Internet Risk Management
An Examination of Internet Risks

William Gallagher Associates
Phone: 888.261.8884
www.WGAins.com

William Gallagher Associates, a leading provider of insurance brokerage, risk management and employee benefits services to firms with complex risks, within industries that include high technology, life sciences, financial risks, healthcare services, energy, and environmental services. WGA has offices in Boston, MA; Princeton, NJ; Columbia, MD; Atlanta, GA; and Paris, France.

I. Introduction

Over the past decade, the Internet has become critical to businesses, both as a tool for communicating with other businesses and as a means for reaching consumers. Unfortunately, the risks for businesses that rely on the Internet have significantly increased as well. Businesses that traditionally have relied on physical security such as locks and safes to protect their vital business information now face a more insidious virtual threat from miscreants who use the Internet to carry out their attacks without ever setting foot in an establishment. More often than not, these crimes are conducted from outside the United States. It seems that not a day goes by without a news report on yet another business that has been affected by an Internet attack of some degree. Indeed, the frequency of these reports does not indicate the true scope of the problem: according to recent studies, an estimated 80% of network hacks in the financial sector go unreported, and 46% of the fastest growing small companies in the United States have suffered breaches in information security, with 83% of those companies suffering monetary losses and 25% suffering network downtime.[1] One recent report estimated the damages from such attacks at two thirds of a billion dollars in 2003.[2] Even more ominous, in a recent survey by the Pew Internet & American Life Project, 66% of the technology experts surveyed predicted that there will be at least one devastating attack on the underlying infrastructure of the Internet as a whole or on the country s power grid within the next decade.[3]

These attacks can affect even the most security-conscious businesses — in early January 2005, it was reported that George Mason University, which the National Security Agency has designated as Center of Academic Excellence in Information Assurance Education, had been victimized by hackers who may have stolen the names, photographs and Social Security Numbers of more than 32,000 students and staff. [4]

Internet threats can take the form of specific attacks such as hacking directly into a particular business s computer network with the intent to steal proprietary business information, non-specific attacks such as viruses and/or attacks on the Internet s infrastructure, or attacks that may have both direct and indirect effects, such as distributed denial of service (DDoS) attacks that overwhelm Internet servers with requests for information, thereby taking down either individual websites or many websites that share a computer server. Businesses can take some steps to protect themselves, such as ensuring that their antivirus software is up-to-date and installing firewalls. But such steps cannot protect against all attacks and the failure of such steps can open businesses up to direct losses and to liability for losses suffered by others.

In addition to the risks created by Internet attacks, the increasing reliance on the Internet exposes many businesses to potential liability for trademark and copyright infringement, defamation, and privacy claims.

Furthermore, traditional insurance forms such as Property, Commercial General Liability (CGL) and Technology Errors & Omissions insurance policies do not cover many of the risks associated with cyberspace. The following is a brief summary of how some of these insurance policies respond to cyber risks:

- The Property policy covers only tangible property and not data. Additionally, Property policies tend to focus on perils that are typically involved in losses to tangible property such as fire, explosion and wind. Business Interruption insurance is sold as part of a Property policy that tracks both the definition of property, as well as the perils. While the form may cover loss of income when a business sustains a fire loss, it will not cover e-revenue loss due to a DDoS attack.

- Standard Crime forms only safeguard against losses resulting from fraud or theft of money, securities or other tangible property. Computer fraud or information theft, which results in damage or deleted information assets, are deemed intangible and, therefore, not covered.

- The CGL policy covers claims for physical injury to tangible property, including loss of use of such property. It also covers claims for loss of use of tangible property that has not been physically damaged. The CGL policy does not cover property damage to or loss of use of intangible property, nor does it cover loss of use of tangible property that has not been physically injured, when the loss of use arises out of a defect, deficiency, inadequacy or dangerous condition in the insured s product.

- Additionally, while the standard CGL policy includes coverage for Personal and Advertising Injury, coverage does not apply if the insured is in the business of advertising, broadcasting, publishing, telecasting, telemarketing, etc. Any information on a website, including banner ads, can create legal third-party exposure to alleged libel; slander or defamation; copyright, title or trademark infringement; or invasion of privacy. Whether it is static or dynamically generated content, visible or hidden text, there is a risk that someone accessing the information may find it offensive or intrusive.

- Most standard Technology Errors & Omissions (E&O) forms provide coverage for property damage to or loss of use of intangible property and loss of use of tangible property that has not been physically injured when the loss of use arises out of a defect, deficiency, inadequacy or dangerous condition in the insured s product. However, E&O forms typically exclude losses arising from breach of security and/or failure to prevent unauthorized access -- critical exposures to an Internet/Media technology company. A breach of network security can result in claims from customers whose client information was stolen, denial of service claims from customers who can’t access a site, as well as claims from anyone to whom a deadly computer virus is transmitted, whether by accident or not.

II. Liability and Loss Scenarios

A. Computer Hacking

As the recent George Mason University incident reveals, hackers can often obtain access to the computer systems of even technologically savvy businesses. Whether the business itself has failed to provide adequate safeguards or the security systems that have been installed were themselves vulnerable, the end result is the same: potential direct financial loss to the business and potential liability claims from persons whose sensitive information has been compromised. Consider the case of a company in the business of selling goods to consumers. Visitors to the company s website can browse a product catalogue, select items to purchase, and pay for their purchases with their credit card. As many online businesses do, the company provides an option to save the users personal and credit card information on its servers to make future purchases easier. To encourage online sales, the company assures its customers that its systems are secure. Nevertheless, a hacker exploiting a known flaw in the company s security systems has the opportunity to steal the information and use it to run up charges on the credit cards of thousands of unsuspecting consumers and the potential to steal their identities. Although the company thought its systems were secure, it turns out that its network administrator had failed to apply a patch that had been released weeks earlier which would have prevented the information loss. The company now faces potential liability to its customers for negligence in the protection of their financial information, as well as massive loss of goodwill. The company also faces the cost of an investigation and potential fines from the Federal Trade Commission for misrepresenting the security of its network.[5]

In a slightly different scenario, in the early 2000 s, hackers stole hundreds of thousands (if not millions) of credit card numbers from an array of online businesses, including CD Universe, Creditcards.com, and Western Union, and threatened to release that information on the Internet unless the companies paid a ransom. When the ransom was not paid, the information was released. Such hacking victims face potentially millions of dollars in third-party damages.

Another company recently found its website shut down by its domain registrar when the registrar s domain administrator suddenly began receiving unsolicited emails advertising the company s products. The registrar maintained a strict anti-spam policy and the domain administrator immediately deactivated the company s domains, despite the company s insistence that it never sent unsolicited emails but only sent email to people who had affirmatively signed up to receive them. The deactivation of the website resulted in immediate financial losses as customers who wished to purchase products could not do so. Further investigation revealed that a disgruntled individual had registered the email address of the domain registrar s administrator to receive the company s emails, in a successful effort to cause the registrar to shut down the website. Although not, strictly speaking, a hacker attack, these events demonstrate the impact that a single individual can have on a company s ability to conduct its business on the Internet.

Liability arising out of the release of confidential or financial information is not limited to the hacked companies themselves. The designers of hacked websites, computer security consultants, third-party network administrators and network designers all face potential claims by those whose information was stolen, as well as by the hacked companies for deficiencies in their work.

B. Internet Attacks and Viruses

Computer viruses and DDoS attacks pose significant direct and indirect risks to businesses that use the Internet. In a DDoS attack, a hacker uses a virus to infect thousands of computers around the world. At a specified time, those zombie computers simultaneously launch repeated requests for information from a targeted website. The resulting traffic overwhelms the computer servers hosting the target and renders the website unavailable for an extended period of time. Such attacks have affected well-known companies such as Amazon.com, eBay, Buy.com, E*Trade and Datek, but they have also been launched against lesser known companies whether as part of an extortion attempt, by competitors interested in disrupting their business, or by disgruntled former employees or customers seeking to exact revenge for some real or perceived slight. In fact, the tools needed to carry out a DDoS attack are freely available with a little researching on the Internet.

A former employee of a Manhattan computer consulting firm recently pled guilty to hacking into his former employer s computer system and deleting information that rendered the firm s clients websites unavailable for several days. The consulting firm s damages were estimated in excess of $100,000, simply to recover the lost data and to repair their relations with their clients.[6] But the consulting firm also faced potential liability for the business lost by its clients as a result of the breach of security. Similarly, in August 2004, a federal grand jury indicted the CEO of Orbit Communication Corporation of Sudbury MA, for allegedly hiring hackers to launch DDoS attacks against several competitors in order to disrupt their businesses. The attacks were estimated to have cost the competitors more than $2,000,000.[7]

Although not specifically directed at particular companies, computer viruses can delete vital data; bring down networks and websites and cause enormous direct and indirect damage. In addition, they can render hard disks unreadable, hijack computers to be used for attacks against other computers, or capture sensitive information and send it over the Internet to the virus designers. Moreover, self-propagating viruses can automatically send themselves to every customer, vendor, or other contact in a company s email address book, thereby causing losses to third parties, resulting in potential loss of goodwill and liability to those parties. It seems safe to assume that most corporations have installed antivirus software to protect themselves against such attacks, but such software is by definition always a step behind the newest virus, and the software must be constantly updated to obtain the latest virus information. Failing to update the software regularly could leave a company vulnerable to infection.

The threat from computer viruses transmitted via email is well known. Less well known is the threat from viruses transmitted via other means, such as through web pages that take advantage of security gaps in Internet browsers and viruses transmitted through instant messaging software such as Microsoft Instant Messenger or AOL Instant Messenger (AIM). Instant messaging software has become increasingly popular in the workplace. As its popularity has increased, so has the security threat. In early March 2005, reports indicated that several viruses transmitted by instant messaging software had begun to appear, and security industry sources indicated that virus writers had begun to focus on instant messaging as a means of propagating viruses because computer users were not as cautious in clicking on links during instant messaging sessions as they

were in clicking on links in email.[8] One report indicated that in the first six weeks of 2005 alone, 10 instant-messaging viruses spread over the various instant messaging networks, more than three times the number tracked over the same period a year earlier.[9]

Computer viruses, however they propagate, represent a significant threat to businesses, both for their potential direct effects — lost files, computer downtime, etc. — and for the potential liability they create to third parties. For example, a design company that contracts to design a product for a customer might lose the relevant computer files to a virus, forcing either an expensive reconstruction of those files or perhaps preventing the company from meeting its contractual obligation. At best, the company would have to absorb the recovery costs and lost productivity. At worst, the company might find itself facing claims of breach of contract from its customer, in addition to loss of goodwill.

As suggested by the hacking cases discussed above, criminal prosecution may punish those responsible for computer attacks — if they are caught. But who pays for the damage caused by them? Civil lawsuits against the perpetrators are not likely to recover much, if anything. And what of the damages incurred by third parties who are affected? In the case of online brokerages, for example, it is easy to imagine lawsuits by brokerage customers who suffered losses because of an inability to trade in their accounts while the brokerage websites were down. Such lawsuits could be based on breach of contract or negligence theories, and could be significant. Banks and other financial institutions are similarly at risk.

C. Trademark Infringement

In addition to the tremendous risks created by Internet attacks and viruses that originate outside a company, businesses also face potential liability for their own Internet-related actions. Trademark infringement is one area where businesses may inadvertently create liability for themselves that would not be covered by traditional CGL policies. As previously discussed, copyright, title or trademark infringement is specifically excluded under the CGL.

Trademark law has both federal and state components. Federal registration of a trademark grants the registrant nationwide rights to the name. State registration provides statewide rights, and common law rights arising from the use of a trademark rather than from registration may have more or less geographic reach depending on the scope of the trademark s use. The touchstone of trademark infringement is the existence of a likelihood of confusion between two users of a particular trademark. Thus, a company located in one state might uneventfully use its name for years without any trademark implications even if a company in another geographic area also used that name because there is no likelihood that consumers will confuse the two. But if one of those companies establishes a website to expand its geographic reach and obtain business from other areas of the country, that company could well find itself in a trademark dispute with a prior user of the trademark in another area of the country that has state law or common law trademark rights. Not only could such a dispute lead to significant litigation costs and monetary damages for trademark infringement, but it could also result in the newer user of the trademark having to give up its name or pay to acquire the rights to the name. An instructive example of the impact of the Internet on trademark infringement arose several years ago, when Amazon.com found itself the defendant in trademark litigation brought by a small feminist bookstore located in Minneapolis that claimed to have prior rights in the Amazon name.

Trademark infringement liability can also arise from the use of trademarked terms in the metatags of a company s website. Metatags are invisible coding that search engines can use to index websites and make them available to Internet users who search on specific terms, including trademarked terms if those terms are included in the metatags of a website. The use of trademarks as metatags has been held by several courts to be trademark infringement.[10] Trademark liability may also arise from the use of a trademarked term on the visible portion of a website.

D. Inadvertent Release of Confidential Information

The disclosure of confidential information through hacking has already been addressed. However, a company may also disclose confidential information, such as financial or medical information, inadvertently in the absence of hacking. Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), healthcare companies must ensure that electronic patient information is stored in a secure and confidential way. Those that fail to do so are subject to investigation and potential fines, as well as potential lawsuits from patients for violations of privacy. For example, the pharmaceutical giant Eli Lilly maintained a list of email addresses provided by users of the drug Prozac, and used those email addresses to send periodic newsletters on issues relating to depression. When Eli Lilly decided to discontinue the service, it sent a notification to all of the people who had signed up. However, due to a programming error, recipients of the notification were able to see the email addresses (many of which had identifiable names) of all of the 669 subscribers to the service, thereby disclosing those individuals treatment for depression to all other recipients of the email. Although the release was unintentional, the FTC brought an enforcement action against Eli Lilly for deceptive advertising. Eli Lilly had touted its privacy policy but failed to ensure that privacy. The FTC complaint alleged that Eli Lilly had failed to adequately train its employees on privacy issues and to implement appropriate supervision as well as other policies to ensure that confidentiality was maintained. The FTC did not require Eli Lilly to pay a fine, but it presumably incurred significant legal expenses during the investigation and it was required to implement substantial additional privacy safeguards.[11] In addition, a number of state attorney generals also investigated the release of confidential medical information, and Eli Lilly resolved those concerns by paying the states a total of $160,000.[12] In addition, Eli Lilly also faced potential lawsuits from the affected subscribers for breach of privacy.

Other companies have inadvertently released financial information, potentially exposing themselves to liability to the people whose information was disclosed. For example, in 2001 OfficeMax inadvertently disclosed customers credit card and other personal information due to a programming error which included the mentioned information whenever one of its customers would email a link from its website to another person.[13]

III. Cyber Insurance Coverage

With respect to the additional exposures created by use of the Internet, a small sector of the insurance industry has developed enhanced forms to fill the gaps in the Property, Commercial

General Liability (CGL) and Technology Errors & Omissions forms. The forms are non-standard in approach, yet most will offer some of the components below:

- *Technology Errors & Omissions* - Standard Technology Errors & Omissions coverage is typically enhanced by the inclusion of professional services relating to or conducted via the Internet. Additionally, coverage is usually afforded by specific coverage grant for breach of security and failure to prevent unauthorized access, exposures inherent to most Internet/Media Technology companies and usually excluded by standard forms. It is also worthwhile to note that the policy territory is usually expanded to include worldwide suits.

- *Web Content Liability* - The Internet/Media liability agreement provides coverage for advertising injury, personal injury, copyright and trademark liability arising out of Internet activities. It is important to coordinate the language of this policy with the CGL so as to be sure coverage is in place for personal injury and advertising injury for non-internet-related activities. Note that any copyright coverage provided is only with respect to Internet activities and that patent liability is specifically excluded. If desired, true intellectual property coverage can be purchased under separate coverage forms.

- *Network Security Coverage* - This coverage comes in two basic types:
  Third Party Coverage provides liability coverage arising from a failure of the insured s product and/or service to prevent unauthorized use of or access to its network. This coverage can apply to claims arising from the transmission of a computer virus, theft of a customer s information, and DOS liability.

  First Party Coverage - This coverage provides reimbursement for loss arising out of the altering, copying, misappropriating, corrupting, destroying, disrupting, deleting, damaging, or theft of information assets, whether or not criminal. Typically the policy will cover the cost of replacing, reproducing, recreating, restoring, or recollecting. In case of theft of a trade secret, the policy will either pay or be capped at the endorsed negotiated amount. First Party Coverage also provides reimbursement for lost revenue as a result of a covered event. In this case, the policy will provide coverage for the period of recovery, plus an extended business interruption period. Some policies also provide coverage for dependent business interruption, meaning loss of revenue as a result of a computer attack on a third party business upon which the insured s business depends.

- *Cyber-extortion* - This coverage provides reimbursement of investigation costs, and sometimes the extortion demand itself, in the event of a covered cyber-extortion threat. These threats, usually take the form of a demand for consulting fees to prevent the release of hacked information or to prevent the extortion from carrying out a threat to shut down the victim s website.

- *Public Relations or Crisis-communication* - This coverage provides reimbursement up to $50,000 for use of public relation firms to rebuild an enterprise s reputation with customers, employees, and shareholders following a computer attack.

- *Criminal Reward Funds Coverage* - This coverage provides reimbursement up to a pre-determined limit, such as $50,000, for information leading to the arrest and conviction of a cyber-criminal.

- *Loss Prevention Services* - Another important feature of a quality cyber-risk insurance program is its loss prevention services. Typically these services could include anything from a free online self-assessment program and free educational CDs, to a full-fledged onsite security assessment. From an insured s perspective, the availability of these services is valuable, however, in some cases the responsibility for payment can fall back to the insured. This can be discouraging as these services can sometimes exceed $50,000. Note that the trend is for the insurer to assume these costs, but be sure to investigate this before you proceed.

V. Conclusion

It is clear that no single risk management strategy can completely eliminate the risks associated with cyberspace. There is no special technology that can make an enterprise completely secure. No matter how much money companies spend on cybersecurity, they may not be able to prevent disruptions caused by organized attackers. Some businesses whose products or services directly or indirectly impact the economy or the health, welfare or safety of the public have begun to use cyber risk insurance programs as a means of transferring risk and providing for business continuity. [14]

Traditional approaches to Internet and network security have attempted to eliminate risk factors through technical and procedural means. This model is just too simple for the increasingly complex world of the Internet. Insurance coverage represents a critical tool in that it provides an essential non-technical control and a transfer of risk. Insurance programs should include a combination of traditional insurance and specific cyber-risk insurance, and they should be provided by top-rated, technology savvy insurers.

Authored By:

William J. Richards, CPCU, CIC is a Senior Vice President of William Gallagher Associates in Boston, Massachusetts with responsibility for the business development, marketing, and servicing of technology clients. With over twenty years of insurance industry experience, his areas of expertise include Directors and Officers Liability, Errors and Omissions Liability, Internet Liability, Intellectual Property and multinational business programs. Mr. Richards has been a guest speaker to both the Boston Bar Association, as well as many prominent law firms in the Boston area.

Mitchell J. Matorin is Counsel at Foley Hoag LLP in Boston, MA, where he practices in the areas of intellectual property litigation and Internet-related issues. He has advised clients in the areas of Internet-related trademark and copyright infringement, liability of interactive service providers under the Communications Decency Act, Internet domain registrations, compliance with the federal Can-SPAM Act and Digital Millenium Copyright Act, and computer fraud and abuse issues.

References

[1]Remarks of Deputy Assistant Attorney General Laura H. Parsky to a Joint Meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council September 14, 2004 (available at http://www.cybercrime.gov/ParskyRemarks091404.htm).

[2]Experts: Cyber-Crime a bigger threat than cyber-terror, report on CNN.com, January 19, 2005 (available at www.cnn.com/2005/TECH/internet/01/18/cyber.security/index.html).

[3]The Future of the Internet: In a survey, technology experts and scholars evaluate where the network is headed in the next ten years, January 9, 2005, at p. 14 (available at http://www.pewinternet.org/pdfs/PIP_Future_of_Internet.pdf).

[4]George Mason Officials Investigate Hacking Incident, Washington Post, January 13, 2005, at p.E1 (available at http://www.washingtonpost.com/wp-dyn/articles/A5188-2005Jan12.html).

[5]See, e.g., Petco Settles FTC Charges: Security Flaws Allowed Hackers to Access Consumers Credit Card Information, Federal Trade Comm n Press Release, November 17, 2004 (available at http://www.computerworld.com/securitytopics/security/story/0,10801,97595,00.html).

[6]Ex-Official Of Local Computer Consulting Firm Pleads Guilty To Computer Attack Charge, U.S. Department of Justice Press Release, Sept. 9, 2004 (available at http://www.cybercrime.gov/cottonPlea.htm).

[7]CEO of Orbit Comm. indicted in hack attack, Boston Business Journal, Aug. 27, 2004 (available at http://www.bizjournals.com/boston/stories/2004/08/23/daily43.html).

[8]Instant Message Work Attacks Increasing, MSNBC.com report, Marcy 7, 2005 (available at http://www.msnbc.com/id/7120241).

[9]Instant Messenger Worms on the Prowl, CNET News.com report, March 8, 2005 (available at http://www.nytimes.com/cnet/cnet_2100-7349_3-5604060.html).

[10]See, e.g., Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999); Playboy Enterprises, Inc. v. Calvin Designer Label, 985 F. Supp. 1220 (N.D. Cal. 1997).

[11]See Eli Lilly Settles FTC Charges Concerning Security Breach, Federal Trade Commission Press Release, January 18, 2002 (available at www.ftc.gov/opa/2002/01/elililly.htm).

[12]Eli Lilly and Company Enters Into Multi-state Agreement to Safeguard Consumers Privacy, New Jersey Department of Law and Public Safety Press Release, July 25, 2002 (available at www.state.nj.us/lps/ca/press/lilly.htm).

[13]See Carol King, Security Glitch at OfficeMax; Retailer Says It's Resolved, InternetNews.com, Feb. 22, 2001 (available at http://www.internetnews.com/ec-news/article.php/4_596241).

[14]See The National Strategy to Secure Cyberspace, February 2003 (available at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf).