

Managing the Cyber Threat

Author: Kent Anderson, CISM

Copyright © 2004 Network Risk Management, LLC. All rights reserved.

Information technologies are changing the way companies do business. By providing the unprecedented capability to connect every aspect of an organization's business, technology allows for dramatic increases in communication and efficiency. It fundamentally changes both the organization's internal operations and its relationships with suppliers, partners, customers and government. These changes are far-reaching, spawning new markets, industries and competitors.

With this unparalleled connectivity come new risks. Many organizations have greater value invested in their intangible assets than in physical bricks and mortar. Intellectual property is often the foundation of a corporation's success. The security of these assets is dependent on the network infrastructure upon which organizations build their businesses. The combination of global connectivity, employee mobility and rapid technological change expose the infrastructure to a myriad of risks in the form of fraud, theft, pirating, industrial espionage and business disruption.

Every day, approximately 20 new web pages are listed on a popular hacker's web site after being defaced. In some cases, the culprits are juveniles posting offensive material and admonishing the system administrators to implement better security. In others, political or environmental "hacktivists" are protesting the targeted companies' business practices or products.

Website defacements are only one – relatively benign – form of computer intrusion. Dozens of other types of computer-related attacks and security breaches occur every day, including theft of customer credit card information, theft of intellectual property, extortion and threats of violence. Furthermore, these are the attacks in which the motive is clear. In many other cases, the targeted company can only detect that an intrusion occurred, without being able to determine either the reason for the attack or its precise effects. In the U.S., a recent annual survey of companies by the Computer Security Institute and the FBI revealed that 90% of all firms have had some type of IT security breach in the past year. 80% of respondents reported a financial loss and 74% responded that the Internet was the most frequent source of attack.

Here are a few questions that executives should consider:

- ⇒ What would you do if “hackers” brought down your web server for a day? How about five days? What if they used your systems to launch Denial-of-Service attacks against other companies?
- ⇒ What would you do if an “anonymous” investor published false financial information about your company on the Internet?
- ⇒ What would you do if confidential information were being e-mailed out of your network? Are you sure you would even know that it had occurred?
- ⇒ How would you manage negative press related to a security incident involving your organization?
- ⇒ Are these threats even credible?
- ⇒ Do you fully understand what the costs or impact to your business would be?
- ⇒ Who would you contact? Law enforcement? Could you handle this “in house”? Should you? What if the source appeared to be from another country?

THE INTERNET: A COMPLEX, HOSTILE ENVIRONMENT?

Computer and telecommunications networks are fostering a revolution in the way organizations do business. The unprecedented ability to interconnect every aspect of a company’s business through the use of networks provides myriad opportunities for increased efficiency and enhanced communications. The emergence of e-business is fundamentally altering both the way companies function internally and the way they interact with suppliers, partners, customers and governmental agencies. These changes are international, creating new markets and competitors.

With this unprecedented connectivity come new risks for the information infrastructure upon which organizations are building their e-businesses. The electronic assets of many of today’s top companies are of greater value than their physical “bricks and mortar”. In this environment, the combination of global connectivity, employee mobility and rapid technological change creates new opportunities for fraud, theft, extortion, pirating, industrial espionage and business interruption.

Technology is not the only source of risk to information infrastructures. Political, physical, environmental, legal and regulatory issues are all factors contributing to the creation of a multi-dimensional problem.

While prevention is the preferred course of action, no security measures are perfect. Organizations must be prepared to quickly detect and effectively respond to the threats they face in the ever-changing e-business environment.

INSIDERS OR OUTSIDERS?

So where do these threats come from? Traditional wisdom holds that insiders are the greatest threat to an organization. This is based on two assumptions: first, insiders have

access and second, that they have **knowledge** of a company's systems, applications and processes.

However, the Internet and e-business are creating a new environment. Consider these facts:

1. As stated above, companies are connecting to the Internet as quickly as possible. These connections occur with little planning and few controls, creating a whole new level of **access** from the outside.
2. With the electronic connection of companies' businesses to their suppliers, customers and partners, the traditional boundaries are becoming blurred. A subcontractor hired by one of your suppliers (without a background check and little management supervision) may now have **access** to and **knowledge** of some or all of your business applications and systems.
3. Most companies no longer build their own proprietary business applications; instead, they purchase standard, off-the-self applications for such things as finance, customer relationship management and order management systems. This standardization allows outsiders to use applications without detailed internal information.

These and other factors have altered the threats companies now face. The distinction between an outsider and an insider is decreasing rapidly. While statistics and experience show that the insider is still a significant threat, the outsider can no longer be ignored. Current security architectures are based on an organizations ability to defend a perimeter, while network and application architectures have created information infrastructures without perimeters.

In other words, ***current security architectures are inadequate to protect present information infrastructures.***

WHAT SHOULD YOU BE DOING?

As stated above, prevention is the preferred course in mitigating risk. However, companies often do not understand the risks to their information assets. A thorough understanding of the risks to an organization's information infrastructure is crucial both to management's ability to make decisions on where controls should be implemented, and to its ability to manage crises successfully. Few organizations invest in a proper risk assessment before implementing controls. Even fewer understand and qualify specific threats in order to evaluate risks accurately. The consequences can be profound. Not only are some threats overlooked, but also resources and budgets are misapplied to threats that do not exist or have minimal impact.

Therefore, the first step any organization's management should take is to make an effort to understand clearly the threats to its information infrastructure. When determining these threats, executives need to look beyond simple technical vulnerabilities in their company's computer systems and networks and consider the full range of threats, including those that involve people, operational and business processes, culture, physical issues and legal and regulatory concerns. Additionally, management need to understand that, while technology enhances capabilities by providing access, people, whether trusted insiders or outsiders, are the source of many threats. It is vital to

understand the source and motives behind illicit activity and the targeting of specific businesses or industries by individuals or groups. With the growing threat from amateur and politically motivated “hackers”, organized crime and other criminal elements, these multi-dimensional threats cannot be ignored.

Based on a thorough understanding of the threats a company faces, executives can make better decisions on how to manage risks in terms of their own business requirements.

In the real world of online business, not all threats can be prevented, nor does it make good business sense to attempt to do so. Therefore, organizations need to be prepared to deal with the inevitable unforeseen incident as it occurs. The first step in managing an incident is to quickly detect that it is occurring. Only then can damage be rapidly mitigated. To effectively manage electronic incidents, companies should:

1. Develop and implement the necessary mechanisms and controls to identify unusual or unauthorized activity;
2. Develop effective, secure and accurate communication plans, action plans and hierarchies of decision-making in the event of a serious problem; roles and responsibilities should be clearly defined;
3. Develop action plans for scenarios and evaluate the cost and impact of reactions against the impact of specific threats; ill-prepared actions often cause as much damage as the original incident. Action plans should address when and how to involve or respond to outside influences such as press enquires, legal actions, law enforcement and communication or extortion attempts from the perpetrators.
4. Communicate with and train staff on an ongoing basis regarding what they should do in the event of an incident and to whom they should report suspicious activity; and
5. Assess incident response plans on a regular basis to ensure they are effective; threats, technology and businesses constantly change.

INVESTIGATING VS. MITIGATING

More often than not, when an incident occurs there are many unanswered questions:

- ⇒ Who is doing this and why?
- ⇒ How did he or she get into the systems?
- ⇒ Is it an employee or contractor (i.e., insider) or an outsider?
- ⇒ Does he or she have other means of gaining unauthorized access or causing damage?
- ⇒ What will the perpetrators' reaction be to attempts to identify them or lock them out?
- ⇒ Has anything been stolen, deleted or otherwise compromised?

Effective decision-making during an incident often requires answers to these basic questions. The answers may be difficult to obtain and require significant investigation. Many company executives find themselves in a dilemma between investigating the

incident to answer these questions and simply attempting to stop activity as quickly as possible.

Investigating computer crime is a complicated and highly skilled activity. It requires extensive technical training and expertise in such areas as data forensics and electronic evidence collection and handling. It often requires the ability to effectively interview potential suspects.

Additionally, investigating an incident often requires allowing potentially damaging actions to continue while evidence is collected and activity is traced. If third parties are involved, there may be questions of liability.

These are just a few of the complicated issues that companies need to address when managing a threat. Executives should not be thinking about what to do for the first time during a real incident. If an organization's leaders have not proactively planned how they would manage a problem, it often doubles the cost or more to investigate and resolve the incident with less than half the chance of successfully determining who is responsible.

Forethought and planning can make a significant difference in the outcome of any crisis.

OTHER PAPERS BY KENT ANDERSON, CISM

["Convergence: A Holistic Approach to Risk Management"](#) published in *Network Security*, Elsevier Ltd., Volume 2007, Issue 5, May, 2007.

Frustration grows as security practitioners feel more pressure and accountability to perform – yet never seem to have the resources to get the job done. "Executives just don't get it" is probably the most common explanation but have we ever stopped to ask if maybe we don't get it?

Every year IT security managers develop new budgets requesting more funds and resources to stem the tide of endless security issues – patching, virus management, provisioning, installation of new appliances, the list goes on. Every year business leaders listen to these requests and usually provide a fraction of the requested increases. This cycle has become a ritual in the IT security profession and fits Albert Einstein's definition of insanity: Doing the same thing over and over again expecting different results.

["IT Security Professionals Must Evolve for Changing Market"](#) published in SC Magazine, October 12, 2006.

IT security awareness is at an all-time high, and organizations are spending and hiring in record numbers. Legislation and regulations are proliferating. Yet, for all this effort, nearly every statistical measure of IT security performance – from the number of incidents and vulnerabilities to the cost and impact of a security breach – is bad news. In what other endeavor would so much investment be permitted with such poor results?

The potential for disruption from malicious or accidental threats is growing, yet our ability to manage risk has never been more uncertain. Throwing more money at IT security will not close the gap.

["Managing the Cyber Threat"](#)

Technology is not the only source of risk to information infrastructures. Political, physical, environmental, legal and regulatory issues are all factors contributing to the creation of a multi-dimensional problem. While prevention is the preferred course of action, no security measures are perfect. Organizations must be prepared to quickly detect and effectively respond to the threats they face in the ever-changing e-business environment.

["Intelligence-Based Threat Assessments"](#)

Few organizations invest in proper risk assessment before implementing controls. Even fewer have the capability to understand and qualify specific threats to their information assets in order to assess risks accurately. The consequences can be profound. Not only are some threats overlooked leaving inadequate controls, but also scarce resources and budgets may be misapplied to threats that do not exist or have minimal impact. This paper will discuss threat assessments, risk assessments and information infrastructures in general and provide an overview of an intelligence-base threat assessment model.

["Criminal Threats to Business on the Internet: A White Paper"](#)

This paper looks at the increasing trend of criminal activity against information systems, from the low-level, amateur intruder to organized crime, industrial and international espionage. In addition, the author looks how this activity is likely to evolve in the near future.

["International Intrusions: Patterns and Motives"](#)

Summary of the author's investigation of international intrusions presenting a classification model of attributes and motives displayed by intruders and explaining common patterns of activities. The author argues that common methods of investigating computer intrusions are limited in scope; therefore, security solutions and tools have limited effectiveness.

ABOUT NETWORK RISK MANAGEMENT, LLC

Network Risk Management, LLC (NRM) provides clients with ***informed risk management strategies™***. Informed decision making not only reduces loss and exposure to potential risks, it allows executives to make effective investment decisions concerning risk management. NRM provides solutions to two broad clientele – enterprise and security providers.

Enterprise risk management is a complex matter, involving more than technical considerations – it involves people, policy, process and technology. In order to meet these requirements, NRM developed an **ENHANCED SECURITY ASSESSMENT FRAMEWORK (ESAF)™** methodology.

The **ESAF™** methodology to assist enterprise clients streamline their security organization and operations using four guiding principles:

1. **Alignment** of security with business objectives to enable and support the organization;
2. **Convergence** of security strategies to maximize return on investment – traditional models of separate security functions are wasteful and hinder management of cross-functional risk;
3. **Risk-based** decision making founded on understanding the unique threats and risks to each organization; and,
4. **Strategic** focus to transform the security organization from tactical and fire-fighting to strategic and pro-active.

Services include (for both physical and IT security):

- Threat and risk assessments
- Standard security reviews
- Strategic security architecture analysis
- Incident response evaluation and planning
- Policy review and development
- Executive awareness presentations and briefings
- Training programs for security personnel

NRM also assists *security providers* in creating competitive offerings through development of security service portfolios, reference architectures, differentiated capabilities, competitive assessment, go-to market strategies and other support services.

ABOUT KENT ANDERSON, CISM

Mr. Anderson is considered a leading authority on security, with more than 21 years of experience in the field. He is the founder and Managing Director of Network Risk Management, LLC (NRM) located in Portland, Oregon.

Mr. Anderson's international experience includes risk and threat assessment, designing and managing security organizations and operations, investigations and developing security businesses.

Mr. Anderson's expertise is founded in understanding the real-world threats. He has led or coordinated numerous international investigations including espionage, industrial espionage, computer misuse (hacking), sexual harassment, threats of violence, extortion, fraud, intellectual property thefts, copyright infringement and product counterfeiting. These investigations have resulted in the successful prosecution of 10 individuals and numerous successful civil cases.

Mr. Anderson has been quoted by numerous publications including the Washington Post, CNN, Associated Press, Reuters, USA Today, Los Angeles Business Daily, Singapore Business Times, Danish National Radio (DR) and the BBC.

He has provided training and assistance to various law enforcement and government agencies including the FBI, U.S. Secret Service, Department of Defense, Department of Justice, FLETC, Scotland Yard, the German BKA, the Russian MVD and Norwegian, Danish and Swiss police. Additionally, he provided consulting to the Organization for Economic Cooperation and Development (OECD) on international harmonization of computer crime laws and the British Houses of Parliament on the development of the U.K.'s Computer Misuse Act.

He has held positions as Senior Vice President of IT Security and Investigations with an international business risk consultancy, as Director in the Dispute Analysis & Investigations group of PricewaterhouseCoopers, LLP and as the European Information Security Manager for Digital Equipment Corporation.

Mr. Anderson is a Certified Information Security Manager and serves on Motorola's Research Visionary Board and on ISACA's Security Management Advisory Committee.

Contact Network Risk Management, LLC to find out how your organization can implement *informed risk management strategies™*:

Kent Anderson, CISM

Managing Director

NETWORK RISK MANAGEMENT, LLC

Portland, OR USA

+1 (503) 203-8295

kea@aracnet.com