



LJN'S

LEGAL TECH

Newsletter®

Volume 21, Number 6 • September 2003

IT Security: It's Now or Never

By Tom Gelbmann

Information technology security is a critical issue for all law firms. Yet, security initiatives are often dismissed as high cost/low return and put on the back burner. This low priority status persists despite the significant operational and financial impact a security breach would have on a firm. It is only when a major event such as the recent confluence of the Northeast blackout and the Blaster and SoBig worm attacks, or the nefarious actions of a disgruntled employee hit the public consciousness that attention rapidly re-focuses on security matters.

As the practice of law is perhaps the most information intensive of professions, we cannot avoid the implications of the digital age. The use of information technology in law firms has risen to the point where systems and technology serve as the nervous system of the firm. Loss of critical information systems and services could put the firm on life support. Even a thumbnail calculation on the financial impact of a security event that damaged systems and services would disclose a sizeable cost in terms of lost revenue, lost productivity, recovery costs and loss of client confidence.

In simple terms, if a firm loses its information systems for an extended period, it may be out of business. With this much riding on the availability of information technology, IT security is truly a *now or never* proposition.

PRACTICAL APPROACH

Just as there are few, if any, absolutes in this world, no computer network can ever be considered completely secure. Security Management is essentially the process of minimizing threats; lowering the potential risk of a loss event, and minimizing the cost impact of an incident in terms of business interruption, losses in revenue, client confidence and competitive advantage as well as replacement and recovery costs.

A practical approach for establishing a comprehensive security program for computers, networks, systems and information assets begins with establishment of benchmarks for the appropriate level of security. To arrive at this threshold, two key components must be understood:

- The threats and the vulnerability to these threats; and
- The financial impact of a loss from a security breach.

Once these components are understood, an IT security framework can be created aimed at mitigating threats and minimizing the financial impact in line with the security benchmark.

Just as each organization is unique, there is no one-size-fits-all solution for a comprehensive IT security framework. However, a comprehensive security strategy will involve the combined components of management, policies, and tools. Consider the following to be a starter set of basic elements that should be included in an IT security program:

EXTERNAL THREATS

Addressing external threats is the equivalent of locking the doors and windows. The primary goal is to provide an effective defense against intrusions from the outside world. Intrusions can come through any electronic communication facility connected to the network. Most commonly this is the Internet connection or any direct data communication link.

FIREWALLS/PROXY SERVERS/DMZ.

This is a group of tools used to enforce security policies between two networks. The Internet, with all its benefits and value, is a very dangerous place. Internet access presents a constant threat to a firm's network, with continual scanning and bombardment by hackers looking for opportunities to do damage or establish a launching point for further damage.

A firewall is essentially a software program or piece of equipment that can filter attempts to enter a firm's private network from unwanted sources. Proxy Servers and a DMZ (demilitarized zone) are tools that can augment security in concert with firewalls and related devices, thereby strengthening overall network security.

- **Antivirus software.** Computer viruses and related types of malicious code (worms, Trojan horses, logic bombs) are the modern day plague on computer systems. Though the technical makeup and sophistication of computer viruses continue to evolve, one key fact remains the same: A virus must have an entry point into a system in order to cause problems. The most common entry point is through e-mail, but other avenues also exist, such as portable media and downloads from Web sites.

Filtering software and virus scanning represent the first line of defense at entry points to the network. Continuous scan-

ning on servers and personal computers must also be a part of the security strategy. Effective antivirus protection requires administrative attention to manage frequent updates to antivirus software enabling detection of the newest forms of viruses.

• **System software maintenance.** While we all wish that software flaws and security holes in operating systems did not exist, the reality is that “evildoers” will continually find these flaws and try to exploit them. Until operating system software becomes perfect, the best practice is to stay current with patches and updates.

This point was proven with the recent episode of a virus/worm threats — the Blaster virus — that caused considerable disruption around the world. A patch to address this threat was posted on Microsoft’s Web site nearly a month before Blaster struck.

• **Laptop security.** Laptops present an additional set of threats, as they are used both inside and outside the network. Additional security measures must be taken with laptops to not only protect the network when these units are reconnected, but also to secure the contents on the hard drive.

Protective measures to consider include the use of a Virtual Private Network (VPN) connection for remote access to the network through the Internet, encrypted hard drives, passwords on start up and screensavers, and software firewalls for units that may be connected to alien networks.

INTERNAL THREATS

Assuming the doors and windows are properly locked, the next step is to ensure the network is well patrolled and protected from internal threats that can be just as formidable and damaging as external threats.

Tom Gelbmann is an independent management consultant who has helped lawyers realize lasting value from information technology for over 16 years. He can be reached at Gelbmann & Associates: 651-483-0022 or tom@gelbmann.biz.

Surveys by the FBI, the Computer Security Institute and Pantos and Associates all set the odds of a computer security incident as being 70% likely to come from “the inside.” Employees may attempt to read each other’s e-mail, access confidential records, or simply import a virus on a floppy or laptop. One of two strategies can be followed: Lock down everything and grant permissions on a needs basis; or consider everything open and lock down only sensitive areas. The correct strategy is as much a management issue as it is a technology issue.

• Access control and Passwords.

Access to systems, files and services is granted to individuals (users) through an authorization process that validates the identity of the individual through combination of user ids and passwords.

Historically, passwords have been treated with little respect. They are often shared or posted in plain sight, and frequently consist of an easily guessed word. Just the opposite should be the norm. Passwords represent the keys to a firm’s valuable assets, and should be afforded the highest level of protection possible.

Best practices call for establishment of a standard of personal accountability in which any action taken on the system under a given user id is considered to be the personal responsibility of the individual. Once this standard is in place, password confidentiality can be supported by following additional best practices aimed at eliminating the use of simplistic passwords (eg, minimum of 6 characters, combination of letters, numbers and special characters, and changing passwords on a regular basis).

• **Management.** A variety of policies and practices are also part of a comprehensive security program to ensure security objectives are achieved. These policies cover a

The publisher of this newsletter is not engaged in rendering legal, accounting, financial, investment advisory or other professional services, and this publication is not meant to constitute legal, accounting, financial, investment advisory or other professional advice. If legal, financial, investment advisory or other professional assistance is required, the services of a competent professional person should be sought.

LEGAL TECH Newsletter®

PUBLISHERMarjorie A. Weiner
ASSOCIATE PUBLISHERSofia Pables
EDITOR-IN-CHIEFAdam Schlagman, Esq.
MANAGING EDITORSteven Salkin, Esq.
ART DIRECTORClaire C. O’Neill-Burke
GRAPHIC DESIGNERLouis F. Bartella

BOARD OF EDITORS

RICHARD C. BELTHOFF JR. Wachovia Corp.
Charlotte, NC

JEFFERY M. DUNCAN, ESQ. Banks Hofer Gibson & Lione
Chicago

TOM GELBMANNGelbmann & Associates
St. Paul, MN

RICHARD K. HERRMANN, ESQ. Blank Rome LLP
Wilmington, DE

ADAM E. JAFFE, ESQ. Huron Consulting Group LLC
New York

ROSS KODNERMicroLaw Inc.
Milwaukee

JOSEPH D. LEEMunger, Tolles & Olson LLP
Los Angeles

STEPHEN T. MAHERMiami

DAVID L. NARKIEWICZ, ESQ. Montgomeryville, PA

D. CHAD McCOY. Parr Waddoups Brown
Gee & Loveless
Salt Lake City, UT

DONNA PAYNEPayne Consulting Group
Seattle

ALAN PEARLMANThe Electronic Lawyer
Northbrook, IL

JOEL B. ROTHMANTechnology Risk Solutions LLC
Boca Raton, FL

JOHN J. SROKADuane Morris LLP
Philadelphia

ERIC H. STEELESteele Scharbach Associates LLC
Chicago

DANA H. SHULTZDana Shultz & Associates
Oakland, CA

GEORGE J. SOCHA JR. SochaConsulting LLC
St. Paul, MN

ALAN J. STEINBERG, J.D., LL.M. Steinberg & Steinberg, LLC
Creve Coeur, MO

SUZANNE D. WISNIKWiz Business Systems, Inc.
Norristown, PA

LJN’s Legal Tech Newsletter® (ISSN 0738-0186) is published by Law Journal Newsletters, a division of American Lawyer Media. © 2003 NLP IP Company. All rights reserved. No reproduction of any portion of this issue is allowed without written permission from the publisher. Telephone: (800) 999-1916, Editorial e-mail: steves@palawnet.com, Circulation e-mail: subs@palawnet.com

LJN’s Legal Tech Newsletter P0000-223
Periodicals Postage Pending at Philadelphia, PA
POSTMASTER: Send address changes to:
American Lawyer Media
1617 JFK Blvd., Suite 1750, Philadelphia, PA 19103
Annual Subscription: \$249

Published Monthly by:
Law Journal Newsletters
1617 JFK Boulevard, Suite 1750, Philadelphia, Pa 19103

wide range of issues related to management of an appropriately secured IT environment:

System Administration. Access to system administration functions must be tightly controlled. These functions provide access to the full breadth of the network including authority to access files, update system configurations, install software and grant access rights to system users.

Establish a system of checks and balances to ensure no one person can operate independently. While this may sound a bit heavy handed, keep in mind that such measures can serve as a protection to individuals as well as protection of the firm's assets. External technical service providers who need hands on access to the network should not only be bonded, but also should be subject to confidentiality agreements. These individuals should also be given access to only what is necessary to complete their tasks, and subject to the same system of checks and balances noted above. Additionally, access can be limited in terms of time of day. Temporary user accounts should expire when they have completed their work.

Physical Security. Control over physical access to network components is a frequently overlooked aspect of overall security. Access to computer rooms and communications closets that house file servers and network components should be limited to only those who require physical contact with the equipment, namely system administrators and technical service providers. Access is generally controlled through a card key access system that also provides automated logging of each entry.

Backup and recovery. Everyone backs up, but not everyone stores backup media in a secured, offsite storage facility. Too often we see firms doing a diligent job of backing up only to have the media remain on site and unprotected from loss due to theft or misplaced or damaged files. Surprisingly, some firms still allow file tapes to be taken home by the System Administrator. It's a simple and cost effective measure to have daily or weekly backup tapes picked up for storage at a professional records management facility and rotated appropriately.

Backup is only half of the solution. Recovery of data from backups is equally important. Files should be restored from backups on a regular basis to ensure backups are what everyone thinks they are. These exercises also keep staff trained on the proper procedures and validate there are no problems with the media.

Periodic Audits. As with any management program, oversight and review of the IT security program is essential. An annual security audit by an independent expert can be used to benchmark progress, identify vulnerabilities that require attention, fine tune security policies and procedures, and provide a basis for decisions on allocation of resources.

Response/Recovery. Despite the best-laid plans, losses will occur. Security programs that include the elements discussed above can pay dividends by minimizing the scope and impact of a security event. The final component of a well-conceived IT security program includes detailed plans and procedures to respond to security breaches as quickly and com-

pletely as possible.

Recovery plans need to be in place before a problem occurs. These plans should cover moderate level problems such as restoration of lost systems and data, eradication of computer viruses, as well as recovery from catastrophic events. Planning should address likely scenarios and produce written plans that define what needs to be done and who needs to do it. Once in place, these plans should be reviewed and practiced on a regular schedule, and kept current as the environment changes.

Keep in mind that you need not experience a full-scale disaster to reap the benefits. The Northeast blackout is a good example. Parts of the plan can be referenced as required, such as calling trees for notification of staff, replacement of damaged equipment, recovery procedures, emergency contact information and procedures.

GETTING IT DONE

Address security on the front end, build it into new systems and infrastructure upgrades and make it part of everyday activity. Just as you wouldn't leave a stack of \$100 bills on the seat of your unlocked car, don't leave your firm's information assets vulnerable. Take the necessary steps to protect the network. If internal staff does not have the time or experience to plan, design and implement an IT security program, enlist experienced professionals to assist.

Balance protection measures with risk and productivity. Each organization must find the right balance, based on a clear understanding of its IT security threshold.

With an effective IT security program in place, perhaps you will sleep better at night.

