Changing the Mind-set—Creating a Risk-conscious and Security-aware Culture

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC, an advisory consulting firm. He has designed and implemented enterprisewide electronic business solutions, information risk management and security strategy and programs, enterprise resiliency capabilities, and threat and vulnerability management solutions for key, global customers in a range of industries, including financial services, insurance, energy, government, hospitality, aerospace, health care, pharmaceuticals, media and entertainment, travel, and IT. Pironti acts as a trusted advisor to senior leaders of numerous organizations on information security and risk management and compliance topics.

Creating a risk-conscious and security-aware culture within an organization can provide more protection to an organization's information infrastructure and associated data assets than any technology- or information-security-related control that currently exists. Adversaries and the threats they pose to information are more advanced and daunting than ever and show no sign of becoming less concerning in the future. To effectively address this issue, information risk management and security functions must create and cultivate cultures within their organizations that embrace information risk management and security as a business benefit rather than another hurdle on the path to success.

An organization's personnel are its lifeblood. Without the support and personal investment of its personnel, an organization's information risk management capability will always be limited in its ability to provide value and to support the achievement of critical business goals. This article discusses how organizations of all sizes and geographies can adopt a variety of concepts, tools and techniques to create or enhance a risk-conscious and security-aware culture.

USING RISK MANAGEMENT TO REMOVE THE FEAR OF SECURITY

Business leaders and stakeholders often consider information security to be an obstacle and a cost of doing business, rather than a business benefit. When developing business processes and technical designs, business leaders and stakeholders often delay security's involvement in the early stages, fearing that security may prevent them from meeting their goals, while adding unneeded overhead and control requirements. On the other hand, security practitioners constantly stress how much more effective they can be if they are engaged early on in development. The most effective way for an information security organization to change this mind-set is to introduce and embrace the concept of risk management as the primary focus of the engagement process, and to address security as a supporting activity.

Consider the psychology associated with the words *security* and *risk*. In many cases, when a businessperson thinks of the word *security*, the first words that come to mind are prevention, disablement and disempowerment. A 2008 IDC study performed for RSA Corporation found that the majority of senior managers surveyed believed that IT security risk is the largest single obstacle to innovation in their businesses.[1] This is a fundamental result of experiences that they have often had when interacting with security, and this negatively drives their perception of the functions and capabilities that security provides. Often, when that same individual hears the word *risk,* what typically comes to mind is understanding, management, control and empowerment. Therefore, alignment with risk at the onset often leads to greater acceptance than security does—in both terminology and approach.[2]

Changing the mind-set of an organization's business leaders and stakeholders requires information security personnel, functions and organizations to fundamentally adjust their approach and behaviors to align their activities with a risk *first* and security *second* approach.

RISK MANAGEMENT AND SECURITY VS. SECURITY AND RISK MANAGEMENT

Information security professionals have recently embraced the concept of risk management, but often treat it as a subordinate and supportive element to security. Evidence of this can be seen in the current industry naming convention, which happens to be: *information security* and risk management. *Security* is identified first, and creates the perception that it is more important than *risk management*. This point of view may be acceptable to an organization's information security personnel, but it is often perceived as counterproductive to its business leaders and stakeholders.

To properly align with business requirements and expectations, the naming convention and approach that makes more sense is *information risk management and security*. This simple change in name and significant change in approach allows the business leadership and stakeholders to first evaluate the risk associated with their information infrastructure and associated data assets, and to then identify the level of security that is acceptable and required for the organization's protection and risk appetite.

BUSINESS AND INFORMATION RISK PROFILE

It is important to implement tools that enable business leaders and stakeholders to understand their risk appetite and risk management requirements as well as parameters needed to align and manage their business activities in relation to those risks. A key tool that can be used to create a risk-conscious and security-aware culture is the business and information risk profile. This profile establishes the bounds of acceptable loss, compromise, disruption or disablement of key and material business functions, individuals, activities, information and processes for an organization. An organization's business and information risk profile also provides a framework and limits to which the information risk management and security teams can align their own activities to ensure that business expectations are met.

The information risk management and security functions of the organization can use the opportunity to assist in the development of these profiles as an occasion to frame themselves as advisors and consultants to the business. They can identify information threats to the organization and quantify the likelihood and business impact of threats if they are realized. They can also identify, develop, implement and maintain information security control objectives and controls to align with the risk tolerances established by the business and information risk profile. Following this process can result in the information risk management and security functions being viewed by business leaders as empowering both information resources and protective functions.

FIGHTING THE HYPE CYCLE

Fear, uncertainty and doubt (FUD) has traditionally been the primary methodology used by information security personnel and vendors to convince organizations to invest in information security tools and capabilities. Security personnel often cause individuals within organizations to feel irresponsible if they do not follow security's directives. Individuals often feel intimidated by warnings from information security personnel of attacks that may or may not be realized by the organization. While this has historically caused short-term gains, the long-term outcome typically results in security personnel being avoided and mistrusted. This is also one of the primary reasons why security personnel are often viewed as obstacles to success rather than valued assets.[3]

When creating a risk-conscious and security-aware culture, it is important to resist the temptation to use FUD to drive adoption of points of view and controls. Instead, other techniques such as threat and vulnerability analysis should be used to provide meaningful data and analysis-driven information about the probability and business impact of attack scenarios. This allows the intended audience to have a better understanding of why a concern exists, and it allows for the formation of stakeholders' own conclusions about the quality of the analysis, the level of concern and the degree of protection that is appropriate.

SECURITY BY COMPLIANCE—FEAR THE AUDITOR MORE THAN THE ATTACKER

Before a road map to achieving a risk-conscious and security-aware culture can be developed, it is important to recognize a common roadblock to success.

In many cases, organizations have adopted a security-by-compliance approach as a result of a fear of the auditor/examiner, rather than a fear of the attacker. An example of this

can be found in studies associated with spending on obtaining and maintaining compliance with the Payment Card Industry Data Security Standard (PCI DSS) compared to spending on other information security initiatives. These studies often show that spending on PCI-DSS-related activities often grows, while spending in other information security areas is often reduced even though the benefits may actually result in a more effective information security posture. This can result from a combination of increasing internal and external compliance requirements, as well as providing a way for the business leadership and stakeholders to push back on information security organizations and personnel in relation to proposed requirements and activities believed to be unnecessary.

Security-by-compliance has become a common approach to information security activities in organizations and one of the key mind-sets and cultural behaviors that must be changed.

Unfortunately, many information security organizations and personnel abused the newfound power granted to them by business leaders when information security became an important consideration during the first decade of the 2000 millennium. Frequently, they forced their will on the businesses leaders and stakeholders they supported, often requiring the introduction of numerous performance-hindering and, in some cases, business-debilitating information-security-related controls and requirements. They did so based on their perception of what was required to properly secure the information infrastructure and data assets of their organizations instead of using a threat-driven and data-supported approach. Often, they used FUD to convince their business leaders and constituents to follow their guidance or face the prospect of being successfully exploited by hackers.

These same organizations and their business leaders then found themselves skeptical of the requirements being forced upon them. They quickly realized that the attacks and vulnerabilities (from which they were warned to protect themselves) were mostly industry hype and were rarely realized. Information security personnel created and promoted the perception of threat instead of using data-driven intelligence-based threat and vulnerability analysis to identify and quantify realistic threats. Information-security-related regulations and standards (and related audits) have empowered business leaders to push back on information security organizations and professionals. Leaders often believe that external regulations and standards, such as PCI DSS, provide an unbiased template for the requirements and level of investment that they need to implement in order to provide effective information security for their organizations. They have also recognized that unlike hacker attacks that have fluctuating probabilities of occurrence and varying degrees of business impact, there are known negative consequences and outcomes of not being in compliance with external requirements—consequences including fines and reputational concerns.

Compliance to internal and external IT security requirements can be a positive benefit to organizations and should be seen as the beginning and not the end of the IT security journey. When changing the culture of an organization, it is important to impress upon the organization that being compliant with external regulations, standards and guidelines will assist it in passing audits and examinations, but may not comprehensively address its needs for critically important security controls. Unfortunately, in the event of a successful attack and a resultant compromise of an organization's information infrastructure or data assets, the court of public opinion, as well as many legal courts, may not accept compliance as a comprehensive or effective approach to information risk management and security.

> "Being compliant with external regulations… may not comprehensively address its needs."

POLICIES AND STANDARDS FIRST; CONTROLS AND TECHNOLOGY SECOND

When changing culture in organizations, it is important to formally document, publish and drive awareness of information risk management, security expectations and control objectives in advance of their use. These expectations and requirements are most often found in the information risk management and security policies of organizations.

Many business leaders and stakeholders are distrustful of information risk management, security control objectives and associated controls that are presented to them as requirements by individuals and are not based on published policies and standards that have been adopted by the organization. Often, their perception is that these objectives and controls are

optional. If the members of an organization have confidence in the governance process associated with the development and publishing of the information risk management and security policies and standards development, they are more likely to adopt and embrace them.

Implementing policies and standards that cause minimal impact to the activities and behaviors of the target population often results in a faster pace of adoption, leading to positive adjustments to culture. These easily digestible policies and standards should be presented in the context of an information infrastructure and data asset protection road map that identifies the current, as compared to the ideal, capability of the organization and how it supports the organization's overall goals. The policies and standards can then be incrementally enhanced over time as the organization becomes more capable of meeting the identified ideal state.

FOCUS ON THE PROTECTION OF DATA AND BUSINESS PROCESSES, NOT TECHNOLOGY

The commonly used approach to information security is to focus on the protection of information technology based on the assumption that such an approach appropriately protects the organization's data assets. Even accepting the assumption that the organization can effectively maintain comprehensive technology controls, it does not account for the fact that data do not necessarily have to interact with technology, but the organization still has the same security requirements. A more effective approach is to focus on protecting business processes and their associated data first, and the technology with which they interact second.

In this approach, data classification models and standards define the security control objectives and requirements for business processes and data. By applying this method, organizations can ensure that no matter where their data reside, they will have an appropriate level of protection that aligns with the organization's risk appetite. This methodology can also identify situations or environments in which adequate information security controls for business processes and data should not be implemented and should not be allowed to be present until their requirements can be met.

DATA CLASSIFICATION

Data classification supports the perspective that not all data are created equal and their value can and often do change, based on business activities and conditions. By establishing a simple and easy-to-understand data classification practice model, organizations can provide guidance to employees about expectations for the level of protection associated with different data types. Each category of data classification should include descriptors of the type of data that are associated with it, as well as the control objectives that are required. This approach can help remove the mystery of the risk management and security expectations for data and demonstrate that information risk management and security organizations can be flexible.

When developing data classification models, it is important to keep them as simple as possible and to provide a middle-ground designation. This middle-ground designation should provide adequate requirements and controls to prevent accidental disclosure and reasonable due care of the organization's data assets. It should not force the business or its constituents to require business-restrictive controls that may be counterproductive to required or beneficial activities. A three- or five-category data classification model should meet the requirements of the information risk management and security functions. It also provides an easy-to-follow framework for the business audience that will be required to believe in and utilize it.

Data Classification Levels and Designations

Level	Designations
5	Confidential—Restricted
4	Confidential—Customer- or compliance-related
3	Proprietary
2	Internal use only
1	Public

USERS—THE GREATEST ASSET AND THE MOST CHALLENGING ADVERSARY

Many information security professionals and organizations have identified the user community as the weakest link in their information security postures. They often go to great lengths to limit the ability of users to knowingly and/or unknowingly cause negative impacts to the organization and its constituencies. While it is true that users, especially those with privileged access to sensitive environments and information, can easily compromise or damage an organization's information infrastructure and associated data

assets, they can also be the most effective control and greatest security asset. Users have the added benefit of their senses and intuition to detect when something is out of sorts, while current computing-based analysis can perform only rule-based and binary analysis to identify inappropriate activities or behaviors. In this way, the user is still minimally 50 percent smarter than the computer since the computer only knows "*Yes"* or *"No,"* but the user knows "*Maybe."*

In many recent data breaches and information infrastructure compromises, such as the TJX data breach identified in 2007, it is the user who has identified the existence of an incident first and not the sophisticated information security technologies that were employed. Technologies are beneficial in helping in the incident response and investigation activities, but only when they are properly implemented and operated by knowledgeable and capable professionals.

A key part of successfully creating a risk-conscious and security-aware culture is to gain the trust of the individuals whose behaviors are to be modified. By implementing controls and capabilities that are designed to protect the information infrastructure and data assets from their users, organizations may actually alienate these same users and make them feel untrusted. This lack of trust often leads to the users no longer being supportive of risk and security objectives, and to a less-productive and unhappy working environment.

TRUST BUT VERIFY

A trust-but-verify approach to monitoring and oversight of organizational and employee activities can be an effective approach both to manage risk and meet the control objectives required by information security and risk management. Often, organizations and individuals view information security professionals and organizations as lacking faith in their ability to conduct their activities in a security-conscious and trustworthy fashion. This point of view is often fueled by the introduction of governance and oversight controls, such as user activity logging on computing resources that are appropriate in the eyes of information security personnel but can be interpreted as lack of trust and invasion of privacy by the employees being monitored.

By using a trust-but-verify approach to the communications associated with the design and operation of these controls, an organization can present these capabilities as a benefit to both the employee and the organization while, at the same time, minimizing the negative associations. In these situations, it is important first to communicate to both the organization and the affected employees that these controls can help ensure that they will not be subjected to investigation or suspected of nefarious actions since objective proof will exist to rule them out from knowingly being part of any incident.

OVERSIGHT BOARD—REMOVING THE PERCEPTION OF THE IVORY TOWER

One of the strategic elements of a governance process associated with information risk management and security is the introduction and use of an oversight board. Members of organizations often perceive information security as having "ivory tower" syndrome. This happens when a belief exists that information security personnel and their organizations do not have an accurate or intimate understanding of the business conditions and expectations, and arbitrarily institute business-restrictive requirements and controls.

An oversight board made up of business leaders and stakeholders can help remove this perception. This board provides guidance and direction to the information risk management and security functions and personnel to ensure that all the activities align with the expectations of the business.

WINNING THE HEARTS AND MINDS

An effective and well-tested technique that is often used to change a culture is to win the hearts and minds of the population being addressed. The creation of a risk-conscious and security-aware culture requires an organization and its personnel to believe in and derive value from what is being promoted and requested of them.

There are various techniques that an organization can use to affect this, including using an embrace-and-educate approach, as well as identifying personal benefits associated with information security and risk management.

Embrace and Educate—Turning "No" Into "Yes"

Security is often known for saying "no" when it comes to the adoption of new ideas, concepts, technologies and solutions. This is not to say that this negative response is always without merit. It is often the case that until the threats and risk and associated management capabilities can be identified, security takes a cautious and conservative view of new ideas, concepts, technologies and solutions. Unfortunately, this behavior often

drives individuals and organizations to act in a covert fashion if, for example, they perceive the benefits of a technology outweighing the risks of its use. This often leads to a lack of visibility and ability to govern the use of the new technology which may result in a higher risk to the organization than might have occured if the use of the new technology had been allowed.

The adoption and use of an embrace-and-educate approach to new ideas, concepts, technologies and solutions can help change culture and create positive feelings among the information risk management and security elements of an organization. In this approach, the risk management and security elements of the organization recognize and acknowledge the immediate value of the capabilities that the business intends to use. At the same time, this approach educates the organization's user population regarding identified threats and risks associated with these capabilities and the organization's expectations of their use to ensure appropriate levels of security This method also reinforces to the organization and its stakeholders that the risk management and security elements now include an advisory consulting function that actively supports the interests of the business.

The key to the success of this method is to use education and awareness techniques that can be easily understood and internalized by the intended audience. This often means the use of simple and easily understood terms, case studies and examples that are readily identified as being applicable to the organization's business activities.

Personal Benefits

If individuals can derive personal benefit and value in the knowledge, insights and guidance provided to them about risk and security, it is likely that they will change their behaviors in both their personal and professional lives to be more risk conscious and security aware. An example of this is a change in individuals' use of social networking solutions. These capabilities are often used by individuals for personal activities, but increasingly have business benefits as well.

If an organization chooses to block access to these solutions in the workplace in the name of security, individuals will often find covert ways to access them without the organization's knowledge. If the same organization proactively provides education and awareness about the risks and threats associated with these capabilities, presented as an employee benefit and not a business expectation, and also provides user-friendly guidance for their safe use, it will often achieve positive results. Employees often appreciate information presented to them by their employers as a personal benefit, and, as a result, they change their work-related usage behavior to incorporate the guidance provided. The organization can then remove some of the security-related restrictions for the use of these solutions using corporate assets, promote an employee-friendly workplace, regain visibility into their usage, and take advantage of the business benefits they can provide.

EFFECTIVE REINFORCEMENT METHODS

Changing the mind-set and the culture of an organization requires the use of effective and consistent reinforcement of the desired state. In doing so, it is important to identify the learning styles, values and interests of the intended audience. The use of various methods and techniques to deliver messaging is essential to reach a diverse audience. This messaging can include in-person training and seminars, computer-based training and messaging (i.e., screen savers), visually stimulating and thought-provoking strategically placed signage, and positive messaging that demonstrates how the adoption of this new mind-set can promote success and benefit not only the organization, but the individual as well.

There are also opportunities to effectively reinforce the desired state by introducing and maintaining information risk management and security-related considerations into business processes and activities. Information risk management and security activities, including threat assessment, risk profile alignment and control assessments, should also be introduced as an element of consideration and, where possible, as an approval gate in key business processes, including product management, project management, solution development, change management and operations. This ensures that information security and risk management activities are integrated into the business-as-usual activities of the organization that will drive awareness and cultural change.

FOCUSING ON WHAT REALLY MATTERS—THREAT AND VULNERABILITY ANALYSIS

Many organizations find themselves overwhelmed by the numerous ways in which a motivated and capable adversary can compromise their information and information infrastructure. In many cases, organizations limit the adoption of new capabilities

and technologies or adopt new tools without properly securing them. This attitude comes, in part, from the organization's belief that it will never be successful in effectively securing information infrastructure and associated data assets. As a result, investing beyond the minimum requirements is not believed to have true cost-benefit. One of the most effective ways to adjust this point of view and create a risk-conscious and security-aware mind-set and culture is to use threat and vulnerability analysis.

Threat and vulnerability analysis is a key component of any proactive and risk-based approach to securing information infrastructure and associated data assets. It evaluates how an attacker could strike a capability or solution. Then it identifies the probabilities that an attack will occur, and the business impact of a successful attack. This type of analysis allows an organization to navigate through the fear and uncertainty caused by media, vendors who want to sell products, and/or individuals who want to prevent or change the adoption solutions and capabilities.

One of the key components of any threat and vulnerability analysis capability is threat intelligence. It is essential to have accurate and credible intelligence to be able to project the likelihood and potential business impacts of threats. There are various sources of intelligence available, including web sites, mailing lists, news and media outlets, and paid services. Single-source intelligence can be helpful, but is often not enough for analysis activities. Multiple sources of intelligence should be used to produce confidence in the credibility of data.

MANAGING RISK—CONTROL OBJECTIVES AND CONTROLS

Once an organization has identified what risk exists for its information infrastructure and associated data assets, it should implement controls that manage risk and provide protection. The information risk management and security functions should identify and govern control objectives and, in some cases, controls themselves if they have operational responsibilities. In most cases, the identification and operation of controls should be left to the data, process and/or control owners, who can then be advised by the information risk management and security functions to assist them in their efforts. This allows for a more efficient and effective operating model since the individual groups will play to their strengths and not create problems often associated with operating outside of their scope of expertise or responsibility (e.g., information security owning operations for technical controls instead of IT operations).

There are a variety of controls (detective, preventative, corrective and compensatory) that can be introduced to manage risk and meet control objectives for information infrastructure and data assets. It is important that an information risk management and security organization develops a library of controls that can provide varying levels of security. This allows for different tiers of protection based on the organization's risk profile and the data classification levels that the devices and capabilities will access, store, transmit or use. This also provides the business with a variety of options from which to choose what best meets its business goals while working within acceptable guidelines.

FINAL THOUGHTS

The culture of an organization ultimately determines whether or not the organization can successfully and effectively protect its information infrastructure and data assets. Creating a risk-conscious and security-aware culture allows an organization to protect itself. Risk and security will no longer be something that the organization consciously considers and instead will become integrated in business-as-usual activities. Changing culture is not something that can be accomplished quickly. It is a journey, the success of which requires careful attention and constant reinforcement. The effects are well worth the effort. Changing culture often results in converting malicious attacks that would typically cause significant damage and business disruption into operational anomalies that are easily identified, remediated, and have little to no material business impact.

REFERENCES

Payment Card Industry Security Standards Council, *PCI Data Security Standard*, Version 2.0, October 2010

ENDNOTES

[1] Christianson, Christian A.; *Innovation and Security: Collaborative or Combative*, Tech, IDC, Sponsored by RSA, 2008

[2] Security for Business Innovation Council, *Mastering the Risk/Reward Equation: Optimizing Information Risks to Maximize Business Innovation Rewards*, August 2008

[3] Lohrmann, Dan; "Why Do Security Professionals Fail?," *CSO Online*, 9 January 2010