The User Role in Information Security

Building effective and efficient environments in the age of mobility and social networking

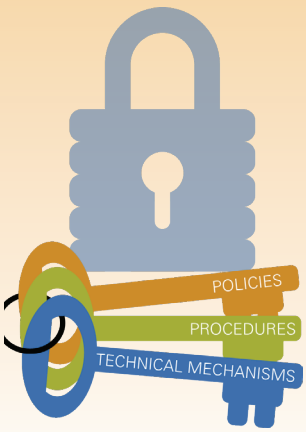
Introduction to Information Security

Information is a critical asset in the operation of any business. The data you capture, record and share every day is the very definition of your relationships with vendors and customers, as well as the foundation for your internal operations and business processes. Protecting it is as important as protecting your cash – and requires just as much care and planning.

Information security is about safeguarding these critical information assets, ensuring the integrity of the data on which you base decisions and transactions, its availability to your business operations and its confidentiality for both you and your customers. It is a process of putting policies, procedures and technical mechanisms in place to protect, detect and correct problems before they threaten your business.

And make no mistake – anything that threatens your information systems does threaten your business. If confidential information about your customers, your finances or your new product line falls into the hands of a competitor, you can lose your competitive advantage at best or suffer significant market losses at worst. Data and privacy compromises make the news today; a security breach that puts your name in the headlines cannot only damage your reputation and your credit rating, but can leave you exposed to lawsuits and even bankruptcy. Increasingly, government is responding to concerns about information privacy and security, creating new regulations about how customer and financial information should be protected. Failure to comply with these regulations can result in punitive fines, lawsuits and even personal liability for breaches.

Every one of these risks carries with it significant associated costs – ranging from the predictable, such as operational losses while you identify and correct the problem, to the unpredictable, such as the time and money you'll need to invest to rehabilitate your marketplace image. If you can manage the risks proactively, you can reduce your total cost of information system ownership simply by saving your organization innumerable complications.



Information Security by Any Other Name

From industry to industry, multiple terms are in use for the mechanisms of information protection, reflecting varying philosophies, methods and areas of concentration. For example, Information Technology (IT) specialists tend to focus their attention on *network security*, while many government organizations are concerned with *information assurance*. In the boardroom, CEOs, COOs and CFOs often strategize about *risk management*, while regulatory departments plan for *compliance management*.

No matter what terminology is used, who leads the effort or what other risks are also considered, all these processes have one goal in common. They seek to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction – and ultimately by doing so, to protect the business.

This paper will use *information security* as inclusive of all industry-specific terms.

Today's Security Environment

The Effect of Mobility and Device Convergence

Our era of technological and social change has led to an unprecedented increase in the number of security threats to information systems. Not so long ago, much of the data relied on for critical business operations could literally be bunkered, locked away in special climate-controlled rooms, with access carefully guarded by information technology experts. Today, mobility and device convergence have permanently changed the game.

Robust computing capability and (Internet Protocol) IP connectivity are everywhere in our daily lives. Our business devices connect us – not only with personal computers, but with smartphones, digital two-way radio systems and location-based asset management systems that let mobile workers stay in touch with the home office from the field. Presentations and proposals, inventories and billing systems, fleet routing and video data – all can follow the worker out into the world, streamlining productivity and reducing operational costs.

Even our leisure time activities are connected. IPTV lets us choose our entertainment on demand and store it for retrieval from the device of our choice. Our cameras upload their images into "the cloud" wirelessly and automatically to either our private networks or the Internet, as we please. Our gaming systems let us communicate and compete with players anywhere in the world. Connected devices let us track our blood pressure or glucose levels and instantly share them with our healthcare providers. We can monitor our workout sessions and post them to our social networks. We can even use "smart home" connectivity to turn on the living room lights and start dinner in the oven remotely, using the office computer or a smartphone.

This age of instant, anywhere access to personal and public information has changed your workers' expectations of business information access. Internet access has become a ubiquitous utility, as essential to modern life as heat and light. Telecommuting has become mainstream. Mobile data is mission-essential. LinkedIn®, Twitter™ and other social networking sites are being used as business tools. Centralized network lock-up has become impossible.

Your end-users are choosing their own profiles for information use and access, bringing their own devices to connect to your network and with them, exposing your business to a whole host of potential new vulnerabilities. Your people are more dependent than ever on technology and the information access it affords. They are more proficient, with and reliant on, mobile devices. Unfortunately, most of them remain naïve about their role in securing the devices and data you rely on and that makes them a source of risk.

The Limitations of Technical Solutions

Most organizations still concentrate most of their information security budget on technical solutions. Technical mechanisms are attractive because they are well-defined. Buy the box – a firewall, an anti-virus program, an anti-malware tool – install it on the network and consider the problem solved. Recently, as more government attention has been focused on information security, "buy the box" has morphed into "check the box" – ensure that all systems comply technically with all the latest regulations and expect that the network is now secure.

Is this approach truly effective? It would seem not. Surveys of IT decision makers indicate that spending on information security compliance has been trending upward at a rate of 10-20% a year. Yet even in the face of increased spending, the number of security intrusions reported annually also continues to rise. According to one group of U.S. security experts and analysts, some 400 breaches were reported in 2009 which compromised over 200 million records. Most disturbing – the same group reported that 80% of those breaches were caused by insiders within the organization.

No technical solution can make your network any more secure than the processes of the people who use it, because poor practices by your own users can easily overcome the best-planned security system. Everyone knows the example of IT mandating the use of strong passwords for network access, and then being immediately undermined by the user who posts his password on a sticky note at his workstation. But the examples in today's business environment are often far more innocuous.

Do all your users understand, for example, that syncing a smartphone at an office PC or using a thumbdrive to ferry work from home to office could expose your network to malware? Do they realize that the handy-but-unauthorized application they installed on their desktop PC or the peer-to-peer network they find so useful for large file transfers could open backdoor access to your carefully secured systems? Does your staff know how to protect their mobile devices – or could a stolen smartphone or a laptop left in a taxi compromise your most confidential data?

Technical solutions and compliance controls are important, but they cannot substitute for a knowledgeable, security-conscious user. That's why enlisting end-user participation to help keep the network secure should be a key goal of information security planning.

Security as Social Process

Us vs. Them

The simplest definition of security is a social one: it is the process of protecting "us" from "them". Defining "us" is not difficult in most circumstances. Insiders share goals, understand their roles in the organization and function within defined relationships. Those relationships are not necessarily limited to staff, but can include vendors and customers/constituents who need to access the organization's information assets. All of "us" need to understand what information assets are kept and why access to those assets may be limited.

Most important, an organization's members need to trust that information is safe within its boundaries. Like a nation, each enterprise stakes out and defends its territory, which can include its mission and purpose, its members and allies and its resources and products. The more critical the mission, the more important it is that the territory be successfully defended against all threats.

Every organization defends against "them" – the source of threat. Outsiders are the most obvious threat and include hackers, spies and other malicious entities that work at breaking down an organization's defenses. Less obvious is the risk created by insiders. For instance, a growing concern in this economy is the former insider who has enough knowledge to be dangerous and enough animosity to use it. However, defenses can also be breached by insiders who carelessly leave the gates down by failing to follow good security practices. Harried tech support experts have even given this particular kind of "system failure" a tongue-in-cheek acronym suitable for scribbling on work orders: PEBCAK – Problem Exists Between Chair and Keyboard.

A Multilayered Solution

When we look at information security as a social issue, it becomes clearer that its solution also needs a social component. As we've already noted, technical solutions, as important as they are, cannot work alone. Trusting a "buy the box" mechanism or a "check the box" operational procedure without involving users is like trusting an autopilot system without putting a pilot on the plane. Artificial intelligence cannot substitute for the common sense of an informed user.

Compliance-based solutions are also important, but regulatory compliance does not necessarily equal effective security. Organizations that have a security standard to comply with often tend to measure their success as a function of technical implementation of compliance controls. That can be dangerous, as it can lead to underestimating or overlooking the importance of other aspects, such as operational procedures and managerial policies.

What is needed for a successful information security solution is to marry all these aspects with behavioral change at every level of the organization. This approach is what the National Security Agency (NSA) has called Defense in Depth – a strategy for multiple layers of defense across the lifecycle of the system that considers the technology in use, the operations of the organization and the personnel involved.

Given this perspective of information security, it becomes apparent that most organizations would benefit most by hardening the weakest link in their information security – that is, investing in personnel competency rather than in another technical defense mechanism. By offering a program of continuing awareness and training on current vulnerabilities and best practice risk mitigation strategies, an organization makes security defenders of all its information system users. That means user awareness is not just a topic for compliance; it is a real tool for reducing total cost of ownership (TCO). With readily illustrated, quantitative TCO returns, the investment in user awareness is easier to justify to senior leadership and buy-in at the top of an organization is the first step toward driving expanded security program capability.

Why Users Must Be Involved

They Know More

Today's networks and systems are faced with the conflicting goals of availability, security and scalability. Users are most concerned with availability – they want to use the tools of their job and, of course, you want that as well. When they perceive information security procedures as interfering with their workflow or personal agenda, they often defeat those procedures either unwittingly or intentionally.

Your users today are more sophisticated about technology's capabilities than ever before; some of them have never known a world without computers and Internet access. They use a greater variety of mobile devices, all with robust computing power, from smartphones and cellular devices, to netbooks and laptops, to multimedia devices like MP3 players, digital video recorders, digital cameras and gaming systems. They have more experience with data portability, so they know how easily digital data can be shared, moved, distributed and repurposed. They know how to sync their portable devices with home and work networks, how to transfer files for use on multiple devices and how to connect everything from phones to televisions and game systems to the Internet.

Most of the people who use your network are perfectly comfortable with the processes of sharing data, because they do it every day at every level of their lives. Families share digitized grocery lists, contact lists, on-line photo albums and downloaded games. Social networks share blogs and tweets, connect through Facebook® or MySpace™, meet online to play together in Massive Multiplayer Role Playing Games (MMRPG), and keep track of each other with breadcrumb trails on web-based community maps. So when you offer them access to your intranet or databases, sharing will come naturally to them.

But They Don't Know What They Don't Know

Unfortunately, most are naïve about their role in defending your information systems, and understandably so. The risks and vulnerabilities can be difficult to comprehend and harder to anticipate.

Information security thinking is often server and desktop focused, giving virtually no attention to protecting the mobile and portable technologies many workers use most. Even experts who focus on security issues can be challenged to keep up with the increasing threats to today's digital data, as hackers often exploit vulnerabilities and defeat security schemes as quickly as new products come to market. For example, the digital rights management system designed to prevent unauthorized copying of Blu-ray™ discs was defeated less than a year after the first title was released. Apple's iPhone® operating system fell even faster; the first "jailbreak" that enabled the installation of unauthorized applications came only 11 days after the device was launched. How can a mere user be expected to keep up?

They Certainly Don't Know What You Haven't Told Them

Users also suffer from a lack of clarity about information security. Many organizations do an inadequate job of defining and implementing good policies, counting instead on compliance measures, technical mechanisms or a thinly staffed, overworked (and sometimes even non-existent) security team to protect them. Even those organizations that have thought through their information security policies often do a poor job of communicating them to users. Many security systems are entirely undocumented. Others are presented as unexplained mandates, which users find easy to dismiss as mere roadblocks to their productivity or, more negatively, as territorial directives from an IT group that is out of touch with their routine work needs.

An informal framework without meaningful and clearly documented procedures can be just as bad as relying exclusively on mandates – it creates the perception that information security is optional and encourages the prioritization of workflow over security. A lack of clear management support can also create a casual attitude that favors workflow over data protection. If senior members of the organization do not prioritize security, users often cannot. Any effort to protect information must be supported by adequate specialist staffing, adequate resources and ongoing education at all levels -- or it risks failure.

In the end, the less involvement with security policy your users have, the less understanding they will have, the less responsibility they are likely to feel and the more risks they will unwittingly take. That means your organization will be more vulnerable, both to internal and external threats. The best and smartest of your people, intent on getting their jobs done, will simply work around your security systems, which could mean unauthorized access sharing, intentional defeat of technical limits or the connection of unapproved equipment to your network. Others will merely halfheartedly follow your poorly explained procedures – and that way lies the madness of passwords posted on sticky notes.

Building User Awareness of Information Security

Define Your Information Security Objectives
Once you have decided to fully involve your users in your information security, they will need training. Good teaching begins with a good lesson plan. In the case of information security, you need to clearly define your objectives and be certain your solution fits them. Only then can you communicate your objectives and your plan clearly and successfully to your users.

The GROW Model is an effective way to approach the challenge. Bring together a team representing all the stakeholders in your information systems, and ask them to consider:

- What is the **Goal** to be accomplished? Be sure your security objective is specific, measurable, achievable and tied to your organization's mission. Ask yourselves, how will we know when we have achieved this goal? Does your measurement consider policy implementation, procedural and behavioral change, and technological aspects?
- What is the **Reality** of your environment? Before you try to move forward, know what your starting point is. Who are your internal experts and your weak links? What is the current user mindset about security? Be sure to fill any information gaps by involving users in your process.
- What are the **Options** that are available based on cost and business alignment? Which of your security challenges are best met by technical mechanisms? By operational changes? By improved user awareness? How will budget affect your choices? How do your options align with any regula tory mandates?
- What is the **Will** of the organization to implement such options? What attitudes and conditions will need to change? Can you commit the needed resources? Will you need outside support?

Once your team has defined your organization's information security objectives, document your decisions and commit to an ongoing process of continuous change management.

Define Your User Groups
User education and awareness programs should not be a "one size fits all" affair. Different sets of users in your organization interact differently with network resources, so plan to address their training with tailored messages. Groups to consider include the executive level, operations, support staff, network administrators, development teams and system engineering. You may find other discrete training groups within your organization.

As you organize, be sure to leverage the social networks within your enterprise to build consensus and support for behavior change. Ensure you have the formal, public support of management. Tap into the expertise of your internal security specialists or, if you lack that expertise, find it outside your organization. Remember that key subgroups, such as work teams, departments or informal networks, can often be more influential than the formal hierarchy. Recruit them to support your information security agenda.

Present Your Policies
When you bring your user groups together, offer them clear policies based on well-defined goals and objectives. Ideally, representatives of each group were included in your GROW strategy sessions. Ask those representatives to report on how each security goal is tied to the organization's mission and how it relates to this group's role in fulfilling that mission. Whenever possible, establish security as a specific objective in job descriptions.

Every discussion of a security procedure should clearly outline the risks that procedure is intended to mitigate. Be frank and specific in describing the potential consequences of a breach. Your people need to understand that security risks can come from both internal and external sources, and that they can include both aggressive attacks and passive vulnerabilities. This is your opportunity to "inoculate" your organization against social engineering threats such as phishing (acquiring sensitive information through fraudulent inquiry such as e-mail or phone calls) and spoofing (masquerading as another by presenting false identification data). Every user should also come away with a clear understanding of how Internet connectivity opens the organization's systems to threats such as cookies, mobile code, denial-of-service attacks and peer-to-peer network backdoors.

Document, Document, Document

To affect real change in user behavior, awareness training will need to become a continual process within your organization. For your users, documentation is the textbook that supports their lessons, defining the technical processes and operational procedures of the information security management framework.

At minimum, documentation should cover these key questions:

- **Who should be using network resources?** Does access extend to outside vendors or customers? Why is some access restricted to certain groups of insiders?
- **What is the purpose and process of user authentication?** What makes a good password and how do you protect it? How does the organization use virtual private networks (VPNs) and other remote authorization tools?
- **What equipment can be attached to the network?** How is the network protected from "infected" systems?
- **How should a possible security breach be handled?** To whom should a stolen notebook or lost smartphone be reported? What is the process for securing data access when an employee is released?

By clearly outlining the roles and responsibilities of users in your information security processes, good documentation helps you further reduce confusion and enhance productivity. Clear documentation also serves notice that information security is a priority for your organization, supported at the highest levels and respected at every level.

Lock In Success

User awareness is an important defensive weapon in your information security arsenal. As users gain a fuller understanding of the risks and potential costs of poor security practices, they can more easily recognize the part they can play in protecting the organization's mission.

Better informed users can be proactive security allies, more readily accepting controls and applying them more consistently. Most important, in accepting shared responsibility for protecting critical information assets, your human assets become more valuable. That means higher value, lower risk exposure and lower costs for the entire organization.

MOTOROLA

Motorola, Inc. www.motorola.com/services/government