



The Expanding Role of Security in Your Business

By Richard A. Diamond ■ *Stradivarius Associates*

Recent events have caused us to re-assess our physical and cyber security. Our systems are not adequately protected, as evidenced by a recent survey: a yearly study by the Computer Security Institute revealed that, in 2000, 70% of respondents replied that they have "experienced unauthorized use of computer systems within the last 12 months," up from 42% in 1996.

As property owners and managers or service providers, you too must take the issue of security very seriously. It touches all of our lives, from the physical aspects such as access and surveillance systems to the digital side where hackers can tap into your critical business systems or viruses can cripple your local network. Any of these will create some potentially severe consequences for your business. Accordingly, we have evaluated some simple cyber security measures that should be implemented in your business because you are At Risk.

The Top Six Rules of Cyber Security

1) Threat and vulnerability assessments should be updated on a regular basis.

Some companies have done threat and vulnerability assessments long ago; others have not attempted to formally assess business security risks. In light of the World Trade Center attacks and the well-documented risks to computers, it is important to schedule these assessments on a regular basis.

Now that the threat model has changed, recognizing terrorism as a business threat is not enough. Business must consider the following:

- Critical infrastructure providers

might now be attractive to terrorists

- Those companies that do not manage "attractive targets" may need to prepare for business disruptions
- They must contemplate the ways in which such an attack may occur
- They carefully assess vulnerabilities by hiring corporate agencies to conduct "attach and penetration" test of their own networks
- They deploy network assessments, which are more thorough than an attack and penetration

2) Effective security policies and procedures should be implemented.

Comprehensive security policies and procedures are the foundation upon which security is built. In certain limited areas, such security has been or soon will be mandated by government regulation (financial and medical records). Companies should identify gaps between their own corporate standards and industry-wide best practices.

Since every organization is different, policies and procedures frequently cover:

- Access controls-user ID's, passwords
- Remote access-authorization to access corporate networks remotely and under what conditions
- Hardware and software configurations-servers and firewalls
- Intrusion detection-types of products deployed, configuration of products upon installation
- Employee monitoring
- Incident response

Finally, security guidelines and training should be defined,

assigned, documented, distributed and reiterated to each employee.



3) Computer security should be assessed and upgraded continually.

Threats must continually be reassessed as the business world changes. Because neither technology nor security are static, computer security and upgrades, must be continually assessed, as well.

On the technology side, some of the considerations follow:

- New vulnerabilities may be discovered in older products, so installing patches may be required

- Old products may be upgraded, and new products deployed, thus introducing new vulnerabilities into a network

Business changes may also require security to be reassessed. For example:

- Outsourcing critical functions may give contractors privileged access to a company's computer systems
- Entering into a joint venture may cause two organizations to connect their networks

- Offering new applications to customers – online shopping or e-commerce – may create links between the public and a company's internal systems. So each business change affecting the information infrastructure creates a need to reassess threats, to identify new potential vulnerabilities, and to take proactive steps to minimize risks.

4) 24 x 7 monitoring, including intrusion detection systems should be deployed.

Computer security experts generally agree that most computer crimes are neither detected nor reported. In part, this is because many computer crimes are not self-evident. If a car is stolen, the owner knows because the vehicle is missing. But if a hacker steals a computerized customer list, the original remains in place, available to the owner.

Studies have attempted to quantify the scope of the computer crime problem:

- In a controlled study, the United States Department of Defense attacked its own machines. Of the 38,000 machines attacked, 24,7090 (65%) were penetrated. Only 998 (4%) of the penetrated sites realized that they were compromised, and only 267 (1%) of those sites reported the attack.

The industry has responded by creating intrusion detection systems (IDS) that use the power of the computer to look for known footprints of attacks or vulnerabilities that hackers have attempted to exploit. Such real-time monitoring is becoming a critical component of network security, but requires the expense of a Network Operations Center (NOC) and staff analyzing reports 24 hours-a-day, 7 days a week.

5) Security incident response plans should be developed, and coordinated with overall contingency plans.

An organization's ability to detect





- Infragard is a joint private sector-FBI organization where threat and vulnerability information can be shared anonymously between organizations and the government.

Conclusion

There is much that a business can do to improve the cyber security aspects of critical infrastructure protection. The question of how much money needs to be spent and how much effort is required will be different for each company because each one has a different risk/cost/benefit profile. Your business clearly is at risk. However, risks can be minimized, and the impact of attacks blunted, through careful preparation. The vast majority of incidents that happen in business today could have been easily prevented had basic security measures been taken such as the ones presented here, an objective achievable at relatively low cost. ■

About the Author

Richard A. Diamond is the President & CEO of Stradivarius Associates which specializes in business strategy consulting for public and private companies around the world. He actively consults with ImagiNet (www.imagi.net) a leading secure managed network service provider, offering a comprehensive suite of network management, online data backup, WAN and security products and services. ImagiNet has operated its "state of the art" Secure Operations Center 24 x 7 x 365 for over 17 years. He can be reached via email at rdiamond@stradass.com.

and quickly respond to simulated attacks should also be tested. While some investigations may be conducted merely to assess damage and restore the security of the attacked system, the primary goal should be to develop the evidence necessary to assign responsibility and take legal action.

Before such testing can be done, an organization should review and document the following:

- Incident management policies, procedures and plans
- Processes to log network activity in the event of an attack
- Evidence collection and maintenance procedures

Cyber security incident response plans should be closely coordinated with physical contingency and disaster recovery plans, especially since future cyber attacks may be coordinated with physical attacks. These plans should address ownership of an incident, escalation procedures, physical and electronic evidence handling procedures, coordination with law enforcement,

and media relations.

6) Information about threats and vulnerabilities should be shared.

As systems have become more complex, securing them has become increasingly difficult. The challenge for the security community has been to ensure that computer users are notified when vulnerabilities are found, and that fixes are implemented.

- Fuller information sharing has historically been impeded by a host of factors. Once a company has been exploited, such public exposure can cause customers and investors to lose confidence, adversely impact equity markets, and create the risk that other hackers will view the company as vulnerable, thus inviting additional attacks.
- To promote the sharing of threat and vulnerability information anonymously, members of various critical infrastructures have created Information Sharing and Analysis Centers (ISACs).