Security Issues During a Business Downturn

The enterprises that protect their digital assets will be better positioned to weather whatever economic storms may come their way.

By Ken Cavanagh, Vice President of Professional Services, Vigilinx Inc.

- Fortune 500 giant lays off 10,000 in latest downturn
- Plummeting stock prices lead firms to cut back on hiring, perks
- US economic recovery much slower than predicted
- E-business failures drop NASDAQ to lowest levels in past 18 months
- 50,000 job cuts at Internet companies in the past year

In recent months, headlines like these have blared from televisions, newsstands, and Web sites. As many companies are reassessing their budgets in the face of the continuing slow economy, each function and department is called upon to justify its contribution to the bottom line—and information security is no exception. During such times, it is essential that enterprise decision-makers understand that information security is a perpetual concern that does not vary with the business cycle.

In good times, when an organization is profitable and growing, it is easier for senior management to recognize, appreciate, and fund information security efforts. Risks such as theft of trade secrets, protection of brand, corporate espionage, and availability of service are tangible, and efforts to mitigate those risks are usually well received. During difficult business cycles—such as the continuing economic slowdown—many organizations re-trench. The total energy of the organization is directed toward the core competencies believed to contribute most to profitability. If the task or resource does not visibly and directly affect the organization's bottom line, it faces downscaling or elimination. Unfortunately, information security efforts are sometimes put into this category—a decision that can have serious repercussions.

Whether a company is a once high-flying dot-com that has returned to earth, or a traditional business experiencing a downturn, the basic rules of information security to protect their current and future opportunities still apply. Indeed, economic downturns heighten such concerns. This article outlines the steps companies should take during this time.

Evaluate your information assets

Organizations should begin by implementing a thorough risk assessment process to identify which information assets are the most valuable, contributing most directly to the organization's bottom line. These may range from the intellectual property of a content provider to the customer data of a healthcare company. Done correctly, this evaluation shows where security assets must be directed—and illustrates the connection between security and the company's revenue stream.

Allocate resources

During business downturns, employees who are the revenue generators for the company are perceived as most valuable. Layoffs and cutbacks are usually directed at the positions seen as staff or cost centers. Unfortunately, this sometimes includes the information security staff. The

fact is, however, that a downturn in no way mitigates the value of the assets you are trying to protect. Without an adequately equipped and well-trained security team, those assets are in danger of loss, destruction, or unauthorized modification. Companies should maintain their in-house security team or augment with outsourced staffing.

Guard against process breakdown

Information security professionals have long stressed that security is not a product, but a process. This is especially true during a downturn. While employees and management are focusing on operations and maximizing profitability, internal checks and balances are frequently seen as luxuries and circumvented. This dramatically increases the opportunity for fraud, exposure, and theft of confidential information. During such times, managers tell themselves that if their firewalls, routers, and other hardware/software devices are operational, they are secure. This thinking is flawed. As security professionals know, process breakdown is far more threatening.

Organizations should ensure that all internal processes, including information security, are kept up to date, continually communicated to all employees, and reviewed as business needs and technology change.

Watch for internal threats

Most studies indicate that insiders are responsible for 60 to 80 percent of all information security incidents. Employees, business partners, suppliers, or anyone else with specific, inside knowledge of an organization is a greater threat than an unknown outsider. During a business downturn, this threat is greatly amplified. While a company struggles through its business difficulties, employees tend to become discouraged, apathetic, angry, or opportunistic. This can spell disaster for an organization's information assets in the following ways:

- Discouraged or apathetic employees are far less likely to care about maintaining quality security procedures. Lack of compliance with accepted security procedures, especially for high-risk systems and data, may unnecessarily expose the organization to outside threats. Ignoring system alerts or virus warnings due to indifference ("Why should we care, we're only going to get laid off anyway") can leave these valuable assets unprotected.
- Angry or disgruntled employees pose an even greater threat. These employees can covertly attempt to destroy or sabotage existing systems and information. The potential damage from these types of attacks is astronomical. Employees with sufficiently high-level security access can damage or destroy the most critical data in the organization. For an e-business, these employees are especially dangerous. Because an e-business' livelihood is based on system availability, any attack that brings the system down for an appreciable amount of time is devastating. While, for example, a law firm's Web site could suffer a loss of availability without crippling the firm, an online auction site or financial trading firm could suffer overwhelming losses if its site was down for even a few hours.
- Opportunistic employees also are a subtle but potentially devastating threat. During normal business times, most organizations encourage their employees to seek out any opportunity to help make the company more profitable. Employees who demonstrate such an orientation are frequently recognized and rewarded by the organization. Conversely, these same employees pose an incredible threat during bad times, should they use their talents for ill rather than good. These employees are motivated not by anger or vengeance, but by self-aggrandizement. A disgruntled employee, for example, will typically launch a destructive action such as a Denial of Service attack. While damaging, it can sometimes be detected early (providing the security resources are still intact) and mitigated. Opportunistic employees, on the other hand, are more likely to launch subtle

attacks such as theft of trade secrets, customer information, patent methods, and other confidential data. The motive here is not to destroy outright, but to make the information available to others for personal gain or profit. This type of attack can be particularly damaging to the future viability of the organization. If the company is contemplating a merger or acquisition as part of its strategy for surviving a downturn, a security breach can be particularly disruptive—with a direct effect on the value of the company.

What special risks do e-businesses face?

The previous issues affect all companies caught in the squeeze of a downturn. E-business companies, however, have additional concerns due to the nature of their business and the relative youth of their enterprise.

Procedural breakdowns

Because most e-businesses are relatively young, they often do not have firmly established security policies and procedures. Security policies, if they exist at all, are usually created "on the fly" and are not fully evaluated against industry best practices or related to the organization's risk assessment (if, in fact, a risk assessment even exists). As a result, inexperienced staff may be faced with security-related issues for which there are no preexisting guidelines.

Tech-savvy staff

E-businesses are disproportionately staffed with young, technically competent personnel. These employees have grown up with computers and have learned through long periods of trial-and-error experimentation how computers work—and how to manipulate or bypass system security controls. If these tech-savvy employees become disgruntled or opportunistic, they have the intelligence to fully exploit the systems and avoid detection.

Inexperienced management

Downturns are a time when the perspective of experienced managers can be most welcome. Unfortunately, not many E-businesses have line executives with experience in riding out business cycles and positioning the company for the next upturn. As a result, the younger employees lack the mentors that can shepherd them through the current economy, leaving them confused, tentative, and less likely to adhere to strict controls.

Insufficient security

The primary—if not sole—focus of many e-businesses has been to build perceived value in advance of an initial public offering, a strategy that is clearly no longer viable. While this made for many paper millionaires, it did not leave much time for, or place much premium on, implementing a structured security effort. As a result, there is often not a fully staffed, funded, and trained internal information security department in place, leaving the system architecture completely exposed and vulnerable to attack.

Lack of established standards/regulations

Traditional industries (such as banking, insurance, health care, and manufacturing) have long-established industry guidelines, which are often supplemented by governmental regulation at the federal, state, and local levels. Although such regulation may seem onerous at times, it also has the effect of institutionalizing accepted practices, including those relating to information security. Adherence to these standards is also a long-standing part of their corporate culture and is indoctrinated into all employees with detailed policies, in-house training, and communications.

E-business companies typically don't have these security "safety nets" in place. In this more relaxed environment, the standards for governance are still being written. The threat of legal action is also somewhat mitigated because there isn't currently much in the way of established legal precedent regarding liability. An environment in which there is uncertainty over standards is one in which the possibility for security exposures is increased.

What can companies do?

Clearly, all enterprises—both traditional and e-business—need to place a premium on establishing or maintaining sound information security practices, irrespective of business conditions. To keep the company sound while trying to weather the storm, businesses should take the following steps to protect their information assets.

Maintain security staffing

Resist the temptation to reduce the information security department's headcount. The value of the information they protect is worth far more than their salaries. If the information security function is already lean, companies must look to traditional methods for offsetting the cost of full-time employees (FTEs) such as consultants, outsourcing and managed services options.

Improve security tools

Organizations must ensure that all security devices, firewalls, intrusion detection systems, antivirus packages, remote access devices, and so on are kept completely up-to-date with the latest operating system releases, applications patches, and security enhancements. Don't fall into the trap of thinking that mere ownership of these devices equals good security. A poorly configured security device is an invitation for disaster. If there are no security tools currently in place, it is imperative that organizations immediately install them. Even if fiscal resources are constrained, company management must find a way to fund at least a base-level layer of security devices. Without such devices, the system environment is wide open.

Remain vigilant

Amid all the scrambling to bolster operations, normal monitoring and review procedures may be overlooked—a potentially fatal mistake. Organizations must assign staff to regularly review and report on system activity. A system log that isn't checked regularly can hardly be effective; indeed, such a situation can give an enterprise a false sense of security until it is too late. Again, companies that find this task to be too much of a drain on resources should investigate a managed security service to augment in-house staff.

Communicate early and often

Too frequently, companies experiencing troubled economic times tend to become tight-lipped internally. Although this is understandable—no one likes to be the bearer of bad news—it often leads to employee fear, uncertainty, and doubt. In this highly charged atmosphere, employees may be more apt to circumvent or defy security procedures. Companies must be certain to communicate all relevant news, both good and bad, to employees as soon as possible. Additionally, companies should continue, if not increase, their security awareness efforts. If employees are constantly reminded of their security responsibilities, it may lessen the temptation to perpetrate "crimes of opportunity" within the organization.

What's next?

As history has shown, business cycles come and go. The bull market of the 90's may have led many into a sense of—as it was famously put—irrational exuberance, fostering the belief that the good times would last forever and success was guaranteed. This, of course, has been proven not true. The fact remains, however, that good business practices transcend good and bad times. One of those practices is sound information security processes. The economic downturn has done nothing to minimize the status of information as a critical corporate asset. Protection of those assets should be a prime directive for any organization—no less important that showing a profit. Indeed, the two are often inextricably linked. The enterprises that protect their digital assets will be all the better positioned to weather whatever economic storms may come their way.