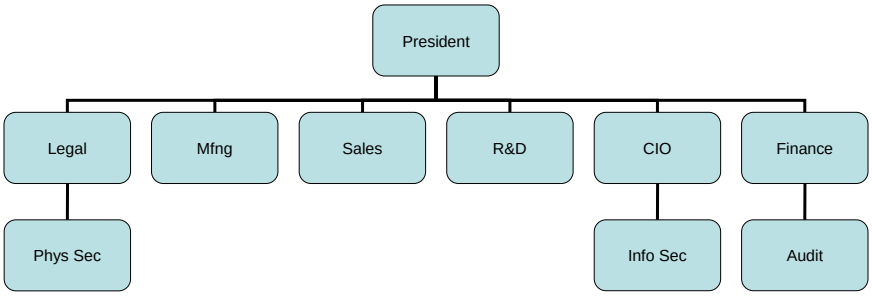
Unreported



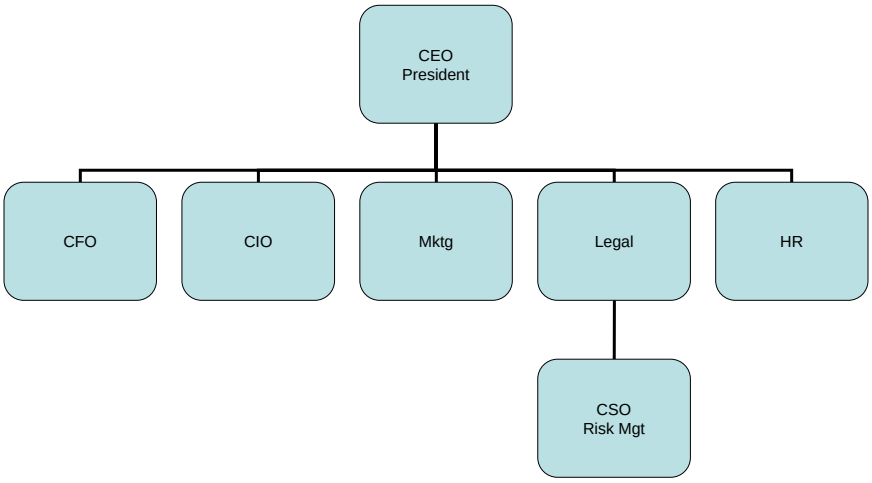
Retail



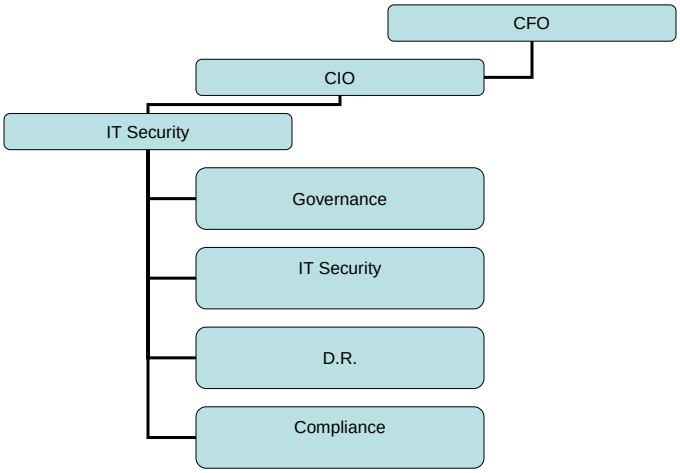
Audio and Video Manufacturing



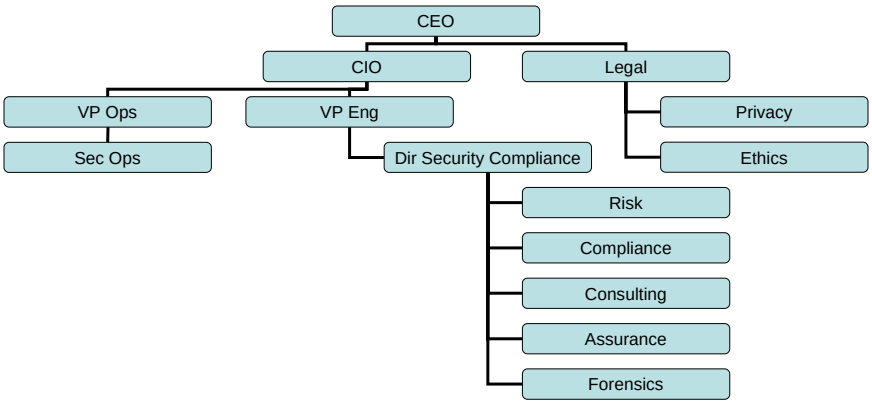
Unreported



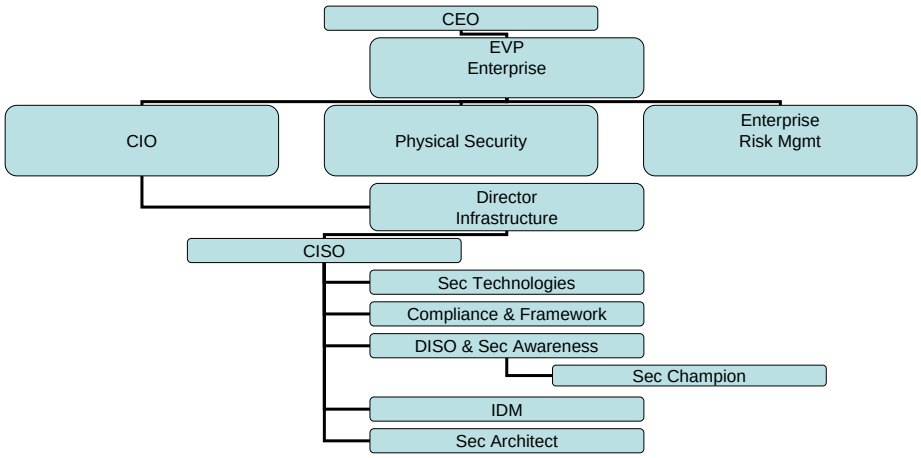
Unreported



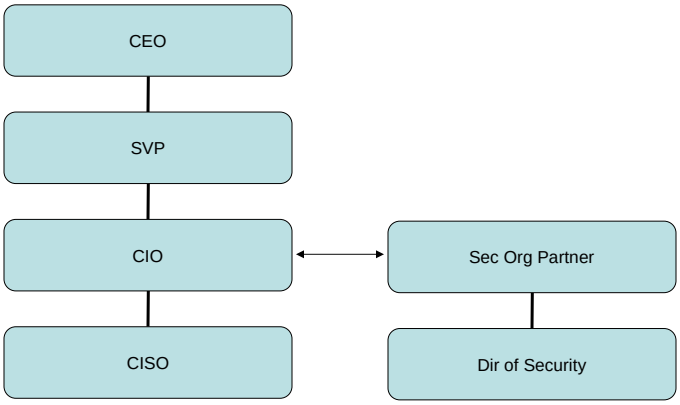
Computer and Electronic Manufacturing



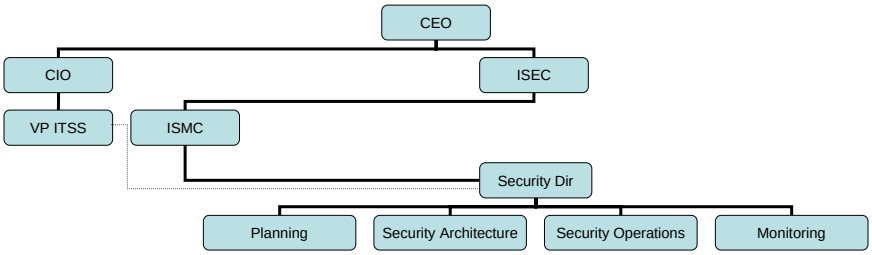
Plastics Manufacturing



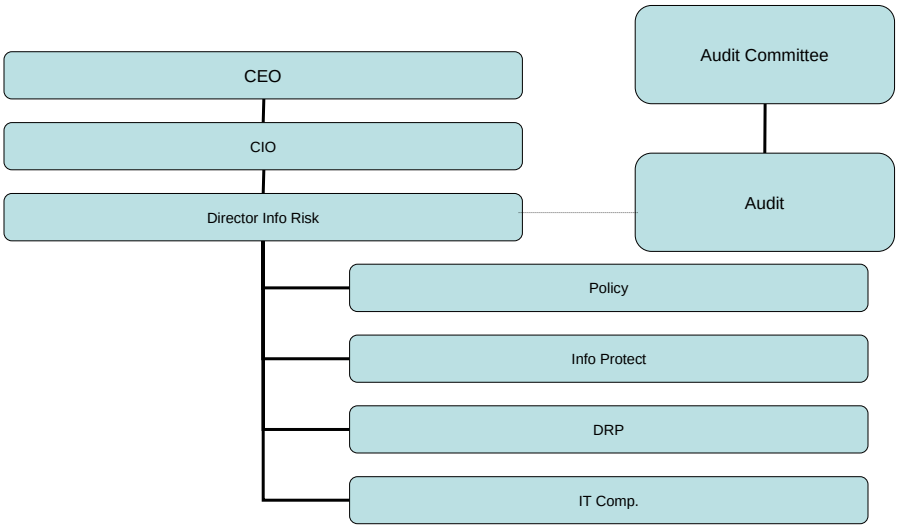
Unreported



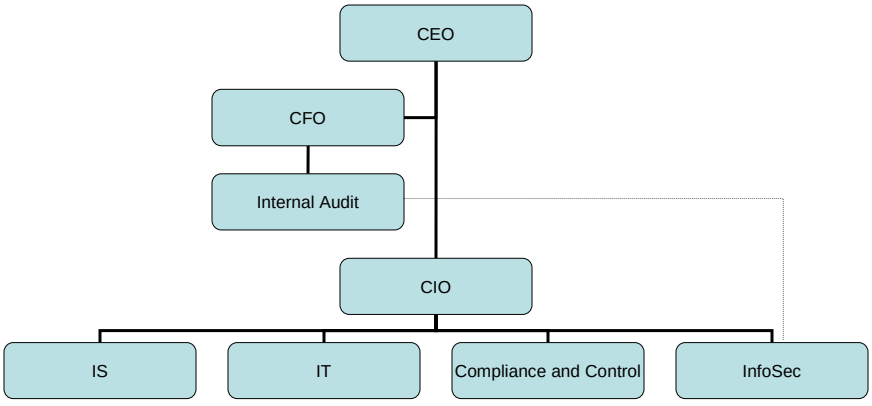
Retail



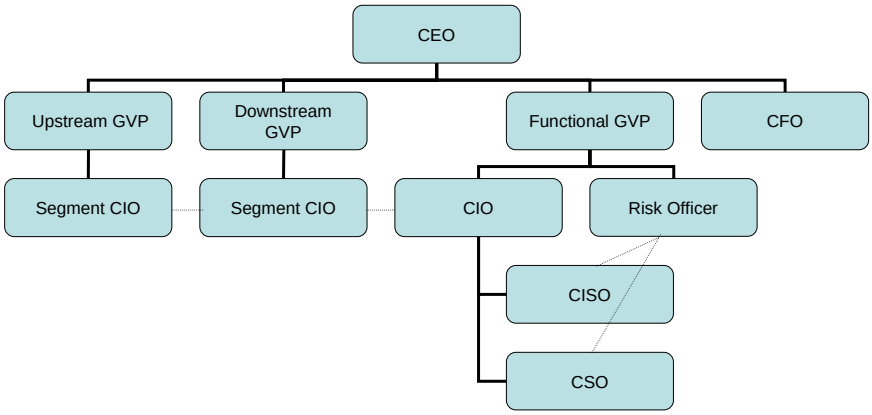
Electromedical Manufacturing



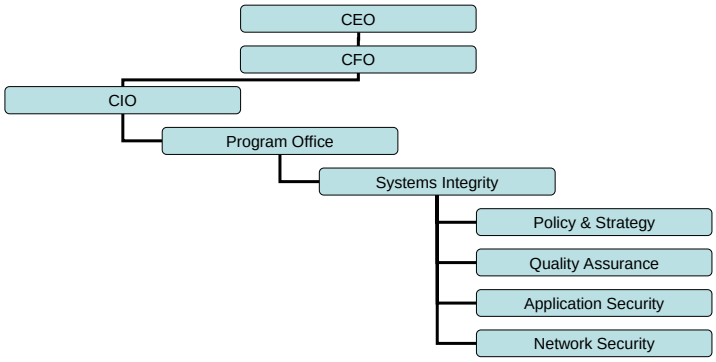
Retail



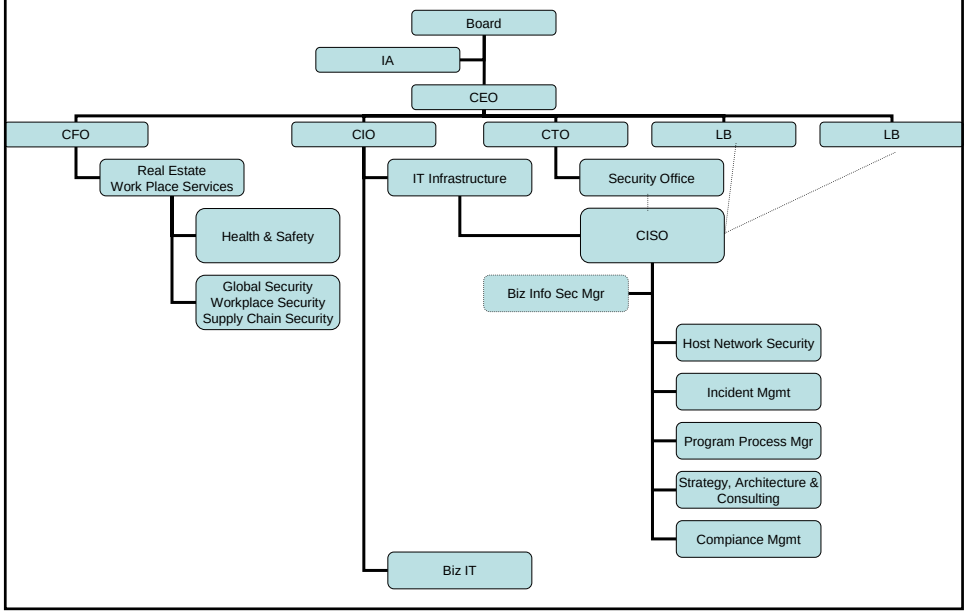
Petroleum Products



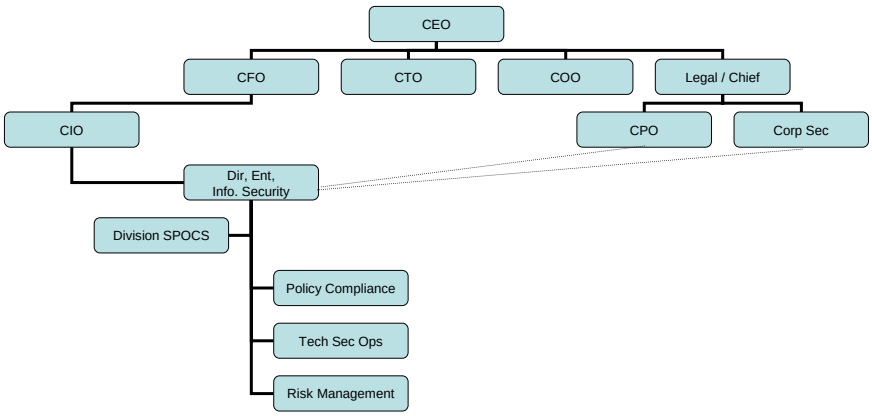
Chemical



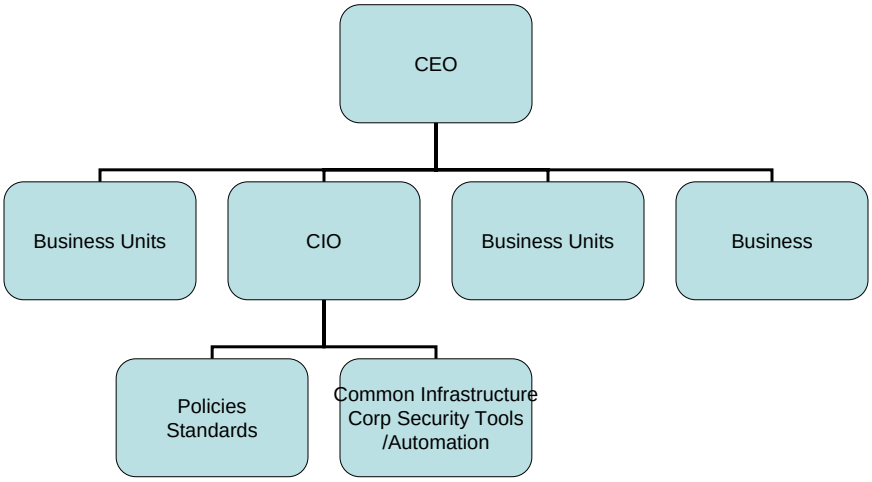
Computer and Electronic Manufacturing



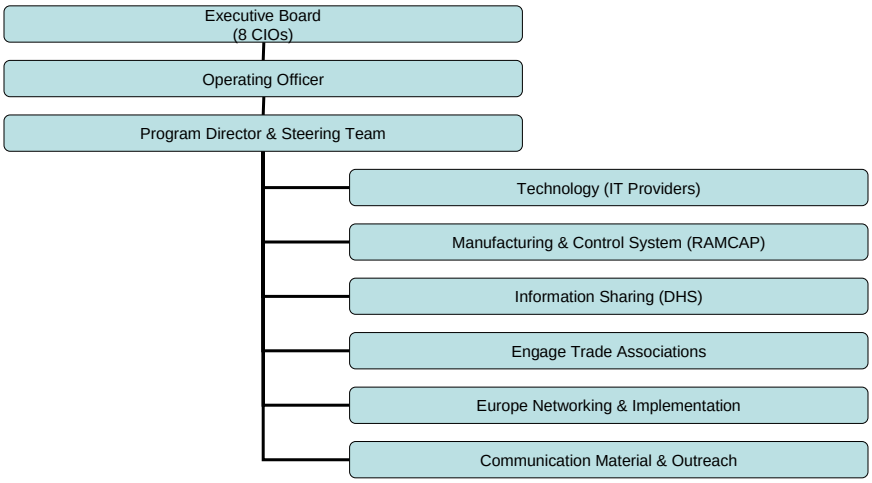
Unreported



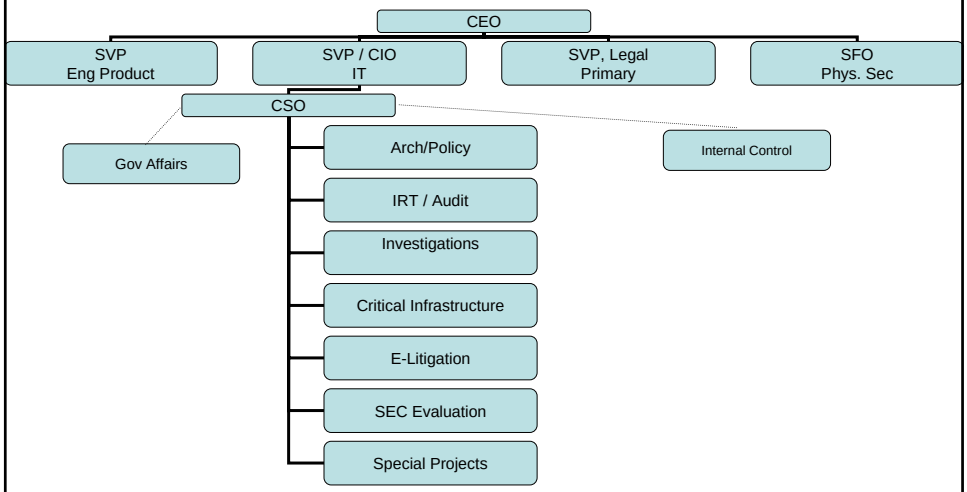
Unreported



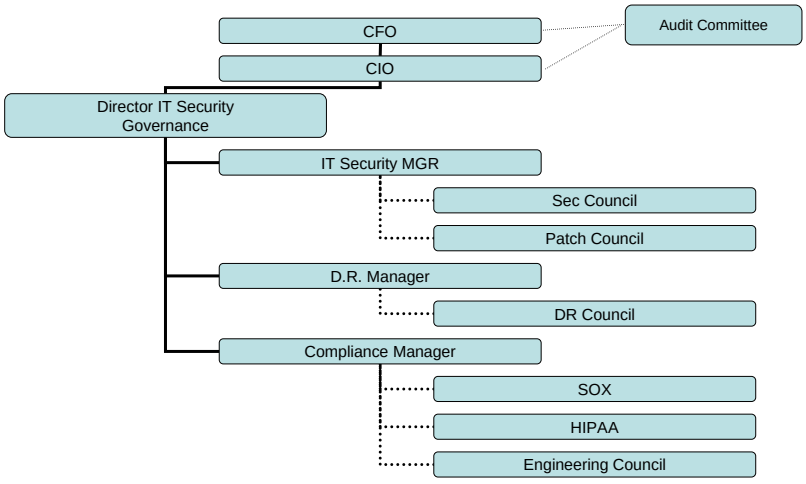
Chemical

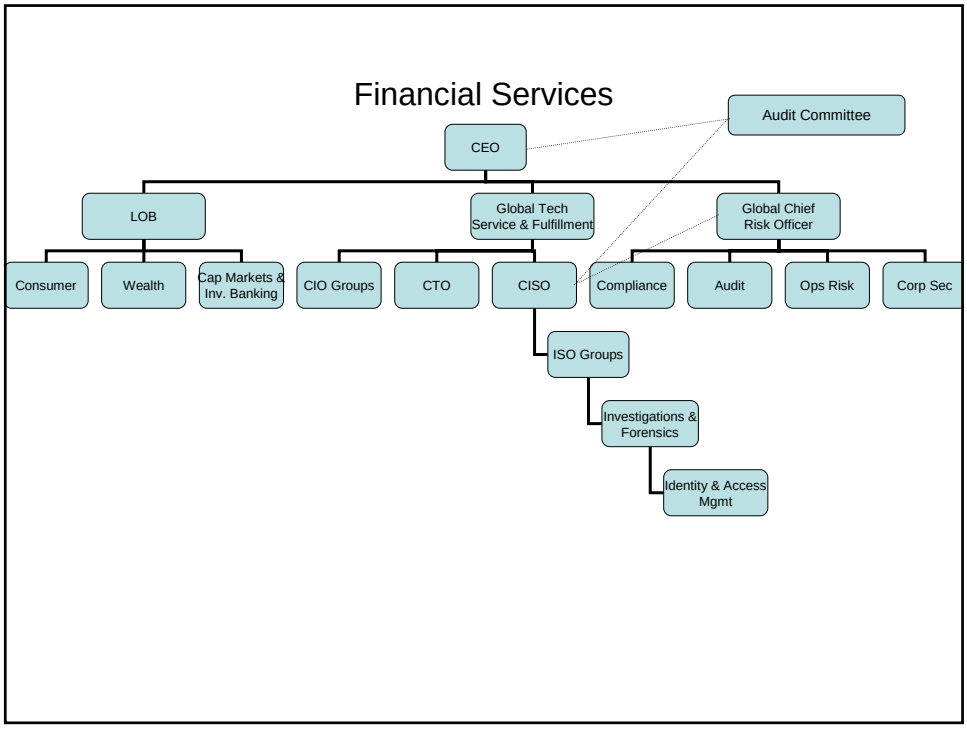


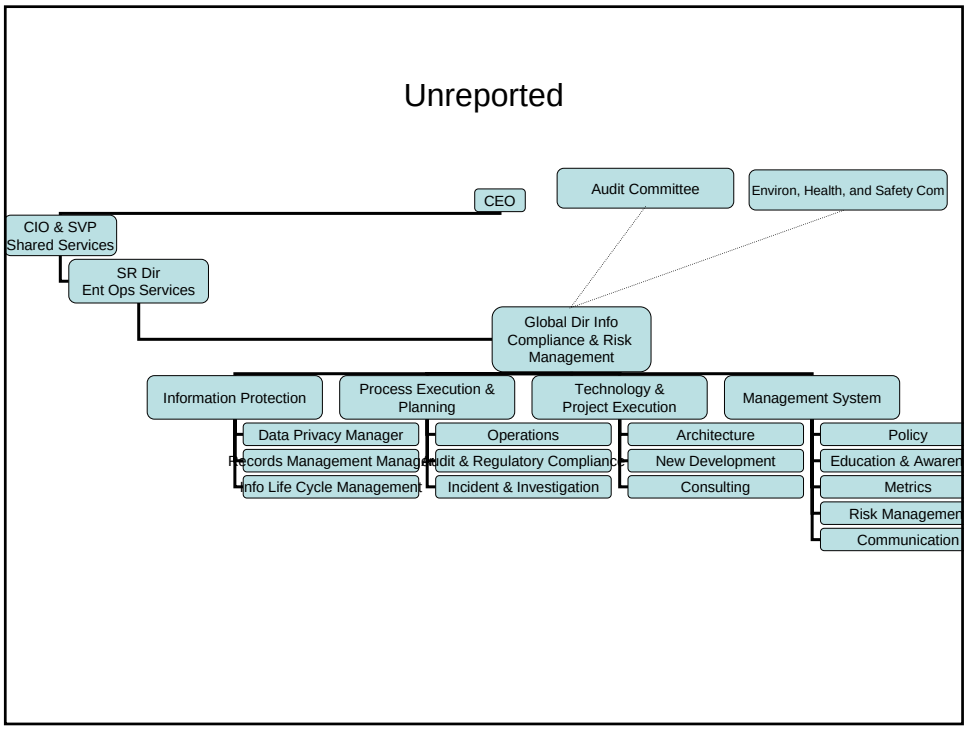
Computer and Electronic Manufacturing



Transportation Equipment Manufacturing




Financial Services
Audit Committee
CEO
LOB
Global Tech Service & Fulfillment
Global Chief Risk Officer
Consumer
Wealth
Cap Markets & Inv. Banking
CIO Groups
CTO
CISO
Compliance
Audit
Ops Risk
Corp Sec
ISO Groups
Investigations & Forensics
Identity & Access Mgmt


Unreported
CEO
Audit Committee
Environ, Health, and Safety Com
CIO & SVP Shared Services
SR Dir Ent Ops Services
Global Dir Info Compliance & Risk Management
Information Protection
Process Execution & Planning
Technology & Project Execution
Management System
Data Privacy Manager
Records Management Manage
Info Life Cycle Management
Operations
Audit & Regulatory Compliance
Incident & Investigation
Architecture
New Development
Consulting
Policy
Education & Awaren
Metrics
Risk Managemen
Communication