How Much Security Is Enough

Julia H. Allen

November 2009

ABSTRACT: Updates to this material are, in part, either adapted or excerpted from Software Security Engineering: A Guide for Project Managers [Allen 2008].

This article provides guidelines for answering this question, including strategy questions to ask, organizational and market characteristics to take into account, and means for determining adequate security based on risk. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken.

INTRODUCTION

One question you will have to answer prior to selecting which security governance and management actions to take and in what order is "How Much Security Is Enough?" This article provides guidelines for determining what strategy questions to ask, determining your definition of adequate or acceptable security, and using these as inputs for your security risk management framework. It is important to make sure that leaders understand the residual risk that remains after mitigating actions are taken, in their language.

Refer to the BSI Risk Management content area and Deployment & Operations, Risk-Centered Practices for implementation details, in addition to other sources cited in this article.

WHAT SECURITY STRATEGY QUESTIONS SHOULD I BE ASKING?

Achieving an adequate level of security means more than complying with regulations or implementing commonly accepted best practices. Each organization must determine its own definition of "adequate." The range of actions an organization must take to reduce security risk to an acceptable level depends on the value at risk and the consequences (impact) if the risk is realized.

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

Consider the following questions from an enterprise perspective. Answers to these questions aid in understanding security risks to achieving organizational goals and objectives as well as project goals and objectives.

- What is the value we must protect? Value can be expressed as a product or service, process, or relationship.
- To sustain this value, what assets must be protected? Why must they be protected? What happens if they're not protected? Assets may include information, technology (hardware, software, and systems), facilities, and people.
- What potential adverse conditions and consequences must be prevented and managed? At what cost? How much disruption can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?
- How do we integrate our answers to these questions into an effective, implementable, enforceable security strategy and plan?

Clearly an organization cannot protect and prevent everything. Interaction with key stakeholders is essential to determine the organization's and project's risk tolerance and its resilience to impact if risk is realized. In effect, security in the context of risk management involves determining what could go wrong, the likelihood of such events occurring, the impact if they do occur, and actions to mitigate or minimize both the likelihood and the impact to an acceptable level.

The answers to these questions can help business leaders and project managers determine how much to invest, where to invest, and how fast to invest to mitigate security risk, including software security risk. In the absence of answers to these questions (and a process for periodically reviewing and updating them), leaders will find it difficult to define and deploy an effective security strategy and thus may be unable to effectively govern and manage enterprise, information, and software security.[1]

---

[1] Refer to Managing Information Security Risks: The OCTAVE Approach [Alberts 2002] for more information on managing information security risk; “An Introduction to Factor Analysis of Information Risk (FAIR)” [Jones 2005] for more information on managing information risk; and “Risk Management Approaches to Protection" [NIAC 2005] describing risk management approaches for national critical infrastructures.

CHARACTERISTICS TO CONSIDER

By evaluating how much and in what ways their enterprise depends on Internet connectivity, IT infrastructure, and digital assets (including secure applications) for business performance and continuity, security-conscious leaders can better determine the degree to which governance and management decisions should take the security of such assets into account.

In Harvard Business Review, Nolan and McFarlan [Nolan 2005] recommend that organizations first determine their defensive IT stance ("how much the company relies on cost-effective, uninterrupted, secure, smoothly operating technology systems") and then their offensive IT stance ("how much the company relies on IT for its competitive edge through systems that provide new value-added services and products or high responsiveness to customers"). These stances apply to information and software security as well.

Additional factors that can aid in making informed decisions are described below.[2] Together with a comprehensive risk assessment, an aggregation of these factors can form a repeatable basis for security-investment decisions.

Organization Characteristics

- Size (number of physical locations, employees, and customers; level of revenue)
- Complexity (organizational units, products, services, processes, systems, structure-for example, centralized or decentralized, co-sourcing and outsourcing relationships, external supply-chain partners, domestic and global)
- Value and criticality of the organization's intellectual property, particularly information stored or transmitted in digital form
- Dependence on IT systems (including secure applications) and the Internet to offer products and services to customers
- Impact of system downtime or disrupted Internet connectivity on the organization
- Impact of system, administrative, or transactional errors on the organization
- Degree and rate of change within the organization (expansions, mergers, acquisitions, divestitures, new markets, etc.)
- Dependence on multinational operations

---

[2] These factors in large part derive from [CGTF 2004], Appendix D, and work performed by TechNet.

- Plans for transnational operations (internal functions transferred offshore or outsourced to offshore locations, geographical expansion into areas representing increased revenue)
- Stakeholder and shareholder expectations regarding the protection of organizational value, reputation, and brand

Market Sector Characteristics

- Potential impact to national, international, or critical infrastructures as a result of outages or interruptions in organizational systems
- Customer sensitivity to and expectations for security and privacy
- Level of sector regulation that pertains to security
- Potential brand and reputation damage of a publicly disclosed security incident or violation of customer privacy
- Extent of enterprise operations that depend on third parties (partners, contractors, suppliers, vendors) and connectivity with third-party networks
- Customers' ability and likelihood to quickly switch to a competitor, based on the competitor's ability to offer more secure, reliable services
- Extent to which the organization does business in a geographically or politically sensitive area where it could be a likely target of damaging physical or cyber attack

DEFINING ADEQUATE SECURITY

Determining adequate security is largely synonymous with determining and managing risk. Where possible, an organization can implement controls that satisfy the security requirements of its critical business processes and assets. Where this is not possible, security risks to such processes and assets can be identified, mitigated, and managed at a level of residual risk that is acceptable to the organization.

Adequate security is defined as

> *The condition where the protection and sustainability strategies for an organization's critical assets and business processes are commensurate with the organization's tolerance for risk. [Allen 2005]*

Protection and sustainability strategies include principles, policies, procedures, processes, practices, and performance indicators and measures, all elements of an overall system of controls.[3]

An asset is anything of value to an organization. Assets include information such as enterprise strategies and plans, product information, and customer data; technology such as hardware, software, and IT-based services; supporting facilities and utilities; key personnel with unique knowledge and skills; and items of significant yet largely intangible value such as brand, image, and reputation. Critical assets are those that directly affect the ability of the organization to meet its objectives and fulfill its critical success factors [Caralli 2004a]. The extent to which software is the means by which digital assets are created, accessed, stored, and transmitted provides one compelling argument for ensuring that such software has been developed with security in mind.

A process is a series of progressive and interdependent actions or steps by which a defined end result is obtained. Business processes create the products and services that an organization offers and can include customer relationship management, financial management and reporting, and management of relationships and contractual agreements with partners, suppliers, and contractors.

Risk Tolerance[4]

An organization's tolerance for risk can be defined as ". . . the amount of risk, on a broad level, an entity is willing to accept in pursuit of value (and its mission)" [COSO 2004]. Risk tolerance influences business culture, operating style, strategies, resource allocation, and infrastructure. Risk tolerance is not a constant; it is influenced by and must adapt to changes in the environment.

Defining the organization's tolerance for risk is an executive responsibility. Risk tolerance can be expressed as impact (potential consequences of a risk-based event), likelihood of a risk's occurrence, and associated mitigating actions. For identified and evaluated risks, risk tolerance could be defined as the residual risk

---

[3] A system of internal controls often includes categories such as administrative, technical, and physical as well as directive, preventive, compensating, detective, and corrective [CERT 2009].

[4] Alternatively, Moulton and Coles [Moulton 2003] define enterprise pain threshold as “The financial or other indicator point at which the executive management of the enterprise will, or should, know that the loss or damage caused by an event, including a control failure related to loss limitation or mitigation for the event, would be of sufficient magnitude to put the enterprise at risk; and, could consequently result in their being held personally accountable by shareholders and/or regulators.”

the organization is willing to accept after implementing risk-mitigation and monitoring processes [Allen 2005].

Risk tolerance can be expressed both qualitatively and quantitatively. One way is to define high, medium, and low levels of risk. An example is a policy to take explicit and prioritized action for high- and medium-level risks and to accept (monitor) low-level risks as the default condition.

So how does the organization manage different levels of inherent and residual risk? How does an organization prioritize risks that require mitigating actions? In quantitative terms, what "value at risk" is acceptable [Allen 2005]?

Example

A retailer decides to enter the e-commerce marketplace but has a low risk tolerance relative to its relationship with existing customers, particularly with respect to fulfilling orders promptly and accurately. To protect these relationships, management allocates necessary resources (people, processes, technology) to ensure that

1. order-to-delivery response times meet or exceed defined targets and
2. order-fulfillment accuracy meets or exceeds defined criteria.

Management is now conducting business online and has installed the resources needed to protect its reputation for timely and accurate fulfillment of customer orders. It has set a target for delivery within seven days of accepting orders and has guaranteed delivery within two weeks by a statement on its Web site. However, how much variation is management willing to tolerate with respect to delivery and order-accuracy targets? Is a five-day average variance around the delivery target too much (based on the value placed at risk (customer relationship) and the magnitude of any impact (lost sales))? The delivery targets and level of variation around these are the risk tolerances [Allen 2005].

DETERMINING ADEQUATE SECURITY

With the benefit of this description, a useful way to address the question "How much security is enough?" is to first ask "What is our definition of adequate security?" by exploring the following more detailed questions:

- What are the critical assets and business processes that support achieving our organizational goals? What are the organization's risk tolerances, in general and with respect to critical assets and processes?

- Under what conditions and with what likelihood are assets and processes at risk? What are the possible adverse consequences if a risk is realized? Do these risks fit within our risk tolerances?
- In cases where risks are beyond these thresholds, what mitigating actions do we need to take and with what priority? Are we making conscious decisions to accept levels of risk exposure and then effectively managing residual risk? Have we considered mechanisms for sharing potential risk impact (for example, through insurance or with third parties)?
- For those risks we are unwilling or unable to accept, what protection strategies do we need to put in place? What is the cost/benefit or return on investment of deploying these strategies?
- How well are we managing our security state today? How confident are we that our protection strategies will sustain an acceptable level of security 30 days, 6 months, and a year from now? Are we updating our understanding and definition of our security state as part of normal planning and review processes?

Example[5]

One of Acme, Inc.'s critical assets is the customer-transaction database, which includes order history. This is used in targeted marketing and sales processes with exceptional results (repeat sales). It has taken three years of staff effort to build and populate this database at an estimated cost of USD $1 million. Ongoing operations and maintenance costs including the protection strategies described below are USD $200,000 annually.

There are specific events, impacts, and consequences that Acme needs to manage and prevent to the extent possible. Competitors regularly attempt to obtain access to this information or to obtain a copy of this information (high risk). Management is sensitive to the risk of disclosure by sales and marketing staff who are approached by competitors to share this information for personal financial gain (medium risk). Third-party attackers have threatened to obtain access to and disclose this information on the Internet (low risk). While Acme believes it offers superior service, creating customer loyalty in the face of competitive pressure to switch, it places the value at risk at USD $10 million.

---

[5] Moulton and Coles offer another example of "how the information security governance concept could be applied at the enterprise level to establish and maintain an adequate control environment" [Moulton 03].

Security requirements for the customer-transaction database include zero tolerance of unauthorized disclosure (violation of confidentiality), continuous validation of data integrity (by automated comparison with a trusted, securely stored version), and 99.999 percent availability (risk tolerances).

Protection strategies include

- principles enacted by policies and procedures that state these requirements and risk tolerances for this asset
- clear assignment of roles and responsibilities and periodic training for staff and managers involved in protecting this asset; financial incentives for those demonstrating innovative approaches to asset protection
- periodic training for staff having access to this asset; immediate removal of access and authorization for any staff member whose responsibilities no longer require a need for access, including any change in employment status such as termination
- infrastructure architecture that fulfills these requirements, meets these risk tolerances, and implements effective controls (strong authentication, firewalls including ingress and egress filtering, enforcement of separation of duties, automated integrity checking, hot backups, etc.)
- review of all new and upgraded technologies that provide database support and in-house and remote access, to determine if any of these technologies introduce additional security risks or reduce existing risks. Review occurs before and after technology deployment.
- regular review and monitoring of relevant processes, and performance indicators and measures including financial performance and return on investment; regular review of new and emerging threats and evaluation of levels of risk
- purchasing insurance for high-impact, low-probability events
- regular audit of relevant controls and timely resolution of audit findings

CONCLUSION

The level of adequate security as defined here is constantly changing in response to business and risk environments and the variation in risk tolerance that management is willing to accept. Effectively achieving and sustaining adequate security based on this definition is a continuous process, not a final outcome. As a result, processes to plan for, monitor, review, report, and update an organization's security state must be part of normal day-to-day business conduct, risk management, and governance-not a one-shot occurrence.

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