IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5167

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

Enhancing Information Security: A Qualitative Risk Analysis Method for Overcoming the Insider Threat

Patricia Y. Logan
Marshall University, 100 Angus E. Peyton Dr., South Charleston, WV 25303-1600, USA, loganp@marshall.edu

Allen C. Clarkson
Independent Consultant, San Antonio, TX, allen.clarkson@gmail.com

ABSTRACT

A number of recent studies document that "the insider" is a significant risk to information security. The results of these studies suggest that a new approach be used to assess, inform, train, manage and mitigate the risk from insider intrusion. An improved method is proposed for assessing risk and applying appropriate controls: a qualitative approach using an insider-based risk assessment (IBRA). This paper explores the risks from insiders, how insiders evade technology, an exploration of the traditional means of quantitative security assessment, and proposes a new method designed to improve the identification of risk from insiders, improve security, and apply controls appropriate to the insider threat.

CONSEQUENCES AND SIGNIFICANCE OF INSIDER THREATS

The risk of intrusion comes from two broad categories: external and internal. The Working Council for Chief Information Officers (2003) published a diagram (Figure 1) that provides a view of the threat landscape [11].

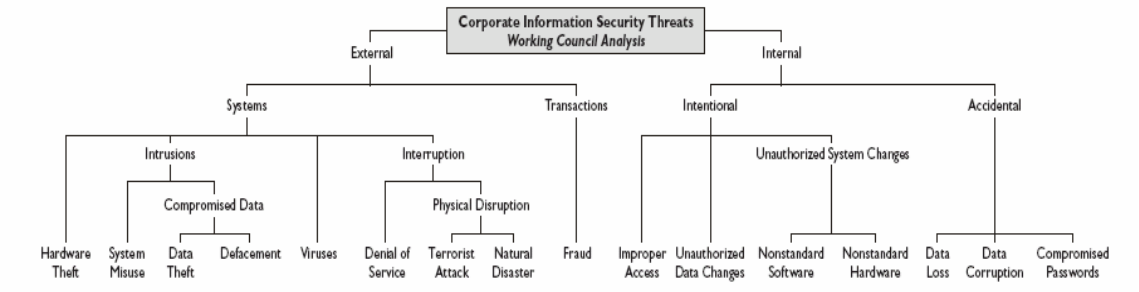
Information security planning and management should properly include the full-spectrum of potential threats. The current security posture of the majority of businesses does not account for threats that originate from the inside and as a result, may be placing information assets at extreme risk. The risk to information security has shifted from the "nameless" external threat to the insider as Gartner estimates that 70 percent of the financial losses caused by security breaches involve insiders.[1,8] Prosecutions by the FBI's CCIPs (Computer Crime and Intellectual Property Section) document over 60 cases prosecuted under 18 U.S.C. §1030 [16] with over one-half of the cases involving an individual with a connection to the company harmed (http://www.cybercrime.gov/cccases.html).

Senior executives often view security through the lens of available technologies that target external threats such as firewalls, VPNs, encryption, and anti-virus tools. These tools are essential to an overall security plan but are often employed as if they provide concrete answers to abstract questions. [2] Technology does not address information security from the "inside-out" but from a perspective of "perimeter" defense. Ernst & Young's *Global Information Security Survey 2004* found that organizations have remained focused on external threats while the internal threats are consistently underemphasized. [15] There is evidence to the contrary that network attack and damage is more likely to occur from inside the organization by an "insider." The classic definition of insiders includes those with an employment or business relationship to an organization. A more precise definition is needed in order to allow organizations to extend their security model to include *all* individuals who come into contact with their computer systems. The Gartner Group's definition extends the meaning of an insider to include:

Individuals with: a fiscal or other interest in the company's future; detailed knowledge of the company's business processes, applications, technology infrastructure or control mechanisms; or the opportunity to access [or] influence the company's processes. [18]

Insider attacks are more malicious and well-thought out than those from the outside. [6, 8] Instead of port scans and buffer overflows on Web servers (the source of most typical attacks on network resources that originate from outside an organization), insiders go after a much broader range of systems and resources with more serious consequences for the organization. Insiders have direct access to systems, possess authorization, take advantage of known security weaknesses, know the network architecture, and the location of data assets. Typical insider strategies include escalating user rights and privileges by stealing or guessing a

Figure 1.



system administrator password and giving themselves access to a system. These strategies effectively evade detection by traditional perimeter defenses. Edwin Bennett, global director of Ernst & Young's technology and security risk services writes, "Companies face far greater damage from insiders' misconduct…because many insider incidents are based on concealment, [and] organizations often are unaware they're being victimized." [15] There is nothing more "fearsome" than a disgruntled network administrator. [1] Perimeter defenses are useless because this class of individual is already inside, knows the procedures, has the passwords, and is aware of how to conceal their efforts.

Four recent studies emphasize the continued need for organizational focus on the insider aspect of information security and crystallize the threat posed by individuals outside the perimeter of technology controls.

The *2004 CSI/FBI Computer Crime and Security Study* (available at http://www.gocsi.com/) includes several indications that the insider threat is significant. The number of intrusions from insiders over a period of 6 years has not declined and in 2004 represented its highest level to date. The study highlights that among those companies reporting between 1 and 5 security incidents in the past year, 52 percent reported an incident initiated from within the organization. More alarming, of all companies reporting known intrusions, 34 percent did not know how many of those incidents arose from the inside. It is clear from this study that many organizations simply do not know what risks may exist inside their network perimeter. The loss estimated from insider attacks (financial fraud, insider net abuse and theft of proprietary information) totaled for the survey responders almost $30 million dollars in 2004. [3]

Security Management Index: The Alarming State of Security Management Practices Among Organizations Worldwide addresses the implementation of the ten points of ISO 17799, an international standard for information system security. The results of this study "suggest a reactive, 'Techno-Centric Solution' perspective for security still prevails." Produced by the Human Firewall Council, it is not surprising that the study indicates a lack of organizational focus on people and management issues in security audits. The study concludes that organizations emphasize technology in a reactive security posture. Instead, security can be made more effective and efficient when it includes, among other things, ". . . programs that integrate people, process and technology." [13]

The *Global Information Security Survey 2004* from Ernst and Young emphasizes the danger of over-looking or under-estimating the insider threat. The study finds that the human aspect of protecting information systems is most often overlooked in preparing an organization's overall security plan. "Employee Misconduct Involving Information Systems" was cited as the second highest threat behind "Major Virus, Trojan Horse or Internet Worm" but not by a wide margin. Technology cannot defend a network against employee misconduct that occurs within the bounds of authorized access and is not checked by organizational scrutiny of information systems. As organizations grow larger, the study states, the potential negative impact of security's weak link in people grows. Insider threats identified in this study include fraud, misuse of data, misappropriation of company data and illegal access motivated by both personal gain and, in the case of disgruntled employees, revenge. [15]

The *Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector* compiled by the U.S. Secret Service and the CERT/CC at Carnegie Mellon [14] is a substantive attempt to quantify the insider threat in one business sector and to begin to describe a methodology for curbing this threat. The *Insider Threat Study* provides some evidence of the fallacy in the belief that attacks come from outside and that good firewalls and occasional vulnerability scanning offer protection: 87 percent of the attacks were from insiders who exploited non-technical vulnerabilities (business rules, organization processes, procedures) and were carried out by those with little technical skill. The *Insider Threat Report* examined incidents of network intrusion and found that:

- 70% of the cases exploited systemic vulnerabilities in applications, processes and procedures
- 78% were authorized users with active accounts
- 81% planned the attack in advance
- 70% performed actions during normal business hours

The conclusions of the study indicate: an increased need for comprehensive security audits that include members of the organization outside of the IT staff; and a correlation between business size and the threat of insider attack (large organizations being less likely to experience an attack than smaller organizations). If security is to be a priority for the organization, the study concludes, its implementation must include individuals from across the organization and not simply technological solutions.

Taken in aggregate, the four studies bear out an important concern: a focus on external threats, such as viruses and malicious hackers, shows a disregard for at least 50 percent of the security issues facing organizations and an even higher percentage of the immediate risks to information resources. It is apparent that existing methods of risk assessment and security awareness programs and training fail to alert organizations to the risk of insider attack.

RISK ASSESSMENTS

Risk to data is represented as the possibility of something adverse happening to the data. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and applying appropriate controls to maintain the risk level. [5] Regardless of the likelihood of a threat, if a vulnerability exists due to the lack of a technology or operational control, the threat impacts security. This approach assumes that each threat can be reasonably quantified and mitigated by employing a specific technology or quick policy change; however, it also tends to view each threat, vulnerability, and control in isolation. The studies discussed in this paper indicate that the greatest single point of failure is insiders—people using procedures and technology.

In the presentation *Demystifying Information Security and Technology Risk Management,* J.R. Reagan of American Management Systems [7] points to the centralized nature of information security assessments. An effective security assessment should help an organization move away from an operational, reactive position to a policy-based proactive one. The assessment should involve individuals across the organization and lead to a security posture that is concentrated on compliance to policies and procedures rather than incidents and response time. Mr. Reagan concludes with the statement, "Security is 99% process and 1% technology."

Despite the general progress that has been made in recognizing the need for good information security, standard, well-defined metrics for analyzing and assessing insider information security risks have not been established and formalized. A number of organizations have published information security risk management guidance (IISF, ISO, OECD, ISF, IIA, SAC, ISACA, CobiT, NIST, GAO). An information security assessment can involve a combination of methods: well-defined algorithms, expert analysis, or subjective judgment. One of the goals of a risk assessment should not be to communicate to decision-makers a quantitative measure that represents a ranking, statistic or value, but to contribute to the organizational knowledge of insider threats and the vulnerabilities that remain when control measures are not applied across technology and operational domains.

Quantitative methods can be time-consuming, complex, and inflexible. Quantitative metrics often miss interactions and view vulnerabilities in isolation ignoring the fact that people interact with technology and policies. Existing methods do not "improve the practice of security" so much as define the state of existing security controls. Additionally, traditional risk assessment methods discourage organizational involvement, and assign the exercise to either an outsourced "security expert" or to an internal auditor. The information gleaned from the risk assessment is not often shared across an organization but remains "bound" inside a weighty document. For an assessment to have maximum value it must inform the participants in the exercise about the "threat landscape," including the interactions of people with the technology and policies that must be viewed as a distinct vulnerability. [5, 8, 9]

The organizations responding to the CSI/FBI 2004 study applied traditional risk assessment methods and used some means of technology and/or security awareness training to mitigate the risk from insider attack and still, 64 percent of the respondents experienced one or more intrusions identified as coming from an insider. [3] People as threats and their interactions with technology and policies are not effectively addressed in classic quantitative risk analysis and assessment. Risk analysis (RA) models often include steps to determine the level of existing protection and the need for further controls. A number of methods have a common set of steps [5]:

- Identify assets
- Determine valuation
- Estimate likelihood of occurrence
- Compute an expected annual loss
- Evaluate new controls
- Project annual savings of the controls

The nature of insider access is that by virtue of physical presence or authorization to a single system, access is available to all assets. Exercises designed to determine valuation may be appropriate for ROI (Return on Investment) but do not expose the vulnerabilities presented by the insider. The likelihood of an intrusion from a human threat agent is difficult to quantify while the extremes of fire, water, wind can be estimated from external sources. The likelihood of occurrence can be estimated for external events but for insiders there is a greater complexity—how do you estimate likelihood for a disgruntled employee with daily access to information assets? There is no statistical data available on the rate of occurrence of insider security threats. Computations of loss and savings are again, exercises more appropriate to ROI.

If the goal is to increase awareness and to apply controls appropriate to insider threats, then quantitative risk assessment methods fail.

Mitigation of risk and effective countermeasures happen from improved practices, policies and procedures. The authors propose a qualitative method to enable the assessment of interactions between the insiders, operational, and technology controls, and the type of threat. Qualitative approaches have often been characterized by subjective risk measures such as ordinal ranking (low risk or value, medium risk or value and high risk or value) in a risk-to-value matrix. These methods emerged from a belief that it was too difficult for an organization to get "real" numbers. The qualitative method also has appealed to management because it appears to be a "least effort" way to prove that they have assessed their risks. A qualitative assessment should examine the ways in which people's access to information is controlled. The ideal situation is to have all access controlled by technology *and* policies (that define operations and procedures) in concert. Figure 2 illustrates this idea of controls with the overlap area (displayed in gray) representing the ideal situation for information access controls.

Insider threat agents commit actions that can be broadly divided into four types of harmful actions: disclosure, deception, disruption, usurpation. The consequences of these actions can result in regulatory sanctions, liability, lawsuit, criminal actions, impair public relations, and as soon in a few cases, bankruptcy. Organizations place controls upon the use of technology and create policies to govern operational procedures to mitigate the risks from a variety of security vulnerabilities. The goals in the method proposed by the authors is to increase the awareness of business stakeholders and IT such that: technology controls should not be exclusively applied as a perimeter defense; that operational controls (policies, procedures) will include insiders; and *both* technology and operational controls would be required to mitigate the risks of insider threats.

In the insider-based risk assessment method, it is critical that both business stakeholders and technical staff interact to complete a scorecard designed to visualize for the participants the insider roles, technology and operational controls. The critical areas reviewed will provide information that can be used to quickly visualize absences of controls that need further review. The questions that should be asked to complete the scorecard are:

1. Identify the insiders by role classification within the organization
2. For each risk category (disclosure, deception, disruption, usurpation) answer yes or no for the existence of technology controls
3. For each risk category (disclosure, deception, disruption, usurpation) answer yes or no for the existence of operational (policy) controls

The first step in performing an insider-based risk analysis is to identify the insiders by role in the organization. Insider status may not always be apparent and should extend to those with physical access as well as technology access to the organization. An example of a situation with physical access could be frequent visitors to a hospital. By virtue of the amount of time a visitor might spend with a patient in the hospital they could easily observe the procedures, actions, and technology that would give them enough knowledge to gain access to a hospital's systems. In the case of technology access, an insider may not have direct physical access. Organizations should consider outsourced relationships, vendors (modem access), and business partners as potential insider threat agents.

The second step is to identify the technology controls in place for each threat classification. These might include: desktop configurations, remote access, and possession of additional devices (i.e., PDAs). Technology controls are most often imposed as a perimeter defense and not as a specific control that should be applied to any technology device that an individual member of an organization might possess or have access to. The absence of technology controls at the desktops can provide opportunities to insiders to elude detection.

The third step is to identify the operational controls that impact each insider role. These would include the business functions, and procedures that present opportunities for insiders to get to information assets. The absence of operational controls that are targeted to insiders can enable insiders to perpetrate an attack. A sample scorecard that might be used by participants is found in Figure 3.

As a cross-section of an organization proceeds through the scorecard, categories for insider threats would be assigned. For example, a

Figure 2.

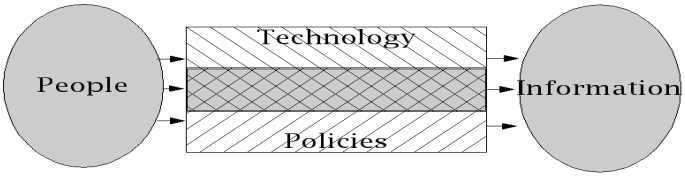
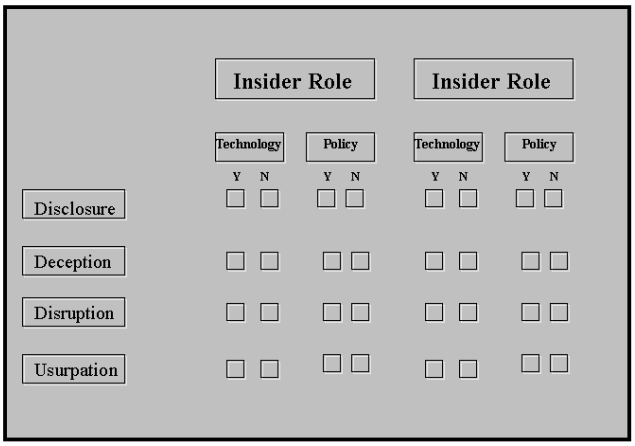


Figure 3.



hypothetical hospital engaging in this exercise as might identify the following to be potential insider threats: doctors, nurses, technicians, maintenance staff, volunteers, vendors, linked physician offices, temporary/contract staff. The risk assessment team then can quickly review the technology that each insider role uses or has access to and the operational controls that govern the insider's use of the technology and the business functions relevant to their role in the organization. Upon completion, a visualization of the "no" responses should reveal the state of potential "failure" of a defense against a particular category of threat for each insider role. The addition of both a technology and an operational control for each category would be recommended. As each new system, improvement or technology is added to the environment the need for a review of risk returns so that the team becomes partners to deliver secure systems.

BENEFITS OF METHOD

How will using this tool add value? It is an easier method than complex audit exercises; involves business, audit and IT components of an organization; focuses on realistic scenarios based on an insider's role and potential threat; does not require complex analysis; and can improve outcomes by improving the controls that mitigate the risks. Using this method in conjunction with traditional security audits may be the best method to manage internal threats, especially for small organizations that cannot afford the more costly professional audits and lack informed staff to apply security measures other than the most basic technology.

CONCLUSION

Being more secure does not mean more security, but better practices. What improves security is not the audit, assessment or the technology but the improvements to over-all information security and the reduction of risk that are accomplished as a result of risk assessment. Spending money on technology is necessary as part of the protection of the perimeter, but without the guidance of an objective risk assessment system, does not provide the expected benefit for an organization's bottom line. The qualitative method proposed will enable management to view risk mitigation as achievable quickly through a simple method of insider risk assessment that targets the interactions of people, processes *and* technology. Adopting this approach will improve the likelihood that insider vulnerabilities will be exposed—not just those linked to a network's configuration.

REFERENCES

[1] Jim Carr, Strategies & Issues: Thwarting Insider Attacks, September 4, 2002, http://www.networkmagazine.com/article/NMG20020826S0011

[2] Darby, C., Understanding Business Requirements: A Blueprint for Digital Security, September, 2002, @Stake Security Briefing

[3] Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R., CSI/FBI Computer Crime and Security Survey, 2004, GoCSI.com

[4] Brett Berger, Data-Centric Quantitative Security Risk Assessment, SANS Institute, August, 2003

[5] Hoffman, L.J. and Yoran, A., Role-Based Risk Analysis, 1997, http://csrc.nist.gov/nissc/1997/proceedings/331.pdf

[6] Kawamoto, D., The Weakest Security Link? It's You, CNET News, July 22, 2004, http://techrepublic.com.com/5100-22-5279558.html

[7] Reagan, J.R., Demystifying Information Security and Technology Risk Management, American Management Systems Inc., 2004, www.tasscc.org/presentations/tec_2004/JR%20Reagan.pdf

[8] Ozier, W., Risk Metrics Needed for IT Security, August 5, 2003, http://www.networknewz.com/networknewz-10-20030805RiskMetricsNeededforITSecurity.html

[9] Bodeau, D., Information Assurance Assessment: Lessons Learned and Challenges, Mitre Corporation, philby.ucsd.edu/~cse291_IDVA/ papers/rating-position/Bodeau.pdf

[10] Williams, R., I Thought My Network Was Secure, September 2003, http://www.naspa.com/03articlesbymonth.htm#september

[11] Trends in Information Security and Business Continuity Planning, Working Council for Chief Information Officers, 2003, www.cio.executiveboard.com/CIO/ 1,1431,0-0-Public_Display-%2073768,00.html

[12] Building a Human Firewall - http://www.humanfirewall.org (visited September 27, 2004

[13] "Study: Security measures often overlook human factor - News.com article, http://news.com.com/Study+Security+measures+often+overlook+human+factor/2100-7355_3-5381187.html?tag=sas.email (last visited September 27, 2004)

[14] Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, www.cert.org/archive/pdf/bankfin040820.pdf

[15] Global Information Security Survey 2004 from Ernst and Young, www.ey.com/.../$file/2004_Global_Information_Security_Survey_2004.pdf

[16] FBI CCIPS at http://www.cybercrime.gov/cccases.html

[17] Security Management Index: The Alarming State of Security Management Practices Among Organizations Worldwide, web.sun.de/Loesungen/solution_sales/ Volume/Security/attach/humanfirewall.pdf

[18] http://www4.gartner.com/DisplayDocument?doc_cd=122474, last accessed September 30, 2004