ONLINE SECURITY[1]

BRETT J. TROUT

Security in the digital age involves a delicate balancing act between the antagonistic principles of security and accessibility. While digital information encrypted, stored on a proprietary media and secured within an armed vault would be relatively secure from theft or modification, the information would be very inaccessible to its owners. Such overwhelming security would make the information nearly useless in the day-to-day operations of the typical company. Conversely, publishing the information on a publicly accessible website would make the information employee friendly, but would expose the information to misuse or modification by third parties.

While technology can help companies protect sensitive information and maximize accessibility to employees, selecting the appropriate technology entails balancing several factors. Companies should not seek the "best" security for their information, only the most "reasonable under the circumstances." What constitutes "reasonable" security measures for a particular piece of protectable information?

Probably the most important factor is "How accessible does the information need to be?". Obviously in an Italian restaurant where proprietary pizza dough is being prepared hourly, high level digital encryption of the recipe would be inappropriate from an access standpoint. An additional factor to consider is cost. While high bandwidth dedicated fiber optic intranets are relatively secure from outside intrusion, the cost of such systems is prohibitively expensive for all but the most valuable digital information. Yet another factor to consider is the user friendliness of the technology. Even a very accessible, low-cost system would be inappropriate if the technology were difficult to access or operate.

The foregoing considerations will be different for every company and every piece of information. Unfortunately, this means there is simply no "one size fits all" approach to information security. Whether security for a particular company means maintaining a single hard copy behind a locked door or encrypting the information onto proprietary media depends on what is reasonable under the circumstances, considering all of the issues at play.

Given that many of today's companies live or die by the information contained within their digital systems, how does a company determine the appropriate level of security required for each type of information? With no truly turnkey system for data security, each company must take a step-by step approach to security. First, the company must investigate the various types of information it needs secured. Second, the company must determine the various threats to that information. Third the company must address the exposure associated with inadvertent disclosure or misappropriation. Fourth, the company must analyze the particular laws governing use, misuse, transfer and storage of the information. Fifth, the company must examine the liability associated with failure to

---

 Excerpted from upcoming 2003 release of *Internet Laws Affecting Iowa Companies, Second Edition*

conform to these laws. Sixth, and finally, the company must develop comprehensive solutions which protect the information, while still making the information available for its intended use. Taking these steps, either on its own or with the assistance of a consultant, will allow a company to develop "reasonable" security options which do not unnecessarily drain corporate resources or interfere with company operations.

The Information

The first step is to determine what information needs to be protected. Much of the information associated with sales brochures and other advertising materials may be protected under various intellectual property laws, and, therefore, may not need to be otherwise secured against unauthorized access. On the other end of the spectrum, a company must categorize trade secrets and/or sensitive customer information. Categorizations may relate to required access, third party value and replacement cost. Categorization allows a company to determine the threat to a particular category of information and, therefore, determine the most appropriate security for that information.

Hacking is the greatest danger to information with little value outside the company, but with very high replacement costs. Such information may include complex internal actuarial information. Appropriate security measures for this type of information may include firewalls, redundant servers and offsite backup resources. Conversely, misappropriation is the greatest danger to trade secrets. Such information might include customer lists or valuable recipes. Appropriate security measures for this type of information may include storage on a stand-alone computer, accessible only by authorized personnel.

Classifying all of the proprietary information utilized by the company and sorting the information into various categories of protection is very important. These activities allow a company to more efficiently guard its sensitive information. These activities also allow a company to avoid the associated expense and inaccessibility concerns associated with protecting information using inappropriate security protocols.

The Threats

Both internal and external forces threaten company information. External threats may include hackers, viruses, and denial of service attacks. External threats are not always sophisticated. Such threats may be as low-tech as phoning an information technology employee within the company and feigning a request from an employee to change a forgotten username and password. Although these types of threats receive a disproportionate amount of media attention, they can be minimized through the use of relatively low cost security hardware and software. A company can also reduce such risks through the judicious implementation of internal security protocols heeded by everyone within the company. While a company must indeed thwart external threats, the most serious threats to a company's information in today's environment come from within.

Internal threats come in two types, unintentional and intentional. Unintentional internal threats may include inadvertent emailing of sensitive information, allowing unsecured access to a website, deleting sensitive data, failing to backup sensitive data, installing

viruses or giving out passwords over the telephone. These inadvertent disclosures may be either random or prompted by an external source seeking to capitalize on such types of security breaches. While unintentional internal threats are a concern, proper security protocols and employee training will significantly reduce their impact.

By far the biggest threat to company data is the intentional criminal act of an employee. Such threats are extremely costly and they may go undiscovered for years. Staying one step ahead, criminal employees often constantly modify their techniques in conjunction with changes to the company security policy. In most instances, the employee is not working alone, but in conjunction with a third party. Third parties are typically necessary to allow exploitation of the information for profit in a way the employee would not otherwise be able to utilize.

Various types of intentional employee activities include customer identify theft, misappropriation of trade secrets, inclusion of surreptitious code, or various other types of corporate espionage. While the poorly executed, large scale employee thefts are the ones that make the news, most such activities are executed on a small scale, with military precision. Accordingly, such activities are often very difficult to thwart. Probably the best remedy for such threats is separate internal investigation authorities and utilization of independent third party security audits.

The Exposure

In 2002, ninety percent of companies reported information technology security breaches within the previous twelve months. Eighty percent of those affected acknowledged financial losses resulting from the breach. Price Waterhouse Cooper reported that hacking costs U.S. companies $1.5 Trillion in the year 2000. Even if these figures are off by an order of magnitude, the problem remains very costly.

In determining the exposure associated with security breaches, companies must take into account: 1) the cost of forensics used to determine the existence and scope of breaches; 2) the damages associated with information moving into the public domain; 3) the damages associated with recreating the information or identifying and correcting alterations; 4) the public relations impact of the breach and; 5) the substantial costs associated with litigation, not only in pursuing the party breaching the security, but in defending claims from third parties relating to the failure to prevent the security breach in the first instance.

The Laws

Under U.S. law, companies are not afforded privacy protection. Accordingly, companies must look to patent, trademark, copyright and trade secret law to protect proprietary material. Under U.S. law, individuals are afforded privacy protections under the Constitution, federal and state legislation, and the common law. Given the number and breadth of privacy protections available to individuals on the Internet, it is important to familiarize oneself with these regulatory frameworks before collecting or disseminating third party information.

Congress enacted the Electronic Communications Privacy Act (ECPA) in 1986 to amend the Omnibus Crime Control Act. The ECPA generally prohibits interception of email and access to stored email, but allows employers to monitor employees. The ECPA applies equally to accessing databases and capturing keystrokes. Title II of the ECPA prohibits intentional acts of an electronic communication service. This relates to any stored electronic communication, whether by email, facsimile, or otherwise. Exceptions to Title II of ECPA include interceptions by the provider of the particular service, such as the employer or an ISP, or access by anyone with authorization, whether the authorization is express, as in the case of a signed acknowledgment, or implied, such as continued use of corporate email after being informed of the company's periodic interception.

Title III of the ECPA prohibits intentional interception of any electronic communication, making it a crime to capture electronic mail while in route. Exceptions to Title III include consent to interception by an employee, whether implied, express, contained within an employment agreement, employee handbook, or email policy. This exception applies only to employer interception of employee email in the ordinary course of business. Based on the foregoing, it is important for employers to provide employees with a specific written email policy, stating the employer can and will review electronic communications, whether in route or stored. Preferably, employers would obtain employees' consent and express written acknowledgement of such interceptions. Additionally, employers must take steps to monitor employees' electronic communications only in the ordinary course of business, and stop reading electronic communication once it is determined the electronic communication is personal.

Congress enacted the CFAA in 1984 to stem computer crime, then amended it in 1996 as the National Information Infrastructure Protection Act. The amended Act criminalizes threats to computer networks, release of viruses or worms, hacking, hijacking, and other destructive e-commerce activity. Under the CFAA it is illegal to knowingly access a computer without authorization, if the purpose is fraudulent, designed to access confidential information, designed to access financial information, or designed to cause damage to a computer system. To bring a case under the Computer Fraud and Abuse Act, the plaintiff must show it has suffered some identifiable damage.

The Liability

Curiously, the basis for many information security problems rests with company executives, rather than information technology employees. Officers and directors often incorrectly assume that the risk of an information technology breach is relatively slight, or that someone else will be held accountable. This is not the case. Along with the perpetrator, the Chief Security Officer, Chief Information Officer, Chief Executive Officer, Board of Directors and the company itself may all be held liable for breaches of information security. While the perpetrator is obviously the most culpable, the perpetrator is often the most difficult to identify and the least lucrative defendant. Accordingly, third parties are looking more and more toward directors, officers and corporations for remuneration in the event of an information technology security breach.

In 2003, Iowa laws will take effect which change the requisite level of care required of officers and directors in making corporate decisions.[2] These new laws state that an officer must act with the care that a person in a like position would reasonably exercise under similar circumstances. While an officer is entitled to rely on employees' performance information and opinions, the officer must reasonably believe that the person relied upon is reliable and competent in the matters presented.

Similarly, these new laws state that a director must make appropriate inquiry when facts of significant concern materialize that would alert a reasonably attentive director to the need for attention or inquiry. In both cases, the law mandates that officers and directors heed security warnings from information technology personnel relating to the adequacy of security protocols and instrumentalities. Failure to heed such warnings may lead to personal liability for officers and directors. Compensatory and punitive damages against the company, injunctions associated with dissemination or use of information technology, loss of reputation and a drop in a company's market capitalization are also possible repercussions.

The Solution

If a company does only one thing to protect its information technology, it must open lines of communication between officers, directors, information technology personnel, marketing, legal and the human resources department. By keeping abreast of the company's information technology activities and security concerns, a company can address security issues before they manifest into a potentially much larger problems. The next step is to designate a Chief Security Officer. The Chief Security Officer should be in charge of not only information technology security, but also physical security as well. As both the physical security and information technology security are dependent on one another, having a single individual in charge of both prevents exposure associated with miscommunication between separate individuals.

The next step a company should take is to identify and prioritize the risks as outlined above. Once the risks have been identified, the company must adopt written security policies. These policies must not only be intelligently designed, but they must be clearly defined and implemented with the appropriate individuals. Finally, once the security system is in place, it is important to conduct periodic security audits. The greatest internal security threats are often associated with the person or persons in charge of internal security for a particular project. It is therefore important that security audits be conducted by impartial third parties, trained to identify internal misconduct.

Implementing any security plan, requires training employees with regard to the plan and responding to any questions or suggestions they may have. Employees are a corporation’s first line of defense in thwarting a security breach. Employees, however, cannot be of much help if they do not understand their responsibilities or the security protocols involved. Corporations must also ensure legal counsel stays abreast of constantly changing laws affecting information technology security.

---

[2] Iowa Code Chapters 490.831 and 490.842

In addition, Corporations must designate individuals or committee to keep current on security options and mandates associated with a particular trade, such as financial or health services. Companies must monitor and document all security activities, reprimanding and docketing any identified violations. It is also important to adopt an employee exit plan, to prevent employees from corrupting, destroying or misappropriating important data prior to their departure. Companies must strive to share non-confidential security concerns with others in the industry, updating policies and technologies in line with, or just ahead of, competitors. Facilitating this transfer of information are organizations such as Infraguard[3] where companies share security information without the fear of unwanted publicity or trade secret disclosure.

In addition to implementing preventative procedures, it is imperative companies implement detection procedures and a response plan designating how breaches of security are handled, documented and reported. Although many companies are hesitant to report security breaches, such reporting enlists the aid of government forensic resources to identify the breach and bring the perpetrator to justice. Security breaches should be forwarded to either the United States Secret Service or Federal Bureau of Investigation. In Iowa, the Secret Service may be contacted at 515-284-4565. Their offices are located at 210 Walnut Street, Suite 635, Des Moines, Iowa 50309. Although a company may report an information technology breach in almost any manner, a standardized cyber threat report form[4] streamlines the reporting process and ensures critical reporting data in not overlooked.

In the Future

Given the magnitude of the losses associated with cyber security breaches, laws will continue to pressure companies to more securely protect their sensitive information and will continue to increase penalties associated with such misappropriation of such information. Indeed, Congress is currently debating raising federal penalties for cyber crimes to twenty years or more. Congressional committees are also discussing laws which would allow companies to turn over secure information without a warrant, if the companies have a good faith belief that the information is related to a cyber attack. Such laws could also authorize authorities to trace Internet traffic and electronic mail during a cyber attack without the need for a warrant. Companies must do their part as well, however, by funneling more resources toward detection, prevention and stiffer physical security. Although not calculable under traditional return on investment parameters, properly directed investment into information technology security is often one of the soundest investments a company can make

As companies increase security and vigilance, those companies falling behind will become the principle targets for cyber thieves, no longer able to penetrate their competitor's increasing security. Additionally, for companies that fail to update technologies and procedures associated with thwarting cyber threats, their directors and officers may find themselves in the midst of personal lawsuits for their failure to fulfill their fiduciary duties. As cyber attacks continue, and lawyers become more savvy as to

[3] http://www.infragard.net/
[4] http://www.steptoe.com/webdoc.nsf/Files/191d/$file/191d.pdf

their cause and prevention, liability will continue to shift toward the deep pockets of corporations, their officers and directors.

Conclusion

Purchasing new technologies and implementing procedures is critical to any information security plan. The most important aspect of any security plan, however, is the sharing of non-confidential information relating to security plans, protocols and perceived vulnerabilities. Companies must use this information to constantly update infrastructure and decrease security threats. Organizations such as Infraguard and other non-profit entities, committed to reducing cyber threats and guarding the nation's information technology pathways can be an invaluable asset to companies seeking to implement comprehensive security plans.

While a company could implement a comprehensive security plan without the assistance of outside resources, exchanging information with contemporaries will make almost any plan more efficient, less costly, more reactive and ultimately more effective. For any company dealing with sensitive information, a comprehensive cyber security plan is a must. Failure to implement such a plan will not only place the company's entire future at risk, but will may even subject officers and directors of the company to devastating personal liability, in the event of an otherwise preventable attack.