

Information Security: What You Don't Know Can Hurt Your Business.

The September 11th tragedy has forced many of us to rethink how reliable our security really is. As concerned as we are about additional physical or biological terrorist attacks, we may have even more to fear from a cyber attack. For many of us information security is something we rely on our IT department or a consultant to manage. As business people, however, we also have a very real responsibility to exercise the same kind of due diligence with regard to information security as we exercise over our financial environment. If we do *anything less*, we place our businesses, our futures, and ourselves at risk.

There are more than enough reasons to take information security seriously, even without the risk of new cyber terrorism. The FBI's 2001 Computer Crime and Security Survey reported that 85 percent of respondents detected computer security breaches within the last 12 months. Sixty-four percent acknowledged financial losses due to computer breaches. The most serious financial losses occurred through theft of proprietary information and financial fraud. Seventy percent said that their Internet connection was a frequent point of attack (up from 59 percent in 2000). Forty percent detected system penetration from the outside (up from 25 percent in 2000).

Okay, the barbarians are at the gates. However, as business people what should we ask about the state of our business' information security? Here is an approach to start.

First, review your information security policy. If you don't have one, or it's been gathering dust somewhere, your organization is not taking information security seriously and you are already at risk. Your information security policy provides the framework and the rules that help protect your information assets and should identify the impact of a security breach.

Second, find out what equipment is being used to enforce your company's information security policy. Do you have a firewall, the foundation of information security infrastructure? Do you have more than one, to protect your corporate headquarters and branch locations? Does your organization use a multi-layered approach to security?

Third, does your organization use intrusion detection? Forewarned is forearmed. What kind of anti-virus protection do you use? Is it updated automatically? How pervasive is the protection? Does it run on all machines? Are computers defaulted to boot from their hard drives?

Finally, does your firewall have a history of vulnerabilities? Do independent evaluation bodies certify it? Can it be configured to prevent damage from computer worms such as Code Red or Nimda? Does it offer a single architecture for access control like stateful packet filtering? Does it offer multiple architectures, such as application proxy filtering?

Enough already? Now that you have some questions to ask, how can you get a handle on what is going on in information security? How do you develop a "context" to evaluate the answers that you hope you will receive? If your company uses vendor A's firewall product X, what does that mean in the context of what your business is and does?

Fortunately, you are not "contextually" alone. **You can** do your own due diligence when it comes to checking for a history of vulnerabilities. Since the core IT security weapon is the firewall, there exist some highly respected security organizations that document security vulnerabilities (or exploitations) that have been discovered in vendors' firewall products. Key organizations that track computer security vulnerabilities are:

- CERT – Computer Emergency Response Center – Carnegie Mellon – <http://www.cert.org>
- CIAC – Computer Incident Advisory Capability – US Department of Energy – <http://ciac.llnl.gov>

- BugTraq – A moderated mailing list and vulnerability database – SecurityFocus.com – <http://www.securityfocus.com/>
- X-Force – Computer Threats & Vulnerabilities Database – Internet Security Systems – <http://xforce.iss.net/>
- The Mitre Corp. - Common Vulnerabilities and Exposures (CVE) - <http://cve.mitre.org/>

What's good here? We are down to a handful of reporting organizations. Each of these entities distributes their findings in the form of Vulnerability Reports, Vendor Notes, Advisories and Incident Reports. The Mitre Corporation's CVE scheme is particularly interesting in that it provides common terminology for security issues and terms.

The following chart (Publicly Documented Vulnerabilities) demonstrates the importance of what can be garnered from these entities. This chart was compiled as of November 30, 2001 looking back to January 2000 by examining the vulnerability filings at the above organizations.

Publicly Documented Vulnerabilities Data Ending November 30, 2001

Vendor	Based	CERT	CIAC	BugTraq	X-Force	CVE	Total**
Borderware Technology	Canada	-	-	-	1	1	1
Cisco Systems	U.S.	-	1	9	3	3	9
Check Point Software	Israel	3	2	19	11	10	20
CyberGuard	U.S.	-	-	-	-	-	0
NAI Labs (McAfee)	U.S.	1	1	7	6	6	7
NetScreen Technologies	U.S.	-	-	2	2	2	2
Nokia *	Finland	1	-	1	1	1	2
Novell	U.S.	-	-	3	4	3	4
SonicWALL	U.S.	-	-	2	3	3	4
SpearHead Security	Israel	-	-	1	1	1	1
Symantec	U.S.	-	-	1	1	1	1
WatchGuard Technologies	U.S.	-	-	9	9	7	9

•All Check Point vulnerabilities also apply to the Nokia firewall since it is a Check Point appliance. The Nokia vulnerability is specific to the Nokia platform.

**TOTAL is the total number of vulnerabilities reported, not the sum across columns since a vulnerability may be reported by more than one source.

If you've gotten this far, then what you're really only left with is **to get on with it**. Don't feel bad about asking questions or poking your nose around. Remember: – **Your Information, Your assets, Your Future, Your ...** – a metal detector is not going to save you!!