1.3.2 Fundamental Elements of Computer Fraud

The basic criteria that must be met for computer fraud to be considered include the following:

- Knowingly access or otherwise use a computer.
- Use or access of a computer without authorization or exceeding authorization.
- Use or access of a computer with intent to commit a fraudulent or other criminal act.

An important federal law governing fraud and related activity in connection with computers is Title 18 U.S. Code, Section 1030. This law was originally enacted in 1986 and is known as the Computer Abuse Amendments Act of 1994. Section 1030 punishes any intentional, unauthorized access to a protected computer for the purpose of:

- Obtaining restricted data regarding national security.
- Obtaining confidential financial information.
- Using a computer that is intended for use by the U.S. government.
- Committing a fraud.
- Damaging or destroying information contained in the computer.

A protected computer under this section is one that has the following characteristics:

- Is used exclusively by a financial institution or the U.S. government.
- If use affects a computer used by a financial institution or the federal government.
- Is used in interstate or foreign commerce or communication.

Additional elements of computer fraud include unauthorized access (or exceeding one's authority), an intent to defraud, and obtaining anything of value, including money and software.

1.4 Insider Threat Concepts and Concerns

The insider threat is an elusive and complex problem. To reduce the problem to its functional primitive state and develop a workable methodology for risk reduction is a large undertaking; however, this book will provide the educational foundation to understand this issue and potential resolution. Although the ICF taxonomy indicates that there are many types of ICF, data input manipulation appears to be one of the most pervasive, based on my research. In addition to being pervasive, it

is the fraud category that I believe has the greatest potential for risk identification and mitigation.

There are two schools of thought in evaluating and analyzing ICF activities, including an evaluation of profiling the behavioral aspects of the insider, based on some type of empirical study, and the evaluation of what motivates people to do certain things given a set of variables (that is, actions based on a set of facts and circumstances). Ostensibly, in the first method of evaluating the insider threat, people and their behavioral characteristics and subsequent nefarious actions are profiled.

The second precept of the evaluation of the insider threat is largely predicated upon profiling data versus people, based on the previously described behavioral traits and circumstances. My research was predicated exclusively on profiling the behavior of data versus people, largely because it was a unique approach to addressing the ICF problem that has not been evaluated or analyzed in substance by anyone, at least in an academic research setting. Equally as important, I wanted to eliminate the objectivity of having to make judgments about people and what motivates them to act or react in a certain way based on a given set of circumstances. In brief, there seemed to be too many variables that I just could not control or feel comfortable in evaluating.

To validate my hypothesis that the insider threat can be identified, measured, monitored, and controlled, I needed to deploy a framework that was predicated upon the Defense in Depth Model concept. This model evaluates the insider threat from a holistic manner compared to a customized micro approach, which would assess risk based on a specific modus operandi, which details the specifics on how an insider computer fraud was perpetrated. The concept of layered security has to start from a robust InfoSec risk assessment process that includes a comprehensive threat assessment, which then surgically adds or removes additional layers of protection to an IT infrastructure, depending on the unique risk profile and culture of that organization. The concept of risk acceptance is very important in my framework, because of the potential for a high overhead for implementing the framework in the long term. Although the framework is extensible and scalable regardless of size or sophistication or complexity of the organization, you do not want to use a 100-pound hammer to nail a single nail. But again, the risk assessment process needs to evaluate the criticality of systems and data and the organization's culture and appetite for risk.

At the risk of oversimplifying my framework, I will introduce a number of concepts or tools that were integrated within the framework that can be used for identifying ICF relative to data manipulation:

1. Application of the risk assessment process.
2. Deployment of the Defense in Depth concept within the Enterprise Architecture.
3. Focus on application security, which is most vulnerable to the insider threat.
4. Consideration of application and system data and metadata journaling requirements that will significantly increase in importance from a computer forensic

and event correlation perspective—note the importance of implementing "surgical" application and system journaling of data and metadata for misuse detection of known ICF vulnerabilities and exploits.

5. Evolution of the software development methodologies in existence today to ensure software security is "baked" into the software development life cycle (SDLC) in both structured software development and Agile programming.
6. Consideration of Web services and a SOA as the future of all "E" data transmissions or transactions both internally and externally over the next decade within the financial services sector and perhaps in other sectors; focus of hacking attacks (external and internal) likely to be on eXtensible Markup Language (XML) source code and EXtensible Business Reporting Language (XBRL) to manipulate data.
7. Need for a macro and micro taxonomy of ICF activities in organizations so as to understand the types and probability of attacks impacting an industry or sector within the critical infrastructure and to identify KFIs, KFMs, and KFSs.
8. Growing role for artificial intelligence (AI) relative to risk governance and management processes for reducing ICF activities, particularly related to anomaly detection (day zero ICF activity). (My research in this area involved experimenting in training and testing a novelty neural network, which uses neural associative memory [NAM] similar to the way the human mind learns and functions. Although my experiment had mixed results from an academic perspective, it holds promise for increased success with additional research and testing to further this eventual science.)

1.5 Defense in Depth

The concept of defense in depth is a practical strategy for achieving information assurance. Presented in this section is a brief discussion of the concept of defense in depth in the context of malicious hacker activity and architectural solutions to either prevent or detect ICF activity (see Figure 1.1).

As defined by The World Bank's *Electronic Safety and Soundness* 2004 publication,

> Defense in Depth is a twofold approach to securing an information technology (IT) system: (1) layering security controls within a given IT asset and among assets, and (2) ensuring appropriate robustness of the solution as determined by the relative strength of the security controls and the confidence that the controls are implemented correctly, are effective in their application, and will perform as intended. This combination produces layers of technical and non-technical controls that ensures the confidentiality, integrity, and availability of the information and IT system resources.[1]

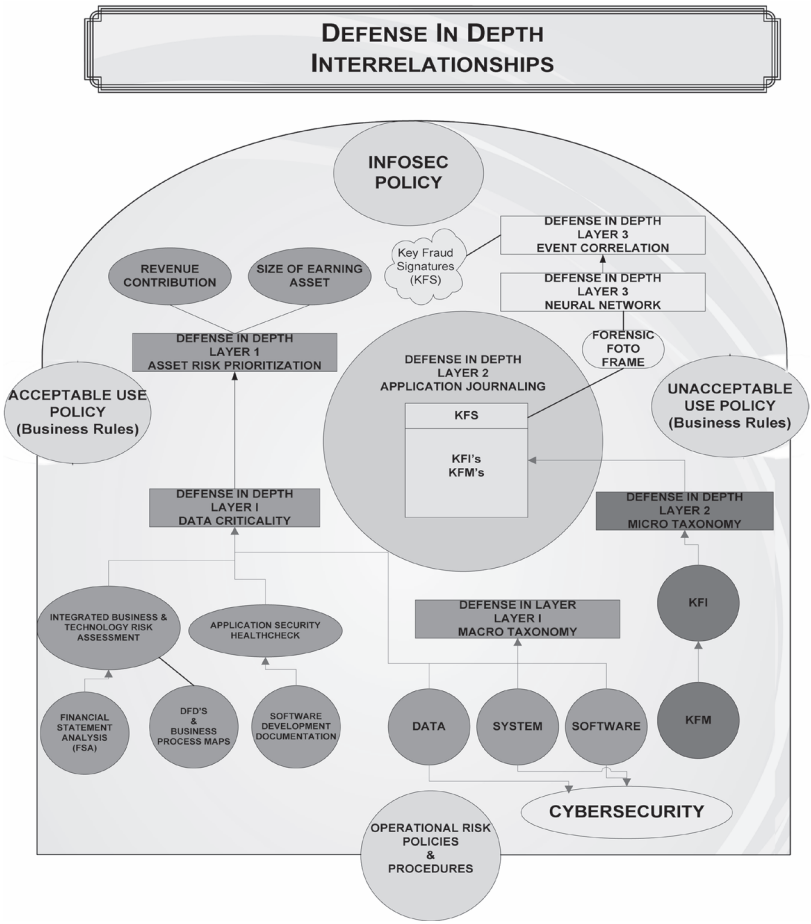

Figure 1.1 Defense in depth interrelationships.

In brief, the concept of defense in depth is important in that it represents a strategy that balances several factors involving protection capability and cost, performance, and operational considerations. It is a best practice strategy in that it relies on the intelligent application of techniques and technologies that exist today. Specifically, the strategy recommends a balance between the protection capability and cost, performance, and operational considerations.

One of the primary goals in the defense in depth concept is to prevent attacks against an enterprise's data and information systems. Threats to an enterprise's systems may originate from many different forms, which may include hackers, insiders, competition, and terrorists. Motivation by these groups and others may include intelligence gathering, theft of intellectual property, and identity theft; however, the primary focus of this discussion is on ICF activity, primarily centered on data input manipulation.

1.6 Conclusion

The ICF problem is a growing threat to the critical infrastructure of the United States, unless several fundamental root cause problems are addressed. The root cause problems for ICF include the following:

- Increased emphasis on network security versus application security.
- Overall absence of comprehensive industry and government standards that provide detailed guidance on methods and solutions for strengthening the software engineering processes to include information security controls during the preimplementation process.
- Lack of comprehensive computer forensic guidelines in the public domain that can be used by IT professionals as industry standards for conducting cyber and internal application risk assessments, particularly relating to acceptable and unacceptable evidentiary forensic data tailored to the specific insider E-crime.
- Lack of a standardized journaling format that could be leveraged by software vendors and the IT software development community at large, without incurring additional overhead and risk of conducting inconsistent and perhaps inaccurate data parsing activities for disparate applications throughout an enterprise.
- Absence of generic industry risk guidelines for defining and determining what data elements are typically at most risk for ICF and leveraging the eventual standardization of journaling data elements for inclusion in event correlation software (i.e., application journaling being correlated with journaling from high-risk network IT infrastructure components) for root cause analysis of potential ICF activities.
- Absence of public- and private-sector partnership for assessing processes and practices to encourage the development and implementation of emerging technologies for the detection and mitigation of ICF through the use of neural networks and other resources and technologies. (One of the specific goals and deliverables for such a partnership should be sanitized data that protect the anonymity of the parties involved in the crime, which could be used by the academic and professional IT community for conducting ICF research.)

Reference

1. Glaessner, Thomas C., Kellerman, Tom, and McNevin, Valerie. Electronic Safety and Soundness: Securing Finance in New Age (World Bank Working Papers). Washington, D.C.: The World Bank, 2004, pp. 159–160.