Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Assessing Threats To Information Security In Financial Institutions

Threat assessment is an essential component of an information security risk evaluation. In order to prioritize vulnerabilities for remediation and to evaluate existing controls, a thorough understanding of potential threat sources is required. Particularly for financial institutions, this activity is a pre-requisite for a comprehensive information security program and a stated regulatory requirement. This paper explores key issues related to threat assessment, including essential elements, methodologies, and common pit...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

ASSESSING THREATS TO INFORMATION SECURITY IN FINANCIAL INSTITUTIONS

GSEC Certification Practical Assignment
Version 1.4b - Option 1

Prepared By:

Cynthia A. Bonnette
GSEC Certification Candidate

Submission Date: July 9, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003. As part of the Information Security Reading Room. Author retains full rights.

Cynthia A. Bonnette
July 9, 2003

ABSTRACT

Threat assessment is an essential component of an information security risk evaluation. In order to prioritize vulnerabilities for remediation and to evaluate existing controls, a thorough understanding of potential threat sources is required. Particularly for financial institutions, this activity is a pre-requisite for a comprehensive information security program and a stated regulatory requirement. This paper explores key issues related to threat assessment, including essential elements, methodologies, and common pitfalls. A recommended approach for completing and documenting this activity is also provided. While the focus of this paper is on financial institutions and related regulatory requirements, the general concepts and the recommended approach for conducting a threat assessment are applicable to other organizations and industries.

© SANS Institute 2003, Author retains full rights.

TABLE OF CONTENTS

SECTION 1.0 - OVERVIEW OF THREAT ASSESSMENT 1

1.1 The Importance of Threat Assessment 1
1.2 Role in Risk Assessment 2
1.3 Prioritization of Security Initiatives 3
1.4 Regulatory Requirements 3

SECTION 2.0 - COMMON PITFALLS AND PROBLEMS 4

2.1 Undervalued Benefits 4
2.2 Measurement Challenges 4
2.3 Focus on Vulnerabilities 5

SECTION 3.0 - KEY ISSUES 5

3.1 Threat Categories 5
3.2 Qualitative and Quantitative Assessments 7
3.3 Rating Methodologies 8
3.4 Critical Factors 9

SECTION 4.0 - RECOMMENDED APPROACH 9

4.1 Scope 10
4.2 Participants 10
4.3 Process 10
4.4 Documentation 11

SECTION 5.0 - FUTURE DEVELOPMENTS AND CONCLUSIONS 11

5.1 Quantification Measures and Models 11
5.2 Automated Assessments 12
5.3 Conclusions 12

SECTION 6.0 - APPENDIX 13

6.1 Sample Threat Analysis Form 13
6.2 References 14

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1.0 OVERVIEW OF THREAT ASSESSMENT

It has been said that, at any given moment, one in five organizations will have experienced a direct breach in security.[1] Security professionals who are charged with protecting their organizations' information assets must understand the source of these attacks, along with their likelihood of occurrence and related impact. However, the process of identifying and assessing threats to information security presents a number of challenges. Each organization must develop and implement a method to evaluate threats based on their unique circumstances and overall risk assessment program. Financial institutions, in particular, face a wide range of threats and are subject to regulatory requirements that must be addressed in the context of their threat analysis.

Threat assessment involves identifying potential sources of harm to information assets and evaluating the probability and consequences associated with their action. A comprehensive threat analysis is part of the overall risk assessment process, which also considers the extent of existing vulnerabilities and the value of information assets that may be compromised. The relationship of threats, vulnerabilities, and risk is demonstrated by the following formula[2]:

RISK = THREAT X VULNERABILITY

In essence, the formula states that risk (the possibility that "bad things might happen") is a function of a threat (a source of harm or attack) acting on a vulnerability (a weakness or deficiency in controls). The severity of the risk will also be influenced by the value of information assets that might be damaged or destroyed due to an exploit.

1.1 The Importance of Threat Assessment

A comprehensive threat assessment is important for financial institutions for several reasons. As noted above, a threat assessment is a key component of an information security risk assessment. In order to develop a security program that properly protects critical data, systems, and other resources, the institution must first understand what it is facing in terms of potential sources of harm that may exploit existing vulnerabilities. However, the nature of applicable threats, including their likelihood and impact, will be different for each institution based on individual circumstances.

Because of the valuable and sensitive information that they handle, financial institutions face a wide range of highly motivated and active threat sources. A recent report from Symantec Corp. noted that financial institutions are the second most likely category of organizations to be attacked, following the power and energy industry. Specifically, the severe event incidence rate increased to 48% for the second half of 2002, from 28% for

[1] IP3 Security Workshop promotional advertisement. URL: http://www.ip3seminars.com.
[2] SANS Security Essentials Course Material, Day 2, "Threat and the Need for Defense in Depth."

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the six-month period ending December 31, 2001.[3] This means that nearly half of all financial institutions represented in the Symantec study experienced a severe attack from an Internet threat source. Accordingly, financial institutions must factor the likelihood and potential impact associated with this threat source into their information security program.

However, Internet based threats, which are the focus of the Symantec study, do not represent the only source of attack on financial institutions. A wide range of human and non-human threat sources exist which must be identified and evaluated. As with their heightened exposure to Internet-based threats, it can be safely assumed that financial institutions will continue to represent an attractive target due to the nature of their business. Sensitive customer information and access to the payment system will always draw the interest of attackers who follow in the footsteps of the infamous bank robber Willie Sutton who admitted that he robbed banks because, "That's where the money is."

1.2 Role in Risk Assessment

Threat analysis represents a key component of the larger information security risk assessment process. The National Institute of Standards and Technology's (NIST) Special Publication 800-30, "Risk Management for Information Technology Systems," outlines a comprehensive nine-step process. The second step involves threat identification, with the goal of creating an estimate of the motivation, resources, and capabilities that may carry out a successful attack.[4] Other widely-recognized industry approaches to risk assessment, including the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology developed by CERT (the Computer Emergency Response Team) at Carnegie Mellon University, also incorporate threat analysis or profiling as a part of their process.[5]

Threat analysis is critical because, in order for a risk to materialize, a threat source must act on an existing vulnerability. In fact, an institution can exist for an indefinite period of time with numerous vulnerabilities but never suffer an exploit due to the lack of a corresponding threat source. However, this is simply the result of good fortune and happenstance—not a reliable security practice. Figure 1 on the following page lists potential threat categories, vulnerabilities that might be exploited, and resulting "outcomes" or consequences.

---

[3] Symantec Corp., Symantec Internet Security Threat Report, edited by Mark Higgins, February 2003, URL: http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0 (a copy of the report requires free registration).

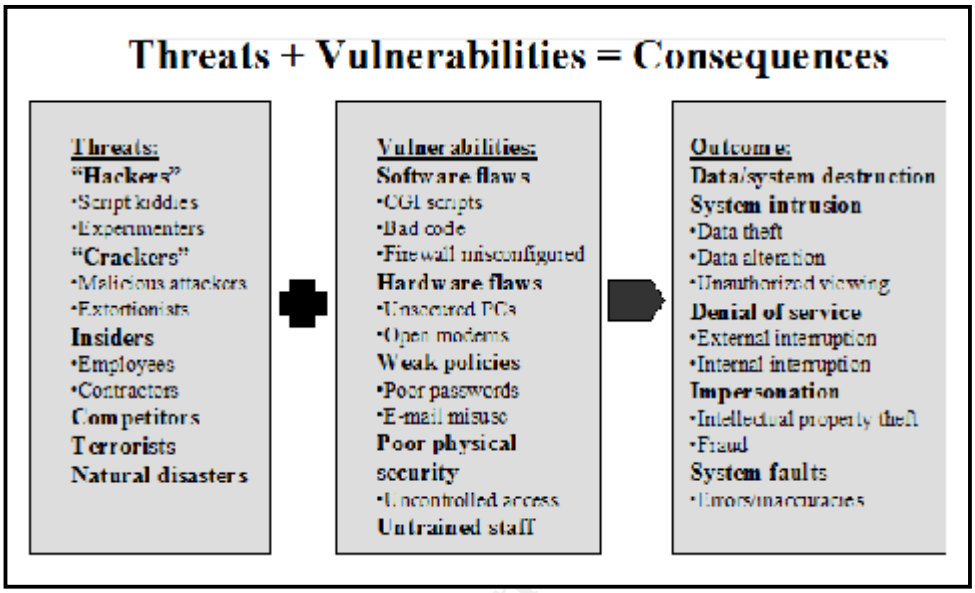
[4] Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis, Risk Management for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Special Publication 800-30, October 2001, URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

[5] Alberts, Christopher and Dorofee, Audrey, OCTAVE Threat Profiles, Software Engineering Inst., Carnegie Mellon Univ., URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

In order to execute due diligence and maintain an appropriate information security program, industry practices require that a risk assessment, incorporating an analysis of threats, vulnerabilities, and their potential consequences be conducted.

Figure 1



1.3 Prioritization of Security Initiatives

One of the most valuable benefits of a comprehensive threat analysis is the ability to prioritize security initiatives, including corrective action to address vulnerabilities. Understanding the relative likelihood and impact associated with identified threat sources allows the information security professional to appropriately allocate resources to weaknesses that are more likely to be attacked. Given the limited resources available to most financial institutions, 100% correction of all vulnerabilities is not a feasible option. Accordingly, the knowledge of where attacks are likely to originate, their motivation, and their behavior pattern represents valuable intelligence that can help formulate a targeted information security strategy.

1.4 Regulatory Requirements

Financial institutions are required by Federal regulation to maintain an appropriate written information security program that is based on a risk assessment.[6] The regulation results from the July 2001 passage of the Gramm Leach Bliley Act, which addresses information security standards in Section 501(b). Specifically, Part III B1-2 requires that each institution identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of

[6] "Security Standards for Customer Information: Guidelines Establishing Standards for Safeguarding Customer Information," FDIC Financial Institution Letter FIL-22-2001, March 14, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0122.html.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

customer information or customer information systems. The financial institution must also assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.[7] Accordingly, financial institutions must conduct and document their threat assessment in order to demonstrate compliance with regulatory requirements, which will be evaluated at periodic onsite examinations.

2.0 COMMON PITFALLS AND PROBLEMS

Despite the clear logical, economic, and regulatory justifications for conducting a threat analysis as part of an overall risk assessment, many financial institutions fail to perform this important activity. Furthermore, many institutions conduct an inadequate or inappropriate threat analysis that provides little benefit. This section explores some of the reasons why many threat assessments remain undone or fall short.

2.1 Undervalued Benefits

The benefits of a threat analysis are not always apparent to executive management, and sometimes even to information security professionals. Because threat analysis can be an abstract activity that is difficult to measure, its benefits are often unrecognized or undervalued. The exercise of identifying and ranking potential threat sources is often seen as an "academic" effort that yields interesting information of uncertain practical value.

To address this misperception, the threat analysis should be conducted according to a predefined procedure that is documented and reviewed by management. The results of the assessment must be put to practical use, as outlined in Section 4 of this paper, and the associated benefits to the institution documented. As a last resort, regulatory requirements represent an indisputable reason why the activity must be done (i.e., the benefit is the avoidance of criticism and penalties).

2.2 Measurement Challenges

The difficulty of precisely measuring the benefits of a threat assessment and the abstract nature of the activity itself often leads to under-appreciation of its worth. The ability to demonstrate the dollars saved by a thorough analysis is challenging, if not impossible to produce. Furthermore, the dollar costs associated with the respective threats and their potential consequences may also defy accurate calculation.

In the absence of quantifiable measurements, a qualitative approach to threat analysis can be performed that demonstrates the importance of the activity and the significance of the various identified threat sources. Rather than measuring threats in dollar terms, the qualitative approach considers their significance in more general and relative terms.

[7] "501(b) Examination Guidance: *Examination Procedures to Evaluate Customer Information Safeguards*," FDIC Financial Institution Letter FIL-68-2001, August 24, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0168.html.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Although not as appealing to a financial institution's executive management and cost-conscious board members, qualitative assessments can be effective and meaningful.

2.3 Focus on Vulnerabilities

Vulnerabilities are often more easily expressed in precise and measurable terms. As such, a vulnerability assessment that yields an enumerated list of weaknesses to address often commands greater attention and response than the less well-defined threat analysis. However, as noted previously, it takes a threat source in combination with a vulnerability to result in an exploit, and therefore both sets of information must be considered in combination.

Ideally, the vulnerability assessments that are performed of technical, administrative, and physical processes and controls will be evaluated in the context of the threat assessment. Consideration of vulnerabilities and threats together allows for prioritization and proper scheduling of corrective action.

3.0 KEY ISSUES

Recognizing that a threat analysis is an essential component of an information security risk assessment and the overall information security program, the critical elements of this activity can be explored. The three essential elements for a comprehensive threat analysis include:

- Identification – Threat identification involves the process of determining what threat sources exist that may result in harm to sensitive or valuable information assets.
- Measurement – Qualitative and quantitative measurements can be used to determine the likelihood that a threat will materialize and the extent of its possible impact on the financial institution, and its stakeholders.
- Evaluation – Based on the estimates of their likelihood and impact, threat sources can be prioritized and a response strategy can be developed.

3.1 Threat Categories

The process of threat identification begins with an understanding of the financial institution's environment, including its business strategy, information systems (automated and physical), policies and procedures, human stakeholders (management, employees, customers), and physical resources (facilities, equipment). Each of these factors will impact potential threat sources, their motivation, method, and consequences. An understanding of threats can best be achieved by grouping them into categories. Three intuitive categories include human, non-human, and mixed threats. Specific examples include the following:

Human – People-based threats can include individuals from inside and outside the organization. This represents the broadest category with a wide range of capabilities

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and motivations. Within this broad category, a number of subgroups can be identified for independent assessment:

- Hackers – These individuals are characterized by their strong interest in computer technology and desire to learn more by playing with systems and testing their capabilities. Often this involves testing systems they do not own.
- Crackers – This group is distinguished from hackers by their more malicious intentions. While claiming a strong interest in technology, their goals tend to be criminal in nature (e.g., theft, destruction, or denial of service to data or systems).
- Insiders – This group includes a wide range of individuals with some degree of legitimate access to an organization's systems (e.g., full and part time employees at all levels, consultants, contractors, etc.). These individuals may cause harm out of malicious intent or innocently damage systems due to error.
- Partners – Service providers, vendors, business partners, and their employees present similar concerns as insiders. Their access to information systems and data can lead to intentional or unintentional damage or compromise.
- Competitors – Foreign or domestic competitors may seek to gain an advantage by exploiting information systems. This may be done with the assistance of hired crackers or others to gain unauthorized access to sensitive corporate data.
- Terrorists – This group may include political or social organizations that seek to gain attention and influence through disruptive and harmful acts. Terrorist attacks can be both targeted and random.

Non-human – The category of non-human threats includes all types of natural disasters such as fires, floods, earthquakes, tornadoes, hurricanes, and severe storms. Generally, this category of threat sources consists of non-targeted events (i.e., a financial institution is not "singled out" by the threat source). However, based on the geographic location, and other circumstances, the possibility of experiencing an event involving one of these non-human threats may be more or less likely.

Mixed – This category consists of threat sources that are characterized by a blend of human and non-human involvement. Examples include malicious code (Trojan horses, viruses, worms, etc.) that is originally created by a person, but then takes on a "life of its own" on the Internet. Such mixed threats may be targeted at specific financial institutions or they may attack randomly.

In CERT's OCTAVE Method, threat scenarios are developed based on known attack sources and expected outcomes. Threats with a common theme are grouped together according to four standard categories including: (1) Human actors using network access, (2) Human actors using physical access, (3) System problems (e.g., hardware defects, software defects, viruses, malicious code, etc.), and (4) and Other problems (e.g., natural disasters, power outages, etc.).[8]

[8] Alberts, Christopher and Dorofee, Audrey, OCTAVE Threat Profiles, Software Engineering Inst., Carnegie Mellon Univ., URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Depending on each financial institution's circumstances, the various threat categories outlined above may be more or less relevant. Therefore, the first step in the threat analysis process involves identifying all potential threat sources so that they can be assessed and prioritized.

3.2 Qualitative and Quantitative Measurements

The next step in the threat analysis process is to measure the various threats in terms of their likelihood of occurrence and their potential impact. Based on these determinations, threat sources can be evaluated and prioritized. Two types of methods for measuring the likelihood and impact include: *Quantitative*, which defines measurements in numerical (or dollar) terms and *Qualitative*, which utilizes general terms of business significance. The best approach depends on the nature of the threat being evaluated. Quantitative measurements are appealing as they are easily understood and compared. However, significant challenges in determining probability estimates and forecasting impact must be met. Regardless of whether a quantitative or qualitative measurement is used, threat value is a function of the likelihood or probability that the threat will materialize, and the potential impact that the threat's exploit will have on the institution. The following formula demonstrates this relationship.

THREAT VALUE = LIKELIHOOD X IMPACT

Measuring the likelihood that a threat will materialize requires an estimate of probability. Depending on a financial institution's prior experience with a similar threat, this might be calculated as a projected number of events per year (e.g., the institution expects to experience four serious virus infections, affecting 25% of PCs, per year). A more simplistic measurement of likelihood is a general estimate of occurrence on a numeric scale (1 – 5) or relative scale (very likely, somewhat likely, likely, not likely).

Impact measurements involve a forecast of the possible damage that would result if the identified threat were to exploit an existing (or future) vulnerability. Impact measurements can be calculated in dollar terms by summing the various costs associated with the exploit (damage to information, damage to equipment, system downtime, repair costs, etc.) However, a number of challenges exist in developing such estimates. In particular, intangible effects (damage to reputation, intellectual property, etc.) can be difficult, if not impossible to calculate. As noted by security analyst John McCormick, "Making an accurate threat estimate depends on a number of factors, including intangibles. For example, will recent publicity raise the ire of the wrong high school student, or will the color of your company's logo make some wacko think your firm operates in the service of Satan?"[9]

[9] McCormick, John, "Determine the Value and Vulnerability of Company Data to Evaluate Security Threats," March 23, 2000, TechRepublic Web Site, URL(Note - web site access requires free registration): http://www.techrepublic.com/article.jhtml?id=r00220000323eje02.htm&src=search.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Consistency in cost estimates can also be problematic, particularly when there is limited experience with prior events of a similar nature. In the absence of cost data, a more general estimate of impact can be assigned using a numerical scale (1 – 5) or relative scale (very serious, serious, material, immaterial).

3.3 Rating Methodologies

The purpose of rating or prioritizing threats is to provide for a means to devote appropriate attention and resources to the development of a response strategy. Clearly threats that pose a greater likelihood of attack and present the greatest potential impact on the financial institution warrant more attention than those of lesser significance. Accordingly, a consistent method of evaluating and rating threat sources is essential.

As discussed previously, quantitative and qualitative measurements may be used to assess each threat's likelihood of occurrence and potential impact. The combination of these factors will determine the overall threat value at a given point in time. However, in order to prioritize a wide range of threats, a ranking based on the comparative threat value is important. This will facilitate the process of assigning scarce resources to the development and implementation of mitigating strategies.

Rating methodologies can be as precise or as general as a financial institution prefers based on their overall approach to threat analysis and risk assessment. As noted above, a calculation of threat value can be determined by combining the probability of occurrence with the estimated cost of impact. These comparative values can then be used to rank or prioritize respective threats. However, in the absence of quantitative values, a more general assessment of threat value can be assigned using a numerical scale (1 – 5) or relative scale (high, medium, low) to represent the threat's overall significance.

Industry experience has indicated that precision in determining threat values has generally not been a deciding factor in establishing or maintaining an effective information security program. Rather, a general understanding of the most significant threats and a corresponding strengthening of controls in certain areas have proved to be a more successful and cost effective strategy. For example, in his August 2001 GSEC Practical, A Perspective on Threats in the Risk Analysis Process, Arthur Nichols outlines an approach that applies general risk categories (certain, high, moderate, limited, and unknown) to threat occurrence and economic risk categories (significant, moderate, low, and value not known) to threat consequence.[10]

One area where financial institutions may be able to leverage existing work for the benefit of their threat assessment involves disaster recovery and business continuity planning. Financial institutions are required to have formal recovery and contingency plans that are based on an assessment of various disaster scenarios. The process for conducting a scenario analysis involves the identification of possible disaster events,

[10] Nichols, Arthur, A Perspective on Threats in the Risk Analysis Process, GSEC-1184 August 31, 2001, SANS Infosec Reading Room, URL: http://www.sans.org/rr/paper.php?id=63.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and evaluation of their likelihood and impact. Given the similarities between this process and the threat assessment for information security, it follows that certain activities, rating scales, and documentation can be leveraged.

3.4 Critical Factors

A comprehensive threat assessment involves identification, measurement, and evaluation. Once these steps have been performed, strategies can be developed to mitigate the threats, along with the vulnerabilities that they may exploit. "The final prioritization of threats takes place when there are indications of targeting against a specific information asset. When this occurs, threats can be categorized as either potential (the attack has not actually taken place) or active (an attack has been attempted or in some other way demonstrated to be feasible). In considering implementation of security controls, these threats, if applicable to the information assets of an organization, should receive the highest effort and priority."[11]

It is important to note that the completed threat assessment yields a picture of the financial institution at a given point in time. As internal and external circumstances change, the threat assessment must continue to be revised in order to remain current and relevant. For example, a financial institution may undergo a merger or acquisition, resulting in staff reductions and a heightened number of disgruntled employees. Such will affect the probability or likelihood of the insider threat. Another example involves computer system changes that increase employee access rights to critical data, thereby affecting the potential impact that an insider threat might present.

To ensure continued relevance, the threat assessment should be updated periodically. Threat categories should be reviewed for continued appropriateness and estimates of likelihood and impact should be re-evaluated. The overall threat ranking and prioritization should be re-assessed based on current circumstances and historical experience. According to regulatory requirements implementing the Gramm Leach Bliley Act, financial institutions are required to revisit and report to the board on the status of their information security program, including the threat assessment, at least annually. The regulation also notes that more frequent updates may be warranted due to significant changes in circumstances.

4.0 RECOMMENDED APPROACH

The fundamental steps of a threat assessment have been outlined above. However, a comprehensive and appropriate process also depends on a number of supporting factors. Properly scoping the assessment, involving the right group of participants, and documenting the results are discussed below.

[11] Anderson, Kent, "Intelligence-Based Threat Assessments for Information Networks and Infrastructures," March 11, 1998 (Revised January 25, 1999), SecurityFocus Web Site, URL: http://www.securityfocus.com/library/490.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.1 Scope

The scope of the threat analysis should be consistent with the overall information security risk assessment. It is generally recommended that both activities be conducted on an enterprise-wide basis (as opposed to an exclusive focus on a single group or area, such as the information technology department). In addition, the threat assessment should consider all potential sources of harm to information assets in any form (physical, electronic, intangible). A properly defined, clearly articulated, and documented scope will ensure that all participants in the process conduct the threat assessment consistently and appropriately.

4.2 Participants

One of the key benefits that a threat assessment brings to the financial institution is a heightened awareness of what it is up against in terms of inside and outside attack sources. However, in order to identify all potential threat sources, it is necessary to include a wide range of participants in the threat analysis process. Specifically, representatives from the physical security area, human resources, information systems security, audit, and legal departments will each offer unique perspectives and experience. A recognized industry best practice involves forming a cross-department committee or working group to conduct the threat analysis. An appropriate leader or chairman for the group is the information security officer, who will use the threat analysis as a key component of the overall risk assessment.

4.3 Process

The process of completing the threat analysis should be in the form of a written procedure that all participants will follow. The procedure should outline the steps of the process and who is involved at each stage. Certain activities can be conducted independently by group members, while other activities are most productive when performed as a group exercise. A recommended four-step process is outlined below:

Step 1 – The information security officer notifies the group members that a threat analysis will be conducted. In preparation, members are provided with a current copy of the procedure, documentation from the prior threat analysis, and a blank documentation form (see example provided in Section 6.1 of the Appendix).

Step 2 – The group members review the information and consider the threat sources that have been previously identified for any changes in perceived likelihood, impact, and overall ranking. In addition, members are asked to consider any new threat sources that should be added to the list.

Step 3 – A group meeting is held to share input and determine consensus. Group members may complete the blank documentation form prior to the meeting or during the session. However, the primary objective of the meeting is to share information and perspectives on the various identified threats and their characteristics. As a result of the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

discussion and the independently prepared documentation forms, a final group assessment will be drafted. The information security officer will ultimately decide any disagreements.

Step 4 – A single documentation form, representing the group's consensus determination, will be prepared by the information security officer. The information security officer will utilize the results in the overall risk assessment process and will submit the threat analysis to senior management for final review and approval.

4.4 Documentation

To ensure that the threat analysis is conducted consistently and according to the financial institution's policy and procedures, the use of a standard form is recommended. The sample form provided in the Appendix offers an example of an effective tool to record the input of the respective participants in the process and the group's consensus. While the sample form is structured for a qualitative threat analysis, it can be easily modified to record the results of a quantitative method. Regardless of the approach employed, documentation serves a number of important benefits:

- Provides a historical record of the analysis to build upon in the future.
- Provides a means for senior management to review, approve, and document their involvement in the activity.
- Demonstrates that the financial institution is meeting its regulatory requirements and exercising "due care".

5.0 FUTURE DEVELOPMENTS AND CONCLUSIONS

The failure to conduct a threat assessment, and the frequent inadequacies observed in those that are conducted, often result from a misunderstanding or under-appreciation of their benefits. Often, a qualitative threat assessment is considered an "academic" exercise due to the intangible nature of the results. Quantitative threat assessments may have the appeal of numerical results; however, their credibility can suffer from the lack of historical data to serve as a foundation. However, these perceived shortcomings are rapidly being overcome as threat analysis gains widespread adoption and experience.

5.1 Quantification Measures and Models

The insurance industry, in particular, is gaining experience with the probability and historical losses associated with a variety of information security events. As new types of insurance coverage (e.g., electronic crimes, data and intellectually property loss, denial of service, etc.) are deployed in the marketplace, experience with actual claims will contribute to new models for calculating risk exposure. Data maintained internally by individual financial institutions regarding security events and data gathered by managed security service providers will also contribute to greater industry knowledge of the costs and probabilities associated with specific threats. As such, quantitative

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

measurements and models will likely improve over time and gradually replace the qualitative approach.

5.2 Automated Assessments

As automated tools for information system audit and policy compliance become more widely used, it can be expected that the information gathered will be combined with the data collected by security event monitoring systems (intrusion detection systems, firewall logging tools, etc.). With the emerging opportunity to correlate and combine this information, automated threat assessment tools become a very real possibility. It can also be expected that these tools will someday be incorporated with new models for quantitative threat analysis, yielding a completely automated assessment process. However, while these tools of the future may offer great value, they will never fully replace the experience, perspective, and intuition of human beings. Leading financial institutions will always combine automated capabilities with human oversight and intelligence.

5.3 Conclusions

A comprehensive threat assessment is a fundamental part of an information security risk assessment. Unfortunately, threat assessments are often disregarded or improperly conducted due to misperceptions regarding their value and benefits. A threat assessment should be properly scoped to identify relevant sources of harm to the financial institution's information assets. Once threat sources have been identified, their likelihood of occurrence and potential impact can be measured in quantitative or qualitative terms. Representatives from key departments in the institution should participate in the process to offer their perspectives in evaluating the relevance and priority of the identified threat sources. The process should also be consistently documented in order to demonstrate that regulatory requirements have been met and that due care has been exercised by the financial institution and its management.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.0 APPENDIX

6.1 Sample Threat Analysis Form[12]

THREAT CATEGORY/SOURCE	RATINGS Likelihood (1)	Impact (2)
Insider (employee, contractor, partner) *Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.*		
Former insider *Consider the potential for abuse of confidential information, sabotage, harassment, bribery, extortion, identify theft, fraud, data corruption/alteration, unauthorized transactions, etc.*		
Hacker/cracker *Consider the potential for unauthorized access, intrusion, Data theft, data destruction, identity theft, financial frauds, Information bribery/extortion, spoofing, impersonation, etc.*		
Malicious code (virus, Trojan horse, etc.) *Consider the potential for data loss or corruption, denial/disruption of service, damage to systems and hardware, etc.*		
Competitor *Consider the potential for abuse of confidential information, sabotage, theft of trade secrets, etc.*		
Terrorist *Consider the potential for data loss or corruption, denial/disruption of service, damage to systems and hardware, etc.*		
Natural disaster (Snow/ice storm, fire, flood) *Consider the potential for denial/disruption of service, loss or corruption of data, harm or inconvenience to staff, damage to hardware/facilities, lack of access to facilities, etc.*		
Other		

Ratings are based on:
(1) Likelihood: Determined on a 0–4 scale, based on probability of occurrence:
0: Remote – Event may only occur in exceptional circumstances
1: Unlikely – Event could occur at some time
2: Moderate – Event should occur at some time
3: Likely – Event will probably occur in most circumstances
4: Almost Certain - Event is expected to occur in most circumstances

(2) Impact: Determined on a 0–4 scale, considering the tangible and intangible consequences.
0: Insignificant - Negligible consequences
1: Minor - Minor consequences, damage, and/or loss
2: Moderate - Significant consequences, damage, and/or loss
3: Major - Serious consequences, damage, and/or loss
4: Catastrophic - Worst case consequences, severe and lasting damage and/or loss

[12] Bonnette, Cynthia, M ONE's Information Security Risk Assessment Guidebook, October 2002, URL (general information): http://www.moneinc.com/resources/pdf/5-M_ONE_IS_Risk_Assessment_Guidebook.pdf.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

6.2 References

"501(b) Examination Guidance: *Examination Procedures to Evaluate Customer Information Safeguards*," FDIC Financial Institution Letter FIL-68-2001, August 24, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0168.html.

Alberts, Christopher and Dorofee, Audrey, OCTAVE Threat Profiles, Software Engineering Inst., Carnegie Mellon Univ., URL: http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf.

Anderson, Kent, "Intelligence-Based Threat Assessments for Information Networks and Infrastructures," March 11, 1998 (Revised January 25, 1999), SecurityFocus Web Site, URL: http://www.securityfocus.com/library/490.

Bassham, Lawrence E. and Polk, Timothy W., Polk, "Threat Assessment of Malicious Code and Human Threats, National Institute of Standards and Technology, Computer Security Division, March 1994, URL: http://csrc.nist.gov/publications/nistir/threats.

Bonnette, Cynthia, M ONE's Information Security Risk Assessment Guidebook, October 2002, URL (general information): http://www.moneinc.com/resources/pdf/5-M_ONE_IS_Risk_Assessment_Guidebook.pdf.

IP3 Security Workshop promotional advertisement, June 2003, URL: http://www.ip3seminars.com.

McCormick, John, "Determine the Value and Vulnerability of Company Data to Evaluate Security Threats," March 23, 2000, TechRepublic Web Site, URL: http://www.techrepublic.com/article.jhtml?id=r00220000323eje02.htm&src=search (access requires free registration).

Mitnick, Kevin and Simon, William L., The Art of Deception, Wiley Publishing, Inc., Indianapolis, IN, 2002.

Nichols, Arthur, A Perspective on Threats in the Risk Analysis Process, GSEC-1184 August 31, 2001, SANS Infosec Reading Room, URL: http://www.sans.org/rr/paper.php?id=63.

Peltier, Thomas R., CISSP, "Information Protection Fundamentals," CSI Editorial Archive Copyright 1998, Computer Security Institute Web Site, URL: http://www.gocsi.com/archive/policy.html.

SANS Security Essentials Course Material, Online Training, June 2003, Materials are available at the GIAC web site, URL: http://giactc.giac.org/cgi-bin/momgate (access requires paid registration).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

"Security Standards for Customer Information: Guidelines Establishing Standards for Safeguarding Customer Information," FDIC Financial Institution Letter FIL-22-2001, March 14, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0122.html.

Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis, Risk Management for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Special Publication 800-30, October 2001, URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Symantec Corp., Symantec Internet Security Threat Report, Edited by Mark Higgins, February 2003, URL: http://enterprisesecurity.symantec.com/Content.cfm?articleID=1964&EID=0 (a copy of the report requires free registration).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 26th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Cyber Defense San Diego 2014	**San Diego, CAUS**	**Nov 03, 2014 - Nov 08, 2014**	**Live Event**
SANS DFIRCON East 2014	**Fort Lauderdale, FLUS**	**Nov 03, 2014 - Nov 08, 2014**	**Live Event**
SANS Sydney 2014	**Sydney, AU**	**Nov 10, 2014 - Nov 22, 2014**	**Live Event**
SANS Korea 2014	**Seoul, KR**	**Nov 10, 2014 - Nov 15, 2014**	**Live Event**
SANS Tokyo Autumn 2014	**Tokyo, JP**	**Nov 10, 2014 - Nov 15, 2014**	**Live Event**
Pen Test Hackfest	**Washington, DCUS**	**Nov 13, 2014 - Nov 20, 2014**	**Live Event**
SANS London 2014	**London, GB**	**Nov 15, 2014 - Nov 24, 2014**	**Live Event**
SANS Hyderabad 2014	**Hyderabad, IN**	**Nov 24, 2014 - Nov 29, 2014**	**Live Event**
Healthcare Cyber Security Summit	**San Francisco, CAUS**	**Dec 03, 2014 - Dec 10, 2014**	**Live Event**
SANS Cyber Defense Initiative 2014	**Washington, DCUS**	**Dec 10, 2014 - Dec 19, 2014**	**Live Event**
SANS Oman 2015	**Muscat, OM**	**Jan 03, 2015 - Jan 08, 2015**	**Live Event**
SANS Security East 2015	**New Orleans, LAUS**	**Jan 16, 2015 - Jan 21, 2015**	**Live Event**
SANS Gulf Region 2014	**OnlineAE**	**Nov 01, 2014 - Nov 13, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**