**Effective Information Security Requires a Balance of Social and Technology Factors**

Tim Kayworth  
Baylor University (U.S.)

Dwayne Whitten  
Texas A&M University (U.S.)

**Executive Summary**

Industry experts have called for organizations to be more strategic in their approach to information security, yet it has not been clear what such an approach looks like in practice or how firms actually achieve this. To address this issue, we interviewed 21 information security executives from 11 organizations. Our results suggest that a strategically focused information security strategy encompasses not only IT products and solutions but also organizational integration and social alignment mechanisms. Together, these form a framework for a socio-technical approach to information security that achieves three objectives: balancing the need to secure information assets against the need to enable the business, maintaining compliance, and ensuring cultural fit. The article describes these objectives and the security alignment mechanisms needed to achieve them and concludes with guidelines that can be applied to ensure effective information security management in different organizational settings.

**INFORMATION SECURITY HAS BECOME A STRATEGIC ISSUE**

Information security continues to be a major concern among corporate executives. The threat of terrorism, a growing dependence on the Internet, globalization, and new government regulations requiring companies to protect data have heightened awareness of the need for effective corporate governance of information security. Further, the staggering financial and reputational loss associated with large-scale data breaches has made executives acutely aware of the need to protect corporate information assets. Not surprisingly, corporate IT executives consistently rank information security and privacy as a key organizational issue.

Since information security is rapidly becoming a core business issue, many firms have sought to elevate the security function through hiring security executives, expanding budgets, or evaluating security investments based on ROI. However, the question remains as to what is the most effective organizational approach or strategy for information security.

Historically, companies have followed a technically focused information security strategy that emphasizes the primary role of technology in designing effective security solutions. Such a strategy places a premium on sophisticated technologies and technically competent security specialists capable of applying various technologies to secure information assets. Moreover, technology—rather than people—is used as the

---

1 Bob Zmud is the accepting Senior Editor for this article.
2 The authors wish to acknowledge the Center for Management Information Systems at the Texas A&M University Mays Business School for its support of this project.
basis of explanation when security breaches occur. And since security is perceived to be a technical issue, the information security group in organizations following this strategy tends to be positioned as a low-level technical function operating independently from the business. The lack of integration between the security group and the business may result in security policies and budgets not reflecting the needs of the business. In such an environment, security tends to be reactive, investment decisions are driven by short-term priorities rather than well-conceived strategic priorities, and security may receive little executive attention.

The more current view is that an effective information security strategy must be balanced, emphasizing both the importance of technology and, when designing and implementing security solutions, the organization’s socio-organizational context. Such a socio-technical security strategy as proposed by Siponen emphasizes the importance of integrating security into mainstream aspects of the business and of taking account of the human element in designing effective security programs. Such a strategy will be strategically focused or business driven and thus ensure that security becomes integrated into the fabric of the organization and is perceived as an important core business issue. While technology is still important, it represents just part of an overall solution that must also include the social-organizational elements of the business.

An effective information security strategy must therefore incorporate two key elements, the first of which is technical competence. Technical competence must be complemented with a strategy to align security both organizationally and socially as part of an overall socio-technical strategy to information security. The benefits of such an approach include improved compliance, security spending and policies better aligned with the business, and fewer security incidents.

The aim of our research was to gain a deeper understanding of how an effective information security strategy manifests itself in practice. Specifically, we explored the types of mechanisms firms use to align security both organizationally and socially to the enterprise. To address these issues, we interviewed information security executives and managers from a cross-section of industries representing a range of security risks, concerns, and maturity (our research methodology is described in the Appendix). Finally, we identified a set of guidelines for information security management.

THREE PRIMARY OBJECTIVES FOR AN INFORMATION SECURITY STRATEGY

There are three primary objectives all security executives must address regardless of the organizational context: balancing the need to secure information assets against the need to enable the business, ensuring compliance, and maintaining cultural fit.

1. Balancing Information Security and Business Needs

A major challenge faced by security executives is the requirement to balance the need to enable the business against the need to secure information assets. For example, if salespeople are to be given access to client data through portable devices, what is the value of providing this data to the sales force weighed against the need to secure valuable client data from unauthorized access or theft? Hypothetically, risks could be eliminated by locking down servers and providing no access to corporate data by salespeople. While this option would effectively secure corporate data, it would also hinder business operations. So an effective information security strategy must be

---

15 The organizations in the research are referred to throughout this article by pseudonyms: FinServ, Petro 1, Petro 2, Distribution, TechServ, ITProducts, Retail 1, Retail 2, TechConsult, OilServ, and Energy.
business driven, simultaneously securing information assets while still enabling the business.

Conversations with security executives revealed three characteristics of a business-driven approach. First, such an approach must align with corporate goals and objectives:

“When I say alignment, what I mean is that we understand the business unit strategy, they understand the accountability we have to protect the corporation as a whole ... we've been able to reconcile those two different sets of requirements into something that allows the business to continue operating. So it's not all about mitigating the risk. For us it's about both.” (Director of Global Security, Petro 1)

Second, being business driven also means it is the responsibility of the business—not the security function—to determine acceptable levels of security risk. Thus for a company like TechServ (which provides technology services), the Product Design Team would be responsible for assessing the level of security risk acceptable for a new product launch. The security team would then take this information and weigh it against the overall security risks to the organization as well as against any government compliance requirements.

The third aspect of a business-driven security strategy concerns risk contingencies. Our interviewees were unified in their opinion that an effective security strategy is not “one-size fits all”; rather, it takes into account the varying risk factors that may be associated with different industries, product lines, or geographic locations. When designing security policies and standards, planners must therefore take account of how business requirements for security may differ even within the same organization. Such differences were evident in TechServ:

“I may not need the level of security tools in a manufacturing plant that I need in a health claims operation. The implementation of security tools has to be tailored to the industry.” (Chief Privacy Officer, TechServ)

2. Ensuring Compliance

The second objective is to ensure that the design and implementation of information security policies comply with any number of external legal requirements:

“Information security is not exclusively about risk mitigation; rather it is a balancing act among operations [business requirements], governance [security requirements], and compliance [legal requirements].” (Director of IT Security, Retail 1)

Increasingly, security managers are faced with the complex challenge of meeting multiple compliance requirements from a growing array of federal, state, and industry standards. FinServ, for example, has to comply with federal compliance legislation (Sarbanes-Oxley and the Gramm-Leach-Bliley Act). Since FinServ is publicly traded, Sarbanes-Oxley requires it to deploy comprehensive IT security controls to ensure the accuracy and reliability of public disclosures and to regularly assess the effectiveness of these controls, reporting such results to the Securities and Exchange Commission. It is also subject to the Gramm-Leach-Bliley Act, which requires financial institutions to develop information security plans describing how the company is prepared for and plans to continue to protect clients’ nonpublic personal information. Finally, FinServ also has to comply with the Payment Card Industry (PCI) standards, which outline certain controls companies must implement to ensure the safety of credit transactions.

3. Maintaining Cultural Fit

The third objective for security executives is to maintain cultural fit, to ensure that underlying values about information security mesh with the values of the organization. Since an organization’s staff members tend to behave in ways consistent with corporate values, cultural conflict may occur when the values associated with an information security program don’t match those of the company. If security programs do not fit the organizational culture, individuals may act inconsistently with information security policies and standards.

The importance of cultural fit was evident at both Petro 1 and Petro 2. The security manager at Petro 2 characterized the company’s organizational culture by using adjectives such as “conservative,” “risk-averse,” “bureaucratic,” and “non-trusting.” Consistent with this culture, Petro 2 self-characterized its security function as being “more secure than the government,” and an independent consultant noted that “control is in their DNA, so their efforts in information security are prodigious.” In contrast, Petro 1’s organizational culture can be described as “open” and “trusting.” Consistent with its open

culture, this organization’s security strategy has been characterized as being more relaxed and open:

“Yes, we do have a security culture, and it is very much informed by our overall company culture. The company as a whole has a very trusting culture. The information security culture is very much tied to that.” (Security Standards and Controls Manager, Petro 2)

Both of these firms have been able to deploy security programs in harmony with the prevailing cultural values of their organizations. To do otherwise would potentially create conflict between the demands of the security program and the values of the firm, leading to employee resistance of security policies.

AN ORGANIZATIONAL STRATEGY FOR ACHIEVING INFORMATION SECURITY OBJECTIVES

An effective information security strategy will enable a firm to achieve all three of the objectives described above. Achieving these objectives will ensure the security function is strategically focused, business driven, and aligned with the organization. Of particular interest is the strategy used to accomplish these objectives. The firms we studied have achieved this through a socio-technical strategy that includes three types of critical risk management mechanisms: organizational integration, social alignment, and technical competence (Figure 1).

With this approach, technology represents one key element of the overall strategy, which must also include organizational mechanisms to integrate security with the mainstream business and social alignment mechanisms to align security with the firm’s social context.

We identified nine organizational integration and four social alignment risk management mechanisms, which we describe below. (We do not describe technical competence risk mechanisms in this article because there is a wealth of published material in this area of information security.)

Organizational Integration Risk Management Mechanisms

The nine organizational integration mechanisms identified in our research are summarized in Figure 2. Each mechanism can be classified as either a formal organizational structure or a coordinating mechanism. Coordinating mechanisms can be further broken down into coordinating structures and coordinating processes.

Formal Organizational Structures. All firms had a formal information security organization headed by a Chief Information Security Officer (CISO) with management accountability over the entire security function. Regardless of the structure of the companies we studied, virtually all security functions were centralized so they could develop and deploy uniform enterprise-wide policies and standards. In terms of

![Figure 1: A Strategic Framework for Effective Information Security](image-url)
Effective Information Security Requires a Balance of Social and Technology Factors

reporting relationships, each security organization was part of the corporate IT function with the CISO reporting at most two levels from the CIO. These CISOs can therefore regularly participate in security planning processes that are subject to review by the CIO or higher levels in the corporate chain of command. This contrasts with other firms, where the security function operates as an isolated technical group. The danger of such isolation is that:

“You’re off in left field somewhere, and you don’t get the [executive] support you need. You have a lot of people doing things they don’t

<table>
<thead>
<tr>
<th>Figure 2: The Nine Organizational Integration Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mechanism</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td><strong>Formal Organizational Structures</strong></td>
</tr>
<tr>
<td>Information security organization</td>
</tr>
<tr>
<td>Information security executive</td>
</tr>
<tr>
<td>Internal audit function</td>
</tr>
<tr>
<td><strong>Coordinating Structures</strong></td>
</tr>
<tr>
<td>Information security steering committee</td>
</tr>
<tr>
<td>Information security liaisons</td>
</tr>
<tr>
<td>Separation of security governance from operations</td>
</tr>
<tr>
<td><strong>Coordinating Processes</strong></td>
</tr>
<tr>
<td>Top-down security</td>
</tr>
<tr>
<td>Information security embedded within key organizational processes</td>
</tr>
<tr>
<td>Flexible application of uniform standards</td>
</tr>
</tbody>
</table>
Each organization had an internal audit group whose primary role is to conduct independent assessments of information security controls and policies and to convey these results to management. As mentioned by the security manager at TechServ, “A very strong corporate audit function is required to ensure that the operational [controls] are meeting the requirements of the strategy.”

ITProducts’ internal audit group develops an annual audit plan for information security and then subsequently spends two to three months auditing the security function. At Petro 2, the information security function receives a detailed report from internal audit providing its assessment on security controls and policies. This report forms the basis for subsequent actions taken by the security function to ensure the controls and policies are compliant with internal standards. One of the main benefits of a strong internal audit function is its availability to assist with security issues from the inception of a project right through to its implementation.

**Coordinating Structures.** The firms we studied were very deliberate in their use of information security steering committees as a means to facilitate security planning and budgeting processes, and to ensure that the security function maintains alignment with business strategy. Through this structural mechanism, the information security function is able to gain valuable insights from the business to facilitate strategic decision making. Additionally, steering committees provide a forum for the security function to communicate security pressure points to business managers. Comments from security managers attest to the importance of these steering committees:

“We [information security] basically report to an executive committee that’s made up of representatives from three business units. [We] talk about capital we’re about to spend over the next five years; our strategic capital plans and our tactical plans are developed from there.” (Manager of IS Security, Retail 2)

“We go to [the steering committee] to gain alignment, to understand what the strategies are for the business and then to present back to them—here are the pressure points that we’re seeing, and what steps should we take, if any, to mitigate those?” (Director of Global Security, Petro 1)

A second coordinating structure is the use of information security liaisons to represent the interests of the corporate security function among the various business units. This practice was most evident at Petro 1 and Petro 2, which deploy security liaisons physically among business units to act as advisors and consultants on security-related matters. For example, a security liaison on a firewall support team might report administratively to IT operations and functionally to corporate security for oversight of firewall policies and standards. At Petro 2, security advisors are responsible for promulgating corporate security standards and for making sure that such standards are embedded into any new products or services offered by business units.

A third universal coordinating structure in the firms in our study was to maintain separation between security policy making and operations (i.e., between policy making and execution). The typical arrangement was for the corporate security function to be responsible for setting security standards and policies with either the IT organization or other business units’ IT personnel responsible for the execution of these policies. For example, ITProducts’ corporate security organization creates the security policies, which are then subjected to a technical review and subsequent approval by a corporate security advisory team and final approval by the CIO. Once the policies are approved, the IT organization is responsible for their execution. The benefit of this separation is that it keeps security planners from being distracted by operational details:

“When we were contemplating splitting up governance and operations, at the time, I was very much opposed to it. [But] having lived [with] it now for a year, I recognize that, because I was consumed with a lot of operations activities, we had policy making and compliance activities that were getting too little attention. I do think that this is a good structure for information security.” (Director of Global Security, Petro 1)

A second benefit of separating security governance from operations is that it helps to maintain independence between those tasked with making policy decisions and those responsible for executing the decisions:

“When our firewall team gets a request to open up a specific port, they will come to my team to ask, ‘Is this appropriate?’ We’ll do the appropriate risk assessments, and then we’ll make the ruling on whether or not it should
be done. If we say yes, then they execute that. But they’re not accountable for making the decisions; they’re only accountable for executing the decision.” (Director of Global Security, Petro 1)

**Coordinating Processes.** The firms in our study were using a *top-down security process* that enabled them to generate detailed security requirements based on actual business needs. To accomplish this, they start by defining high-level business requirements for information security and then refine these to progressively more detailed technical specifications. Both Petro 2 and TechServ provide excellent examples of this top-down approach.

At Petro 2, the security strategy is informed by a set of guiding principles originating outside the security function. This framework provides a basis for developing more detailed security practices and, finally, detailed operating procedures. Similarly, at TechServ, the security function bases its strategy on a set of guiding principles that, in turn, drive general requirements, specific security standards (about 500), and, finally, technology-specific security implementation procedures (e.g., how to implement password security in a Linux environment). Thus the security programs for both of these firms are formulated at the very highest levels based on business needs and then refined further to the level of technically detailed security implementation guidelines.

The Chief Privacy Officer at TechServ sums up the elegance of the business-driven top-down approach to information security strategy:

> “The best thing that we put in place was a strong policy and standards structure that did not address specific technologies but did address the [business] issues that we’re dealing with. But if you have not put together a good structure of policy and standards which really define your [security] strategy, then, operationally, you’ll be all over the place. I think that’s probably one of the things we did right to begin with.”

Another coordinating process is the practice of embedding security within key organizational processes, such as the IT project management life cycle, with key deliverables required for each life cycle phase. By considering security before and during the development of a project, it is much easier, more effective, and cheaper to successfully integrate security into the project or process. Commenting on this approach, the Director of Technology Advisory Services at TechConsult noted:

> “Your systems are riddled with vulnerabilities, and you can have a much bigger problem later than if you had been more thorough in your development standards in the beginning. By considering these issues early on, you won’t be in that position.”

The Director of Data Center Operations at Retail 2 described a recently completed project that was one of the first to use the new project management security procedures:

> “The key thing is to make sure that security was involved at every part of the project, not just after it was implemented. So in each of the phases—requirements, design, development, implementation—we have particular deliverables from a security standpoint that are required.”

The final coordinating process we identified is the flexible application of uniform standards. Those companies in our study with international operations tended to apply security policies uniformly across global operations. The advantage is that consistent application of uniform security policies provides an environment that is easier to manage from a security executive’s standpoint:

> “It is important to have a consistent framework and foundation for high-level security policies. This helps from a management and enforcement point of view. As people travel and rotate assignments internally, they also know what is expected of them regardless of where they work.” (IT Security Manager, ITProducts)

The downside, however, is that implementing security policies uniformly across geographic regions may prove challenging, particularly when there are significant cultural differences. To reconcile these differences, firms provide some level of local flexibility in the application of uniform standards:

> “What we’re finding is that the policy itself is universal; we expect everyone to adhere to the same policy, but our compliance program is different in different parts of the world. In the U.S., it’s primarily employees who are expected to live up to their responsibilities, and we really don’t go looking, for the most part, for evidence of impropriety unless there’s something that causes us to suspect
something. We flip that on its head outside the U.S.; in certain locations, we spend a lot of time actively looking for evidence. The policy itself is fine, but the implementation and the compliance activities around it will be quite different in different regions.” (Director of Global Security, Petro 1)

**Social Alignment Risk Management Mechanisms**

Another aspect of aligning information security with the business is to develop a culture that embraces the value and importance of security. By promoting such cultural awareness, employees will be motivated to follow corporate security practices willingly rather than through tough control and monitoring practices: “Security groups who want to control everything will fail.” (IT Security Manager, ITProducts)

Similarly one of the interviewees from Petro 1 remarked:

“At the end of the day, when you think about what makes an information security program work properly, you can legislate, you can monitor for compliance, but as with a lot of things, you’re really counting on all of your employees and contractors to do the right thing in the situations they’re presented with.”

(Director of Global Security)

The social alignment mechanisms used by the firms in our research to align security from a social perspective fall into two categories—cultural and leadership. We identified three cultural mechanisms and one leadership mechanism (see Figure 3).

### Cultural Mechanisms

The first mechanism for establishing the required culture, used by all the firms we interviewed, is to deploy some type of formal security awareness training and educational program. The programs were varied in nature and included such techniques as web portals, newsletters, ad-campaigns, and security-awareness programs. These programs tend to be formal in nature and driven from the top down rather than in a more organic fashion.

The second mechanism is for security managers to develop their own informal networks. Our interviewees are very active and adept at forging strong relational ties with key organizational constituents and external partners. In contrast to top-down awareness programs, this activity is organic in nature as security managers and executives seek to build collaborative relationships with other key stakeholders on security-related issues.

### Figure 3: The Four Social Alignment Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Description</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cultural</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security awareness programs</td>
<td>Organizationally sponsored security awareness, training, and education programs.</td>
<td>To increase the overall awareness of information security and to improve compliance-related behaviors.</td>
</tr>
<tr>
<td>Informal networks</td>
<td>Information security personnel engage in boundary-spanning activities to develop close informal relationships with key stakeholders both internally (e.g., IT audit) and externally (e.g., security vendors).</td>
<td>To enhance the level of collaboration between information security and other key stakeholder groups. To improve knowledge sharing on security-related issues among organizational constituents.</td>
</tr>
<tr>
<td>Information security mentoring</td>
<td>The practice of providing informal consulting and advisory services to other areas of the company.</td>
<td>To create greater security awareness and buy-in and enhance the likelihood of organizational members seeking advice on security-related issues.</td>
</tr>
<tr>
<td><strong>Leadership</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive commitment</td>
<td>Senior management actively supports information security as a vital enterprise-wide function.</td>
<td>To establish strong organizational values regarding the importance of information security.</td>
</tr>
</tbody>
</table>
Prior research suggests that security managers may benefit from close, informal social networks in terms of enhanced communication, improved knowledge sharing, and a greater ability to solve complex security-related issues. Further, such networks lead to greater acceptance of security policies and, ultimately, the success of the security program:

“Social networks and relationships are critical to the success of our security program. In fact, I would argue the number one reason for my success is due to the relationships I have strengthened over the years. You cannot emphasize this enough as a requirement for success. Ultimately, everything eventually comes down to people following the rules or implementing the technology. If people trust you, they will follow the spirit of the policies. They will also start to take the initiative on security issues rather than waiting for the security group to dictate action by policy- or compliance-enforcement activities.” (IT Security Manager, ITProducts)

Our interviewees identified numerous social networks they had initiated both internally and externally. Internal networks typically involve information security personnel and groups such as IT audit, IT project teams, and other business units. Interviewees had also established external networks through such groups as the Information Systems Security Association, the Information Security Forum, and (for energy companies) the American Petroleum Institute. Participating in such networks enables security managers to hear how peer companies handle various security issues and, in the words of the Director of Global Security at Petro 1, to “validate when we may be out of alignment with our peers.” Firms also network informally through vendors and suppliers, and these relationships have provided excellent advice:

“We network when we go out and buy security products ... we have to talk to three different vendors, and, also, we have to have vendor references ... we contact the vendor references, and we network that way.” (Manager of IS Security, Retail 2)

The third cultural mechanism we identified is that security managers engage in a great deal of informal mentoring and advising. Such mentoring activity forms a significant part of their jobs and occurs organically; it is crucial to building organizational awareness of security issues. For example, Petro 2’s Security Architect indicated he spends about 50% of his time advising and consulting with internal stakeholders. Members of ITProducts’ security team stated that their primary role as a centralized corporate resource is to collaborate with and advise the rest of the organization on critical information security issues. A benefit of information security mentoring activities is that business partners are more likely to approach trusted mentors and advisors on vital security issues:

“Three years ago, we used to have hundreds of people fall for virus and phishing attacks. Now, when a new threat comes out, I get hundreds of people contacting me to make sure I’m aware of the situation. What a turn-around! We have had zero internal outbreaks this year.” (IT Security Manager, ITProducts)

The level of influence security managers have when mentoring others on security policy highlights the need to maintain separation between security policy-making and operations, to prevent abuses from occurring.

**Leadership Mechanism.** Senior executive commitment to information security is another crucial social alignment mechanism: “You’ve got to have the senior management or executive management backing as well as funding.” (Director of IT Security, Retail 1) This finding is consistent with research in the information systems field that links executive commitment to IS with the ability of organizations to align business and IT strategy. Executive leaders can demonstrate commitment in a variety of ways, including funding, allocation of human and financial resources, promotion of buy-in, and stressing the importance of security to other groups within the company.

One interviewee at ITProducts specifically mentioned that the support from the CIO and CFO had enabled the company to take a more proactive approach to information security. As a result, ITProducts’ security

---


group tended to be allocated a greater level of resources to invest in security personnel, awareness programs, and security-related infrastructure.

GUIDELINES FOR INFORMATION SECURITY MANAGEMENT

Organizations are faced with a dynamic information security environment characterized by constantly changing business requirements, technology risks, and legal compliance issues. Within this environment, they must plan to achieve the three competing objectives for a security strategy described earlier: balancing the security of information assets against the need to enable the business, ensuring compliance, and maintaining cultural fit. Firms that achieve these objectives will have a highly effective information security function and related strategy that is business driven and strategically focused. Our research has examined how companies achieve a strategically focused information security strategy and what such a strategy looks like in practice. From our findings, we have distilled five guidelines for information security management.

1. Determine the Appropriate Balance Between Enabling the Business and Protecting Information Assets

One of the primary tasks security managers face is to determine the balance between enabling the business and securing information assets. Over-protection through strict controls may inhibit business responsiveness, while lax controls may create unacceptable risks for information assets. As security managers seek to determine the optimum balance between these competing objectives, they must consider a multitude of factors, such as the organization’s culture and specific compliance requirements as well as certain information risk factors that are industry- or even firm-specific. The way in which they reconcile these two competing objectives may be idiosyncratic in nature and linked closely to specific contextual factors at the industry or firm level. The end result is that the security orientation may seem paradoxical and look considerably different from one company to the next, even for firms within the same industry.

A prime example is the different security orientations we observed at Petro 1 and Petro 2. The security manager at Petro 2 characterized the company’s orientation as “Deny by Default”—access to information was automatically denied unless a justifiable business case can be made for access. In contrast, Petro 1’s orientation was characterized as “Anytime-Anywhere,” meaning that users would automatically be given access to information provided it could be done safely. So while Petro 2 emphasized the relative importance of securing information assets, Petro 1 emphasized the opposite. In spite of these differences, both firms were judged to be among the most effective at information security.

This example illustrates a key point for security managers: what works for one company may not work for another. Since aspects of different firms’ security environments may be unique, their perceptions of the relative importance of enabling the business and protecting information assets may vary widely. Because of this, security managers should be cautious about adopting “out-of-the-box” security solutions and security practices from other organizational contexts without first examining their own combination of business, security risk, compliance, and cultural factors.

2. Use a Balanced Approach to Achieving Information Systems Security Objectives

Security objectives cannot be achieved through following a purely technically focused strategy. Instead, companies must adopt a balanced socio-technical approach that emphasizes equally the importance of technology and of the socio-organizational context as key elements of an effective security strategy. When pursuing their risk management strategies, security managers must be adept both at applying technology and also at applying organizational integration and social alignment mechanisms to ensure that information security aligns with the business organization and culture. The balanced socio-technical approach will result in the alignment crucial to facilitating convergent intentions, in shared understandings and in coordinated procedures between information security and other organizational constituents. The firms we studied clearly achieved alignment through multiple organizational and social alignment mechanisms targeted at numerous levels of the organization to mutually reinforce the mission, plans, and objectives of information security with the business.

20 Interviewees indicated that the respective cultures of Petro 1 and Petro 2 were a major factor in these different orientations.
21 We draw from Chan’s (2002) discussion of business-IT alignment to adapt to the context of information security alignment with the business organization.
3. Implement Formal Structures to Achieve Security Objectives

Companies must institute formal organizational structures to define decision-making rights and responsibilities for information security. Putting in place an information security organization, a top security executive (the CISO), and an internal audit function will help to facilitate the organizational integration needed to achieve security objectives. Further, these types of structures signal the importance of information security at the enterprise level. However, since all the security managers we interviewed reported to the corporate IT function, our results could potentially be biased in favor of this approach. Other types of formal structure appropriate to achieving security objectives may exist for firms where the security function doesn’t report to the IT unit.

4. Complement Formal Structures with Coordinating Mechanisms

While formal structures are important, our research suggests that, by themselves, they are not sufficient for achieving security objectives. The formal structures must be complemented by both coordinating structures and coordinating processes to facilitate decision making and communication among the different groups performing distinct tasks related to information security. More specifically, a range of coordinating structures and processes are needed to facilitate decision making and communication among constituents such as the CISO, IT audit, the CIO, senior management, and various other business managers. The firms we studied had developed well-defined coordinating mechanisms to complement their formal structures as a means of facilitating the level of integration needed to achieve security objectives.

5. Recognize the Importance of the Social Environment

Security managers and executives must recognize that a social environment conducive to security is vitally important to the overall security program. Developing a social environment through the application of social alignment mechanisms should therefore be a key element of any security strategy. However, we believe social alignment is one of the most overlooked aspects of security and also one of the most challenging and elusive to accomplish. Part of the challenge is that social alignment is a multi-faceted activity achieved through both formal organizational programs and informal organic mechanisms.

The primary formal social alignment mechanism we identified was organizationally sponsored security awareness programs. All the firms we studied had such programs and used a wide range of tactics to build awareness among organizational members of the importance of information security.

Our interviewees suggested that informal social alignment mechanisms are equally important as formal awareness programs. Foremost among these is executive leadership. Those interviewed indicated top management was keenly aware of the importance of information security and very supportive and engaged in security initiatives. Such interest signals the importance of information security to the rest of the organization and helps to establish a strong value system surrounding security. The message conveyed to the firm’s stakeholders when they see top management championing the cause of information security may be as important a part of the firm’s security program as are the objectives, policies, procedures, and technologies.

Leadership is also important at the level of information security executives. Security executives must be business-savvy and have the social skills to interact with constituents both inside the firm and externally in boundary-spanning roles to build informal social networks. Forging such relationships provides a social framework for the mutual transfer of knowledge pertinent to security and for security professionals to mentor their business counterparts in sound security practices. Additionally, the social capital developed through such mentoring relationships is likely to result in business partners being more likely to approach security professionals for advice.

While technical skills are important, they do not appear to be the primary qualification for being an effective security executive.

23 Malone discusses the importance of coordinating mechanisms as a means to coordinating work among multiple organizational stakeholders. See Malone, T. W. “Modeling Coordination in Organizations and Markets,” Management Science (33:10), 1987, pp. 1317-1331.

24 The CISO of Petro 2 had a financial/accounting background. While not having technical expertise, he had access to others in the security team with deep technical knowledge.

CONCLUDING COMMENTS

There is no “silver bullet” for effective information security; no single technology or mechanism is
sufficient to ensure success. Rather, effective security is achieved holistically through the application of multiple organizational and social alignment mechanisms combined with competence in technology as part of an overall socio-technical strategic focus to information security. Because of the multi-faceted nature of this approach, information security executives and senior management alike should consider information security as a business issue—not a technical one. This focus underscores the importance of having business-savvy CISOs and senior managers who recognize the importance of a strategically focused enterprise-wide information security program. As security executives seek to develop such programs, they should focus on the application of the general management guidelines provided in this article. Given the context-specific nature of information security, these guidelines can be applied to ensure effective information security management in different organizational settings.

APPENDIX: RESEARCH METHODOLOGY

To achieve our goal of understanding effective information security governance practices, we chose to conduct field research through interviewing corporate IT executives and security managers from firms judged to be highly effective in their security programs. A specific interview protocol was designed to gain insights about features of the security strategy as well as specific organizational processes, structures, and social relationships that facilitated the security strategy. All companies in the sample had security managers reporting to the IT function.

The companies selected for the research were identified through the objective ratings of a third-party consultant to ensure they were effective in their approach to information security. The consultant’s rating was based on the degree to which each firm’s information security program was judged to be comprehensive in terms of having an overall security strategy and top management support. As a secondary measure of effectiveness, we relied on self-reported data from the security executives interviewed. All respondents were relatively satisfied with the effectiveness of their security programs using “a lack of reported incidents” as their primary metric. Finally, we selected mostly large, complex organizations in the belief that such organizations would have fairly mature information security functional groups.

As the table on the next page shows, we interviewed one or more people from 11 organizations, 5 of which were Fortune 100 companies and 3 Fortune 500 companies.

ABOUT THE AUTHORS

Tim Kayworth

Tim Kayworth (timothy_kayworth@baylor.edu) is Associate Professor and Department Chair of Information Systems at Baylor University’s Hankamer School of Business. His research focuses on understanding the role, value, and governance of information technology in organizations. His work has been published in MIS Quarterly, Journal of Management Information Systems, European Management Journal, DATABASE, and other leading MIS journals and conferences.

Dwayne Whitten


---

26 A full list of interview questions is available by request from the authors.
27 There is some evidence indicating cyber security incidents might go unreported or at least under-reported. See Predictions for Security and Privacy Report, Aberdeen Group, January 7, 2003.
### Description of Participating Organizations and Managers Interviewed

<table>
<thead>
<tr>
<th>Organization Type</th>
<th>Organization Pseudonym</th>
<th>Participant Titles</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fortune 100 Companies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Services</td>
<td>FinServ</td>
<td>• Security Director</td>
</tr>
<tr>
<td>Petroleum</td>
<td>Petro 1</td>
<td>• Security Lead to Global Operations Services Group</td>
</tr>
<tr>
<td>Petroleum</td>
<td>Petro 2</td>
<td>• Security Standards and Controls Manager</td>
</tr>
<tr>
<td>Food Distribution</td>
<td>Distribution</td>
<td>• Director of Security</td>
</tr>
<tr>
<td>Technology Services</td>
<td>TechServ</td>
<td>• Chief Privacy Officer</td>
</tr>
<tr>
<td><strong>Fortune 500 Companies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware Manufacturing</td>
<td>ITProducts</td>
<td>• IT Security Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Security Architect</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IT Auditor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Network Security Manager</td>
</tr>
<tr>
<td>Clothing Retailer</td>
<td>Retail 1</td>
<td>• Director of IT Security</td>
</tr>
<tr>
<td>Clothing Retailer</td>
<td>Retail 2</td>
<td>• Director of Data Center Operations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manager of IS Security and Quality Assurance</td>
</tr>
<tr>
<td><strong>Other Companies</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology Consulting</td>
<td>TechConsult</td>
<td>• Director of Technology Advisory Services</td>
</tr>
<tr>
<td>Oilfield Services</td>
<td>OilServ</td>
<td>• Security Operations Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Global Operations Manager - Information Security</td>
</tr>
<tr>
<td>Gas and Oil</td>
<td>Energy</td>
<td>• Information Security Manager</td>
</tr>
</tbody>
</table>