

Management Update: Eight Steps Needed to Define Reasonable Security

Gartner RAS Core Research Note G00129076, Vic Wheatman, Paul E. Proctor, 8 June 2005, R1637 06262006.

A recurring and deceptively simple question is, “How much security is enough?” The answer needs to be customized to each organization. No law defines due care in security. Eight elements should be considered, including the affordability of security technologies, procedures and techniques.

ANALYSIS

Achieving Compliance

Many laws and regulations adopted in the past decade impose information security requirements on companies and agencies. Some, such as the Health Insurance Portability and Accountability Act (HIPAA), California SB1386 and the European Union Privacy Directive, relate to consumer privacy, whereas others, such as the Sarbanes-Oxley Act, focus on the sanctity of data and systems for trusted record keeping and reporting. Security technology providers latch onto these requirements and promote their products and services as helping organizations become HIPAA-compliant, Sarbanes-Oxley-compliant and so forth. However, no certification exists to ensure that a product or service will enable an organization to achieve compliance.

Missing an Opportunity

Historically, enterprises have grudgingly responded to regulations, doing the minimum necessary. Gartner believes this approach means missing an opportunity.

- First, regulations attract management attention and can make budget processes somewhat easier. In fact, Gartner believes, based on our regular contact with clients, that regulatory compliance is being used to fund pet projects.
- Second, regulations should not be the focal point. Organizations should be executing effective risk management in any case because it is good

business. For example, they need to protect data about their customers as a key customer relations element: The loss of confidence for violating customer trust can result in lost revenue.

While incidents may not result in material fines, they may lead to loss of customer confidence, brand damage, lost revenue and stock price impact. In the worst case, a government finding that an organization did not appropriately protect itself may result in a corporate fine, individual liabilities for staff or executives, and, potentially, jail sentences. Further, the organization may be open to unlimited civil liability in the form of class action lawsuits.

Organizations should focus on doing what is right for the business regardless of the presence – or absence – of laws that seemingly suggest doing something different.

But What Is “Good Enough”?

The global legal community is searching for a standard definition for security. A recent publication by Baker & McKenzie titled “Trends in the Law of Information Security” examines three trends shaping the information security landscape: an increased recognition that providing information security is a corporate legal obligation; the emergence of a legal standard by which that obligation will be measured; and a new emphasis on a duty to disclose breaches of security.

The legal community has also been searching for the standards and associated qualitative best-practice and quantitative spending benchmarks by which they can measure (or litigate) whether a CIO is exercising “due care,” legally defined as “that level of care, skill, and treatment which, in light of all relevant surrounding circumstances, is recognized as acceptable and appropriate by reasonably prudent similar providers” – a term that in itself begs for a “standard.”

Most U.S. states have relied upon “The Revised Model Business Corporation Act” originally developed by the American Bar Association as a guideline for state government laws. It contains language requiring a corporation director to discharge his duties in good faith, with the care an ordinarily prudent person in a like position would exercise under similar circumstances, and in a manner he reasonably believes to be in the best interests of the corporation.

In discharging their duties, directors can rely on information, opinions, reports or statements, including financial statements and data, if prepared or presented by a person the directors reasonably believe to be reliable and competent.

The language of these guidelines attempts to define good faith, duty of care and the underlying business judgment rules. The phrase “with the care an ordinarily prudent person in a like position would exercise under similar circumstances” shows that the standard is not a fixed standard, but a relative one based on circumstances.

The standard of due care is, by definition, dependent on the circumstances and determined at the time of enforcement. The best way to attain it is to have visibility into what your peers are doing and develop good, measurable processes.

There is another consideration as to why laws do not attempt to define due care in security. Laws should only be guidelines or sets of requirements that must be met; they should not attempt to prescribe specific solutions or technologies. First, prescribing solutions for all cases is impossible, since the circumstances are so varied that no law could begin to anticipate them all. Second, IT changes so fast that what is an adequate solution today could be antiquated in just a year or two. Further, because the threat environment is changing, any definition of “good enough” is only temporary. Specificity has deliberately been left out of most regulations to accommodate such factors.

Organizations may use selection criteria, including the size, complexity and capabilities of a solutions provider. Cost can also be used as a criterion for selecting appropriate controls.

Most regulations are structured as requirements that must be met, and guidance may indicate a choice of general strategies or approaches that may be used to meet those requirements. They leave it to the implementers to decide the reasonable thing to do in a particular, real-world situation. But how does one decide what is reasonable?

Gartner now provides guidance on the issues organizations face in attempting to define “due care” for their specific circumstances.

1. The State of the Technology

Organizations need to examine the status of commercially available computer technology and, specifically, information security technology. There is a contrast to be made between security point solutions that address single vulnerabilities and those that address enterprisewide frameworks. Some vertical market sectors that rely on specialized IT business suppliers often find that those suppliers, reacting to a market that in the past has not strongly demanded security, have been slow in implementing the most recently available information security mechanisms. File protection is particularly weak in many systems.

2. The Expense

Organizations always need to assess the affordability of security technologies, procedures and techniques. Offsetting the expenses are the savings that would accrue from changing manual, paper-intensive processes to more efficient computerized, and sometimes automated, processes. Fuzzy, or soft, benefits will also result from better customer care and better information on which to make a variety of

decisions. The expense of not implementing security can be fines under various federal and state laws, legal costs and the costs of paying judgments in civil legal actions. There are further costs in the loss of business because customers lose confidence, as well as in lowered stock price.

3. Likelihood of Failure

Given the growing list of failures in systems, the likelihood of a technological security failure should be considered fairly high. Given the rapid movement to use Internet-related technologies (such as Web services) for risky applications, such as accessing computerized patient records, combined with the population of cybercriminals and the cybercurious wanting to use sensitive personal healthcare information for various intents, the chances of an intentionally caused failure are also high.

4. How Much Harm Can Result From Security Failure?

This can be measured in two fundamental ways: the harm caused to an individual whose private information is made public or used for identity theft or otherwise used to cause harm, and the harm caused to the organization through penalties, litigation and loss of confidence leading to loss of business. Can the harm mean potential civil liabilities, or is there potential for an enterprise to suffer in the marketplace through a lowered stock price as a result of a security problem, such as the loss of personally identified data? If an intellectual property theft occurs, what can be the potential costs? In many past cases, competitiveness has been shattered, critical bids have been lost, and valuable research (such as geophysical data gathered by a natural resources company) has essentially been stolen.

5. Known, Anticipated Security Threats

Organizations must continue to assume that the Internet is a hostile environment for sensitive information and that steps must be taken to protect that information. Unfortunately, organizations must also assume a certain degree of employee

motivation to steal and sell valuable information. Insider theft of corporate information is a huge source of loss. A large healthcare provider might consider employee motivation to sell patient lists to a marketing firm targeting certain types of patients or to tabloids wanting information on celebrities. A retailer must consider the possibility of identity theft by insiders. All organizations need to consider the motives of external threats, be they disgruntled former employees, industry espionage agents, or in the case of national governments, politically motivated hackers attempting harm on critical infrastructure.

It is important that an organization execute ongoing risk assessments that consider the value of corporate assets and the adoption rate of new technologies and business practices (such as outsourcing) to determine reasonably anticipated risks. The organization must use these assessments to help select risk mitigation measures.

6. Availability of Standards

Reasonable security in the absence of widely accepted standards is difficult, but the marketplace offers a confusing array of security-related standards. Some are for industry-specific transactions, such as electronic data interchange transaction sets. There are technical standards, such as Web Services Security, SSL (Secure Sockets Layer), S/MIME (Secure Multipurpose Internet Messaging Extension) and PGP (Pretty Good Privacy). Compounding the problem is the fact that while official standards may exist, they are not always uniformly commercially implemented, or they may be inconsistently implemented among vendors. Often, products use proprietary methods that may be accepted as de facto standards.

In the case of information security practice standards, the International Organization for Standardization's ISO 17799, called the "code of practice for information security management," the IT Governance Institute's COBIT (Control Objectives for Information and Related Technology) – an audit tool – and others each provide a framework resembling a standard for approaching due care in security. The market seems to be gravitating toward the ISO

standards because they offer a comprehensive outline for evaluating each element related to information security.

7. Best Practices

A definition of due care implies reference to what others are doing. An organization should at least do what its peers are doing – on average. Accordingly, it is important that security-responsible individuals participate in peer groups focused on security to share essential “war stories” and compare notes on solutions and approaches. This helps to create a defensible case for all audiences including internal and external auditors, regulatory enforcement bodies, and executives.

8. What Does the Auditor Say?

A part of the process of defining due care involves an auditor. Self-assessment is a useful information-gathering technique that can help determine the degree to which a chosen standard is being met, but self-assessment is not a credible way to determine what the standard is. An auditor’s opinion is a powerful statement lending credibility to a case that an organization has met the requirement for due care. There is no definitive assertion of what equals compliance; therefore negotiation with the auditor may be required. Calling for a second opinion when there is disagreement is an option.

Compliance auditors are focused on fixing controls, particularly around financial systems, to prevent management from overriding those controls. Identity and access management and logging elements

become important here, but Gartner has found inexperienced auditors requiring implementation of obsolete security solutions. In other cases, auditors have required actions beyond best practices to compensate for a control weakness or past failure somewhere else in the organization’s system. Ultimately, the auditor’s opinion is what matters most in determining that the organization is practicing due care and commercially reasonable security, ideally based on evidence that the organization has performed risk assessments to define reasonable security for its circumstances.

Bottom Line

- Organizations and agencies trading in sensitive personal or corporate information should determine the reasonableness of any evaluated security mechanism using the guidelines Gartner provides here.
- Not only is an environmental scan required to determine industry practices, but a strategic plan for security, with companion policies anticipating new risk factors and new requirements, must be developed.
- The definition of “due care” is specific to the organization.
- Nevertheless, the individuals responsible for the information security of their companies or agencies should recognize due care when they see it.