

# Printing Faces Cybercrime

Michael Zeldes, Senior Vice President, HUB International

Every business faces risks that could potentially damage the reputation and success of the company. Some are obvious: food poisoning in a restaurant, for example, which can lead to a large claim and defamation of the business. Other challenges, however, cannot be anticipated so readily. Overcoming and adequately preparing for the different types and levels of risk inherent in the printing, publishing, and graphic imaging industries (both hidden and obvious) are vital to the continued operation of the business. Being educated about the growing risks that now exist and that your business is exposed to—coupled with the right coverage in case of a loss—positions your business for a healthy and successful future.

## New Opportunities, New Risks

Changes in digital technology have transformed the industry of commercial printing but also introduced new risks. In the age of the Internet, email, and electronic files, the rapid evolution of the industry means traditional printing has moved to the digital press, with a growing dependence on and high proportion of prepress print work now being done on computers.

Web-based technology and extensive public and private computer networks allow for faster and more convenient business functions and transactions. Though more efficient and cost-effective, digital printing is also more exposed, fraught with new and complex risks.

Printing businesses that work digitally are faced with blind spots—vulnerabilities often invisible in the course of daily business operations. These vulnerabilities are time bombs, with the potential to cause major disruption including lawsuits, damage to reputation, and consequently loss of income. Every business secret, customer list, employee file, product design, trade secret, and private document is at risk of exposure to hackers and cyber thieves twenty-four hours a day. It is not a matter of “if” a business will experience a cyber security breach, but “when.”

“Cybercrime” is reported to be the fastest growing crime in America, according to Brian Grow, who covers the topic for *BusinessWeek*. What might have been irrelevant to a commercial printer five years ago now has the potential to disrupt business operations or even

sabotage a company. Today, nearly every company is at risk of being a victim of cybercrime—the printing industry is no exception.

Cybercrime is any number of data security breaches that disrupt the operation of a business. It could include the interruption of E-business; identity theft; the unauthorized access, theft, or dissemination of confidential information; the corruption of data; viruses, worms, Trojan horses, or other malicious code/hacker attacks; phishing schemes; or even libel, slander, or extortion attempts.

Privacy is increasingly an illusion. Many printing businesses ask their clients to upload files to an FTP site and then retrieve the information. But businesses can no longer assume what is given to them by a customer is secret. Consequently, their obligations to customers are under attack. Doing business today is like getting undressed in front of a mirror—with the windows wide open.

## What Are the Threats?

Threats to businesses come from all different sources: the result of a lost or stolen PDA, laptop, smart phone, or other mobile device; hackers who get a thrill from breaching companies’ security systems or wish to test their “skills”; other businesses trying to steal company trade secrets or competitors’ clients; vengeful vendors with whom the company no longer conducts business; or disgruntled former employees to whom there is nothing more satisfying than receiving recognition in the form of seeing confidential information he or she provided plastered all over the Internet—even anonymously.

So what are the top five IT threats of 2010?

1. Malware. Software designed to infiltrate or damage a computer system without the owner’s informed consent.
2. Botnets. Groups of computers infected with malicious code and controlled by an outside master.
3. Cyber Warfare. The use of computers and the Internet in conducting warfare in cyberspace.
4. Threats to VoIP. Disrupting or “stealing” voice communications over the Internet and mobile devices.

## 5. Fraudulent online activities. The evolving cyber crime economy is engaged in fraudulent online activities.

These threats are real and difficult to defend against because they mutate all the time, as the culprits consistently seek to outsmart their targets. Brendan Connors, co-owner, MOSAIC, a waterless print communication company located in Cheverly, Maryland, feels confident his company has taken adequate measures to protect MOSAIC's digital assets, but says he's always willing to learn more, given the dynamic nature of the technology industry.

"I don't hide from new technology; but I am pretty tight with our data—our clients rely on it," says Connors, and despite being "the future of technology," cloud computing causes him some concern. "It's great that data can be out there 'on a cloud' somewhere, but what if my Internet connection fails or cyberterrorists break into the system and steal their data?" he asks. "That could end the company. I'm not willing to take that risk. Our information is controlled within our walls—our level of security resembles that of a bank."

Even institutions that are supposed to be cyber-security fortresses are vulnerable to attack. Recent media coverage spotlighted privacy breaches committed against Goldman Sachs, the New York Stock Exchange, and federal agencies. A quick online search unearths thousands of incidents of cyber breaches ranging from small businesses to large corporate conglomerates. The website, [www.privacyrights.org](http://www.privacyrights.org), lists new cases of privacy breaches daily and also offers a good perspective on the latest trends and tips on how to stay aware of your risks and what to do to protect yourself.

A number of firms, such as IntraLinks, Inc. ([www.intralinks.com](http://www.intralinks.com)), offer secure, digital workspaces where businesses can collaborate and share highly confidential documents online through a password-protected site.

### Mitigating the Risks

Cyber attacks are costly on businesses, particularly small and medium-sized companies (the majority of the printing industry) whose businesses could be wiped out given their limited resources. According to a recently released *U.S. Cost of Data Breach Study*, data breaches have direct cleanup costs of \$204 per customer. In some states, companies are required to notify customers of even a suspected breach. These privacy notification costs can cost up to \$30 or more per customer. In addition, there are the potential liability costs from lawsuits and opportunity costs that arise from a damaged reputation and loss in customer confidence, which have longer lasting consequences.

Even adequate firewall protection and sophisticated encryption techniques are sometimes not enough to defend against a malicious attack. Knowing the risks, and insuring against them, is the best way to protect your interests.

According to Frank Pecoraro, underwriting consulting director technology practice, CNA Insurance Company, printers need to consider the impact of a security breach on their internal networks, which would likely result in inhibited production. "Printers can be heavily reliant on the Web and/or their networks to perform their printing operations. If a company is relying on networks and the system is affected because of a security breach, virus, or similar peril, and they can't operate or generate revenue, that breach is not covered by a standard policy," warns Pecoraro.

Since anything Web-based can't be used, both first- and third-party liability issues arise. "A first-party exposure exists should their systems be shut down or impaired by a virus, hacking event, unauthorized employee, or security breach. The same holds true if the network security breach causes a job to be printed incorrectly, if the jobs is sent to the wrong address, or if a job misses a deadline. The printer could be sued by the client," says Pecoraro.

Cyber-liability insurance, also referred to as Cyber Security/Privacy Liability Policy, for Internet-based risks addresses the growing risks associated with conducting business electronically. Cyber insurance protects businesses, improves productivity, minimizes the likelihood of loss, and offers peace of mind by providing the necessary coverage that traditional Property, General Liability and Errors and Omissions (E&O) insurance cannot address alone. Traditional insurance policies are unlikely to protect against data security breaches or protect only against specific exposures, leaving gaps in coverage. Most general liability insurance policies exclude cost of recall, correction, reproduction, and reperformance if the result of a cyber security breach.

Coverage options are now available that provide first- and third-party protection for risks incurred by Internet and network operations and protect printing businesses from additional hidden exposures and lawsuits stemming from plagiarism, copyright infringement, defamation, invasion of privacy, trademark infringement, intellectual property theft, and more as a result of a digital security breach. Cost depends on the revenue size of the company.

*Continued on page 19*

Others may ask many questions, some of which may be difficult to answer. Dismissing such questions as an annoyance is a mistake, according to Limoli. "I feel strongly this is where we, as leaders, lose an opportunity to grow this type of employee into a more informed and well-rounded employee." It is in "taking that extra time either on the production floor or in a one-on-one setting in your office" that will bring those long run dividends.

Different communication styles on either side of a discussion can cause misunderstanding and costly mistakes. A gender difference can be a barrier to effective communication, as can a cultural difference. Recognizing one's own communication style, that of others, and how the two relate is essential to effective communication. Pay attention to the silent portion of conversations. Often a vital part of the message, silence can imply agreement, express dissent, convey anger, suggest an insult, or perhaps request more time to think. Understanding diverse communication styles will help a manager discover the best way to motivate individual employees.

### Managing Diversity

Managing diversity and cultivating cooperation often requires a production manager to wear the human resources hat. Even in larger corporations with a separate HR department, the production manager must deal with many issues unrelated to traditional production management duties. The major workforce diversity categories in the U.S. are gender, race, national origin, age, disability, domestic partners, and non-Christian. A melting pot approach to these differences, assuming people will automatically want to assimilate, does not work in today's environment. Managers must recognize that employees do not set aside their beliefs, values, and preferences when they walk in the door to work. Vine points out that "study after study shows respect of employees and getting their buy-in 'for real' and not 'for show' makes all the difference." Corporate mission or value statements are just words until managers take actions that actually show the respect often mentioned.

A manager must embrace diversity by recognizing, respecting, and valuing individual differences. Explore the differences with open and non-judgmental communication. Assist employees in understanding each other. Make available a path for employees to deal with emotional or other issues they bring from home life. A positive culture of respect and teamwork takes time and energy by management to maintain. The benefits resulting from such efforts include increased productivity and job satisfaction and decreased absenteeism, tardiness, or turnover.

### Final Comment

Greater effort placed on communication and human resource management can transform an average manager into a highly effective manager. Effective management can reduce costs and errors, helping the company stay competitive in this changing industry. When every little bit matters in this on-demand world, shifting one's focus can make a difference between failure, surviving, or thriving.

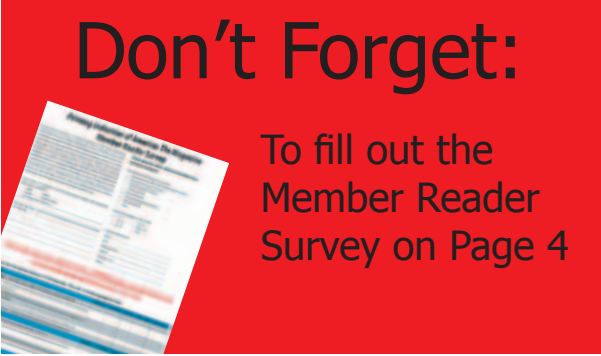
*Be sure to attend Patty's "Bindery Production Manager's Panel" at the BIA Mid-Management Conference being co-located with the Offset and Beyond Conference May 17–19 in Baltimore, Maryland. For more information visit [www.printing.org/biaconference](http://www.printing.org/biaconference). Patty Traynor is founder and president of Lancaster, Pennsylvania-based Finish On Demand, Inc., a full-service, short-run bindery designed to meet today's demands for high quality and fast turn-arounds. She also is a director of the Binding Industries Association (BIA). She can be reached at 717-392-5000 or [patty@finishondemand.com](mailto:patty@finishondemand.com).*

### Continued from page 11

It is important to select the right insurance professional to assess your exposures and analyze how to best mitigate your risk. One who specifically works with printing businesses would be best, as they can pinpoint where your greatest risks may lie and advise on the latest trends in coverage options and carriers offering the most comprehensive and cost-effective solutions.

In this digital age, it's evident that the exposures are only going to grow rather than shrink in the future. Keeping on top of the latest security and risk management tactics to implement in your operations is imperative. Having the right insurance program is also key, as one claim can lead to disaster. By staying prepared and educated, your business will help overcome the many potential breaches lingering out there.

*HUB International is a leading insurance and risk management firm. Michael Zeldes can be reached at 212-338-2353 or [Michael.Zeldes@hubinternational.com](mailto:Michael.Zeldes@hubinternational.com). For more information on HUB, please visit [www.riskfirewall.com](http://www.riskfirewall.com).*



**Don't Forget:**  
To fill out the  
Member Reader  
Survey on Page 4