IRMI.com
Your Resource for Risk and Insurance Solutions™

THE GROWING RISK OF CYBER ATTACK AND OTHER SECURITY THREATS

THE RISK REPORT
Volume XXXI, No. 3, November 2008

KEVIN G. COLEMAN
The Technolytics Institute
http://www.technolytics.com/

The threat of cyber attack on the information systems of business, government, industry, and individuals is at an all-time high and continues to increase virtually unchecked. It is no longer a threat posed by casual hackers, pranksters, and criminals. Hacking, cracking, and cyber attacking has been professionalized. A substantial change in the quality, sophistication, and lethality of the online weapons used in cyber attacks became evident in 2004. Experts all agree that this trend will continue for the foreseeable future and that more and more actors are becoming involved in the high-stakes world of cyber weapons and defenses.

Using the Internet to steal information is one of the most damaging and fastest growing problems faced by organizations today. Given that some experts estimate that over 80 percent of the value of many organizations is derived from their intellectual property, it should be no surprise that data espionage activities have raised sharply over the last 5 years. According to research conducted by Spy-Ops, the amount of information theft has grown 68 percent in 2008 versus the same time period in 2007. Make no mistake about it, we are at war, and our systems and networks are under attack. In its report, Spy-Ops identified the following critical measures:

1. Every quarter second a file is stolen containing information that, if used, could compromise an individual's identity. An identity is stolen about every 3 minutes, resulting in an average loss of over $3,000.
2. Theft of intellectual property (IP) has seen, and will continue to see, double-digit growth. IP theft undermines our economy, our competitiveness, and in many cases, our national security.
3. The Pentagon is cyber attacked 3 million times a day. It has been reported that nearly 27 terabytes of data was stolen from Department of Defense (DoD) last year. There are no estimates of how often major businesses experience cyber attacks. However, one 20-year veteran special agent stated that he is aware of over 100,000 systems that have been totally compromised.

The information theft and data brokering businesses have become so lucrative that cyber thieves are now collecting discarded cell phones and old computers and are recovering deleted data from the onboard storage. The brokering of stolen information has become big business and is continually attracting new actors. It is no longer the rogue hacker doing this. Nation states, organized crime, terrorist groups, and even major corporations have all gotten into the business of information theft.

Identity theft is a derivative of information theft. It is important to realize that any piece of information may be used in conjunction with other information to identify an individual and can result in identity theft. Identity theft includes credit card fraud, check fraud, ATM fraud, mortgage fraud, and criminal impersonation. This is a significant problem that has seemed to go virtually uninhibited by our security measures. To put information theft into context, in 2006 Idaho' s gross state product was $51 billion, while identity theft for the entire United States cost consumers and businesses $56 billion.

Intellectual property is an intangible item that has significant commercial value. It can take various forms, from patents and trademarks to industrial designs to even something as commonplace as a customer list. Many organizations are unaware of just how valuable their information assets are, but it can be argued that information and IP now make up well over half of many organizations' net worth. Lost, stolen, or missing laptops, USB thumb drives, or backup tapes are common sources of data leakage or IP theft. Consider this exposure in light of the fact

that, on average, over 10,000 laptops are left at airports across the United States every day.

It is important to note that not all information theft comes from the outside. With job portability, people change jobs more quickly and have little reservation about taking sensitive information with them. Nearly 40 percent of professional-service sector employees change jobs yearly, and many of them take, copy, or destroy sensitive data. This poses a serious threat to organizations of all sizes and regardless of industry. Just recently, one company sued a former employee for $13 million for leaking sensitive information after he quit.

Cyber attackers are getting more sophisticated and aggressive. Business, government, and industry needs to get smarter about their cyber defenses. We are locked in a stalemate, nosing ahead one minute and falling behind the next, and the contest will not end anytime soon. As new security technologies are developed to combat the problem, new vulnerabilities and exploits emerge. So where do we stand? No one knows for sure, but one estimate suggests that about 150 million personal computers (PCs) currently connected to the Internet have been compromised.

Cyber Weapons

A new class of well-architected and professionally designed cyber weapons emerged in 2004 and continues to evolve and advance unchecked. In the spring of 2008, the North Atlantic Treaty Organization (NATO) cyber defense chief stated that cyber attacks and computer-based terrorism pose the same threat to national security as a missile attack (albeit, few cyber weapons actually pose a threat to life).

There are approximately 10,000 distributed denial-of-service attacks daily. Some of these occur not over periods of hours but days and weeks. Another important figure is that, on average, about 200 new computer viruses appear every month. If that picture is not bleak enough, consider that Spy-Ops estimated that in 2007, some 120 countries had cyber weapon development programs underway as did at least a dozen terrorist/extremist groups and multiple criminal enterprises.

There are many cyber weapons available to attack people, businesses, and governments. While many of these have been around for quite some time, a relatively new and more advanced cyber weapon, Storm Worm, was first detected in January 2007 and has reappeared in various permutations since. Created by a Russian-based criminal network, the hybrid piece of malware rapidly infected between 50 and 90 million PCs in Europe and North America, and continues growing almost unchecked. It is a worm, a Trojan, and a bot combined, encompassing a broad range of capabilities. The Storm Worm is:

- *Self-defending*—If the malicious code detects it is being deleted, it replicates itself.
- *Self-morphing*—The code changes its structure to avoid signature-based security software.
- *Self-propagating*—The code looks for new networks and systems to infect.
- *Man-in-the-Browser*—This code is capable of modifying that user's Web transactions on the fly.
- *Persistent*—It is baked into drivers or firmware so as to remain operational even if a hard drive is formatted.

FIGURE 1
THE CYBER WEAPON GLOSSARY

Backdoor—Refers to any hidden method for obtaining remote access to a computer.

Botnet—This collection of zombie (compromised) computers is remotely controlled (think robot) and used by an individual or group for malicious activities like spamming and DDoS attacks without the knowledge of the owners of the computers.

Directed Energy Weapons (DEW)—These weapons focus energy to damage or destroy enemy equipment, facilities, and personnel.

Distributed Denial of Service (DDoS)—These attacks flood a computer, server, or network with so much traffic that the system shuts down or cannot operate.

Electro-Magnetic Pulse (EMP) Generators, eBombs, and Transient Electromagnetic Devices—These create an electromagnetic pulse that can damage semiconductors.

Keyloggers—These programs monitor and record each keystroke a user types.

Malicious Code—This includes any software used for clandestine disruption, destruction, or information collection.

Rootkits—This malicious software keeps itself, other files, registry keys, and network connections hidden from detection.

Software Vulnerability Exploits—Errors in software programs create the opportunity for hackers to compromise the computer system by installing unauthorized software or conducting unauthorized operations.

Spyware—Software surreptitiously installed on a computer to intercept or take partial control over the user's interaction.

Storm Worm—This complex and sophisticated computer program allows remote control and manipulation of the infected system.

Trojans—These are software programs in which harmful code is contained inside apparently harmless programming or data.

Viruses—These computer programs spread by copying themselves and infecting others.

Worms—Refers to self-replicating computer programs that do not alter files but reside in active memory and duplicate themselves.

Earlier this year, a possible new approach to cyber attacks was uncovered—counterfeit computer equipment and microprocessors. An estimated $70+ million of counterfeit network cards were discovered by the Federal Bureau of Investigation (FBI). It was reported that these counterfeit products had made their way into multiple government agencies, including the DoD. In another case, federal agencies cooperating with international law enforcement seized 360,000 counterfeit microchips. At this time, it is unknown if the counterfeits were just cheap knockoffs or actually had been altered to hide malicious code or circuitry.

Testing each microchip to verify it has not been compromised is not economically feasible nor practical. Think of everywhere microprocessors and microchips are used. In one report, new cars were said to contain as many as 50 microchips that do everything from control the engine to regulate the air conditioning. Counterfeit microprocessors and computer equipment are perhaps the greatest challenge in the race to secure cyber space.

Disclosure and Costs

There are many laws domestically as well as internationally that cover cyber security and information breaches directly and indirectly. Given the materiality of these incidents, they can even rise to the level where they are covered in the United States under Sarbanes-Oxley (SOx), but are not often reported. One report suggests that only 25 percent of organizations falling victim to cyber attacks report the intrusions to law enforcement. While that number is low, some experts believe that in all actuality, the number is less than 10 percent.

Cyber attacks can devastate computers, information, and networks. However, the damage does not stop there. A report by Intelomics estimates that, in the days following disclosure of a cyber security breach, a publicly traded company can see a 1–5 percent drop in stock price. In one recent incident, the day following the disclosure of the cyber incident, a publicly traded company lost over $400 million in market capitalization, while the overall stock market rose about 50 points. It may only be a matter of time before the Security and Exchange Commission begins to investigate cyber incidents to determine if they were properly disclosed in a timely fashion.

A rule of thumb for valuing the cost of a cyber breach is $120 per record, reflecting the costs associated with internal investigation, notification and crisis management, and regulatory costs. Not included are diminished

brand equity and loss of customers. Last year, Forrester Research estimated the cost of the TJX breach at over $125 billion, while the IT security portal Dark Reading reported that the total costs could be as high as $4.5 billion. Either way, that is one big price to pay!

The other side of the equation is lost sales. Online sales have grown steadily since e-commerce was first implemented back in the mid-1990s. An average of multiple estimates places 2008 e-commerce at around $235 billion. If a cyber attack would disrupt transactions for 1 hour, it would cost the U.S. economy over $26 million. If the attack disrupted U.S. e-commerce for 1 day, the U.S. lost sales would be over $630 million. A week-long disruption would cost approximately $4.5 billion and, without question, would cause severe damage to the U.S. economy. With the potential losses so great, and the disruption so significant, the Internet is a prime target for attack by terrorists, rogue nation states, and criminal enterprises.

Cyber Security Intelligence

Since the early 2000s, the government has initiated programs to protect U.S. information networks from cyber attack and to foster government-private sector cooperation in developing security measures. The National Security Agency is applying its unique expertise and capabilities to develop the fundamental technology to create a national cyber-intelligence collection, cyber-attack detection, and response capability. However, cyber intelligence has and continues to lag behind the threat level. The full support and cooperation of the private sector is vital in protecting our critical infrastructures against cyber attack. NATO's head of Computer Incident Response Capability Co-ordination Centre said a determined cyber attack on a country's online infrastructure would be "practically impossible to stop." Another challenge is enabling collaboration between the multiple agencies given the mandate to collect this threat intelligence.

Current intelligence sources, techniques, and surveillance capabilities offer little assistance in gathering cyber intelligence. Consider the fact that conventional weapons and weapons of mass destruction plants require a significant infrastructure to manufacture and produce their products. This is untrue of cyber weapons. An office in a strip mall with a broadband connection or simply a house in a suburban neighborhood could serve as a cyber weapons plant. Gathering intelligence about cyber weapons and their capabilities currently focuses on the weapon being used and forensic analysis *after* the security event. This reactive approach must rapidly change to a proactive collection of cyber intelligence.

China is indeed a cyber intelligence challenge, most specifically as a cyber weapons developer, but so are Russia and Iran, as well as many entities involved in organized crime. In fact, according to Spy-Ops, there will be 138 countries and over 20 terrorist organizations with active cyber weapons development programs by year's end.

The ability to collect intelligence on all the nation states and terrorist organizations developing cyber weapons will be a challenge. When you add to that the number of criminal organizations involved in the development and sale of cyber weapons, it will be daunting. So who is leading in this arms race? It is hard to say because the rankings change frequently. At this time, and based on several years of research, the top 10 players in the cyber arms race are:

1. United States
2. China
3. RBN Russian Business Network
4. Iran
5. Russia
6. India
7. Israel
8. North Korea
9. Japan
10. Pakistan

Software packages and tools used to test security are easily adapted and used as cyber weapons. The only major infrastructure needed to develop a cyber weapon is a computer, and computers are readily available all over the world for a few hundred dollars. There are numerous Web sites that have free software downloads that can be used to create or accelerate the development of cyber weapons. Brain power is the only other component needed to create a cyber weapon of mass disruption. China, with 16 million students, has overtaken the United States as the world's largest higher education system, and is beginning to take the brainpower lead. Falling behind in computer science, engineering, and mathematics does not bode well for our ability to defend the nation in cyber space.

In the past, we have used the size of national armies or possession of nuclear weapons or other weapons of mass destruction as a measurement of threat. That is rapidly changing right before our eyes. To be a global super power today, you need three things.

- A sound growing economy that can support investing in the future and military might
- An educational infrastructure that produces a highly educated workforce
- A globally recognized technology sector

These are interrelated; you can't have one without the others. This is particularly true when it comes to becoming a cyber warfare global superpower.

Cyber Espionage

The United States has been the prime target for foreign economic collection and espionage and for the theft of export-controlled proprietary information for decades. That fact has not changed. All that changed is that the mechanisms now used for these activities are computer based. Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary, or classified information) from individuals, competitors, rivals, groups, governments, and enemies for military, political, or economic advantage using illegal exploitation methods within the Internet, networks, software, and/or computers. Intelomics, a provider of cyber intelligence, contends that cyber espionage reached epidemic proportions several years ago and has continued to grow. In December 2007, the Director General of MI5, the United Kingdom's counterintelligence and security agency, sent a confidential letter to 300 chief executives and security chiefs at banks and accounting and legal firms warning them that they were under attack from "Chinese state organizations." This is an unprecedented act.

International corporate spies and organized crime pose a moderate threat to the United States. They have the ability to conduct cyber espionage on a large scale. Intelomics reports that current cyber-espionage efforts are being funded by well-resourced organizations. These are not the same independent hackers of years past. These organizations are both government backed and private entities for hire with impressive technical capabilities. According to defense and intelligence sources, the Internet is the primary mechanism for elicitation between foreign entities and cleared U.S. companies and their employees.

Cyber espionage activity is expanding significantly, and the most common perpetrators are overseas companies hoping to gain an upper hand in competitive bidding, products, technology, or negotiating business deals with large companies based in the United States and Europe. Intelomics lists the top 10 high-priority technologies sought by foreign entities:

1. Information Technology
2. Bio Technology
3. Communications Technology
4. Lasers and Optics
5. Aeronautics
6. Nanotechnology
7. Armament and Energetic Materials
8. Electronics/Semiconductors
9. Space Systems
10. Materials and Processing

Many of these technologies have both military and commercial applications. Defense Security Services identified the top techniques used to gain access to our information about these sensitive technologies: requests for Information, attempts to acquire controlled technology, and the solicitation of marketing services. These three methods account for three-quarters of the attempts made by over 100 foreign entities. It is clear, espionage activities are on the rise, and as technology advances, new techniques will be developed to steal our secrets.

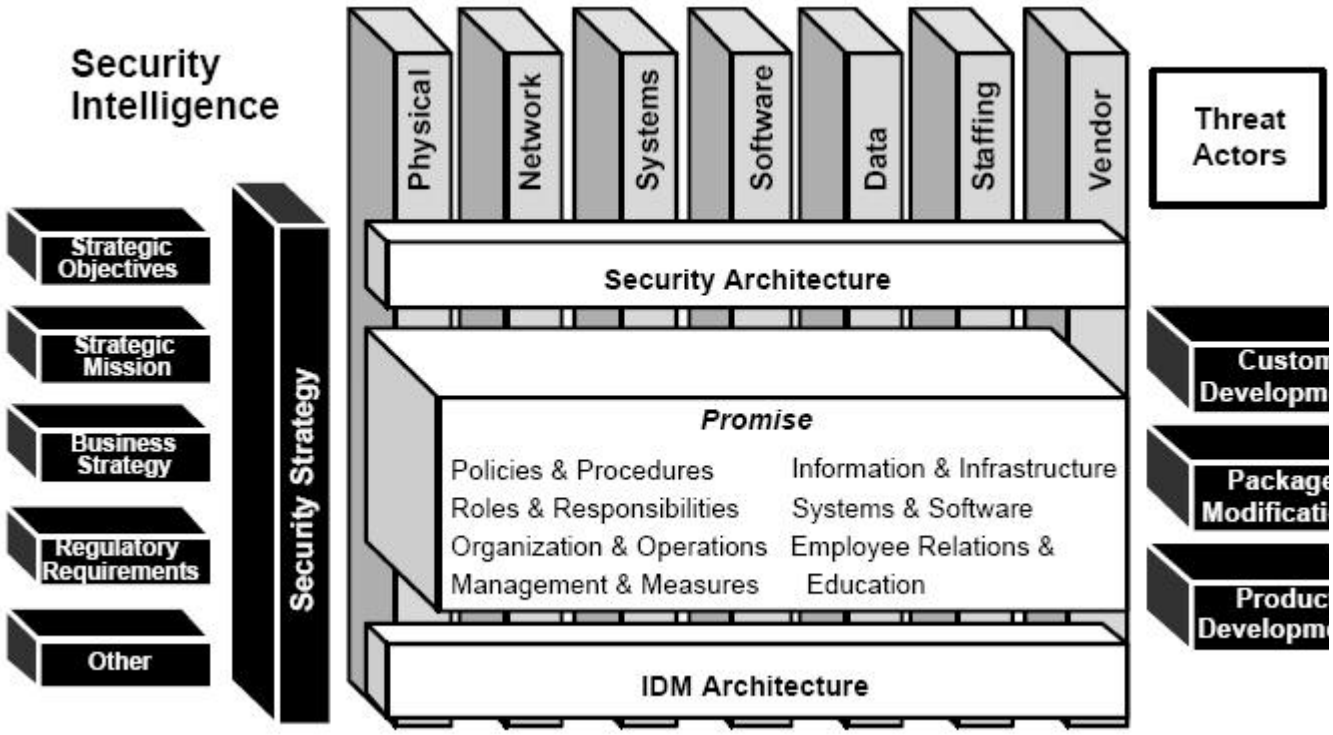
Cyber Defenses

Adversaries will not attack just one part of our infrastructure; they will go after several parts. Given this, a defense strategy needs to be developed with multiple dimensions of protection. Security professionals have introduced a model-driven approach to cyber defense engineering to provide increased understanding of the threat space in this highly dynamic environment. Multiple dimensions are necessary because attacks come in multiple forms, and any single component might fail. Given the constructs, it has become common to use a "defense in-depth" strategy, using multiple, independent dimensions to protect computer systems and the

information they contain.

Recently, there has been considerable interest in these models due to the increased threat posed by advanced cyber weapons and the threats of cyber attack. Figure 2 shows the current state-of-the-art in terms of multidimensional defense in depth security models. The multidimensional security model implemented in conjunction with a multilayer security technology model provides strong defenses against the current state of security threats. In addition, it builds the solid foundation necessary to grow and evolve as the threat environment changes over time.

FIGURE 2
CYBER ATTACK DEFENSE MODEL



The challenge facing every organization today is the sheer quantity of threats whose risks must be managed. In the latest threat models created by Intelomics, over 25 threat/risk categories are identified. Given that each category has multiple manifestations, large international organizations become overwhelmed when they try to manage each risk separately rather that addressing risk holistically with the model and managing the unique aspects of each threat.

New technology products are necessary to defend against cyber attacks. New security scanners are needed with advanced heuristics and behavior modeling/analysis features in addition to advanced probes that search deep inside the operating system to defend against the most advanced cyber weapons. Until then, think about a check-sum application to detect changes in space on the hard drive!

Cyber Insurance

Insurance is one way to finance the cost to recover from cyber losses. That said, traditional insurance policies cannot be relied on for protection from most electronic losses. Specialized property and liability insurance policies are available from a few insurance companies to cover losses associated with unauthorized access to or theft of data or e-business activities, computer viruses, denial-of-service attacks, as well as alleged unauthorized e-

commerce transactions. However, this is a relatively new line of insurance that has not yet gained wide acceptance by corporate America.

FIGURE 3
SOURCES OF INFORMATION AND HELPFUL WEB SITES

National Strategy to Secure Cyberspace

2008 Annual Threat Assessment

Critical Infrastructure Protection Board

Federal Bureau of Investigation Investigative Programs, Cyber Investigations

Spy-Ops

Intelomics

Conclusion

The world has just awakened to the threat of cyber attack and cyber warfare. For the first time, the threat of cyber attacks were addressed in the 2008 Annual Threat Assessment by the U.S. Intelligence Community required by the Senate Armed Services Committee. Consider that plus NATO stating that a cyber war can become a very effective global problem because it is low-risk, low-cost, highly effective, and easily deployable. It is almost an ideal weapon that nobody can ignore.

Modern life is now dependent on information processing. Our financial systems, our transportation systems, our water and electrical utilities, and all other critical infrastructures have become dependent on our information and communications infrastructure. That being said, infrastructure is the most vulnerable to malicious vandalism, terrorist attacks, criminal activity, and cyber warfare. The growing threat to our information, systems, and networks mandates that organizations of all sizes take immediate defensive actions. Failure to do so can and will have dire consequences, not just for the organization that fails to implement the proper defensive measure, but potentially for all others who are connected to the network. Cyber security and integrity is truly a weakest link problem. We are only as secure as the computer with the weakest protection that is or can be connected to the network. An unprotected computer is compromised within 1 hour after it is connected to the Internet.

Should we expect the federal government and our military to solve this problem? No! This takes cooperation between individuals, businesses, the computer industry, the telecommunications industry, and the government and military to resolve this pressing issue. Other than weapons of mass destruction, this threat is unprecedented. The fact that these weapons can be bought or built for several hundred to a few thousand dollars, coupled with the fact that an attack can be launched from and target anywhere in the world makes the problem that much more dangerous. This is one of the biggest risks we face today. All organizations should carefully assess their cyber risks, implement holistic defense systems, and consider the need for purchasing specialized insurance to protect against losses that occur in spite of the protective safeguards that are in place.

KEVIN G. COLEMAN
The Technolytics Institute
http://www.technolytics.com/

Kevin Coleman is a Certified Management Consultant and Strategic Advisor and former Chief Strategist of Netscape. With nearly 2 decades of experience, he advises leaders of businesses and governments throughout the world. His business clients include Pepsi, FedEx, GE, Dell, Sun, BEA Systems, Intel, Novell, Lockheed, Michelin, Ford, and other business icons. Almost one quarter of his consulting has been with organizations based outside the United States, providing him with a unique perspective on the challenges, risks and opportunities of international business. He has researched and written about subject matter critical to national security and has

testified before Congress as well as provided dozens of briefings at the board of directors level.