

Internal Terrorism

Internal terrorism is a growing and costly phenomenon in American business. Current or former employees with access to sensitive information or IT systems can wreak havoc on day-to-day operations and ultimately a company's survival.



Phil Canders is a Business Vitals CIO consultant who helps organizations with issues that threaten information security and business survival.

What do you mean by “internal terrorism”?

I am talking about employees who are disgruntled, careless, or simply bored and use their access to IT systems and information to cause problems for a company.

What “acts of terror” are they committing?

Some of it is subtle, like reading the confidential email of the CEO. That by itself is troubling, but when someone shares proprietary information—financial statements, a business plan, a formula for a new drug or personal financial information—with a competitor or uses it to extort money, the acts of terrorism can cause business failure.

Is this problem widespread?

Internal security breaches are a big threat. A 2002 study by PriceWaterhouseCoopers found that 40 percent of the companies polled had suffered employee-related losses of confidential information. The financial impact was staggering. Between July 2000 and June 2001, U.S. companies lost up to \$59 million in intellectual property and proprietary information.

This sounds like a problem for large companies.

Regardless of size, if someone is sharing confidential information, the survival of the organization is threatened. It is only natural to want to trust people. Yet unauthorized

access to information goes on every day. Organizations cannot afford to be complacent about protecting proprietary information.

What can be done?

Many companies host their own email because it is viewed as a low risk IT function. Yet email is often a company's largest point of risk. Do you want a disgruntled employee to have the power to sabotage your business using email? Selective outsourcing of email to a neutral partner like Business Vitals is a simple, highly effective fix.

How can Business Vitals help?

The best place to start is with a penetration test and vulnerability assessment. This will identify unauthorized access and insufficiencies in IT hardware or software. We then tailor a plan that might entail remote monitoring and management of IT functions, firewall management, and ongoing network health and security checks. Organizations must have data confidentiality, integrity and availability. Business Vitals supplies the strategy, structure and safeguards to make this happen.



Business
VITALS™

888.287.8483

www.businessvitals.com