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

ITP4598

Developing Intelligence-Based Threat Definitions for Global Information Security Management

Alexander D. Korzyk, Sr.
Department of Business, University of Idaho, Moscow, Idaho 83844, USA, akorzyk@acm.org, voice) 208-885-5958, **fax) 208-885-6296**

ABSTRACT

One of the major problems with global information security management is the piecemeal nature of pertinent information. An alert or item of interest might not mean anything in and of itself; however, combined with other items of interest and data, the last item might be the piece of the puzzle missing to uncover the nature of suspicious activity or unexplained problems. This research attempts to define how the pieces of data can be combined into information forming the basis of a possible scenario. Information systems using the database approach have generally failed to provide adequate information security because databases are not generally designed to discover facts or knowledge. Unlike databases, Model bases are generally integrative facilities that allow the capture of not just data, but the combination of data and information to form knowledge by storing combined data in a scenario. The proposed new threat definition model classifies the internal and external forces facing a trans-national organization from the relatively common operating environment for many organizations and the intra-organization environment. Businesses using information systems need to continuously monitor their common operating environment (COE). This threat definition model identifies the sources of macro-level potential threat forces and micro-level potential threat forces. These include nation-states, terrorists, hackers, and even software developers worldwide. Keywords: Threat Definition, scenario, military intelligence, information system security

I. GLOBAL THREAT SPECTRUM

A. Global Security Threats

Many governments have developed an information age threat spectrum for global security threats, shared threats, and local threats. Global security threats generally consist of eight critical infrastructures, information warfare, and global intelligence. The eight critical infrastructures that depend upon secure and survivable information systems (listed alphabetically) include: 1) Banking and Finance; 2) Electrical Power; 3) Emergency Services; 4) Gas and Oil Storage and Transportation; 5) Government Services; 6) Telecommunications; 7) Transportation; and 8) Water Supply. The U.S. saw firsthand how Information Warfare can be carried out by criminals, organized crime, terrorists, corporations, hackers, friendly governments and potential adversaries on Sept. 11, 2001. The global intelligence system did not detect the terrorist plot a priori even though there was a significant trail of information uncovered by the FBI, United States National Security Agency, Echelon, and United States Central Intelligence Agency in the weeks (Elliott, 2002). Perhaps had there been an integrative intelligence-based information security system that could have used current technology to thwart the attack, events might have been altered

B. Shared and Local Threats

The public and private sectors of a nation-state encounter several threats. The development and use of an integrative intelligence-based information security system becomes even more important when the public and private sector face the same common threats. Terrorists, hate organizations (such as the Aryan Nation, KKK, etc.), industrial espionage, organized crime, malicious mobile code, network failures, etc. can be used to acquire information to validate threats. Sources of information about local threats can provided acquired from insiders, vendors/contractors, consultants, institutional hackers, recreational hackers, natural disasters, accidents, and system failures. Any single security incident by itself might be meaningless but when security incidents are combined into patterns fitting a defined threat scenario, defensive options can be developed prior to the exploitation.

II. INTELLIGENCE-BASED THREAT DEFINITIONS

Prior to the use of an information system, a thorough assessment of vulnerabilities given that certain threats exist, an in-depth risk assessment, and risk evaluation will allow the formation of scenarios. Management needs a method to determine which threats are most likely to exploit particular vulnerabilities and the impact of that exploitation on the information system. The creation of threat scenarios allows management to do "what-if" exercises, which simulate security incidents. Mitre Corporation has assembled an extensive list of common vulnerability exposures (CVE) (Mann and Christey, 1999). This CVE is a crude integrative facility that links intrusions to security incidents by the exploitation of a reported vulnerability. Unfortunately, the distribution of information about the CVE database is post facto and there is no scenario associated with the CVE, usually just a defect in the software or software design creating the vulnerability.

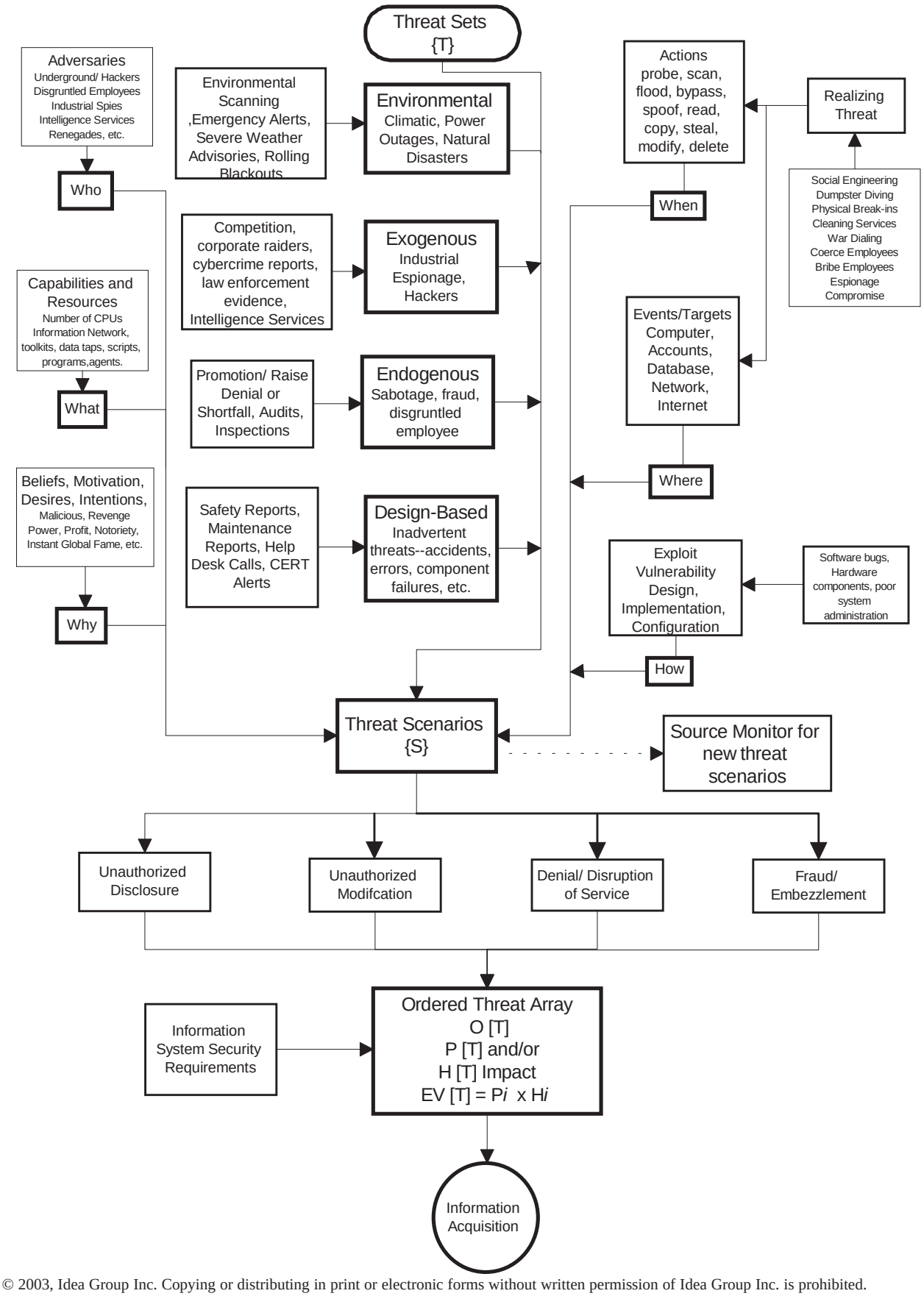
A. Environmental Threats

The High Level Global Threat Definition model (see Fig. 1) will allow information system designers to address threats given known vulnerabilities in the system design. It defines the threats that an information system faces and possible threat scenarios. All threats can be categorized into four types: environmental, exogenous, endogenous, and design-based (Sutherland, 1988). Environmental threats include climatic threats, primarily due to related severe weather, but can also come from extreme heat or cold exposure, and electrical surges from lightning strikes. . Natural disasters such as earthquakes, hurricanes, floods, tornadoes, and landslides, give little warning before occurring. Enterprises should have disaster plans in place along with a backup facility ready to provide continuous service.

Figure 1. High Level Global Threat Definition Model

B. Exogenous Threats

Exogenous threats include the most often-sensationalized cyber crimes



committed by hackers, criminals, and industrial spies. Despite efforts of the national governments to gain the cooperation of industry, many incidents do not get reported for fear of damaging publicity. Intense business competition often keeps enterprises from taking adequate countermeasures, as security generally is not considered essential for survival; however, enterprises report increasing numbers of cyber crimes daily to law enforcement agencies, even though the cyber crimes often get leaked to the media. The number of attacks from outside the organization is gradually equalizing with the number of attacks from inside the organization. Attacks had reportedly been generally occurring at 70% internal from 1985-1995. Since 1995 internal attacks have generally decreased to approximately 60% while external attacks have increased from 20 to 30% (CERT/CC, 2002

C. Endogenous Threats

Endogenous threats include many cover-ups committed by upper management to prevent embarrassing or reputation damaging information from reaching the media. Sabotage committed by disgruntled employees can be devastating, particularly to smaller enterprises with relatively few employees. A classic threat is the long-term employee who is passed over for promotion in favor a much shorter-term employee. Even a more common threat is the hard-working employee who receives no annual raise or a small raise of 2-3%, compared to a slack employee who receives an annual raise or large raise of 7-10%. One of the most common endogenous threats has been computer and wire fraud. Employees such as accountants with access to sensitive information or high dollar threshold limits are prime suspects for corporate espionage. Many companies monitor the Internet sites accessed by employees, but few monitor the content of electronic mail messages sent. An e-mail can easily contain sensitive information without the appearance of a sensitive message. Large business documents are a favorite tool within which to hide sensitive information. So unless the company monitors the content of each e-mail message and attachment to the email message to a fine level of granularity, a disgruntled employee can easily subvert the company by releasing sensitive information outside the company. Periodic inspections of employee e-mail have been ruled legal actions by an employer as have a full audit of documents transmitted by employees using company computer equipment (Daymont, 2002).. Unfortunately, security controls for endogenous threats has generally been much less emphasized than exogenous threats in the design and development of information systems.

D. Design-based Threats

Design-based threats include simple threats such as accidents destroying the physical computer or mistakes destroying the data or software due to poor system design or inadequate training of users. System administrators and database administrators often do not receive sufficient training for new or updated software and may end up deleting or modifying computer files unintentionally. Software bugs often do not become evident until after the release of software packages to the general public. Patches to correct the software bugs are not generally made until enough reports are made and the software bug is validated. Computer Emergency Response Team Alerts inform users of security related flaws that must be corrected to be protected from various other threats.

E. Elements of Threat Scenarios

Sets of threats together form threat scenarios consisting of who, what, why, when, where, and how. The threat sets combine to form threat scenarios. These scenarios consist of six types elements (Sengupta, 1992). The "who" elements include various adversaries, such as the computer underground, hackers, disgruntled employees, industrial spies, renegades, and foreign government intelligence services. The "what" elements include various capabilities and resources, such as the number of computers, an information network, hacking toolkits, data taps, scripts, programs, and software agents. The "why" elements include various beliefs, motivations, desires, and intentions, such as malicious retribution, revenge, power, profit, notoriety, and instant global-wide fame. Game Theory provides some mathematical foundations for what motivates the "who" element. A cooperative game is one in which the players communicate to plan strategy before taking action (Auman, 1967). In determining the rules of the game, the "when" elements include the specific times of various actions such as probing, scanning, packet flooding, bypassing, spoofing, reading, copying, stealing, modifying, and deleting files or objects. Game theory describes the interactions between the players, which is essentially a choice of strategy determining the outcome of the interaction (King, 2001). If information technology, particularly the Internet, is considered a common property resource, one can call what is happening with crime and abuse on the Internet as a Tragedy of the Commons. Game theory considers the Tragedy of the Commons as a multiperson extension of the Prisoners' Dilemma, which points out that individually rational action results in both players made worse off in terms of their own agenda (Von Neumann and Morgenstern, 1974). The status of information system security can be considered in dominant strategy equilibrium as the "why" of the threats such as to defend when threatened. It is the interactions between the players which this research will try to manage. The "where" elements include various events/targets, such as computers, computer accounts, passwords, databases, networks, and the Internet. Prior to an information system threat or during the early stages of a realizing threat, the "who" may use several techniques to acquire more information about their target or to find a target. These techniques include social engineering, dumpster diving, physical break-ins, cleaning services, war dialing, coercing employees, bribing employees, espionage, and compromise. The "how" elements include the exploitation of a vulnerability, such as a design vulnerability, software bug, hardware component, insecure implementation or configuration of the system due to poor system administration. Multiple instances of any element type occur and the combination of all six element types normally combines into one threat scenario. Each threat scenario generally results in one of four outcomes: unauthorized disclosure, modification, denial or disruption of service, or fraud/embezzlement.

III. CONCLUSIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

There is information overload in the current global information security system causing international intelligence failures. By using intelligence-based threat definitions to classify threats for use by threat scenarios we may finally allow the global collaboration of intelligence to become a reality and prevent future intelligence failures. A model for acquiring the necessary information for the threat scenarios needs to be developed.

REFERENCES

Auman, Robert J. A Survey of Cooperative Games Without Side Payments, in Essays in Mathematical Economics, Princeton University Press, Princeton NJ, 1967.

CERT/CC. Security Incident Statistics. http://www.cert.org, 2002.

Daymont, Josh. EMAIL Security Juggling the Risks, SC InfoSecurity Magazine, Vol. 12, No. 5, May 2002.

King, William. Game Theory. http://william-king.www.drexel.edu/top/eco/game/. Dec. 6, 2001.

Mann, David E. and Christey, Steven M. Towards a Common Enumeration of Vulnerabilities. In the Proceedings of the 2nd CERIAS Workshop on Vulnerability Databases. Bedford, MA, January 8, 1999.

Reuters. Hackers could threaten airline safety. http://www.msnbc.com/news/468457.asp, September 27, 2000.

Sengupta (1992) *Scenarios.* In the Proceedings of the Hawaii Information Conference. Hawaii, 1992.

Sutherland, J. W. "Intelligence-Driven Strategic Planning." *Journal of Technological Forecasting and Social Change*, Vol. 34, pp. 279-303, 1988.

Von Neumann, John and Morgenstern, Oskar. Theory of Games and Economic Behavior. Princeton University Press, Princeton, NJ, 1974.