



Part of the **TechWeb** Business Technology Network

**securitypipeline**  
FEATURING SECURE ENTERPRISE MAGAZINE

[White Papers](#)  
[Sponsor Resources](#)  
[WebCasts](#)

SEARCH

search [advanced search](#)

[Free Newsletter](#) [Glossary](#) [Contact Us](#) [About Us](#)

[NEWS](#) | [TRENDS](#) | [HOW-TO](#) | [PRODUCT FINDER](#) | [DESKTOP](#) | [NETWORK](#) | [INFRASTRUCTURE](#) | [POLICY & PRIVACY](#)

May 19, 2005

## Opinion: Small Businesses Need To Stop Ignoring Security

By Rob Enderle

[Security Pipeline](#)

By the time small businesses start worrying about security, it's too late. We ignore risk until threatened by an attack or natural disaster. If we're lucky, the threat passes us by, and we fall back into denial. If we're unlucky, disaster hits, and it puts us out of business.

Denial about security is self-defeating because the cost of loss is devastating. That's especially true of small businesses, where profit margins are often razor-thin.

I've had personal experience working in, and near, companies that learned those lessons the hard way. The lucky companies only lost information of financial value. In one instance, a security breach resulted in seven dead.

Moreover, as president and principal analyst of the Enderle Group, I'm a small businessman myself. In other words, I don't just advice small businesses on security — I live it.

The time to think about preparing for a disaster or other loss is before the loss has occurred. It is not a trivial process. We'll start out by reviewing the layers of security you need and close with disaster preparedness.

### The Layers of Security

**Physical Security:** This is the first layer and often — unfortunately — the last for many companies. Physical security means making sure your buildings are locked, your equipment is properly secured in the buildings, and that people getting into secured areas are authorized to be there. Many thefts of personal computers in small businesses resulted from people walking in off the street and walking out with a laptop computer containing critical data.

I worked at a company with an office in England in an upscale business neighborhood. People used to come and go, leaving their laptops on their desks and assuming, since the door required a badge to enter, that they were safe. One afternoon, a thief walked in and grabbed several laptops, either by catching the door before it closed or by being let in by someone else and not watched. We lost weeks of work.

In a second instance, at a company in Silicon Valley, a thief came in through open doors and helped himself to notebook computers while the cleaning crew was straightening up. Once again, we lost several weeks of work. This office had full perimeter and zone security which was worthless because the cleaning crew turned it off and failed to secure the room while they were working.

More chillingly, businesses need to make sure that unauthorized people don't bring weapons into the workplace.

I've been involved in that kind of security breach several times. A guard who reported to me was playing with his gun in the restroom (don't ask). He shot and killed a transformer by firing through four walls. He also ensured that future security guards were unarmed.

In another instance, two off-duty police officers were wrestling. One of them was armed where he shouldn't have been, and drunk. My staff ran for help and no one was hurt.

When I first moved to Silicon Valley to take a job in human resources, my departing predecessor was faced down by an irate husband whose wife was being abused by her manager. This guy felt that since he couldn't find the manager the HR director would do.

And, finally: I worked four blocks away from ESL Corp., when Richard Farley killed seven people at the company with a shotgun. Farley's was one of 23 workplace spree killings between 1986 and 2003 chronicled in a [brief report by the University of Massachusetts Lowell Department of Work Environment](#).

Weapons have no place in the workplace. But they do show up there and employees need to know what to do if someone behaves in a hostile and violent way. Customers, competitors, spouses, and ex-employees can often turn deadly and knowing what to do can save your life and the lives of others.

Companies need to make sure procedures are in place to physically protect employees. Companies need to establish rules that prevent large numbers of employees from traveling on the same airplane or working in the same physical location unnecessarily, so that one disaster can't incapacitate a catastrophic number of people.

**System Security:** We increasingly live in a virtual world. People don't have to enter into our sites to steal our data or damage our systems. Anyone who has access to a system can do significant damage to it unless extreme care is exercised. One laid-off CIO used his unrevoked authorization to [erase most of the critical company databases](#) because he didn't feel he had been treated with the proper respect.

Security managers need to make sure that employees have the correct authorization for systems they need, and that authorizations can be quickly changed based on changing employment. People should not have access to systems they don't need to have access to, and access should be eliminated once the need passes.

**Software Security:** Viruses and spyware protection must exist both on the individual systems and at the perimeter. Perimeter protections can include firewalls and e-mail products and services. Companies need to block attacks before intrusion and catch those that get through as quickly as possible. Remote workers who can be a huge source of problems, particularly if they are using an inadequately protected VPN (Virtual Private Network) pipe.

The elimination of spam needs to be part of any comprehensive security plan

**Security Maintenance:** Risks are always changing and evolving. Security is not a set-and-forget problem. On a regular basis you need to patch systems, assess vulnerabilities, and upgrade protection to stay ahead of those who are ever improving their methods to damage your business or access your data. Making sure you maintain a focus on securing your business.

**Consider A Security Service:** Most small businesses simply do not have the bandwidth to do security right. Just as you often use an outside company to install new hardware, or insure your business, an outside firm with the proper focus on your business segment may be the most important part of any plan. You want to focus on your business and not spend most of your time worried about threats that are hardly unique to you.

### **Disaster Preparedness**

With the number of global disasters we have had in the last year it is important to extend beyond simple security and look at preparing for a disaster. Billions are lost every year due to natural and man-made disasters. It has never been a more important time to consider this as part of any comprehensive security plan.

The Enderle Group studied small-business disaster preparedness last year. We found that only about 20 percent of small businesses consider disaster preparedness to be important, and only 2 percent of small businesses are adequately prepared for disaster. These statistics might actually be optimistic.

The potential loss for unprepared small businesses is high. [The 9/11 attacks cost an estimated \\$30 billion](#), with over a third of that damage likely to have hit small and medium businesses. [The Asian tsunami cost business insurers \\$4 billion](#), and the damage to business was much higher, because most small businesses in the areas were uninsured.

While replacing physical plant and equipment is important, the loss of electronic assets is what puts nearly [25 percent of small businesses hit by a disaster out of business](#) entirely. In other words, if a small business closes its doors due to a natural disaster, there's one chance in four that those doors will never re-open again.

But you can be prepared. One of the best [documents I have found to prepare a small business for a disaster](#) is provided free on the web by the Institute for Business and Home Safety and the Public Entity Risk Institute. It is called "Open for Business " and it provides a comprehensive guide to preparation. It includes the forms you need to prepare for most disasters, including employee information forms.

Another reference document I've found useful recently is the "[Terrorism Insurance and Risk Management](#)" guide, provided by Business Contingence Planning and Insurance. That document describes how poorly small businesses prepare for disaster, and the kinds of insurance these firms should consider.

Large enterprises can maintain adequate staffing and competence in this area, with the best having Chief Security Officers. Small businesses, on the other hand, are just as much at risk, and the loss is vastly more personal, because the managers and the owners are often the same people. Security management is something that can, and should, be largely outsourced to others. Spend time finding the right company before the next disaster shows up on your doorstep.

*Rob Enderle is an analyst specializing in emerging personal technologies. He heads the Enderle Group, and has been an IT analyst since 1994. He spends his free time building computers and playing with personal technology prototypes. He can be reached at [renderle@enderlegroup.com](mailto:renderle@enderlegroup.com). Contact the editor of Security Pipeline at [mwagner@cmp.com](mailto:mwagner@cmp.com).*

## SECURITY PIPELINE MARKETPLACE (sponsored links)

### [Improve the Return on Your Security Investments.](#)

LURHQ's Managed Security Services help enterprises maximize their security investments. Click here to learn why leading enterprises have chosen LURHQ as their Managed Security Services Partner.

### [Stop Spam at the Mail Server with CanIt-PRO](#)

Roaring Penguin's CanIt-PRO anti-spam solution offers customizable spam and virus control for enterprises, campuses and ISPs. Designed for the mail server, CanIt-PRO lets you stop spam on YOUR terms. Click for free 20-day evaluation software.

### [Information Security & Compliance Consulting](#)

Learn more about how expert VeriSign security consultants help enterprises protect critical data, meet compliance requirements, and maximize their return on security investments. FREE Optimizing Security Compliance white paper.

### [Security Within - Configuration based Security](#)

Configuration and policy based security systems are a pro-active way to defend against IT security attacks. Click here to request our white papers, "Security Within - Configuration based Security" and "Policy Management vs. Vulnerability Scanning".

### [Cost-Effectively Secure Sensitive Data](#)

Encrypting data in servers and databases can address security gaps and privacy legislation. Ingrian DataSecure Platforms offer granular encryption, seamless integration, and centralized security management. Combat data theft--with unprecedented ease and cost effectiveness. Download a white paper that outlines best practices for securing data.

### [Buy a Link Now](#)

[Neterion >> 10 Gigabit Ethernet iSCSI SANs: Fast, Reliable and Truly Global](#)

[How does your pay rate? Check the InformationWeek Salary Survey](#)

[Mobilized Solutions Guide: Find and compare solutions for your business](#)

[Top Requested White Paper Categories from TechWeb White paper Library](#)

[Top ten search terms from the TechWeb TechEncyclopedia](#)

Sponsored Links: [White Papers](#) [Sponsor Resources](#) [WebCasts](#)

[News](#) | [Trends](#) | [Product Finder](#) | [How-To](#) | [Desktop](#) | [Network](#) | [Infrastructure](#) | [Policy & Privacy](#)

[Original Articles](#) | [Free Newsletters](#) | [Security Glossary](#) | [Contact Us](#) | [About Us](#) | [Privacy](#)

[TechWeb.com](#) | [InformationWeek](#) | [Network Computing](#) | [Network Magazine](#) | [InternetWeek](#) | [Optimize Magazine](#) | [CommWeb](#) | [Wall Street & Technology](#) | [Bank Systems & Technology](#) | [Insurance & Technology](#) | [IT Pro Downloads](#) | [Intelligent Enterprise](#) | [Advanced IP Pipeline](#) | [Business Intelligence Pipeline](#) | [Compliance Pipeline](#) | [Database Pipeline](#) | [Desktop Pipeline](#) | [Developer Pipeline](#) | [Enterprise Applications Pipeline](#) | [IT Utility Pipeline](#) | [Linux Pipeline](#) | [Messaging Pipeline](#) | [Mobile Pipeline](#) | [Networking Pipeline](#) | [Outsourcing Pipeline](#) | [Personal Tech Pipeline](#) | [Security Pipeline](#) | [Server Pipeline](#) | [Small Business Pipeline](#) | [Storage Pipeline](#) | [Systems Management Pipeline](#) | [Web Services Pipeline](#) | [RFIDinsights](#) | [Oracle-PeopleSoft Insider](#)

