Abstract

Information security has traditionally been defined as “the preservation of confidentiality, integrity, and availability” (ISO/IEC 17799, 2000), abbreviated as C.I.A. This definition has been inherited from the definition of computer security, that dates back to the 1960’s when the primary concern was physical protection of mainframes (Whitman and Mattord, 2003). Since that time, organizations have experienced both a PC and an internet revolution, resulting in an evolved environment with new aspects of information security. This paper considers the expanded scope of information security, and then discusses why the C.I.A. definition does not adequately address the current scope. A new definition is proposed that is intended to increase both clarity and measurability of the concept of information security.

1. Introduction

Definitions lay the foundation of a research topic. They provide cognitive clarity and are essential for valid measurement of concepts under study (Locke, 2003). Information security has traditionally been defined as “the preservation of confidentiality, integrity, and availability” (ISO/IEC 17799, 2000). This definition has been inherited, nearly verbatim, from the definition of computer security, which also emphasizes ensuring the confidentiality, integrity, and availability (C.I.A.) of IS assets (e.g., NSTISSC, 2000; Pfleeger and Pfleeger, 2003). The C.I.A. definition was developed to address an environment characterized by (Whitman and Mattord, 2003):

- Mainframe computers housed in a centralized data center
- External hackers or saboteurs being the primary sources of computer breaches
- Military and government being the primary drivers of computer security standards

Both the business and technical environments of the early days of computer security have changed significantly. A revolution of personal computers led to a subsequent revolution of networking technologies, the Internet, and the resultant decentralization of
information and computing assets. Characteristics of this evolved environment, and their implications for information security, include:

- Employees are said to be responsible for an estimated 61% - 81% of violations to existing information security safeguards (Dhillon, 2001), calling into question the focus of information security on external hackers and unauthorized access.

- Legislation aimed at protecting privacy (HIPAA, Gramms-Leach-Bliley Act), ensuring ethical reporting of breaches (California 1386), and ensuring the integrity of financial reporting (Sarbanes-Oxley Act) are each associated with information security (Geffert, 2004; Spears and Cole, 2006). Key elements to these laws are responsibility and accountability, resulting in increased emphasis on managing security, to include having documented controls and audit trails in place.

- Security managers must justify spending on information security (which was not as much of an issue with early military or government computer security initiatives). As such, organizations need a means to measure the effectiveness of security efforts. Elusive measures of C.I.A. do not allow this, and thus, a new definition of information security is needed to enable effective measurement (Anderson, 2003).

- Inadequate information security may result in an organization losing customers or business partners; a damaged reputation; a loss in stock price; or a lawsuit. Such consequences elevate information security to a corporate governance issue of strategic importance (Rastogi and von Solms, 2005), as opposed to merely a technical issue for the IT department.

- In the early days of computer security, governments and companies protected data stored in mainframes from enemies and competitors by ensuring physical protection of the mainframe. Today, Internet and mobile computing technologies make data easier to access, manipulate, and distribute both from within the organization and remotely. This increased distribution and accessibility of information, via legitimate means, places greater need for policies and procedures for safe computing.

- Competitor firms often employ aggressive competitor analysis techniques to piece together information obtained through legal means (Kulczycki, 1997). This calls into question information security focused solely on confidential access.

The definition of information security (to protect C.I.A.) has not evolved to capture this new environment and the resulting demands placed on information security. The definition does not provide cognitive clarity, nor distinguish information security from related concepts. One could argue that the C.I.A. definition is typically used in information security research out of habit, and because it is so entrenched in industry standards.

The next section of this paper examines existing definitions of information security and related terms, and then highlights aspects of the current environment that are not
addressed by these definitions. A new definition is proposed in Section 3, followed by concluding remarks.

2. Industry-accepted Definitions

2.1. Definitions of Information Security and Related Terms

A list of definitions of information security and related terms is extracted from industry guidelines and textbooks and presented in Table 1. As shown, computer security, information assurance, information security, and information systems security are all defined very similarly with no clear distinction among these terms. With the exception of the definition of information security in ISO 17799 (a widely-accepted standard of information security best practices), the terms containing the word information are slightly distinguished from computer security by referencing information separately from systems. Otherwise, all the definitions in Table 1 basically say the same thing with slight variations in wording.
<table>
<thead>
<tr>
<th>Term</th>
<th>Source</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer security</td>
<td>CERT Coordination Center, 2006</td>
<td>“Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.”</td>
</tr>
<tr>
<td>Computer security</td>
<td>(NSTISSL, 2000, p. 11)</td>
<td>“Measures and controls that ensure confidentiality, integrity, and availability of IS assets including hardware, software, firmware, and information being processed, stored, and communicated.”</td>
</tr>
<tr>
<td>Computer security</td>
<td>(Pfleeger and Pfleeger, 2003)</td>
<td>“The purpose of computer security is to devise ways to prevent the weaknesses from being exploited.” (p. 9) “[…] we are addressing three very important aspects of any computer-related system: confidentiality, integrity, and availability.” (p.10)</td>
</tr>
<tr>
<td>Information assurance</td>
<td>(NSTISSL, 2000, p. 29)</td>
<td>Information operations that protect and defend information and information systems by ensuring their availability, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.</td>
</tr>
<tr>
<td>Information security</td>
<td>(ISO/IEC 17799, 2000, p. viii)</td>
<td>“[…] is characterized here as the preservation of confidentiality, integrity, availability.”</td>
</tr>
<tr>
<td>Information security</td>
<td>(IT Governance Institute, 2001, p. 9)</td>
<td>“The objective of information security is protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity.”</td>
</tr>
<tr>
<td>Information security</td>
<td>(Whitman and Mattord, 2003, p. 9)</td>
<td>“[…] is the protection of information and the systems and hardware that use, store, and transmit that information.”</td>
</tr>
<tr>
<td>Information systems security</td>
<td>(NSTISSL, 2000, p. 30)</td>
<td>“Protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.”</td>
</tr>
</tbody>
</table>

Table 1. Definitions of information security and related terms

2.2. Why the C.I.A. definition of information security may be inadequate

In general, the C.I.A. definition does not acknowledge the employee or strategic related aspects of information security. The Introduction section of this paper lists several examples of issues that fall under the information security umbrella. These examples highlight issues that information security is tasked to address, but that are not specific to C.I.A. They include:
Risk management via policy and documented controls
Unintentional acts by trusted personnel (which may be inherent in business processes, and not necessarily due to individual employee carelessness)
Accountability and responsibility for adequate information security practices
Information that is publicly available, but when pieced together, is sensitive

Baskerville (1992) distinguishes information systems security from computer security by stating that the former must include both “manual systems and human processors.” He goes on to explain that the human component brings behavioral aspects of information security, such as motivation, cognition, and the role of the system in its organization. Dhillon and Backhouse (2000) also highlight the human component in information security, such that security is viewed as a social and organizational issue since information systems must be operated and used by people. In addition to the C.I.A. aspects of security, these authors propose adding responsibility, integrity of organizational members, trust, and ethical norms and behavior as principles of information security (Dhillon and Backhouse, 2000). Ethical norms can deter insecure practices of trusted personnel (Rindfleisch, 1997) and can direct behavior in unforeseen contexts where formal rules do not exist (Dhillon and Backhouse, 2000).

Indeed, issues of ethics, trust, and responsibility are increasingly associated with information security. Recent legislation has officially expanded the scope of information security to include these aspects. For example, HIPAA and the Sarbanes-Oxley Act require firms to assess risk, implement, document and evaluate controls that protect information. These laws also require accountability that adequate controls are in place. The traditional C.I.A. definition does not mention risk, controls, policies, documentation, or accountability. Nor does that definition indicate the strategic importance of information or information security.

In summary, the human component and its related behavioral aspects are what distinguish information security from computer security. Yet, this is not reflected in the C.I.A. definition that is nearly identical for these two concepts. A second distinction could be made between data versus information security. It may be suggested that computer security is concerned with protecting data, whereas information security is concerned with protecting information. Information has meaning, and resides in both electronic and manual forms. Meaningful information brings strategic aspects to information security. Again, this is not explicitly reflected in the C.I.A. definition.

3. Proposed Revised Definition of Information Security

“Definitions may change when new knowledge is discovered, but new definitions do not necessarily contradict previous ones” (Locke, 2003, p. 416). The purpose of a new definition of information security is not to contradict the existing definition, but to add clarity to the meaning of this concept as its use has evolved. When formulating a definition, it is helpful to not only examine existing definitions in the literature, but also
to consider the reality surrounding the concept’s usage, in which case dictionaries may be a useful aid (Locke, 2003).

The dictionary (Webster’s New World Dictionary, 3rd College Ed.) defines security as the state of being or feeling secure; state or sense of safety; something that assures safety; and protection or defense against attack, interference, espionage, etc. Safety is defined as freedom from danger, injury, or damage; devices for preventing an accident or undesirable effect. A definition of information security is proposed by taking into account the literature, dictionary definitions, and the actual practice of information security. The proposed definition depends on the interpretation of safety:

In the context of information security, safety encompasses C.I.A., as well as any other undesirable effect associated with access control, authorization, non-repudiation, competitor analysis, and emergency preparedness.

Information security is defined as the practice of protecting organizational information of value from both intentional and unintentional acts that adversely affect its safety and providing reasonable assurance of this protection via adequate controls and accountability.

The proposed definition applies to all forms of information, to trusted personnel, as well as to external hackers. Information of value acknowledges that information security should be targeted at information of strategic importance to an organization, which implies a top-down (i.e., business-driven) approach to information security. Although the definition does not mention trust explicitly, a sense of trust is implied by way of reasonable assurance and accountability. Ethics are not explicitly mentioned. However, the proposed definition targets desired outcomes, and in doing so, is intended to implicitly capture the necessary behavior to realize these outcomes. Finally, the proposed definition contains elements of protection, safety, and risk management.

4. Conclusion

This paper has examined the traditional C.I.A. (confidentiality, integrity, availability) definition assigned to information security that was inherited from computer security. The C.I.A. definition has been found to miss critical aspects of today’s information environment, and does not distinguish information security from related concepts. Specifically, the C.I.A. definition does not adequately incorporate employee or strategic related aspects of information security.

In an effort to provide cognitive clarity and increased measurability of the concept of information security (Locke, 2003), a new definition was proposed. Information security is defined as the practice of protecting organizational information of value from both intentional and unintentional acts that adversely affect its safety and providing reasonable assurance of this protection via adequate controls and accountability. This definition is open to debate and further revision.
Acknowledgments: This work was supported in part by a grant from the eBusiness Research Center at The Pennsylvania State University.

References


