e-Sher®
Underwriting Managers
Protecting the Business of e-Business

News for You

Why Every Business Today has e-Business Risk—and What You Should do About It

By Philip Pierson
Founder and Manager, e-Sher Underwriting Managers
Irvine, California

Every day it seems like the news media reports a new virus, denial-of-service attack, or hacking incident that wreaks havoc with commercial and government enterprises. If your response is "Thank goodness we're not an Internet company… it can't happen here," think again.

E-business risk is not the sole province of the "dot.coms." Virtually every business operating in today's marketplace is dependent on a computer and some type of electronic network. This universal dependence means that almost every business enterprise is at risk for some type of attack or accident that could disable the business operations, causing potentially large losses in revenue and business opportunities and damage to its reputation, even putting the business at risk for a lawsuit due to third party liabilities.

If you think that cyber crimes and system failures cannot affect you, ask yourself if any of the following parameter fit your business.

We use computers and our computers are networked.

All networks are susceptible to viruses, worms, internal and external sabotage, theft or destruction of databases and proprietary information.

We maintain proprietary data in our system.

Disgruntled employees and thieves have been known to steal proprietary data and hold it for ransom. These extortion attempts can cost millions of dollars. Companies pay because they weigh the cost of the ransom against the cost of re-creating the data, the "down" time of being out of operation, and the loss to their competitive position in the market if their competitors obtain the proprietary information or trade secrets.

If the database also contains confidential information—such as customer's financial or medical information—its theft and potential disclosure (even accidentally) could create substantial third party liabilities.

It's conceivable that we may have one or more unhappy employees, vendors or customers, during our history.

Sabotage is more likely to come from inside than outside the company. Disgruntled employees are the primary culprits; in times of economic uncertainty and layoffs, getting back at the company by disabling their computer network can seem like the perfect revenge. Vendors and customers who are angry with the company can also be tempted to retaliate electronically.

We use networks for management information systems.

If the network is disabled, the business grinds to a halt. Employees cannot work, orders cannot be taken, bills aren't paid.

Our inventory is on an electronic POS system, without hard copy back-up. Also, our supply chain is electronic.

A network failure could interfere with your ability to find and ship products, and to obtain the materials you need to continue to manufacture and sell goods and services. Today, the "person" who applies the rivets to the side of a vehicle may well be a robot. If the electronic support system goes down, so will the computerized manufacturing processes, bringing the assembly line to a stand still.

We have a Web site.

A Web site is a potential point of entry to a hacker. It can also create its own set of liabilities for electronic publishing. Plagiarism and libel related to Web site content open the company to lawsuits and potential damages.

If e-commerce is conducted on the Web site, a "denial of service" attack can completely disrupt the order taking and fulfillment process.

We are electronically connected to our trading partners or customers.

The inability to communicate and exchange information could not only damage the company's ability to conduct transactions, but also create liabilities with trading partners who can be infected with viruses and worms, or who lose business and productivity because they do not get the information they need from you to fulfill their obligations.

We use e-mail.

E-mail communications, internal and external, are the communication medium of choice for most businesses today. If this communication is interrupted, business suffers. E-mail is also a primary way in which viruses infect systems and companies, and are passed on to clients and other trading partners. Also, employees' inappropriate use of e-mail can boomerang on the company, resulting in such liabilities as sexual harassment charges for off-color stories that are circulated, or defamatory comments that are meant to be private but which are deliberately or accidentally disclosed.

We use the most popular operating systems and software programs.

Hackers delight in creating viruses that can disable the most widely used systems. What greater triumph than to infect the world's most popular platforms and applications, damaging commercial entities all over the world?

We have employees working off-site or in remote locations, and/or people outside the company—such as vendors and consultants—have access to one or more of our systems.

You may have excellent security within your company's main operations, but what about when employees access the system from home, from a hotel when they are on the road, or when they are at a remote worksite? How can you impose security standards in these multiple locations? If one or more of your customers, vendors, or trading partners has access to your systems, you have even more vulnerabilities.

The true picture of e-business risk can be quite sobering. However, once you realize your exposure, there are remedies.

Strengthen internal security.

The first step is to identify where your risk exists, and look for ways to strengthen security. While the IT department may claim "everything is secure," it is usually best to have this analysis done by a computer security specialist. Your IT staff has many other priorities besides security, and a specialist has the means to be current with all the latest potential types of intrusions or accidents.

Once risks are identified, tools to strengthen security can be put in place. These tools can include software packages that identify intrusions immediately and pinpoint their source so that damage can be documented and the problem fixed as quickly as possible, policies to cover how security is imposed and what your employees do if there is a breach, and stronger virus detection programs.

Calculate liability.

This analysis should also calculate the potential liabilities for a breach or loss in the areas in which the company is vulnerable, from both a first party and third party perspective.

"First party" losses are those that impact the company itself: downtime due to an inability to use the system, lost business because orders can't be taken or filled, the cost of public relations assistance needed to manage a crisis.

"Third party" losses are those that impact other parties—your clients who cannot get materials or goods delivered, trading partners and clients who are infected by a virus transmitted from your company, individuals whose private financial or medical data is inadvertently or intentionally revealed.

Arrange risk transfer.

Once the company has done what it can to reduce risk from internal and external sources, it can look into “risk transfer” in the form of an insurance policy that will cover losses and liabilities due to e-business accidents.

The policy should be selected on the basis of the following criteria: coverage of first and third party liability, written especially for cyber-risk, and offered by a carrier with a specialty in this area and with underwriters and claims experts experienced in this new risk management area and a strong financial rating.

The carrier’s commitment to the e-business market can also be assessed by the package of risk management services that may augment the policy—everything from discounts on security software to information and assistance to managing a crisis should one occur.

Although initially the potential for e-business risk may seem overwhelming, a careful analysis and prompt action can reduce these risks and put appropriate coverage in place for reimbursement of losses should an incident occur.

It’s important to remember that virtually no business is immune from these risks in today’s economy. Once that reality is faced, the right actions can be taken to protect the company, its assets and its reputation.

Philip Pierson is founder and manager of e-Sher Underwriting Managers, a company that works in conjunction with leading edge security assurance developers, counselors and intelligence experts to provide policyholders with high quality risk and security assessments and products, to avoid or at least mitigate damage to computer networks and information assets before they occur. For more information, visit **www.e-sher.net** or contact Mr. Pierson at **philip_pierson@swett.com,** 949-477-6646.