Cyberterrorism: Basic Components of Defense

By Michael Kirk
September 2001

SANS GIAC Level One Security Essentials [Mar 28, 2001]
Practical Assignment Submittal, version 1.2f

Acts of terrorism can be designed in different ways, from biological weapons to chemical weapons to weapons of mass destruction. Terrorist threats can also include attacks against the information and systems upon which people, organizations, or governments rely. September 11, 2001 is a day that will be remembered for a very, very long time. Icons of democracy and commerce, and the strength to defend our freedom and values, were viciously and ruthlessly attacked by merciless terrorists. These acts of war committed against the United States are gruesome and heinous. The grim truth is that terrorism is a reality with which all nations must face - this includes Cyber-Terrorism.

The Federal Bureau of Investigation defines terrorism as " the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 CFR Section .85)"[1] Cyber-terrorism, or info-terrorism, is the application of this definition to information technology systems and their data which people rely upon. Information systems that support the nation's power grid, major financial institutions, nuclear power plants, and the military could all be used to cause violence against our nation. "Most people think that America has not been the target of a major attack since Pearl Harbor 60 years ago. Yet every day, foreigners invade U.S. computers and Internet servers, causing economic damage that last year totaled about $17 billion and may be higher this year."[2]

The physical borders of the United States are protected by the United States Army, Air Force, Navy, Marines, Coast Guard, FBI, CIA, National Security Agency (NSA), etc. The United States' information systems are much softer borders though and can be more easily penetrated. If the same ruthlessness exercised on New York City, The Pentagon, and the flight that crashed outside of Pittsburgh, PA was perpetrated upon the information systems of the United States, the effects could be catastrophic. A special congressional commission is concerned that future attacks against the United States could include a cyberattack used in conjunction with a physical weapon compounding the destruction.[3]

The National Infrastructure Protection Center (NIPC) was established in 1998 within the Federal Bureau of Investigation to take on the mission of serving "as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is based." [4]

In the August 2001 edition of Information Security, Ron Dick, the Director of NIPC states, "Our society is increasingly relying on new information technologies and the Internet to conduct business, manage industrial activities, engage in personal communications, and perform scientific research. While these technologies allow for enormous gains in efficiency, productivity, and communications, they also create new vulnerabilities to those who would do us harm. The same interconnectivity that allows us to transmit information around the globe at the click of a mouse or push of a button also creates unprecedented opportunities for criminals, terrorists, and hostile foreign nation-states who might seek to steal money or proprietary data, invade private records, conduct industrial espionage, cause a vital infrastructure to cease operations, or engage in Information Warfare." The NIPC serves as the focal point for the "partnership between the government and private industry to reduce our vulnerability to attack and increase our capabilities to respond to new threats."[4] "This is the only place in government where criminal-intelligence, counterintelligence, foreign-intelligence and private-sector information - sometimes proprietary - comes together for strategic analysis." [5] (Thieme, p. 64)

According to Michael Erbschloe, author of the book, *Information Warfare*, "In terms of the frequency of hack attacks, certainly most of them are originating in the United States. But the more damaging attacks and the people who seem to have the most ill intent are coming from outside the United States."[6] After witnessing the attacks of September 11, 2001, the possibility that a cyberterrorist can do harm to our country from thousands of miles away seems very real.

The President's Commission on Critical Infrastructure Protection stated that, "Today, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives, and the perpetrator would be harder to identify and apprehend." [7]

Ron Dick commented that "Luckily, we haven't seen any "cyberterrorism" incidents in the United States so far, but I think we'll see them in the future as the people involved in state-sponsored terrorist organizations become familiar with the technology. We're seeing the technology being used for state-sponsored espionage. I can't go into details, but it's happening, and some nations are talking about waging information warfare."[8] (Thieme, p. 64)

Many feel that the United States is not adequately prepared for the task of fighting criminals and terrorists in the cyber-arena. Governments have historically moved slowly and deliberately and that contradicts the rapidly and constantly changing threat of technology risks. "While the threats are growing, some believe that the government's top organization for preventing cyber-terrorism, the Nation Infrastructure Protection Center, is not up to the job. The GAO reported this spring that NIPC lacked both staff and technical expertise and sometimes operated amid confusion because of its roles and responsibilities have not been fully defined." [9]

Organizations cannot fully rely upon government agencies to provide solutions to all of their cyber-threats. Private and public organizations both need to exercise their own due diligence in addressing the risks associated with cyber-terrorism. Whether that threat is classified as a teenager sniffing a network for vulnerabilities, an extortionist trying to download credit card numbers, or a terrorist trying to open the flood gates of the Hoover Dam in Nevada, organizations need to take ownership of their own defense against cyber-terrorism.

Whether the systems and data to be protected are owned by the government or industry, the first line of defense against cyber-terrorism is a solid foundation in the pervasive controls governing security administration and practice. If a technology environment is to be adequately protected, a solid security foundation must begin with heightened organizational awareness, active vulnerability management, and comprehensive disaster recovery planning.

Information security awareness must begin at the top of any organization. Management needs to ensure that each individual throughout the organization understands that they have a role in maintaining the security and integrity of the organization. Security awareness should flow through an organization as blood flows through the human body. Most organizations are comprised of business components that are interdependent upon one another. Just as blood and oxygen are crucial to each and every body part, security awareness is critical to the components within the entire organization. If one component is not healthy, the entire organization can become infected. This mindset must not only be supported by executive and senior management, but also demanded.

Security awareness programs should be developed based on best practice methodologies and supported by management with an appropriate budget. Breaches in organizational security should be brought to employees' attention. Quarterly reminders, security audits, company postings, and a section in the monthly newsletter are effective means by which to elevate, as well as to maintain security awareness within an organization. Security awareness should also include an organization-wide security program and plan with specific, strategic goals that are aligned with the business objectives of the enterprise. Since technology is not static, the security plan must be reassessed and updated on a regular basis to appropriately reflect changes within the organization as well as within technology.

Vulnerability management is the second critical component to providing a solid line of defense against cyberattacks. Vulnerability management can be defined as the active management of system security including monitoring for security weaknesses and intrusion detection and diffusion. A network of systems is either 100% secure or it has vulnerabilities. Since there is no such thing as a 100% secure system, vulnerability management accepts the fact that security weaknesses exist and manages them proactively rather than after-the-fact.

Vulnerability management includes the security configuration and protection of the organization's operating systems and network security, including server and firewall security, and application security. Vulnerability management includes assessing internal threats in addition to the external risk exposures to the technology environment.

In a recent review of the Commerce Department's information technology controls, "Investigators who examined the Commerce Department's security controls concluded there are "significant and pervasive computer security weaknesses that place sensitive Commerce systems at serious risk, " said Robert F. Dacey, director of information-security issues for the General Accounting Office, the auditing arm of Congress." [10]

Representative James Greenwood, the chairman of the of the House Commerce Committee's oversight panel, stated that the "GAO reports that its hackers gained access to one system, only to find that a Russian hacker had been there before them without the department's apparent knowledge." [11]

Other security weaknesses noted were systems lacking passwords or with passwords that could be easily guessed, and that powerful user privileges were granted too broadly across the users. Essentially the Commerce Department, which is entrusted with business secrets as well as military secrets, failed to prevent and detect cyber-attacks in a real-time capacity. The control environment over the Commerce Department's information technology environment also failed in the detective monitoring role of auditing its own systems.

The term "you get what you pay for" is painfully obvious in the review of the Commerce Department conducted by the GAO. The Commerce Department simply lacked the requisite skills to understand and manage the environment's technology risks. An organization is only as strong as its weakest link. The weakest link is typically the human factor within the organization and may present itself as a vulnerability risk through social profiling or a lack of technical competency.

Intrusion detection is a critical sub-component of vulnerability management and is used to actively manage system weaknesses. Organizations need to implement and maintain an ongoing early warning detection system for intrusion. The technical competency to understand the risks and to recognize and manage technology attacks has caused organizations to compete for skilled talent in the labor market.

An intrusion detection system (IDS) must be deployed within the network topology and include the active monitoring and analysis of traffic at the network level. Personnel must have an understanding of hacker techniques and be able to determine vulnerabilities and points of attack. The IDS must also include a strong set of policies and procedures for adequate response to an incident and to protect the actions of the respondents.

Some organizations may wish to go beyond protecting their systems and implement deception systems. Deception systems, also referred to as "honey-pots" or "shadow boxes", typically consist of the following components in one capacity or another: detection, notification, interception, protection, reaction, and reconnaissance. Deception systems can be used to identify attackers as well as to assess internal and external weaknesses. Deception systems are often technically sophisticated and require the budgetary commitment to employ the required technical skills. Even simple deception systems though can serve as a deterrent to attackers since there are so many poorly secured systems available. Intrusion detection and deception systems need to be deployed with the depth and expertise to technically match the skills of the attackers. [12]

The third component to a solid foundation in an organization's defense against cyber-terrorism, is a comprehensive disaster recovery plan (DRP). Disaster recovery planning is a minimum basic step in security planning. An organization should make the commitment to develop an entity-wide, comprehensive business continuity plan.

Management needs to understand that a disaster could negate the ability of their organization to provide uninterrupted service to its customers and users. The continuous operation of business-critical and mission-critical systems, including communications, is a requirement for the viability of an organization.

Disasters can present themselves in a variety of different forms, but can essentially be categorized as either natural or man-made. Natural disasters, such as the flooding of the banks of the Mississippi, sometime provide limited warning. Although if the groundwork of a disaster recovery plan does not exist, a four hour lead time may not be enough time to get the kids home safely from school, let alone to perform a full system archive. Man-made disasters do not typically provide the luxury of a forewarning. As related to man-made disasters, i.e., cyberattacks, DRP can be thought of as a contingency for failed vulnerability management.

Management's support is crucial to disaster recovery planning. Forming a disaster recovery team must be one of the first priorities. The team must include executive sponsorship with operations management in addition to information technology personnel. After the development of the DRP team, a complete risk assessment must be made of not only the critical systems, but also of the critical processes. Critical processes may include manual processes in addition to automated processes. The identification and prioritization of critical processes and systems will assist in identifying vulnerabilities within the organization. The priority ranking of the critical processes and their supporting systems and applications must be based on the potential impact that a disaster may present to the organization.

Planning for the recovery of information is based on the implementation of best practice methodologies for data backup. A prioritization of the importance of the data should be made through a data classification scheme. A determination of where data

should be backed up is just as important as what data needs to be backed up and how often the back up should occur. Essential information may need to be maintained in multiple locations to spread the risk of a single strike shutdown.
Off site recovery options exist, but may not be available if the vendor is suffering in the disaster along with your organization. Whether a vendor-provided solution is procured, a DRP must still be developed and managed internally.

Documenting and testing the plan will help to break the plan down into manageable sections and to reassess the adequacy of the plan. DRPs should be revisited on an annual basis at a minimum. DRPs should also be reassessed based on changes in conditions, such as the acquisition of another company or modifications to the technology environment. Testing of the plan is vital. Regular testing of the plan and evaluating its thoroughness and adequacy is a core requirement to establishing a defense against cyber-terrorism.

The events of September 11, 2001 remind all of us as to just how vulnerable we are. Although our government has established the NIPC to address threats and attacks against our country's critical infrastructure, the United States government cannot be counted on to stand guard over every organization's network. Each and every organization must take the necessary steps to protect their own information technology environment. Steps in building a secure technology environment must begin with organizational awareness, vulnerability management, and DRP. The United States has had it eyes opened to the reality and impact of physical terrorism in our country - let us hope that September 11, 2001 also serves as a wake-up call to the very real threat of cyber-terrorism.

List of References:

1. U.S. Department of Justice, Federal Bureau of Investigation, Counter Terrorism Threat Assessment and Warning Unit, Counterterrorism Division. " Thirty Years of Terrorism - A Special Retrospective Edition, Terrorism in the United States 1999" URL: http://www.fbi.gov/publications/terror/terror99.pdf (September 2001) ***

2. Geewax, Marilyn (Cox News Service). "Computer Terrorism A Rising Threat" The Columbus Dispatch, August 12, 2001: A1.

3. Thibodeau, Patrick. "U.S. Commission Eyes Cyberterrorism Threat Ahead" ComputerWorld, September 17, 2001. URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO63965,00.html (September 2001) ***

4. Dick, Ron. "A Message from Ron Dick - Director of the National Infrastructure Protection Center" National Infrastructure Protection Center Welcome Page. URL: http://www.nipc.gov/about/about.htm (September 2001) ***

5. Thieme, Richard. "Center of Attention, Ronald Dick interview by Richard Thieme" Information Security, August 2001: p. 62 - 70.

6. Geewax, Marilyn (Cox News Service). "Computer Terrorism A Rising Threat" The Columbus Dispatch August 12, 2001: A1.

7. Geewax, Marilyn (Cox News Service). "Computer Terrorism A Rising Threat" The Columbus Dispatch August 12, 2001: A1.

8. Thieme, Richard. "Center of Attention, Ronald Dick interview by Richard Thieme" Information Security August 2001: p. 62 - 70.

9. Geewax, Marilyn (Cox News Service). "Computer Terrorism A Rising Threat" The Columbus Dispatch August 12, 2001: A1.

10. Geewax, Marilyn (Cox News Service). " Commerce Computers Easy Prey" The Columbus Dispatch August 4, 2001: A1.

11. Geewax, Marilyn (Cox News Service). " Commerce Computers Easy Prey" The Columbus Dispatch August 4, 2001: A1.

12. Barry Schlossberg. "SNET: Design and Implementation of a Deception System" The ISSA Password May/June 2001: p. 14.

*** Denotes internet resource.