Framing Security as a Governance and Management Concern: Risks and Opportunities

Julia H. Allen

October 2006

ABSTRACT: This article briefly describes six "assets" or requirements of being in business that can be compromised by insufficient security investment. Conversely, adequate security investment can reduce risk and create business opportunity. The article closes by describing barriers that must be overcome when forming security governance and management programs.

INTRODUCTION

Although security investment justifications typically focus on the negative consequences of realized security risks, organizations should consider how investing in security can help them to

- enable new and improved types of products and services
- improve market and brand position by being known as a trusted partner and a trusted provider of products and services
- communicate with customers in a reliable, cost-effective, timely manner
- conduct transactions with greater integrity and privacy, thus ensuring business throughput, customer satisfaction, and customer confidence, which can help to create and sustain customer loyalty
- enable new types of customer/supplier engagement, including more timely and reliable value- and supply-chain interactions
- provide more secure access to enterprise applications by internal and external staff

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

AREAS OF RISK AND OPPORTUNITY

Certain intangible business assets are particularly at risk of compromise due to insufficient security investment. Conversely, adequate security investment in these areas can create business opportunity.

Asset #1: Trust

Achieving and preserving trust are essential goals of security governance and management. Regarding trust, Larry Ponemon writes that

> *The trusted enterprise is an organization embracing a set of corporate values and behaviors that guide all business practices. It is a highly ethical organization that treats its customers, employees, partners, and shareholders with respect and stewardship. The CEO and board are deeply engaged in managing the organization's operating risk in a way that delivers maximum value in a safe and secure environment*
>
> *Dan Geer states*
>
> > *<a data-cke-saved-href="/articles/best-practices/governance-and-management/governance-and-management-references" href="/articles/best-practices/governance-and-management/governance-and-management-references" wp1012337"="">The central truth is that information security is a means, not an end. Information security serves the end of trust. Trust is efficient, both in business and in life; and misplaced trust is ruinous, both in business and in life. Trust makes it possible to proceed where proof is lacking. As an end, trust is worth the price. Without trust, information is largely useless [Geer 04].*

Trust has many meanings: protecting customers, employees, and their information; protecting market share; sustaining market and customer confidence; preserving reputation; and enhancing brand. Trust is hard to build and easy to lose in the face of a public breach of security or customer privacy. Just consider organizations that have made headlines when their customer databases were compromised, raising widespread concerns about identity theft. Some are finding that regaining lost trust may not be possible.

Asset #2: Stakeholder Value

Every organization survives and thrives by creating value for and satisfying its stakeholders. Value is created, preserved, or eroded by leadership decisions and actions, ranging from strategy to day-to-day operations.

Stakeholders may include customers, employees, shareholders, partners, suppliers, vendors, consultants, investors, rating agencies, governments (local, state, and national), surrounding communities, citizens, and other communities of interest such as regulators, certifying bodies, and professional associations. From the perspective of enterprise security, stakeholder interests are likely to include

- accurate reporting of the returnbs, effectiveness, and productivity of the enterprise
- creation, preservation, and enhancement of the organization's reputation

- availability and reliability of services (business continuity, business resilience)
- demonstrated due diligence with respect to protecting against malicious attacks (internal and external) and accidents that can be anticipated
- ensuring only authorized access to enterprise information
- protecting the privacy of stakeholder information

As one example of investing in security to reduce risk and create opportunity, Barclays Bank in England "is purchasing antivirus software for all 1.6 million of its online banking customers. The software will update automatically once it is installed. The bank also plans to deploy a text-messaging system to inform customers when funds are transferred with the use of their online banking details." This is a good example of using security as a marketing tool to build customer confidence. It also demonstrates how investing in security can cut costs. "Over time, the cost of implementing these measures will probably be recouped from the time and resources that might otherwise have been spent in dealing with security breaches" [SANS 06].

Asset #3: Ethics and Duty of Care

To fulfill their duty of care under current U.S. regulations, leaders must exercise a level of care that a reasonably prudent and careful person (including a leader of a similar organization) would have used under similar circumstances. Negligence is defined as the failure to do so [Westby 04], [Braun 04]. Leaders who make their decisions with due care, in good faith, and without conflict of interest may receive protection for these decisions under a judicial principle called the Business Judgment Rule. Taking effective and demonstrable action to protect critical information assets is a way for leaders to demonstrate that they are acting in a reasonable manner.[1]

But fulfilling a duty of care is not necessarily enough. Given the growing marketplace demands for integrity, transparency, and responsible oversight, demonstrating ethical and socially conscious behavior is becoming a required core competency for many organizations. Organizations must safeguard customer

---

[1] The standard of what is reasonable evolves as organizations become more aware of the issues and establish controls (i.e., as the practice becomes more mature). The evolution of what constitutes prudent or acceptable behavior argues for organizations to revisit their decisions about risk and deployed controls periodically to ensure that they continue to achieve and maintain an acceptable level [Gerdes 05].

data and use information, systems, and networks in a way that satisfies widely agreed-upon expectations. These expectations are established by social norms, obligations, norms for responsible Internet citizenship, and enterprise and professional codes of ethical conduct.[2]

Policies describing ethical use of information need to address ownership, privacy, and the potential risks to an enterprise and its stakeholders. Stakeholders are becoming more educated, understanding the extent to which their action or inaction may harm others, comprehending the consequences of unethical behavior, and demanding that the legitimate interests of others be respected.

It may be useful for an organization to view its computing networks as the organization's nervous and circulatory systems, with information as the lifeblood that is created, transmitted, and stored in these systems. Useful questions to ask[3] include

- What responsibility does an enterprise have for protecting the information in its computer systems, particularly information that belongs to others?
- What responsibility does an enterprise have to keep its information systems from being used to harm others?
- What are the organization's worst-case scenarios for security and information compromise? Most likely scenarios?

As these questions are answered and formally documented, they help define a minimum standard of due care that serves to establish, at any point in time, a definition of an adequate or appropriate level of enterprise security.

Asset #4: Compliance and Legal Liability

Enterprise-wide security governance can help an organization comply with new laws and regulations and avoid legal liability related to statutory or common law. Failure to protect stakeholder interests with respect to certain categories of information or failure to prevent unauthorized access to personal information may have serious legal consequences.

---

[2] The Open Compliance & Ethics Group (OCEG) defines voluntary boundaries as those selected by management, including public commitments, organizational values, contractual obligations, and other voluntary policies. They define mandated boundaries as those established by external forces including laws and government regulation [OCEG 08].

[3] Informed by "An Emerging Information Security Minimum Standard of Due Care" [Braun 04].

Relevant Laws and Regulations

The following U.S. laws, along with many others, must be considered when addressing security at governance and management levels. They provide regulatory incentives for leaders to pay closer attention to the subject:

- the U.S. Public Company Accounting Reform and Investor Protection Act of 2002 (also known as Sarbanes-Oxley (SOX)), mandating expanded public-company financial-control audits, including information security as it relates to the financial reporting process
- the U.S. Federal Information Security Act (FISMA) of 2002, ensuring the effectiveness of information security controls over information resources that support federal operations and assets
- the U.S. Gramm-Leach-Bliley Act (GLBA) of 1999, protecting personal information for financial-institution customers
- the U.S. Health Insurance Portability and Accountability Act (HIPAA) of 1996, protecting personally identifiable health information held by certain entities
- the California Database Protection Act (CA Senate Bill 1386) of 2002, requiring organizations to notify any resident of California if their personal information has been, or may have been, accessed illegally
- the U.S. Federal Trade Commission Standards for Safeguarding Customer Information of 2002 specifies expected data privacy standards; failure to comply may constitute unfair trade practice [Aguilar 06], [FTC 02]

According to Orson Swindle, former commissioner of the U.S. Federal Trade Commission,

> *We're going to probably see a broadening or extension of the safeguard rule in the Gramm-Leach-Bliley Act to cover a significant number of organizations that handle sensitive information but that aren't financial services institutions. There is a new awareness that personal information is very valuable, and it needs to be protected whether we're talking about a financial institution or a university or a shoe store [Scalet 06].*

SOX, more than any other current legislation, has had the greatest influence on security governance. (See also [Brown 05].) This is because the statute makes leaders of public corporations responsible for establishing and maintaining adequate internal controls.

SOX does not specifically address information security requirements, but security has emerged as a critical foundation for SOX compliance. The following SOX provisions have security implications:

Section 302: The CEO and CFO must certify the accuracy of financial statements. Financial data must be accurate and complete.

Section 404: The CEO, CFO, and auditor must attest to the effectiveness of internal controls. Companies must protect, monitor, and report on the effectiveness of controls.

Section 409: Companies must disclose material changes to financial conditions on a real-time basis. They must spot breaches or deviations that potentially signal a material change.

Section 802: Companies must retain and protect audit records. They must ensure records are available and unaltered as dictated by corporate policy. Companies must adopt proper security measures to ensure compliance with these provisions.

A similar security-boosting effect derives from California Senate Bill 1386,[4] Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) of 2006, and European Union (EU) Directives on data protection and privacy and electronic communications, which are affecting multi-state and multi-national organizations, respectively [CRS 05].

In the government arena, the U.S. Office of Management and Budget (OMB) has made eliminating vulnerable systems in government and for government contractors a direct responsibility of senior executives. The OMB demands immediate periodic reporting from all agencies on the security-configuration requirements they are implementing and the extent of implementation.

With these new regulations in place, an IT-centric approach to security without adequate governance can lead to omissions or commissions that, if pervasive or critical, can be considered significant deficiencies. When key internal controls,[5]

---

[4] Since the ChoicePoint data compromise of March 2005, over 30 U.S. states have enacted customer security breach notification laws [PIRG 06, CML 06]. In May 2006, The US House of Representatives Judiciary Committee approved the Cybersecurity Enhancement and Data Protection Act of 2006. If it becomes law, failing to inform the FBI or Secret Service of a security breach that affects 5,000 or more individuals would be "punishable by up to five years in prison" [Kaplan 06]. In June 2006, 12 industry leaders, as part of the Consumer Privacy Legislation Forum, lent their public support for congressional action to create a national consumer privacy law [CDT 06].

[5] "Over the decades, the U.S. Securities and Exchange Commission (SEC) has ruled that internal controls include policies, procedures, training programs, and processes other than financial controls. The SEC has clearly defined internal controls to include the 'safeguarding of assets against unauthorized acquisition, use, or disposition'" [Tarantino 04].

including financial controls, are affected or the organization has failed to correct significant IT-security control deficiencies identified in the preceding year (such as in patch management), management may have to make a formal statement of "material weaknesses" [IIA 05].

Litigation Risks

Compliance issues related to legislative and regulatory programs (and the criminal and civil liabilities that can arise from violating them) are only one part of legal-liability exposure. Significant liability also can result from national and state court litigation claims based on a breach of contract, tort, or property rights. Civil litigation, in which private parties bring causes of action before the courts, provides an effective platform to promote computer security. Moreover, cyber security and critical-infrastructure strategies issued by the U.S. federal government in 2003 help "establish standards of security conduct and accepted notions of security risk that are likely to be applied in civil litigation" [Matsuura 03].

Governing and managing for enterprise security reduces the likelihood of legal action by ensuring that the accountability framework and necessary level of oversight are in place for

- the informed selection and implementation of effective security controls
- their application to information and information systems
- regular reporting on the effectiveness of these controls

Using this approach, security controls can be adequately identified, architected, implemented, and tested in conjunction with all other internal controls and in concert with both internal and external audits. In our experience, this is the most effective path for mitigating risks associated with the liability exposures described here.

Asset #5: Customer and Partner Identity and Privacy

Concerns about the risks associated with personal privacy and identity are growing. Violations of these and their constituent costs, legal consequences, and effects on organizations and individuals are regularly reported in the media. According to Privacy Rights Clearinghouse, a non-profit consumer organization, over 88 million people have had their personal information placed at risk since the ChoicePoint data breach in February 2005. They identify more than 100 cases reported in 2005 and more than 130 as of July 2006.

As stated in the Citadel report "An Emerging Information Security Minimum Standard of Due Care,"

A business that obtains consumers' personal information has a legal duty to ensure that the use and handling of that data complies in all respects with representations made about the company's information-security and privacy practices [Braun 04].

A recent poll of 1150 adults conducted by the Cyber Security Industry Alliance reports the following:

- Only 44% of respondents feel their information is safe when engaging in e-commerce.
- 50% avoid making purchases online because they are afraid their financial information will be stolen.
- Only a third (34%) say banking online is as safe as banking in person.
- 94% say identity theft is a serious problem.
- Only 24% say businesses are placing the right emphasis on protecting information systems and networks.

As identity theft and related privacy violations become more prevalent, public backlash from consumers and legislators could be significant. Increasingly, consumers and business partners expect a certain level of standard security practice to be in place in any competent organization. This expected level of standard practice will likely continue to escalate.

However, reputation need not be considered solely in negative terms. Leaders should also ask, "How much is it worth for us to be seen by our customers and business partners to be actively concerned with safeguarding their information?" Proactive approaches to security can enhance an organization's reputation as a trusted partner.[6]

Nearly all organizations collect, process, store, disseminate, and transfer customer information in some form, most likely digital. Protecting this information and preventing actions that can cause unintended disclosure and abuse are increasingly required to meet legal standards and preserve customer trust. Given the business implications, a comprehensive information security program should be implemented and managed enterprise-wide.

---

6 Charette, Robert. Review comments to [Allen 05], June 2005.

Asset #6: Ability to Offer and Fulfill Business Transactions

The Internet has equalized access to information worldwide. Risks and opportunities increasingly derive from who you are connected to and who is connected to you rather than from where you are physically located. Today's marketplace is driven by consumers. They have ready and direct access to those with whom they wish to transact business, and they can change their choices for any reason and at any time. Sometimes the needs and requirements of consumers are different from, or even at odds with, the needs of the business.

An organization's ability to competently offer and fulfill business transactions is most visible to the customer. Making items easy to find quickly and conveniently, with accurate and competitive pricing, immediate order confirmation, and timely delivery contributes to the growth of Internet-based business.

Correspondingly, vendors and suppliers in an organization's supply chain are becoming increasingly dependent on Internet-based communication and transactions conducted through web applications, electronic data interchange, and email.

Information security is to the economy of tomorrow what contract law is to the economy of today. It extends trust and thus enables economies to expand. A robust economy is one in which transaction costs-discovery, negotiation, arbitrage, settlement, and adjudication-are, in the broadest sense, low. The Internet and the electronic commerce it enables have low transaction costs compared with their predecessors. However, the nature of electronic communication is that it is location-independent, essentially instantaneous, and-unless modified-anonymous [Geer 04].

This is another example of the opportunity and risk inherent in transacting business on the Internet. A security-conscious organization considers all aspects of its transaction-handling processes as part of its approach to enterprise-security governance and management.

BARRIERS TO CONSIDER

Several pervasive barriers can make enterprise security a daunting undertaking that requires tenacity and perseverance. When effectively overcome, these barriers can also represent opportunities that may reduce the potential for loss, preserve and enhance business value, and create marketplace advantage.

Continuous Effort and Investment

Security is hard, often annoying, and something most people and organizations would rather not deal with. There are formidable disincentives to addressing security at more than just a tactical, technical level. As a networked community, we don't fully understand what it means to put an effective security program in place, and there are currently no reliable measures and benchmarks for knowing if we've done enough.

Achieving a particular state of security is no guarantee that it can be sustained. Security is not a one-time project with a beginning and an end. It requires continuous improvement comprising planning, executing ("doing"), checking the results, and then taking further action (see Plan, Do, Check, Act). Continuous improvement requires attention and investment, and security investments often come at the expense of something else in terms of accounting and economic opportunity.

Enterprise-Wide Scope

Attending to security at the enterprise level is often hard to justify. For those responsible for security, it is often difficult to persuade senior leaders of the need to implement enterprise security in a systemic way. For most organizations and people, security is an abstract concept, concerned with hypothetical events that may never occur. In this respect, it often has some of the same characteristics as insurance.

Security cannot be contained or delegated to a specific function or department within an organization. Although many have treated it as such, missing constituent elements of people and process, security is not just a technical problem. Many functions and departments within the organization need to interact to create and sustain an effective security solution that includes strategic, technological, organizational, regulatory, economic, and social considerations. This includes making sure security is adequately addressed during the requirements, design, and development of any software-based system, rather than waiting until the system is deployed.

Intangibility

Security is sometimes described as an emergent property of networks and the organizations they support. What this means is that the precise location where security is enacted cannot be identified, as its condition is often reflected in the intersections and interactions of people, process, and technology. As the organization and the underlying network infrastructure change in response to the changing risk environment, so will the security state. Effective security can be

thought of as an attribute or characteristic of an organization. It becomes evident when everyone gets involved, creating a culture of security that displaces ignorance and apathy.

No Consistent Practice or Measures

There are no widely accepted (de facto or de jure) standards of best practice (with the possible exception of ISO 17799 [ISO 05a]) or security performance measures. However, a growing number of guidelines and checklists identify practices that are considered acceptable by most professionals, thus passing the test of reasonable practice.

Unfortunately, these guidelines are frequently not applied, or even consulted. The Internet's security state today is far worse than it would be if generally accepted practices were properly deployed to address known problems. This shortfall is evidenced by the number of vulnerabilities reported to the CERT Coordination Center (CERT/CC), many of which have known solutions that have not been implemented. This is particularly alarming for national critical infrastructures such as telecommunications, transportation, banking and finance, and electricity, oil and gas, and water distribution. Clearly, the existence of accepted sets of good practices and metrics does not guarantee widespread use.

Cost/Benefit not Easily Quantifiable

Actions taken to secure an organization's assets and processes are typically viewed as disaster-preventing rather than payoff-producing (again, like insurance), which makes it difficult to determine how best to justify investing in security, and to what level.

The benefits of investing in security are often seen only in events that do not happen. As it is impossible to prove a negative, what value does an organization place on cost avoidance? This difficulty has dogged not only security but also efforts to improve software quality, conduct proper testing, keep documentation up to date, maintain current configuration and hardware/software inventory records, etc. [Braithwaite 02]. Unlike insurance, where the causes of loss are essentially known or change very slowly, the nature of what is considered a security threat and the number and type of vulnerabilities affecting information and systems are constantly evolving and changing.

Perceived Impediments to Productivity

Furthermore, security safeguards are often seen as having negative consequences such as added cost; diminished application, system, and network performance; and user inconvenience (for example, multiple means for authentication that

change regularly and are hard to remember). "While internal auditors often identify vulnerabilities within a business system, their recommendations for more stringent system controls are in many cases overruled because of direct costs of implementing and maintaining those controls or because they introduce unwelcome inefficiencies" [Taylor 04a].

This situation is difficult to improve without a significant increase in the reporting of incident cost/loss metrics to estimate probable losses that would have occurred had steps not been taken to reduce risk exposure. Such metrics are analogous to insurance actuarial data, which provides a statistical basis for estimates of loss [Gerdes 05].

CONCLUSION

In short, security is hard to define and implement. Security is not supported by a universally accepted standard, can be seen as having negative impacts such as cost and inconvenience, and is usually seen as-at best-a way to avoid disaster or business impact (cost) rather than a way to provide benefit and competitive advantage.

An effective approach to governing and managing enterprise security must confront these barriers head-on, offering counterpoints and benefits to anticipate and offset each barrier. Increasing awareness, knowledge, and understanding of security is a necessary first step toward changing common beliefs. This includes framing the security value proposition to include risk and opportunity.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120