SCS5607 ETHICAL HACKING AND DIGITAL FORENSICS

UNIT-III

COMPUTER FRAUD

Insider Threat Concepts

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.

The 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).

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.

Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector

The primary findings and implications of this research are as follows:

- Most incidents were not technically sophisticated or complex. They typically involved exploitation of nontechnical vulnerabilities such as business rules or organization policies (rather than vulnerabilities in an information system ornetwork) by individuals who had little or no technical expertise.
- The majority of incidents were thought out and planned in advance. In most cases, others had knowledge of the insider's intentions, plans, or activities.Those who knew were often directly involved in the planning or stood to benefit from the activity.
- Most insiders were motivated by financial gain, rather than by a desire to harm the company or information system.
- A wide variety of individuals perpetrated insider incidents in the cases studied.Most of the insiders in the banking and finance sector did not hold a technical position within their organization, did not have a history of engaging in technical attacks or "hacking," and were not necessarily perceived as problem employees.
- Insider incidents were detected by a range of people (both internal to the organization and external), not just by security staff. Both manual and automated procedures played a role in detection.
- The impact of nearly all insider incidents in the banking and finance sector was financial loss for the victim organization. Many victim organizations incurred harm to multiple aspects of the organization.

- Most of the incidents were executed at the workplace during normal business hours.

A Framework for Understanding and Predicting Insider Attacks

A Framework for Understanding and Predicting Insider Attacks”2 provides a high-level recap of what research related with this ICF.The highlights of this methods state the following:

- An insider attack is considered to be a deliberate misuse by those who are authorized to use computers and networks. We know very little about insider attacks, and misconceptions concerning insider attacks bound.
- Considerations must be made when defining “insider attack”:
    - Numerous definitions for the term “insider attack” have been proposed.Tugular and Spafford2 assert that inside attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization’s security policy.
- Insiders would usually be employees, contractors and consultants, temporary helpers, and even personnel from third-party business partners and their contractors, consultants, and so forth. It is becoming increasingly difficult to maintain a hard and fast distinction between insiders and outsiders.
- Many “insider jobs” have turned out to be the result of complicity between and insider and an outsider.
- Myths and misconceptions include the following:
    - More attacks come from the inside than from anywhere else.
    - Insider attack patterns are generally similar to externally initiated attacks.
    - Responding to insider attacks is like responding to outside attacks.
- Tuglular and Spafford have proposed a little-known but nevertheless intriguing model of insider attacks. This model assumes that insider misuse is a function of factors such as personal characteristics, motivation, knowledge, abilities, rights and obligations, authority and responsibility within the organization,

- and factors related to group support. The creators of this model have pointed out that insider attacks are more likely to occur under conditions such as breakdown of lines of authority within an organization
- The 3DP (three-dimensional profiling) model is a criminological or profiling model developed by Gudatis. This model examines and applies the methodology of conventional criminal profiling to computer crime. Specifically, the model focuses on insider attacks and prescribes an organizationally based method for prevention. The utility of this model is twofold in that it allows for the assessment of an incident or attack using profiling in addition to the usual technical tools, and it provides organizations a way to evaluate and
- enhance their security processes and procedures from a human perspective as a preventative measure.
- Einwechter proposed that a combination of intrusion detection systems (IDS)—network intrusion detection systems (NIDS), network node intrusion detection systems (NNIDS), host-based intrusion detection systems, and a distributed intrusion detection system (DIDS) be used to detect insider attacks.
- Collecting and analyzing data that is likely to yield multiple indicators are, in fact, the only viable directions given how subtle and different from conventional (external) attacks insider attack patterns often are. Although IDS output can be useful in detecting insider.

Methodology for the Optimization of Resources in the Detection of Computer Fraud

There are surprisingly few common forms of computer fraud manipulation in fact, just these three:

Input Transaction Manipulation Schemes

Unauthorized Program Modification Schemes

File Alteration and Substitution Schemes

Input Transaction Manipulation Schemes

• *Extraneous Transactions*: Making up extra transactions and getting them processed by the system is a rather straightforward form of input manipulation. A perpetrator may either enter extraneous monetary transactions to benefit him- or herself, or he or she may enter file maintenance transactions that change the

indicative data about a master file entity (customer,vendor, product, general ledger account, salesman, department, etc.) in some way that he or she will later exploit.

• *Failure to Enter Transactions*: Perpetrators can obtain substantial benefits simply by failing to enter properly authorized transactions. One of the simplest examples involved action on the part of check-processing clerks who simply destroyed their own canceled checks before they were debited

to their accounts. The same thing can happen in a customer billing system. File maintenance can also be excluded dishonestly with similar benefits.

• *Modification of Transactions*: Fraudulent gains can be realized by altering the amount of a properly authorized monetary transaction. For example, aperpetrator may reduce the amount of charges against a particular account or increase payment into a particular account. Another scheme involves

changing indicative data on file maintenance transactions. Examples are name, address, monthly closing date, account type and status, privileges, and so on.

• *Misuse of Adjustment Transactions*: Misuse of adjustment transactions is a common ingredient in input manipulation schemes. Here the term “adjustment” refers to monetary corrections of past errors or inaccuracies that have come about in a system through physical loss or spoilage of materials.

• *Misuse of Error—Correction Procedures*: Millions of dollars have been embezzled by perpetrators under the guise of error–corrections. Although many of these abuses are special cases of previously mentioned methods of manipulating input, it is felt that error–corrections are often a problem and deserve special attention. Ways that perpetrators abuse error–correction

Unauthorized Program Modification Schemes

• *Difficulty in Detection*: Program modification schemes are the most insidious and difficult to detect. Even though the reported instances of such cases is fairly low, leading auditors and security consultants share a chilling view of reported statistics: reported incidence bears no relation to the actual enormity of the problem.

Reasons for Enormity of Problem: To explain this commonly held view, consider the following:

Some program modification schemes are untraceable.

All program modification schemes are difficult to detect.Motivation for perpetrators is high because a single blitz can effect large benefits rapidly with little chance of detection or prosecution.Larcenous strategies for modifying programs exist.

• Computation of applicable service charge
• Computation of discounts
• Payroll withholding computations
• Computation of retirement benefits
• Computation of interest on savings
• Computation of welfare, Medicare, social security, or unemployment benefits
• *Undocumented Transaction Codes*: By programming the computer to accept undocumented types of transactions, perpetrators can arrange to receive substantial profits in a very short time. Once having made provisions for processing of the extra transaction type, there are several means to get the necessary transactions into the system. The transactions may be computer generated, input by the programmer where controls (or lack of controls) allow it, input via the addition of an extra input file, and so forth.
• *Balance Manipulation*: Simple, undisguised balance manipulation is a method that involves assuming that processing results will not be properly reviewed. A dishonest programmer can modify appropriate programs so that all totals and balances appear to be correct for any given day. The work factor involved in modifying all programs involved is typically high, so the programmer will more often attack just one or two programs.
• *Deliberate Misreporting with Lapping*: A program that was manipulated to cause misreporting either fails to apply a charge to a perpetrator's account (the charge gets applied to another account) or credits a perpetrator's account with a payment (the account that should have been credited is not posted). Either way, certain problems are bound to arise.
File Modification: Altering programs to effect secret changes in account status is a fairly common programming technique for computer fraud.
• *Fudging Control Totals*: This tactic is often combined with other programming schemes. The approach involves processing that occurs without being properly reflected in control totals.

File Alteration and Substitution Schemes

• *Access to a Live Master File*: One fairly common form of fraudulent file alteration is to obtain "access to a live master file" and (using a program specially written for the purpose, a general retrieval program, or a utility) to make surreptitious changes to

the file. Changes may include modification of monetary amounts or changes to other data.

• *Substitution of a Dummied-Up Version for the Real File*: This scheme depends upon one of two possible sequences of events. In either case, the scheme begins with the perpetrator obtaining access to the master file, possibly under the guise of making a copy for use as test data. Then the file is run against a program, either in-house or at a service bureau. The program creates a similar file, containing only a few modifications. The newly created file is then substituted for the live file and returned to the data library.

Access and Modification of Transaction Files Prior to Processing: Possible fraudulent actions that may be involved in this type of scheme include addition, modification, and deletion of input transactions.

Managing the Insider Threat

Training and technology go together, hand in hand, to help prevent insider attacks. For example, if an employee is not properly trained and held accountable for password management their computer might easily be broken into. First one must identify all of the authentication and business rules in order to make educated decisions per level of risk associated with the insider threat. Workflow rules grant people permissions only for what they are allowed access to within a system. Such role-based access controls with a workflow infrastructure will manage many of the risks associated with the Insider threat. Each user should only be granted access to data if the user has a valid need to know.

- Authentication
- Privileges

Physical Security Issues

- Physical access to networked systems facilities made by employees, contract employees, vendors, and visitors should be restricted.
- Access to sensitive areas should be controlled by smart card or biometric authentication.
- Consoles or administrative workstations should not be placed near windows.
- Alarms to notify of suspicious intrusions into systems rooms and facilities
- should be periodically tested.

- The backgrounds of all employee candidates should be vetted. This is especially important for candidates requiring access to the most sensitive information and mission-critical systems.
- Rooms or areas containing mission-critical systems should be physically segregated from general work spaces, and entry to the former should be secured by access control systems.
- Employees should wear clearly visible, tamper-resistant access and identification badges, preferably color coded to signify levels, or extent, of their access to critical systems.
- All vendor default passwords should be changed.
- All unused ports should be turned off.
- All users must affirm that they are aware of policies on employee use of e-mail,Internet, Instant Messaging (IM), laptops, cellular phones, and remote access.Someone should be responsible for enforcing these policies.
- All servers should be placed in secured areas. Always make sure server keys are securely locked.
- Employees should consistently log off their accounts when they are absent fromtheir workstations, and portable devices should be locked to workstations.
- All sensitive data stored on user hard drives must be encrypted.
- Technical documents and diagrams that contain sensitive information such as TCP/IP addresses, access control lists, and configuration settings should be stored in secure spaces.
- Passwords should never be issued over unsecured channels (for example, cell phones, IM, cordless phones, radios, etc.).

The Insider Threat Strategic Planning Process

The concept of information security governance, with an emphasis and goal in providing a more accurate and cost-effective methodology for conducting an integrated (business/technology) risk assessment, threat assessment (internal and external threats), and privacy impact assessment evaluation. There are two common risk assessment methodology mistakes made by the management of many organizations, which are centered around performing only a technical versus a business risk evaluation to conclude on the
integrated risk profile of that organization. The second mistake also being made by organizations is the absence of management's comprehensive threat analysis, which includes the identification of not only external threats but internal threats as well.
The component within the information technology (IT) infrastructure that has received the least amount of consideration when evaluating risk within an organization is analyzing the impact of the insider threat.

The goal of information security and the risk assessment process is to enable organizations to meet all business objectives by implementing business systems with due care consideration of IT-related risks to the organization, its business and trading partners, vendors, and customers. Organizations can achieve the information security goals by considering the following objectives:

- *Availability*: The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information and systems.
- *Integrity of Data or Systems*: System and data integrity relates to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and that systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.
- *Confidentiality of Data or Systems*: Confidentiality covers the processes, policies,and controls employed to protect customers' and organizations' informationfrom any anticipated threats or hazards, including unauthorized

access to or use of the information that would result in substantial harm or inconvenience to any customer or institution.

- *Accountability*: Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports nonrepudiation, deterrence, intrusion detection and prevention,after-action recovery, and legal admissibility of records.
- *Assurance*: Assurance addresses the processes, policies, and controls used todevelop confidence that technical and operational security measures work as intended. Assurance levels are part of the system design and include the fourelements listed above (availability, integrity, confidentiality, and accountability).

Understanding the Information Security Governance Process

- An IT professional needs to understand the components of a financial institution's IT infrastructure.
- The analyst should consult with management about how they determine the integrated business and technology risk profile of their organization by assessing whether:IT is aligned with the enterprise business objectives and to deliver value and security within the final product.
- Information technology risks are clearly identified and mitigated and managed on a continuous basis, as needs dictate.
- Comprehensive information security policies and procedures exist, which at the minimum address the need for an information security risk assessment process that will evaluate the integrated business and technology risk profile of the financial institution. For example, at the minimum, management should
- consider the following components within their technology infrastructure,when determining the bank's risk profile:
    - Logical Access Controls
    - Intrusion Detection Systems, Vulnerability and Other Network Testing
    - Firewall Security
    - Journaling and Computer Forensics
    - Computer Incident Response

Cyber-Security Risk Governance Processes for Web-Based Application Protection (Understanding the External Risks and Internal Information Security Risks)

An important component of the risk assessment process involves cyber-security (Figure 3.1). Electronic security or "cyber-security" refers to the protection of information assets from internal and external threats. Protection of these assets includes managing risks not only to information, but also to critical information systems infrastructure, processes, and platforms such as networks, applications, databases,and operation systems, wherever information is collected, processed, stored, transmitted, and destroyed.

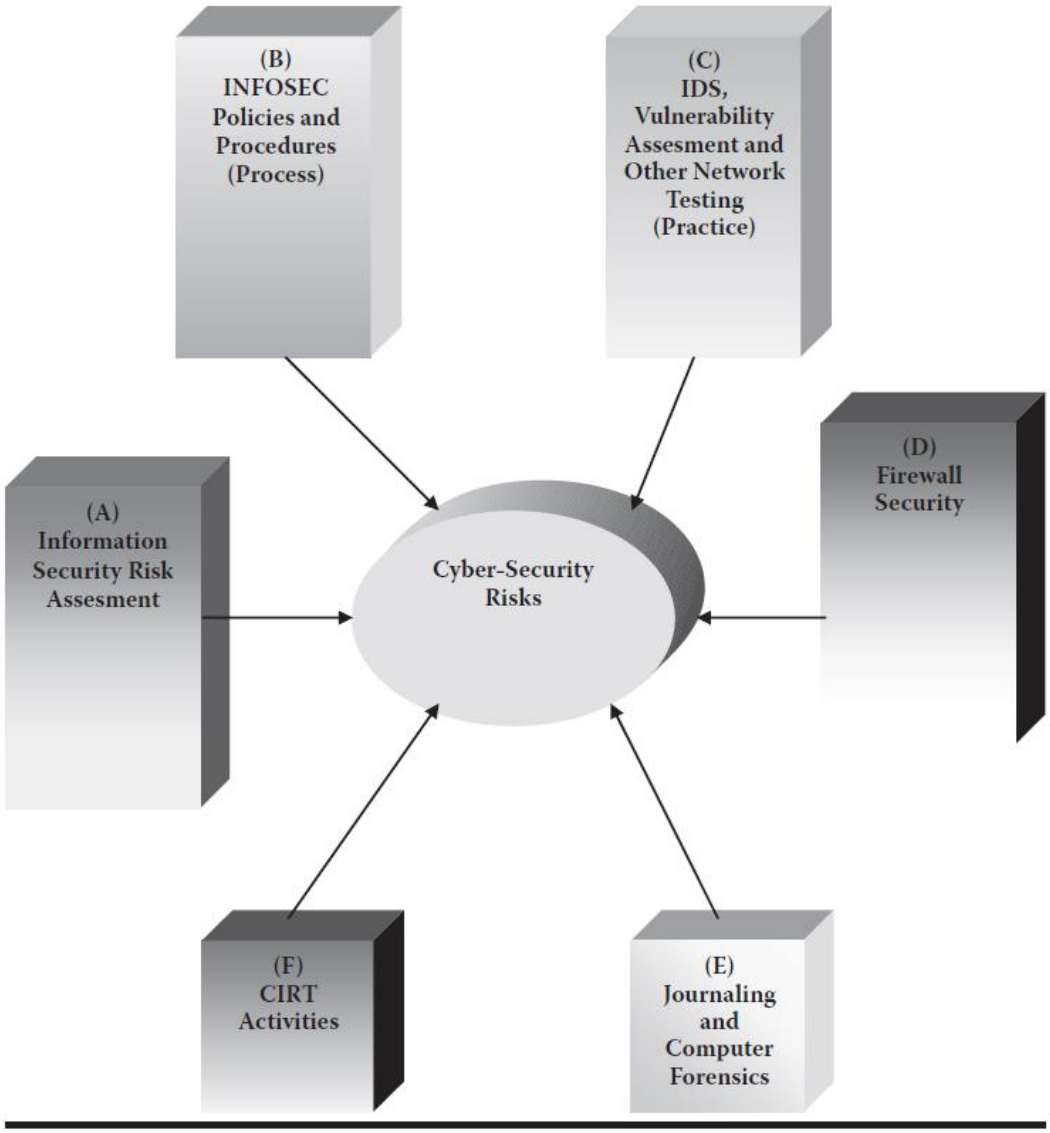

Figure 3.1 Cyber-security risks.

Refer to the diagram above and the listing of the categories:

- An Information Security Risk Assessment
- Information Security Policies and Procedures
- Intrusion Detection Systems (IDS), Vulnerability Assessment, and Other Network Testing
- Firewall Security
- Journaling and Computer Forensics
- Computer Incident Response Activities

The Risk Management Process

The concept of risk management and governance can be best described as the process of identifying, measuring, monitoring, and controlling vulnerabilities and threats as they impact the objectives of a business or organization.

Total Risk = Threats × Vulnerability × Asset Value

- Gathers data regarding the information and technology assets of the organization,threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements.
- Analyzes the probability and impact associated with the known threats and vulnerabilities to its assets.
- Prioritizes the risk present due to threats and vulnerabilities to determine the appropriate level of training, controls, and testing necessary for effective mitigation.
- Classifies and ranks sensitive data, systems, and applications
- Assesses threats and vulnerabilities.
- Assigns risk ratings.

What Should Be Included in the Risk Management Process?

The Tailored Risk Integrated Process (TRIP)

Prior to reviewing the TRIP risk assessment methodology, it is important to understand the basic security control categories as listed in Table 3.1.

Table 3.1 Security Controls

Security Control Class	*Security Control Family*
Management Security	• Risk Assessment • Security Planning • System and Services Acquisition • Security Control Review • Processing Authorization
Operational Security	• Personnel Security • Physical and Environmental Protection • Contingency Planning and Operations • Configuration Management • Hardware and Software Maintenance • System and Data Integrity • Media Protection • Incident Response • Security Awareness and Training
Technical Security	• Identification and Authentication • Logical Access Control • Accountability (Including Audit Trails) • System and Communication Protection

The TRIP methodology would bridge the current risk assessment InfoSec gaps not only to ensure accurate identification of technology, but also to ensure business risks are identified (integrated risk approach). Ideally, any risk assessment needs to begin with an assessment of business-critical applications, privacy considerations,and core data elements within an application or system.

The recommended industry approach is as follows:

The TRIP Approach

• Identification of critical business processes.

• Identification of critical applications and systems and data that support a

business unit’s operations.

• Identification of critical IT infrastructure components that support the critical applications and systems.

• Inherent risk identification.

• Control identification.

• Threat and vulnerability modeling.

• Residual risk identification.

• Net residual identification (factors IT infrastructure components).

• Risk acceptance, transfer, and elimination.

TRIP Advantages

- Provides more focused and efficient risk identification process by analyzing InfoSec risks locally at each business unit first through a TRIP versus evaluating all integrated risks—evaluating all integrated risks may include an evaluation of InfoSec risks and controls governing IT infrastructure components and applications which may not represent the high risks within the enterprise.
- Provides a more accurate integrated enterprise-wide risk assessment by evaluating a business operation and supporting applications and systems first and then selecting only those IT infrastructure components that directly or indirectly impact the critical business operations and supporting applications and systems.
- Provides cost savings of not having the increase financial overhead of performing an enterprise-wide risk assessment that covers the entire IT universe compared to the more efficient, logical, and risk-based approach using the TRIP methodology.

The TRIP Strategy

Periodic security testing based on integrated business and technology risks engages either an internal evaluation (i.e., audit/compliance) or third-party technology production application risk assessments.

The scope of controls testing includes at the minimum an assessment of control objectives and points identified for each critical production application and system,as described below:

- Control Points
- Application Access Controls
- Data Origination and Input Controls
- Processing Controls
- Output and Management Information Systems (MISs)

Security Controls in Application Systems Controls (ISO 27001)

Following are methods to achieve that objective:

- Input Data Validation Data: Input to application systems will be validated to ensure that it is correct and appropriate.
- Control of Internal Process: Validation checks will be incorporated into systems to detect any corruption of the data processed.
- Message Authentication: Message authentication will be used for applications where there is a security requirement to protect the integrity of the message content.
- Output Data Validation: Data output from an application system will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Table 3.2 Dashboard Rating Criteria

Fully Implemented	*Partially Implemented*	*Not Implemented*
	Confidentiality	
INFOSEC Policies, Procedures, and Practices provide strong documented controls to protect data confidentiality. Strong indication of favorable practices governing data confidentiality.	INFOSEC Policies, Procedures, and Practices need strengthening to ensure the existence of strong documented controls to protect data confidentiality. Preliminary indication of unfavorable practices governing data confidentiality.	INFOSEC Policies, Procedures, and Practices are Critically Deficient to ensure the existence of strong documented controls to protect data confidentiality. Clearly defined weaknesses governing data confidentiality.
	Integrity	
INFOSEC Policies, Procedures, and Practices strongly protect data integrity through a high level of controls governing authenticity, nonrepudiation, and accountability. Strong indication of favorable practices governing data integrity.	INFOSEC Policies, Procedures, and Practices need strengthening to ensure a strong level of data integrity exists through a high level of controls governing authenticity, nonrepudiation, and accountability. Preliminary indication of unfavorable practices governing data integrity.	INFOSEC Policies, Procedures, and Practices are Critically Deficient to ensure a strong level of data integrity exists through a high level of controls governing authenticity, nonrepudiation, and accountability. Clearly defined weaknesses governing data integrity.
	Availability	
INFOSEC Policies, Procedures, and Practices provide a strong internal control standard to protect the timely availability of information technology resources (system & data). Strong indication of favorable practices governing data availability.	INFOSEC Policies, Procedures, and Practices need strengthening to protect the timely availability of information technology resources (system & data). Preliminary indication of unfavorable practices governing data availability.	INFOSEC Policies, Procedures, and Practices require fundamental improvement to protect the timely availability of information technology resources (system & data). Clearly defined weaknesses governing data availability.

Table 3.3 Application Criticality Matrix

1. The Taxonomy (category) of Application	11. Bank Regulatory Implications (Two-Factor Authentication Implications)	21. Significance to Internal Threats
2. O/S[a] Platform	12. Health Care Industry (HIPAA[d]) Implications	22. Impact on the Information Security Scorecard Rating
3. Data Classification	13. Bank Regulatory Implications (BASEL II)	23. Access Controls Safeguards
4. Age of Application	14. Bank Regulatory Implications (FFIEC[e])	24. Data Origination/Input Safeguards
5. Significance to Disaster Recovery	15. Federal Government Implications (i.e., Office of Management and Budget, National Institute of Standards and Technology, Presidential Decision Directives, Federal Information Security Management Act [FISMA])	25. Processing Safeguards
6. Financial and Regulatory Reporting	16. Education/Experience of Technology Personnel	26. Output Safeguards
7. Impact to Operational Risk	17. Attrition Rate of Technology Personnel	27. Data Confidentiality
8. Impact to Reputation Risk	18. History of Audit Findings (Internal/External)	28. Data Integrity
9. SEC SOX 404[b] Implications	19. Application External/Internal Interfaces	29. Data Availability
10. GLB[c] Act Implications	20. Significance to External Threats	30. Threat Modeling Results (i.e., Probability and Impact of Attacks, Based on Application and Network Vulnerabilities to Attacks)

Source: © Dr. Kenneth C. Brancik. CISA. CISSP.

The results of the HeatMap rating should directly correlate with the production application system security rating component of the InfoSec dashboard/scorecard (see Table 3.4).

Number	*Category*	*2006*	*2005*	*Security Trend*
1	Security Policies and Standards	G	G	›
2	System Development and Security Architecture	R	Y	
*3	Production Application System Security	Y	R	
4	Network Security	G	Y	
5	User Authentication and Access Controls	G	G	›
6	Security Monitoring	R	Y	
7	Vendor Management for Security	R	Y	
8	Incident Response (including computer forensics)	R	R	›
	OVERALL	R	Y	

Net Residual Risk (NRR)

The NRR goal is to evaluate application risk in context with the IT infrastructurecomponents that interface with a critical application or system.

Determine the level of NRR that incorporates the risks and controls of the supporting IT infrastructure used by a critical application or system:

Step 1: Determine the **Inherent Risk Rating**

Step 2: Internal Controls Rating

Step 3: **Residual Risk Rating**

Step 4: Risk Assessment Rating

Step 5: Probability of Occurrence

Step 6: Business Impact Assessment

Step 7: Business Continuity Planning (BCP) Assessment

Step 8: IT Infrastructure Components

Step 9: Technology Impact Assessment

Step 10: Interfacing Applications

Step 11: Platforms (Operating Systems [O/S])

Step 12: Architecture

Step 13: **Net Residual Risk (NRR)**

Step 14: Risk Acceptance, Transference, or Elimination

The term NRR needs to be evaluated in the context of high, medium, and low after considering various factors such as probability of occurrence, business impact assessment, and BCP.

The Threat Assessment Process(The Integration Process)

A common omission in the threat modeling process is to focus exclusively on identifying known versus the unknown external threats and to exclude an evaluation of the insider threat (known and unknown).

A significant number of the preliminary critical steps needed for completing a thorough risk modeling process, which includes the following steps (the steps are not in sequence order as this will be contingent upon each organization based upon its existing operational processes and practices):

- *Identify Key Business Assets*: This is the first important step required for performing an integrated risk assessment.
- *Identify Critical Data and Systems*: This step was performed during the integrated risk assessment process.
- *Identify Core Business Transaction Data Elements*: The identification of core business transaction data elements was completed during the integrated risk assessment process.
- *Identify Sensitive Data Elements that are NPPI*: Sensitive data elements were identified so as to ensure compliance with GLB, HIPAA, and the breach notification requirements.
- *Data Flows*: The data flows of critical core business transaction data elements and sensitive data elements were determined during the integrated risk assessment process.
- *Metadata*: Any available metadata should be collected on core business transaction data and NPPI data for compliance and regulatory purposes.

- *Key Fraud Indicators (KFIs)*: KFIs are data elements that have been determined to contain NPPI information that would be the most vulnerable to an external or internal defalcation or breach. There should be a direct correlation between the values identified as KFIs and the total of NPPI data. The KFIs can be thought of as a subset of the total NPPI data.
- *Key Fraud Metrics (KFMs)*: The KFM is a by-product of the identification of KFIs and is used to establish a means for establishing a numerical baseline for what is a normal value for a particular area.
- *Key Risk Indicators (KRIs)*: Key risk indicator is the parent term used to describe the key core business and sensitive NPPI and KFI data flows within an enterprise application or with external third parties.
- *Control Point Determination*: Control points are identified at each stage of a transactions journey through the application and components of the IT infrastructure (i.e., network through to a third party, to its final resting or storage repository).
- *Optimizers*: Optimizers (IT infrastructure and software controls) are identified.
- *Residual Risk Rating*: A completed qualitative assessment through a residual risk rating (inherent risk-mitigating controls); a completed qualitative residual risk rating gives values of high, moderate, and low. *Net Residual Risk Rating*: A completed qualitative NRR rating designates values of high, moderate, and low.

The Strategic Planning Process for Reducing the Insider Threat

- Figure 3.3 provides a general framework for the steps involved in establishing a method for identifying, measuring, monitoring, and controlling the insider threat.
- The strategic planning process should be an iterative and dynamic process that has several moving parts as detailed in Figure 3.3. Any changes within any component will have a ripple effect on each of the interconnected processes; consequently, each dependent process needs to be reevaluated against those changes.

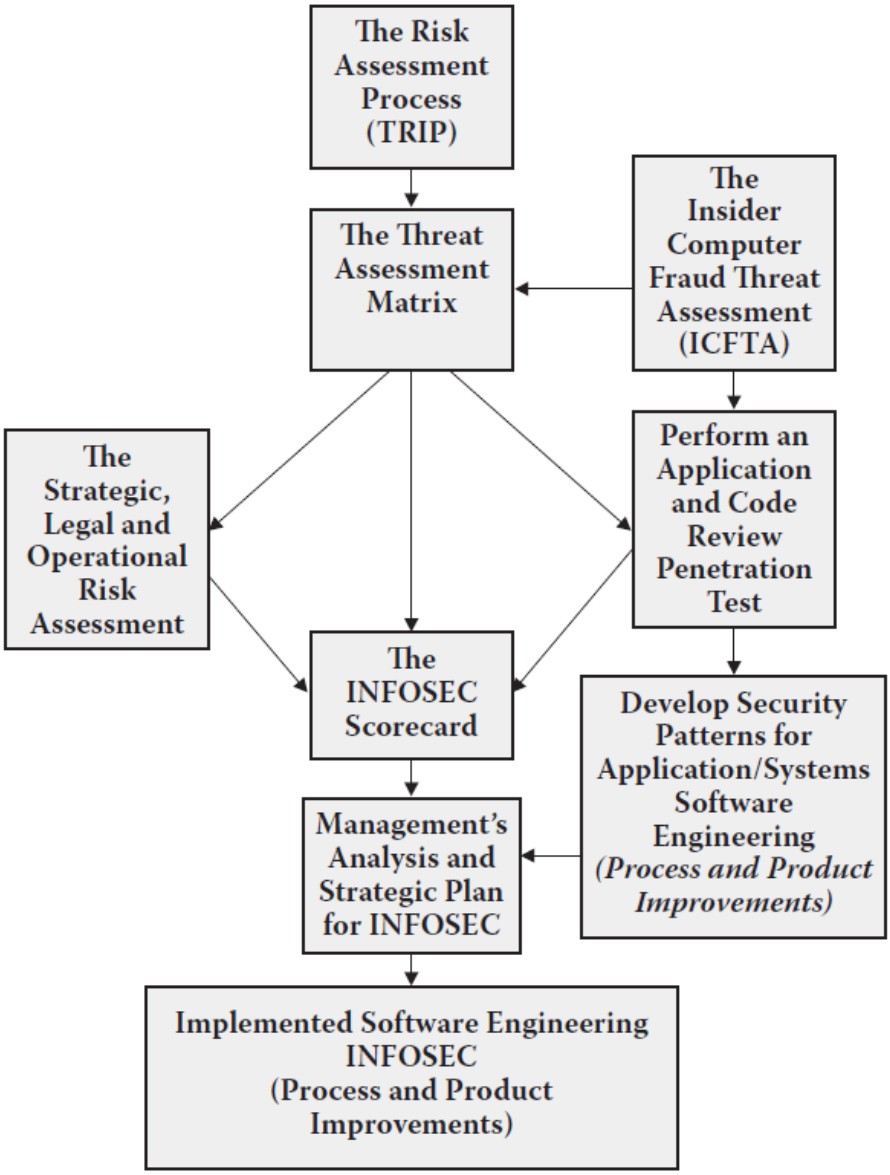

Figure 3.3 The strategic planning process for reducing the insider threat.

The Threat Assessment Matrix

Throughout our discussion of risk assessment, the importance of control points and their role in tracing the flow of critical data between various applications and systems has been highlighted.

One of the primary goals of the Threat Assessment Matrix is to crystallize what criteria should be used to evaluate the severity of a particular threat so that uniformity and consistency can be applied in the ratings assessment across an enterprise, regardless of its source.

The Threat Assessment Matrix is structured so that each control point rating will be consistent in format. Specifically, the following ratings criteria will be itemized for each control point:

1. Summary
2. Probability
3. Impact
4. Confidentiality
5. Integrity
6. Availability
7. Auditability

Insider Computer Fraud Threat Assessment (ICFTA):

The ICFTA should be used to assess what applications or systems are vulnerable to ICF activities. Analyzing the ratings concluded from the completion of ICFTA (high, moderate, low) and considering the level of NRR should establish the basis for determining how effective each is against an insider threat to an application or system.

Control Point: Access Controls	*Low Risk, Strong Controls (1)*
Summary	Rating: (1) Low risk, based on strong controls and the threat source not possessing either the motivation or technical skills to commit the defalcation. Strong security defenses governing the ability to permit or deny access to a system or file. Thorough controls for the effective identification, authentication, authorization, and accountability.
Probability	The threat source is not highly motivated or does not possess the capability of violating access controls to exploit an application or system vulnerability.
Impact	Exploitation of a vulnerability (1) will not result in a high cost for major tangible assets or resources, (2) will not violate, harm, or impede an organization's mission, reputation, or interest, or (3) is not likely to ever result in human death or serious injury.
Confidentiality	InfoSec policies, procedures, and practices provide strong documented controls to protect data confidentiality; strong indication of favorable practices governing data confidentiality.
Integrity	InfoSec policies, procedures, and practices are strong to protect data integrity based on a high level of controls governing authenticity, nonrepudiation, and accountability. Overall, a strong level of favorable practices govern data integrity and exist throughout the enterprise.
Availability	InfoSec policies, procedures, and practices provide strong internal control guidance to protect the timely availability of information technology resources (systems and data). Strong indication of favorable practices governing data availability.
Auditability	Audit trails are available on screen and printed and are also searchable. The data contained in the audit trails can be investigated using various data storage and access methods (i.e., data missing). Based on the ease and completeness of obtaining key data for computer forensic purposes during internal or law enforcement investigations, there should be no problem in collecting and analyzing critical application systems journaling for evidentiary purposes.

***Application and Code Review*:**

One of the primary goals in penetration testing is to identify security vulnerabilities in a network and to assess how an outsider or insider to an enterprise may either deny service or gain access to information to which the attacker is not authorized. For discussion purposes, given the high level of vulnerability of applications and systems to the insider threat, our focus will be on performing an application and code review penetration test (Table 3.28).

Table 3.28 Performing an Application and Code Review Penetration Test for Web-Based and Web Services Applications

Process	*Criteria*
Web-Based Applications	
Discovery:	Analysis of the technology, architecture, and functionality that comprise the application.
a. Technology	Identify the operating system, Web server version, and additional enabled technology associated with the application.
b. Server Scans	Server scans to identify known application functionality or exposures using the appropriate tools.
c. URL Harvesting	Identifying all known universal resource locators (URLs) within the application.
d. Path Disclosure	Identify the path to document Web roots within the operating system.
e. Directory Listing/ Traversal	Attempt to obtain and traverse directory trees.
f. Virtual Directories	Determine use of virtual directories and their limitations.
g. Functionality Mapping	A functionality map outlines the functions that an area performs and the subcomponents that make up that function.
h. Site Mapping	Create a map that logically portrays the application and identifies pages by type (such as static, dynamic, forms, or common gateway interface [CGI]).

Source Code Review:	Examining the source code of pages.
a. Hidden Fields	Hidden fields may reveal data structure (i.e., <meta content = "JavaScript". Developers may want to « hide data sent from the client to the server from the user. The data is only hidden from view and viewing the source code will show the hidden fields.
b. Comments	Search for unnecessary comments/information in the source, providing an attacker inside knowledge of the application.
c. Unnecessary External Links	Search for unnecessary external links that may direct an attacker to an alternate path of attack.
d. Scripting Language Evaluation	Evaluate scripting language usage such as JavaScript, Visual Basic Script, which may provide an alternate form of attack.
Input Validation	Ensuring the input supplied by the user and input into the browser for use within a Web application are the expected or normal values.
Session Management	Managing Hypertext Transfer Protocol (HTTP)-based client sessions are stateless; however, there are various methods that can be used to control the session management process.
Determine and Verify the Method Used to Maintain State	There are basically three methods available to both allocate and receive session ID information, which include: session ID information is embedded in the URL which is received by the application through HTTP GET requests when the client clicks on links embedded within a page; session ID information is stored within the fields of a form and submitted to the application. Typically the session ID information would be embedded within the form as a hidden field and submitted with HTTP POST command through the use of cookies.
Encryption of Session	Determine if the session IDs are encrypted.
Session Characteristics	Determine if the session IDs are incremental, predictable, or able to be played again.
Session Timeouts	Analyze session time-outs for adequacy.

Session Management Limitations	Determine the session management limitations—bandwidth usages, file download/upload limitations, transaction limitations, etc.
Man-in-the-Middle Attacks	Gather sensitive information with man-in-the-middle attacks and then replay this gathered information to fool the application.
Input Manipulation	Make changes to data input to evaluate the effectiveness of the Web-based applications controls.
Cookie	Ensures the persistent cookie that stores the user's ID and time of last log-in requires the users to reauthenticate themselves if they left the computer without logging off or were inactive for a period of time.
Cookies	Provide a means of time-based authentication. Function by sending parcels of text sent by a server to a Web browser and then sends back the text unchanged by the browser each time it accesses that server.
Passing Cookies	Determine whether the server-side application is passing cookie information to the client's browser.
Manipulate Cookies	Attempt to manipulate cookie information to "spoof" any associated server-side authentication mechanism.
Disable Cookie	Disable client cookie support in the client browser and note any session data that is passed via the URL.
Persistent Cookies	Determine whether persistent cookies are used and if excess information is left on the user's system.
Buffer Overflow Attacks	Determine whether cookies are susceptible to buffer overflow attacks.
User Variables	Variables are temporary holders of information which include numeric, true/false, and objects.
Encrypted Variables	Determine whether user variables are encrypted.
Variable Characteristics	Determine whether user variables are incremental, predictable, or able to be played again.

***Strategic, Legal/Regulatory, and Operational Risk Ratings*:**

Evaluating the impact of ICFTA will be manifested within each family of IT risks, which are the strategic, legal/regulatory, and operational risk ratings (Table 3.29). The aforementioned risk families were intentionally excluded from the ICFTA detailed threat assessment so that the application controls could be viewed in totality instead of having to assess each application control ICF risk individually.

Management should analyze the following minimum considerations when evaluating insider computer fraud and evaluate its impact on the Strategic, Legal,and Operational Risk Matrix criteria below:

- The results of the risk assessment process.
- The results of the PIA.
- The results of the threat assessment.
- The qualitative assessment of residual risk and NRR ratings.
- The adequacy of existing management controls.
- The adequacy of existing technical controls.
- The results of the Defense in Depth Model calculation.
- The assessment of the strength of controls in the existing IT architecture.
- The analysis of internal and external audit reports relating to general and
- application controls.

Table 3.29 The Strategic, Legal, and Operational Risk Assessment Matrix—Low Risk, Strong Controls (1)

General Risk Category[a]	*Area of Concern*	*Related Controls*[b]
Strategic: The risk to earnings or capital arising from adverse business decisions or improper implementation of those decisions. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation	Business case	Strategic technology planning; establish goals and monitor performance; conduct research and consult with experts
	Internal/external resources	Provide adequate training; provide adequate support staff; administration of software updates; insurance coverage (e.g., Fidelity Bond)
	Outsourcing arrangements	Perform due diligence on vendors; audit performance; back-up arrangements
	Technological developments	Monitor new developments; budget for technology upgrades
Legal/regulatory/compliance:The risk to earnings or capital arising from violations of, or nonconformance with, laws, rules, regulations, prescribed practices, or ethical standards	Legal framework	Detailed contracts; digital signature; comprehensive disclosure
	Jurisdiction (e.g., laws, taxes)	Consult with legal counsel; well-defined trade area
	Regulatory compliance	Policies and procedures; consult with regulatory agencies; internal and external audit

General Risk Category[a]	*Area of Concern*	*Related Controls*[b]
Operational risk	Security	Authorization; access control (e.g., passwords, log-on IS); authentication; secure data storage; encryption; firewalls/filtering routers
	Operations	Policies and procedures; client accounting; contingency plans; back-up training; audit procedures

The Information Security Scorecard:

The information security scorecard (Table 3.30) is a diagnostic tool for management to evaluate the effectiveness of management's policies and standards and practices to identify measure, monitor, and control information risks and controls. Thescorecard rating criteria and its companion "INFOSEC Scorecard for Corporation XYZ" are intended to establish an enterprise-wide information security component and composite ratings based on a combined total of eight general and application control components.

There are two application components: one for the software development process (preimplementation projects) and the other for production applications and systems. The remaining components should be placed in the generic category of general controls.

Table 3.30 The Information Security Scorecard for Corporation XYZ

Number	*Category*	*2006*	*2005*	*Security Trend*
1	Security policies and standards	G	G	›
2	System development and security architecture	R	Y	
*3	Production application system security	Y	R	
4	Network security	G	Y	
5	User authentication and access controls	G	G	›
6	Security monitoring	R	Y	
7	Vendor management for security	R	Y	
8	Incident response (including computer forensics)	R	R	›
	Overall	R	Y	

Develop Security Patterns for Applications/ Systems Software Engineering (Process and Product Improvements)

The concept of "pattern" is a solution to a problem in a context. The concept of developing patterns is relatively new but is growing in popularity, particularly among those who work in the computer science community.

From a computer science perspective, software engineering has benefited from the use of design patterns, by using developed patterns to capture, reuse, and teach software design expertise. Patterns from a software development perspective might use Unified Modeling Language (UML) diagrams as a tool for implementing software design issues and sample code implementing the pattern and proposed solution.

A pattern definition, whether involving a design pattern for software engineering or security purposes, generally includes the following basic elements:

Context: Environmental assumptions, policy statements

Problem: Security objectives, threats, attacks

Forces: Functional security requirements

Solution: To be determined

Implemented Software Engineering InfoSec Process and Product Improvements

The last phase of the integrated business and technology risk, threat, and privacy impact assessments should consider the following minimum factors prior to deciding to implement the following controls to reduce risks associated with the insider threat:

- *Reevaluation of Software Development Policies, Procedures, and Practices*: Ensure security controls are “baked” into the software development life cycle.
- *Architectural Considerations*: Evaluate additional layers of defense in the Defense in Depth Model.
- *Stricter Access Controls*: Implement more restrictive access controls.
- *Quarantine and Isolation*: Determine the need for compartmentalizing systems and data to reduce the potential for insider misuse.
- *Misuse Detection*: Determine the need for selective application and system journaling of KFIs and deployment of various computer forensic techniques for tracking and trace-back purposes.
- *Anomaly Detection*: Determine the need for developing and deploying advanced technologies to capture information on day zero attack vectors from insiders (i.e., neural networks and behavioral modeling).
- *Recovery of Information*: Possess the technology needed for decrypting sensitive data that may be hidden and protected by the insider in a distributed and fragmented manner of storage.

References

1. Kenneth C.Brancik, —Insider Computer Fraud‖, Auerbach Publications Taylor & Francis, Group 2008.
2. Permission to reproduce extracts from BS ISO/IEC/2700: 2005 is granted by BSI.British Standards can be obtained in PDF format from the BSI Online Shop: http://www.BS l-Global.com/en/shop
3. GTAG (Global Technology Audit Guide), Application Based Controls. The Institute of Internal Auditors, 2005.
4. The FFIEC Information Security Booklet, 2006.
5. Komanosky, Sasha. Enterprise Security Patterns, June 2004. The original source for the security pattern was the 3/03I SSA Password/Journal *Enterprise Security Patterns.*