

Security & SMEs

An Introduction by
Jan Gessin



Introduction to the problem

- SMEs convinced it will never happen to them.
- In many ways SMEs are more of a target than big business.
- Harsh realities of the online environment.
- Government and industry must work together to create a "Culture of Security".
- How can we specifically help SMEs?



It will never happen to me syndrome:

- I am too small and insignificant for anyone to find me on the Internet.
- I don't have anything anyone would be interested in.
- There is so much hype and media coverage, but I don't know anyone who has actually been attacked.
- I don't buy anything online so I don't have to worry.
- I am only online for a very short period of time – just long enough to do my email.
- But I have anti-virus software and a firewall.



WARNING: Don't be so sure:

- Corporations have strengthened their security in recent years in response to increased threats and to comply with new legislation. As a result, hackers are interested in an easier target - small business.
- Small businesses without adequate and up-to-date security measures become easy targets.
- The destructive Mydoom worm affected one out of three SMEs, but only one out of six large enterprises.
- It only takes 15 minutes for an unprotected computer connected to the Internet to be compromised.



WARNING: Don't be so sure:

- Unprotected systems becoming easier to find. Many hackers now have software tools that constantly search the Internet for unprotected networks and computers. Once discovered, unprotected computers can be accessed and controlled by a hacker, who can use them to launch attacks on other computers or networks.
- Most hackers do not care who their victim is. The first hole they find could be anyone's system and it won't matter to them whether you are a small company or a multi-national.



WARNING: Don't be so sure:

- All too often, security breaches come from within, either intentionally or unintentionally.
- Small business employees are generally at greater risk of unintentionally downloading spyware or malware because they haven't been educated to the risks.
- Without strict policies and an educational program, users could download a program or receive an email that is infected.
- If you can't prove that an attack did not originate from your system, a costly legal battle could ensue.



WARNING: Don't be so sure:

- The impact of a security attack can be financially significant. Lacking the resources available to larger businesses, SMEs often find it harder to recover from an attack.
- Regardless of how or why your business is attacked, recovery usually takes significant time and effort. Imagine if your computer systems were unavailable for a week, you lost all the data stored on all the computers in your company, or a competitor was able to access your customer database.
- How long would it take before you noticed? What would these breaches cost your company? What about your reputation as an honest trader? Can you afford to ignore this?



Did you know?

- Carnegie Mellon University estimates that 99% of all reported intrusions "result through exploitation of known vulnerabilities or configuration errors [for which] countermeasures were available."
- Gartner Group says smaller companies particularly lack the security expertise necessary to fend off computer attackers. Its research suggests that, without taking immediate steps to remedy the situation, 50 percent of these businesses will be the victim of a successful hack or a damaging virus outbreak in the next couple of years.



Did you know?

- According to the National Cyber Security Alliance (2004), 62% of computer users have not updated their antivirus software, and a staggering 91 percent in the study have spyware on their computers.
- In June 2004, the Gartner Group reported that online bank accounts had been looted of \$2.4 billion just in the previous 12 months.
- (Australia 2004) Type of computer crime that generated the highest cost was virus/worm/trojan infection, with a total cost of \$7.1 million.



Did you know?

- As society changes, so do the crimes that people commit. As the internet takes on an ever more important role, computer crime emerging as the crime of choice.
- Neither size of company nor type of business guarantees protection from an attack. If you use the Internet, you are vulnerable. However, by following recommended best practices, you will be substantially less vulnerable.



Do you lock the front door?

- We don't leave buildings unlocked at night and yet we leave systems unlocked and vulnerable to attacks.
- We make it easy for the bad guys to find us.
- We think they don't see us.
- Most of all, we just don't think it will ever happen to us!!



There are no excuses!

- Upgrade to latest version of operating system and application software (\$250/open source S/W free).
- Anti-virus software (\$30/free); automatic updates (free).
- Personal firewall (\$50/free); automatic updates (free).
- Software patches/automatic updates (free).
- Strong passwords (free).
- Anti-spyware software (free); automatic updates (free).
- Wary of e-mail attachments and downloads (free).
- Data backups (free).



We must help SMEs become ARMED in the war against security threats:

- A**ssets
- R**isks
- M**anagement plan
- E**ducational process
- D**evelop/adhere to policies

