GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Weapons of Mass Disruption: Dealing with the Asymmetric Threat

© SANS Institute 2003, Author retains full rights.

GSEC Certification Practical
Security Essentials
Version 1.4

Paula Horton

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

WEAPONS OF MASS DISRUPTION: DEALING WITH THE ASYMMETRIC THREAT 1

Abstract *3*
The Asymmetric Threat: An Overview *4*
The Double Nightmare: Cyber and Physical Terrorist Attacks *5*
The Challenge *6*
What We Need To Do *6*
Defense in Depth Strategy *7*
Think Globally…and Horizontally *9*
Conclusion *10*
Resources *10*

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Abstract

In this post September 11 era, there is a new threat awareness and urgency to deal with the complex security issues facing us today. This includes the convergence of physical and cyber threats, where the lines between physical and cyber security are blurred, and the dangers are often unknown -- the asymmetric threat. The asymmetric threat is an old warfare tactic – a way of "not fighting fair" when the perceived balance of power is uneven. It gives the attacker the ability to exploit a powerful adversary's weak points, by using unconventional tactics in unexpected ways to degrade capabilities and introduce chaos.

In this new world order, we must re-examine security threats and vulnerabilities, and re-assess our ways of dealing with them. No longer will the old way of categorizing threats and assigning them to stovepipe organizations work effectively against the asymmetric threat. A new spirit of collaboration is necessary if we are to deal with these challenges effectively. IT and physical security teams must put aside their differences and work together to meet the new challenges and develop a vision that encompasses synergistic security.

One of the best ways to achieve this is by establishing or re-defining a comprehensive Defense in Depth strategy. Along with the Defense in Depth, there should also be a corresponding Defense-in Breadth, which encourages collaboration, and is composed of elements from both the IT and physical security disciplines, to complement and strengthen the overall effort.

This paper discusses how we can begin to deal with the challenges ahead.

© SANS Institute 2003, author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Asymmetric Threat: An Overview

"If instead of attacking our military systems and databases, an enemy attacked our unprotected civilian infrastructure, the economic and other results would be disastrous." -- 1994 Joint Security Commission report

The events of September 11 demonstrated the truth of this statement. The attacks hit Americans suddenly and profoundly. Not since Pearl Harbor had we wondered about how vulnerable we are. The events of that day changed many things, including the way we view our ability to protect against attacks. At first glance, the destruction of the World Trade Center and part of the Pentagon would seem to demonstrate that physical, low-tech terrorist tactics like kamikaze planes would dwarf anything that terrorists could have done in a cyber attack.

However, this new day of infamy brought into focus the sharp reality of what previously had been more of a theory: the asymmetric threat to our security. That is, an attack carried out by a shadowy, worldwide network of extremists. They struck unprotected targets, using methods that no one had anticipated.

Asymmetric attacks are old in terms of warfare techniques, but are used today for physical and cyber attacks. These attacks involve acting in unexpected ways, presenting targeted victims with capabilities and situations that they are unable to respond to quickly or effectively enough to prevent the attack from occurring, or from taking countermeasures. It limits the opponent's advantages, and tests its will and patience.

"The information technology revolution represents the most significant global transformation since the Industrial Revolution beginning in the mid 18th-century…no country in the world rivals the United States in its reliance, dependence and dominance of information systems. The great advantage we derive also presents us with unique vulnerabilities." Lawrence K. Gershwin, National Intelligence Council, June 21, 2001, in a speech to the Joint Economic Committee

Along with the rewards of this information age come new risks and consequences that need to be better understood and managed. Unfortunately, our ability to network has surpassed our ability to protect networks.

At some point in this information age, society crossed the line from simply benefiting from the new technologies, to being totally dependent on them. And this transition seemed to happen without much notice. Except to those intent on information warfare. The asymmetric attack became the way of doing substantial damage to large computer-dependent adversaries.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Double Nightmare: Cyber and Physical Terrorist Attacks

> New tools are enabling attackers to compromise systems, virtually without a trace of what they did…*Information Security Magazine* November, 2002

The September 11 attacks turned two of our strengths – a free and open society, and a superior air transportation system – into deadly vulnerabilities. The attackers were not deterred by our air or military strength. They made it irrelevant. They struck a blow against global openness.

And beyond the physical disaster, when the World Trade Center towers collapsed, so did the telephone system and the switches that handled three million data circuits. Telephone communication virtually melted down in several East Coast cities, forcing people to turn to e-mail to verify the safety of colleagues and loved ones. The Internet proved to be a good way to learn about the attacks as they happened. But by sending a worm, or disabling DNS, an attacker could cut off this means of communication just when we need it the most.

Computer networks create new venues for those with malicious intentions. They are still vulnerable to actual destruction by physical attacks, such as bombs or arson. But at the same time, these networks are the targets of mass disruption. An economy can be crippled by cyber warfare in the form of computer intrusions, hostile insiders within computer firewalls, or cyber terrorists around the world.

In the past, security threats have fallen into two general categories: physical attacks against infrastructures and cyberattacks against information. They have been managed in isolation of each other, and treated as independent "stovepiped" activities. Traditional concepts of security and deterrence don't apply against this new threat. Twentieth century approaches simply will not work. And overcoming these barriers of separate organizations and processes will not be easy.

Computer networks have created linkages that have never existed before. And because of this, identifying what is critical is becoming more difficult and more necessary. The information age, along with its exciting technology, has also given us a new set of security problems.

> *A cyberrattack can originate from any part of the globe…The low cost of equipment, the readily available…cybertools, and the otherwise modest resources needed to mount a cyberattack makes it impossible…to identify or track all potential cyber-adversaries.* David Keyes "Cyber Early Warning: Implications for Business Productivity and Economic Security"

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Challenge

Society, economies, and communities are linked together in a digital nervous system. Disruptions to this nervous system can cascade beyond the vicinity of the initial occurrence, causing regional and national disturbances.

The challenges arise from our dependence on information systems and networks to operate critical infrastructures. There are no boundaries or borders in cyberspace. There is no one nation or group to monitor – cyberattacks are just a mouse click away for anyone who has hostile intentions and access to the web. And the majority of the nation's infrastructures are privately owned and operated, so government action alone cannot secure them. Only a partnership between industry and government will work.

What We Need To Do

> To the extent the country detects a cyberattack but does no know who is attacking (a juvenile, a criminal, a spy, or a nation-state bent on committing information warfare) what resources should it deploy in response? Scott Charney, Article titled *Transition between Law Enforcement and National Defense.*

On July 4, 1776, upon signing the Declaration of Independence, John Hancock warned the delegates to the Continental Congress: "There must be no pulling different ways. We must all hang together." To which Ben Franklin responded, "We must indeed all hang together, or most assuredly, we will all hang separately."

Today, we must all hang together to secure our interconnected information networks, or we will probably be individually victimized. There is a learning curve as we begin to develop a security strategy that includes the private sector and the government working together - and learning to use the strengths of each.

The September 11 attacks on the World Trade Center and the Pentagon make it clear that we must be better aware of our vulnerabilities and develop viable strategies to detect, deter, and counter both physical and cyber-based threats to our people and our infrastructures.

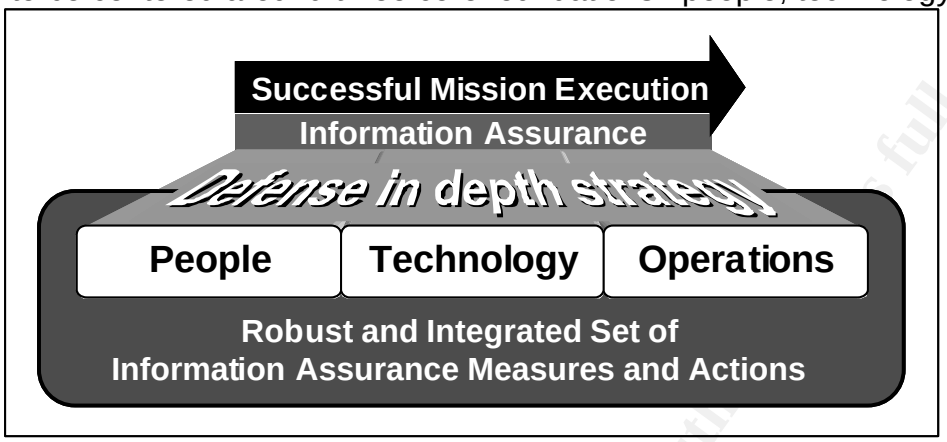
There is a new paradigm for assessing the security challenges that we face – now and in the future – and it is based on the expectation that unrest and global turmoil will continue, and with that, the continuing prospect of the asymmetrical threat. Our security will depend on our ability to develop new strategies for dealing with threats that are resistant to traditional ways of dealing with them.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Defense in Depth Strategy

Defense in Depth combines the strengths and capabilities of people, operations, and technologies to establish multiple layers of protection – similar to protecting a home with multiple defenses.

According to the IATF security framework, an effective Defense in Depth strategy needs to be centered around three core foundations: people, technology and operations.



The Defense in Depth strategy requires a balanced focus of these three primary elements of information assurance:

People: ***Hire, Train, Include, and Reward Good People.***

Achievement of Information Assurance goals begins with senior-level commitment, the assignment of roles and responsibilities, training of personnel and enforcement of personal accountability. This must include physical security personnel and measures to control facilities and protect the critical elements of the IT environment. IT and physical security personnel have the same goal: controlling access. They need to put aside the differences and work together towards this common goal, thus, enhancing overall security. Security is a human social problem, and so people must be at the core of a Defense in Depth strategy.

Technology: ***Evaluated, Effective Solutions to support Defense in Depth.***

Making sure that the right products are chosen. There should be a process for selecting technology. There must be controls in place that are designed to prevent and detect security breaches, and respond in an appropriate manner. And this selection process should conform to the security policy and architecture standards, and be subject to validation by an outside party, and a system/business risk assessment. Technical security measures must be combined with procedural and personnel security measures.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Physical security is the foundation of other security domains, including IT security. If it is weak, that weakness then becomes a vulnerability in the area of information security. For instance, IT technical security may be well implemented, but if an intruder can gain access to a system and compromise it, then despite the technical controls, there is a vulnerability due to a physical security breach.

Operations: ***Enforce security policy, Respond quickly, Maintain/Restore Services.***

Operations focuses on the activities required to sustain an organization's security posture on a day-to-day basis, including compliance to policies, and continuity of the business. Without a comprehensive policy, security will continue to be implemented in a fragmented way – by domain, thus leaving gaps, which lead to vulnerabilities.

Along with this, security operations must encourage the flow of information from "stovepipes" where data is seemingly unrelated and stockpiled, to an atmosphere of collaboration and sharing. As important as information sharing is among various organizations, it would be useless without an infrastructure in place to coordinate the information that is gathered and passed along. An effective security operations organization can fulfill this role of gathering, assimilating, and analyzing information. This is essential in these times of heightened threat awareness, and with that, the increased need to correlate the flow of information with the goal of maintaining normal operations.

An effective Defense in Depth strategy needs to be a coordinated effort – a Defense in Breadth that includes the open sharing of information and support with physical and IT security professionals, law enforcement, and intelligence agencies included as players. Centers of excellence do exist in government, in education, and in the private sector, and we need to leverage and build on them. Cross sector cooperation on information is imperative.

And finally, to make it all work effectively, there must be an ongoing security awareness plan to maintain the appropriate level of focus and ensure continuing compliance.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Think Globally…and Horizontally

> "Today, the cyber economy is the economy…Corrupt those networks and you disrupt this nation." Condoleeza Rice, US National Security Advisor *March 23, 2001*

Cybersecurity lies at the core of our economic prosperity, which is our "nerve center". And in his first National Security Presidential Decision, released on March 5, 2001, President Bush emphasized that national security depends on America's opportunity to prosper in the world economy.

It is imperative to think horizontally, to be mindful of the connections between physical infrastructures and networks in cyberspace that create interdependencies in which the weakest links become targets. For instance, technical mitigations are useless without trained people to use them and operational procedures to guide them. These interdependencies require us to think differently about security.

The events of September 11 made us realize that we must move from complacency, the belief that "it could never happen here", and move toward a new way of thinking – one that questions safeguards, and whether they are adequate enough in this threat environment.

We need new organizations, new practices and new tools – in a new spirit of collaboration. The security challenges that we face are too complex to be addressed as they are being done today: ad hoc and reactively.

Synergistic Security

Using this new vision, we need to develop a security strategy by acknowledging that security is a shared burden and responsibility, and by taking a holistic approach to managing security. An approach that recognizes and utilizes the significant capabilities of all sectors of society: government, academia, and private industry. The asymmetric threat requires a comprehensive, unified response in order to prevent it, protect against it, and to respond to it. And along with a new, holistic strategy, there must be a roadmap to achieving synergistic security. At the very least we must take the following actions:

- Reassessing our assumptions about what is critical and vulnerable, and how we will ensure security.
- Developing and /or revising a Defense in Depth strategy, built around the cornerstones of a secure organization: People, Technology, and Operations.
- Implementing or expanding upon a Defense in Breadth strategy, which calls for the inclusion of an expanded team of security collaborators. This ensures that

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

physical security, IT security, as well as other knowledgeable personnel, such as legal, facility operations, Human Resources, etc., are an integral part of the security organization.

- Increasing and encouraging information sharing between users and administrators, the public and private sectors, as well as the intelligence communities.
- Improving and broadening the scope of analysis, including the correlating of seemingly unrelated data by a cross-section of specialists, and early warning capabilities, with the goal of moving away from reactive mode as the primary method of security vigilance

Conclusion

Security once meant digging a moat around the castle, now it must involve industries, governments, and their systems – all-interoperating. Telecommunications, energy, banking, transportation, water, and essential government services are now connected to each other in one way or another in this information age.

> "It is very important to concentrate on hitting the U.S. economy through all possible means…look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck…" Osama Bin Laden, December 27, 2001

Post September 11, we are in a time of uncertainty, and security professionals must understand the implications of what we do not, can not, and will not, know about the future security environment, and future security threats. Accounting for, and dealing with uncertainty has always been a big analytical challenge. But in today's uncertain world, we need to be skilled in dealing with mysteries, secrets, and threats. Critical thinking and collaboration may be the security professional's most important attributes.

Resources

Skoudis, Ed, "infosec's Worst Nightmares", Information Security Magazine, November, 2002 Volume 5, Number 11
http://www.infosecuritymag.com/2002/nov/nightmares.shtml

IATF Forum, "Security Framework", Release 3.1, September 2002
http://www.iatf.net/framework_docs/version-3_1/index.cfm

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Loeb, Larry, "information assurance powwow Part 2…Delving Deeper into IA", The West Point Conference, August 2001
http://www-106.ibm.com/developerworks/security/library/s-confnotes2/?dwzone=security

Andriole, Steve, "Improving Biz/IT Convergence An Action Plan", CIO Information Network, CIO Insights, 27 September 2002
http://cin.earthweb.com/insights/article.php/10907_146838/

Wilson, Thomas R., "Global Threats and Challenges", Defense Intelligence Agency, Statement for the Record, Senate Armed Services Committee, 19 March 2002
http://www.senate.gov/~armed_services/statemnt/2002/March/Wilson.pdf

Bennett, Robert F., "Security in the Information Age", New Challenges, New Strategies, Joint Economic Committee, US Congress, May 2002, including a compendium of articles by the following authors:

Keyes, David, "Cyber Early Warning: Implication for Business Productivity and Economic Security"

Charney, Scott, "Transition between Law Enforcement and National Defense"

Wong, Nancy, "Critical Infrastructure and Information Assurance: A Working Context and Framework"

Montgomery, Mark, "Cybersecurity Policy: Moving from Nouns to Verbs"

Rasmussen, Michael, "Information Protection: Assuring Stakeholder Value in a Digital Age"

http://www.house.gov/jec/security.pdf

Analytical Services, Inc, "Homeland Defense Strategic Thrust", Anser Homeland Security Report, 11 February 2000
http://www.homelandsecurity.org/FRExecSum.cfm

Schwartau, Winn, "Asymmetrical Adversarialism in National Policy", March 2000
http://www.infowar.com/chezwinn/articles032000/AsymmetricalAdversarialism.shtml

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Huston, Brent, “A Higher View of Defense In Depth”, Security Strategies, IT World.com Newsletter, 20 February 2002
http://www.itworld.com/nl/security_strat/02202002/

Tippett, Peter,” Defense in Breadth” Executive View Column, Information Security Magazine, February 2002
http://wwwinfosecuritymag.com/2002/feb/columns_executive.shtml

Lang, Thresa, “When Worlds Collide: Physical and Information Security”, SC Infosecurity News, 26 June, 2002
http://www.infosecnews.com/opinion/2002/6/26_03.htm

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.