

Cyberterrorism Prevention Checklist

by

Frank Fiore and Jean François

As CEO, CIO, or other top executive of your organization, you need to be *certain* that your departments understand the threat of cyberterrorism. Take this checklist of actionable items to your senior management meeting. Find out whether your IT, security, and human resource personnel have put in place the necessary security precautions to protect you from becoming an unwitting collaborator with cyberterrorists.

Intelligence Gathering

This area includes three possible security lapses that allow for penetration of systems with the goal of stealing information or sensitive data. The key here is to get your organization, company, or institution on a wartime footing and control access to your building, personnel, and information systems.

1: Identity Impersonation and/or Identity Theft

You may think this is an obvious problem, but you'd be surprised how many organizations—businesses especially—fall down on this simple yet effective threat prevention.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Access controls</i>	Physical Plant Security Manager	Are badges, ID cards and/or other verification methods required by security and other personnel before allowing building entry?	Personnel who are not carrying proper ID should be challenged internally.
<input type="checkbox"/>	<i>Document controls</i>	Human Resources	Are organizational phone books and contact/vendor lists restricted to the premises?	These documents should be treated as though they contain organizational secrets. Whenever possible, shred out-of-date paper documents that reveal information about company internal activity.
<input type="checkbox"/>	<i>Information procedures</i>	Human Resources	Are all inquiries via phone, email, or other correspondence method checked for authenticity?	No one should ever assume that someone is who they say they are. Inquiries should always be forwarded to appropriate personnel for handling. A paper audit trail should be kept and required for any information requested.

2: Spyware

Spyware is software that sits on your system and tries to be invisible while collecting as much information as possible to be sent offsite.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Scanning programs</i>	IT Dept.	Are systems regularly scanned for viruses, Trojan horses, etc.?	Viruses and Trojan horses have become more sophisticated, so more aggressive checking is needed.
<input type="checkbox"/>	<i>Firewall and intrusion-detection system</i>	IT Dept.	Is the internal network protected by a firewall coupled with intrusion detection?	Watch all inbound and outbound traffic. Look for odd or new traffic patterns.
<input type="checkbox"/>	<i>Third-party software audits</i>	IT Dept.	Do you regularly audit third-party software to detect unauthorized programs?	Spy-Software.org offers a system for auditing software.

3: Internal Threats

This area is often overlooked by organizations, but employees can be a great source of information-gathering for unauthorized use.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Background checks</i>	Human Resources	Are background checks performed on job applicants before they are hired? Are references checked carefully?	Current events show that false information on résumés is nothing new. If projects are of great importance, terrorists may be interested in getting jobs that will provide access to information via computer systems or grant access to unauthorized users' malicious programs.
<input type="checkbox"/>	<i>Corporate intelligence organizations</i>	Human Resources, executive staff	How do you address potential threats from corporate intelligence organizations?	Organizations like SCIP (Society of Competitive Intelligence Professionals) use a systematic program for gathering, analyzing, and managing information that can affect your company's plans, decisions, and operations—otherwise known as <i>corporate espionage</i> .

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Disgruntled employees</i>	IT Dept.	How are you preventing the possibility of damage done by employees?	Employees can modify or destroy data. Keep good long-term backups and have a disaster recovery plan in place.
<input type="checkbox"/>	<i>Backdoor threats</i>	IT Dept.	How are you addressing the possibility of malicious code or products created inside the organization?	Have an audit/review process in place for data, source code, security access and procedures, and so on.
<input type="checkbox"/>	<i>Testing backups</i>	IT Dept.	Is our backup data recoverable? Is recovery regularly tested to make sure that the backup data and the restoration system actually work (and work correctly)?	A malicious computer user can cause small corruptions in data that, if not regularly checked by restoring backups, will not be discovered until vital information is needed. Furthermore, it's important to know that in the event of a recovery, critical data will be available—and to know what special steps may be needed to restore that data.

Systems Damage

This area includes four possible security lapses that allow for the disruption or damage of data and your information infrastructure.

4: Breakdowns in the Human Firewall

People are the weakest link in a security plan. Proper training can prevent a majority of security lapses.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Inquiries</i>	All personnel	Are all inquiries referred to a designated point of contact?	Don't voluntarily disclose any information.
<input type="checkbox"/>	<i>Point of contact</i>	Human Resources	Who is designated as the single point of contact for organizational questions?	Don't allow just anyone to talk about company business. The best intelligence gatherers know how to take what looks like uninteresting pieces of information and use them to get more, or tie them together to make a bigger picture.
<input type="checkbox"/>	<i>Awareness</i>	All personnel, especially Security	Are you always aware of who is working around you and whether he or she belongs in that area?	For example, the soda machine being refilled is no excuse for the person doing it to be wandering around different offices unescorted.

5: System/Browser Vulnerabilities

Bugs or other code flaws can allow an unauthorized user to execute arbitrary code.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Bounds checking and code reviews</i>	IT Dept.	Are you vigilant in checking bounds and reviewing code?	Don't let speed override good programming practices. Take the time to do periodic case reviews for security and to make sure that nothing was "slipped in."
<input type="checkbox"/>	<i>System patches</i>	IT Dept.	Do you keep system patches to current levels?	Every reputable vendor publishes patches to keep applications and other programs current. Keep track of vendor alerts and apply patches in a reasonable period of time and in a consistent fashion.
<input type="checkbox"/>	<i>Alternative heterogeneous applications or platforms</i>	IT Dept.	How can we use alternative applications (Eudora, Opera) or platforms (Mac, Linux, BSD) to prevent system infection?	Using non-mainstream applications and platforms makes system infection more difficult.

continues

continued

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Filtering executable attachments</i>	IT Dept.	Are executable attachments filtered from incoming and outgoing email?	If it's vital that programs be sent via email, nothing that can be executed as a program should be sent through email without being examined on a "sandbox" system that can contain an outbreak.
<input type="checkbox"/>	<i>Educating users</i>	IT Dept.	How are you educating users to keep them from opening unexpected or unverified attachments?	Show users what can happen. Do demonstrations and hold regular updates. To prevent hoaxes from spreading, don't let users propagate this information on their own.

6: Wireless Insecurity

Wireless networks are being installed by organizations at a rapid rate, opening their networks to “drive-by hacking.”

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Media access control (MAC) addresses</i>	IT Dept.	Does our system use MAC addresses?	It's very easy to change a MAC address on a system to gain entry.
<input type="checkbox"/>	<i>Wired Equivalent Privacy (WEP)</i>	IT Dept.	Does our system use WEP to protect data?	Don't rely on WEP to protect data; it's open to compromise.
<input type="checkbox"/>	<i>Default configs</i>	IT Dept.	Does our system use default configuration files?	Change the default SSID to something that's difficult to guess.
<input type="checkbox"/>	<i>Strong user authentication</i>	IT Dept.	Does our system employ strong user authentication?	Implement an authentication system that mandates that computers and users be authenticated before they can use wireless resources.
<input type="checkbox"/>	<i>Virtual private network (VPN) technology</i>	IT Dept.	Can we use VPN technology to secure data sent over wireless links?	Encrypted data is very difficult to get to and enhances overall security in a wireless environment.

continues

continued

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Wireless LANs</i>	IT Dept.	How are you monitoring wireless LANs for hijackers?	Use tools to make sure that only authenticated users and authorized systems are on your wireless network. Audit as needed.
<input type="checkbox"/>	<i>Wireless deployment in a DMZ (demilitarized zone)</i>	IT Dept.	Are our wireless setups deployed in a DMZ or behind a proxy/filtering firewall?	Keep wireless traffic where it can be controlled safely, away from sensitive systems or the wired LAN.

7: Denial-of-Service (DoS) Attacks

These attacks are becoming more and more sophisticated, and in some cases initiated as a side effect of some other attack.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Filtering RFC 1918 addresses</i>	IT Dept.	Are RFC 1918 addresses filtered both inbound and outbound?	These addresses are known non-routable addresses on the Net, meaning that if used in an attack they're untraceable.
<input type="checkbox"/>	<i>Spoofed addresses</i>	IT Dept.	Are spoofed addresses prevented from leaving our network?	Use documented best practices to keep RFC 1918 and smurf attacks from being able to leave through the edge routers of your LAN or WAN.
<input type="checkbox"/>	<i>Monitor bandwidth</i>	IT Dept.	Are you watching for spikes or high loads?	Unauthorized transfers usually show up as unexplained high bandwidth use during off-peak hours.
<input type="checkbox"/>	<i>Scan internal hosts and devices</i>	IT Dept.	Are you scanning regularly for any compromises or security breaches?	Use available tools and check to make sure that systems on your LAN belong there and have not been compromised by known exploits.

System Hijacking

In this area, three possible security lapses allow the use of established communications vehicles for clandestine operatives to secretly communicate with others.

8: Steganography

Steganography is the art and science of hiding the fact that communication is happening. It involves hiding messages inside text, images, sounds, or other binary files for clandestine communications.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Unauthorized software</i>	IT Dept.	Do you regularly check for unauthorized software on organizational computers?	Use tools to control user level access and prevent software from being installed without administrator permission.
<input type="checkbox"/>	<i>Newsgroups and web sites</i>	IT Dept.	Do you regularly check newsgroups and web sites for comments made about us—both good and bad?	Many mailing lists and Internet information sites can raise awareness by matching activities of crackers directly and learning what they are doing in real-time.
<input type="checkbox"/>	<i>Inbound and outbound email</i>	IT Dept.	Are both inbound and outbound email scanned for unusual contents such as MP3 files, PIC files, and so on?	Email is the one tool that can easily pass through firewalls. All data coming in and leaving should be checked to make sure it's safe before being passed on to the user.

9: Tunneling

Tunneling allows communication in an environment where communication may not be possible due to firewalls or proxies that limit traffic. Many networks assume that having a firewall or proxy server prevents internal users from going to unauthorized sites or passing internal data to the outside world. That's a bad assumption. For example, an application called HTTP-Tunnel allows people behind a firewall (which allows only web surfing) to use *any* Internet application. HTTP-Tunnel runs as a SOCKS server or via port mapping and can tunnel both TCP and UDP.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Corporate espionage</i>	IT Dept.	Do you regularly review logs and traffic passing through proxies and firewalls that are not work-related?	Theft of company secrets will continue to grow with international competition and tighter R&D budgets.
<input type="checkbox"/>	<i>Bypassing corporate security policies</i>	IT Dept.	Have you set limits and policies on which ports are acceptable to access?	Keep honest people honest; allow access only to the ports inside and outside your system that people really need to do their work. Publish these regularly and make it policy to regularly update employees on what they are allowed or not allowed to do.

continues

continued

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Productivity and espionage</i>	IT Dept.	How are you checking for unauthorized VPN traffic originating from inside our LAN?	If someone is stealing information or making unauthorized entries, a virtual private network (VPN) is one way to mask this activity. All VPN technologies use well-known ports, so look for activity that doesn't belong.

10: Worms, Trojan Horses, and Viruses

These attacks are becoming more prevalent and much more sophisticated. Next-generation worms, Trojan horses, and viruses will be more intelligent and attack through multiple methods of distribution.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Unauthorized software</i>	IT Dept.	Do you regularly check for unauthorized software on organizational computers?	Use tools to control user level access and prevent software from being installed without administrator permission.
<input type="checkbox"/>	<i>Anti-virus software updates</i>	IT Dept.	Are anti-virus software updates installed in a timely manner?	Make it a point to keep updates as automatic as possible or on a daily schedule to get the latest protection available.
<input type="checkbox"/>	<i>Alternative heterogeneous applications or platforms</i>	IT Dept.	How can we use alternative applications (Eudora, Opera) or platforms (Mac, Linux, BSD) to prevent system infection?	Using non-mainstream applications and platforms makes system infection more difficult.

continues

continued

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Educating users</i>	IT Dept.	How are you educating users about how malicious programs propagate and how to prevent infection?	Publish all policies and procedures and make users acknowledge them. Keep a FAQ and encourage questions by letting question authors be anonymous.
<input type="checkbox"/>	<i>Proxy/firewall filters</i>	IT Dept.	Are you using filters to find malicious programs and their signatures coming into or leaving the LAN?	Check inside the firewall as aggressively as when checking at the firewall.

Disinformation

This area includes two possible security lapses that allow for the dissemination of propaganda such as the following:

- Spreading false rumors electronically that are picked up by the media as true
- Cracking into news servers to plant false or misleading stories
- Entering false or misleading information in databases, thus undermining the effectiveness of organizations relying on that information

11: DNS Poisoning and Domain Hijacking

DNS poisoning is convincing a name server that a domain has a different IP address. *Domain hijacking* involves stealing a domain at the registrar level.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>DNS servers</i>	IT Dept.	Are our DNS servers secure? Do we require our DNS peers to secure their servers?	Use the latest security features of DNS and use best practices for safe deployments both inside and outside the firewall.
<input type="checkbox"/>	<i>Passwords</i>	IT Dept.	Do we require passwords for domain registration and changes?	Password-protect domain name information at registrars to prevent the domain from being redirected to another site or stolen.
<input type="checkbox"/>	<i>Domain changes</i>	IT Dept.	Can domain changes be made via email?	Email can be forged. Require an SSL-encrypted web page or PGP signed and encrypted email for all changes to domain information.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Authorized DNS zone transfers</i>	IT Dept.	Are authorized DNS zone transfers required to prevent revealing names and IP addresses of our systems?	Viewing DNS is the first step to locating the weakest link on a LAN. Only allow DNS information to be visible to those who need to see it. Don't allow zone transfers to reveal what may be private areas of your LAN.

12: Changing Web Site Contents

Web site defacement is widespread and has evolved to being used as a method of distributing propaganda, rumors, and misinformation (as opposed to just plain vandalism).

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Staging servers</i>	IT Dept.	Are staging servers used to update site content?	Production servers should be read-only. This provides two security benefits: a) There is a live copy of production data on staging servers for fast recovery. b) Having production servers that are read-only makes them very difficult to crack or modify.
<input type="checkbox"/>	<i>User authentication</i>	IT Dept.	Is user authentication mandated for access to sensitive data?	Single sign-on simplifies tracking users and makes it easier for them to remember one username and password for all their access.

<input checked="" type="checkbox"/>	Area of Concern	Person(s) or Group(s)	Question(s) to Ask	Notes/Rationale
<input type="checkbox"/>	<i>Software patches and security policies</i>	IT Dept.	Do you maintain software patches and security policies on web servers?	Verify that web servers are secured by best practices and regularly review them to make sure that they match the security policy as it evolves (or as best practices evolve) to keep systems secure.
<input type="checkbox"/>	<i>Hardened DMZ</i>	IT Dept.	Are web servers kept in a hardened demilitarized zone with intrusion detection outside the firewall?	With this setup, if your web servers are compromised, that's as far as the intruder can get.
<input type="checkbox"/>	<i>Code reviews</i>	IT Dept.	Do you conduct regular code reviews to prevent common exploits such as buffer overflows from exposing the servers?	Buffer overflows or "stack smashing" has been around for a very long time. Good programming practices need to be passed on to junior programmers and practiced by all.
<input type="checkbox"/>	<i>Separate database and application servers from web servers</i>	IT Dept.	Are database or application servers and web servers kept separate unless on a machine that's designed for this purpose?	For example, AS400s or mainframes.

About the Authors

Frank Fiore is an e-business expert, columnist and consultant, and author of several books on e-business topics published by Pearson imprints:

- *The Complete Idiot's Guide to Starting an Online Business*
(Que, 2000, ISBN 0-7897-2193-7)
- *e-Marketing Strategies*
(Que, 2000, ISBN 0-7897-2475-8)
- *Successful Affiliate Marketing for Merchants*
(Que, 2001, ISBN 0-7897-2525-8)
- *TechTV's Starting an Online Business*
(Que, 2001, ISBN 0-7897-2564-9)

He is also the author of *Dr. Livingston's Online Shopping Safari Guidebook* (Maximum Press, 1996).

Frank has been involved with e-business from its inception on the Net; with his experience as both an e-business expert and a direct marketer of products, he knows e-business from both sides of the transaction. He is currently the Official Online Shopping Guide for About.com and has been interviewed for numerous TV and radio talk shows and print media on the subject of e-business and online shopping.

Jean François has more than 15 years of experience working in distributed computing environments. He has received the National Defense Medal for participation in Operation Desert Storm and held a Top Secret/SBI/SCI Clearance from 10/91 to 4/96. Jean has held positions as director of managed services for Opnix, Inc. and chief technology officer for EBIZ Enterprises, Inc., and is the president, CEO, and founder of MagusNet, Inc. MagusNet was founded on the idea of using Linux to provide businesses with consulting on security systems using proxy/filtering firewalls, as well as general UNIX system administration and applications using GNU tools such as Linux and other free operating systems like FreeBSD/Openbsd. Today MagusNet is primarily a security services company, providing Internet users with an anonymizing public proxy as a free Internet service. He has been a featured expert on radio, TV, and print, and in online forums.