Best Practices for Protecting Electronic Business Data

Companies are under attack from cyber-criminals, hackers and spies. Is your data at risk?

COMPILED BY MILES Z. EPSTEIN
EDITOR, COMMERCE

WITH THE DATA BREACH AT SONY in the news and their high-value data exposed for all to see—including their clients who compete for big-ticket entertainment contracts—the risk of cyber hacking has come front and center for business leaders around the nation and the world. *COMMERCE* asked legal experts to recommend best practices for protecting electronic business data, which is increasingly being compromised by cyber-criminals who know how valuable this information is. Is your data at risk?

Callagy Law, LLC
By Thelma Akpan, Esq.

While there is likely no foolproof way for companies to protect themselves against the most innovative and nefarious cyber hackers, companies must be able to proactively detect cyber security breaches as soon as possible to minimize the damage in the face of such a threat. Develop a plan. Even the best systems need to be actively monitored, so it is important that a company's database is managed by cyber security to be able to detect and stop an attack as soon as possible. A company should do this by creating or improving upon existing policies, including the use of data encryption; employee training; limiting sensitive data to only those who need it; the implementation of security software on all devices; and instituting policies on how to choose and when to change passwords, among other in-house and outsourced policies and programs. Most important, companies should restrict the use of e-mail as it is a treasure trove of information for cyber criminals. As employees frequently communicate anything and everything via e-mail, access to this information could be most detrimental to your organization and clients. Adopt a "if it should never be made public, it shouldn't be communicated on e-mail" posture regarding all e-mail communication.

Connell Foley LLP
By Peter J. Pizzi, Esq., CIPP/US, Co-Chair, Cyber Security and Data Privacy Group

With cyber-crime becoming an all-too-real source of potential harm for businesses, it is imperative that companies plan for a cyber-attack. The following measures help prepare for and protect against such a prospect. First, know what data you have, where it resides and who has access to it. Implement the most rigorous protection systems for the most critical data. Next, test your policies and practices under the protection of the attorney-client privilege, engaging outside vendors (through counsel) to attack your systems and point out weaknesses, allowing you to make improvements and enhancements where needed. Remember, no system is foolproof. If you don't have a cyber-incident response plan, make one and test it. Conduct a real-time exercise with management to simulate the handling of a cyber-attack. Consider improving or enhancing your data policies and practices, including password hygiene and retention policies, and your practices for data control, monitoring, security and destruction. Check with your insurance consultants to determine whether cyber-incidents are covered and/or whether you need cyber coverage from a specialty underwriter. Ultimately, you need to know your company's legal rights and responsibilities, and identify which professionals and law enforcement agencies to contact in the event of a cyber-breach.

Day Pitney LLP
By Michael J. Dunne, Esq., Partner

Protecting electronic information against attacks, and the effects of those attacks, involves policies and processes, not just technology. Policies and processes must take many factors into account, not the least of which is the legal framework in which the business operates. Policies and processes should address obligations imposed by various state, federal and, at times, international laws, and the policies and procedures that may be put in place to obtain certain legal protections and advantages. For instance, a business needs to ensure it has policies and processes in place to respond to any suspected security breach as required by applicable law. It should also have policies, not just technology, that set clear boundaries on employee and third-party access rights. Well-drafted access policies may assist in asserting both trade secret claims and claims for violations of the federal Computer Fraud and Abuse Act. Similarly, well thought out and implemented policies on passwords—and the use of tokens and other security procedures that are not required by law—can yield significant legal protections. A

continued on page 88

continued from page 86

solid focus on policies and processes will deter many bad actors, and can act as a sword and a shield against the rest.

Genova Burns LLC
By Charles J. Messina, Esq., Member, Intellectual Property Law Practice Group

From eBay to SONY, the number of U.S. data breaches continues to increase and have a crippling effect on businesses. Regardless of whether the type of data stored by your company is subject to state and federal regulatory requirements, your firm should be diligent in creating and adhering to best cybersecurity practices. The National Institute for Standards and Technology (NIST) released a cybersecurity framework in February 2014, setting forth a variety of best practices for managing cybersecurity risks. NIST recommends, among other things, implementing robust password and system log-in protocols, controlling access to systems, utilizing automatic updates to software on all electronic devices (hackers can easily find vulnerabilities in outdated software), and investing in backup systems. As a starting point, an outside consultant should be hired to assist with identifying sensitive IP, and to objectively test the fortitude of a company's technological defenses. Even with state-of-the-art technology, many data breaches result from disgruntled employees and hackers exploiting human error, i.e., employees accidentally installing malware or clicking on a phishing link. These types of issues can be prevented by implementing, and constantly monitoring, cybersecurity policies for limiting the access of data, installation of new software, and downloading of files from external sources.

Gibbons P.C.
By Peter J. Torcicollo, Esq., Leader, Data Privacy & Security Task Force

Executives know that their organization's valuable data and confidential information is under attack from hackers. Experts believe most sensitive systems have already been infiltrated. What to do? Your company is probably already encrypting data regularly and utilizing intrusion protection and detection systems, but common sense practices can avoid a catastrophic event. (1) Appoint a Chief Information Security Officer who understands the threats, how to mitigate risk, and can interface with security vendors and federal agents. (2) Periodically invite federal cyber agents to meet with your IT staff and CISO—they may be able to share critical, emerging information. (3) Ensure your company has an incident response plan—and drill using it. (4) Appoint legal and communications department representatives to your crisis management team. (5) Consider an information security audit to identify files left behind from any prior intrusions. (6) Exercise healthy skepticism when IT tells you, "Our system is very safe." (7) Procure a cyber-insurance policy—don't assume existing policies cover this risk. If you suffer a verifiable intrusion, consider contacting federal agents immediately to assist in hardening your system and preventing future intrusions. Finally, consider pushing for a prosecution to create a general deterrent against cyber criminals.

Hoffmann & Baron, LLP
By Lou A. Budzyn, Esq., Partner

To minimize damage resulting from external hacking, best practices used in maintaining trade secrets should be implemented. Under trade secret notions, access to information should be restricted. In the same way filing cabinets were locked in the past, critical information—drawings, formulations and the like—should be isolated from publicly accessible networks, such as the Internet and cloud-based computer networks. This information can be stored on internal networks or media and accessed as needed. However, isolation of electronic files may be in tension with internal sharing and remote access. Where remote accessibility is necessary, VPNs (virtual private networks) and other secure systems should be considered. Although systems may be administered securely over the Internet, the Internet itself is not secure. VPNs provide an additional layer of security. Limiting access to information also can be leveraged to minimize any damage doable by a disgruntled employee. A bell cannot be un-rung and the release of restricted information has a lasting effect. Accessing of information may be monitored for irregular patterns, such as after-hours activity, accessing of files not in an employee's area of responsibility, and so forth. Pattern spotting can preempt the spread of restricted information.

Jackson Lewis P.C.
By Joseph J. Lazzarotti, Esq., Shareholder, Morristown Office

The loss of intellectual property (IP) could be as crippling to an organization as personal data of customers or employees, if not more. Yet, the compliance standards and best practices that have developed to safeguard health, financial and other personal information are often not applied to IP and other company data. They should be, and in addition to leadership and resources that CEOs can provide, there are some critical steps companies should be taking. Regular risk assessments are vital, as companies can't protect data they don't know exists, or prevent access routes they don't know about. For example, understanding where employees store data—such as personal flash drives—is essential to practically safeguard it. Considering that payment processing and HR departments frequently have far better practices and procedures than other departments, companies should eliminate silos to leverage and coordinate those good practices and procedures to protect all confidential information, including IP. In addition, companies need to practically and regularly train employees about what their security policies require. Employees can also be responsibly monitored to ensure compliance and thwart

continued on page 90

continued from page 88

insider threats. Finally, companies must understand what data vendors maintain for them, and how they protect it. Strong contract provisions concerning data security are critical.

Lowenstein Sandler LLP
By Mary J. Hildebrand, Esq., Partner, Tech Group, Chair, Privacy & Information Security Practice

Best practices to protect intellectual property (IP) should be practical in nature and implemented on a proactive basis. While external hackers and cybercriminals often grab headlines, employees and other insiders present the greatest threat to IP security. There are five immediate steps to take, which will address IP at risk. (1) Make sure that employees and third-party vendors sign nondisclosure agreements. (2) IP in electronic form should be subject to controlled access on a need-to-know basis, protected by appropriate security measures (e.g., firewalls, passwords and state-of-the-art security tools), and monitored regularly. (3) For departing employees, ensure that their access credentials are immediately revoked, and as part of the exit interview, obtain a written statement that no IP is being removed. (4) Develop and implement company policies that provide guidance on identifying IP, appropriate protective measures and how to respond in the event of a security incident. (5) Provide active, comprehensive training to all employees, and conduct regular security audits, with appropriate and thorough follow-up. If your company operates in foreign jurisdictions, be aware that technical surveillance and theft may not be illegal under local law, so security protocols should be adjusted accordingly. Above all, recognize the risk and be realistic.

McCarter & English, LLP
By Scott Christie, Esq., Partner

To mitigate the risk of a data breach, companies must elevate data security responsibility to senior management and, as envisioned by the New Jersey Identity Theft Prevention Act, implement a written information security program that integrates administrative, physical and technical security measures. On the administrative side, elements should include collecting and maintaining only data reasonably necessary to accomplish business purposes, limiting data access only to employees as necessary to perform job responsibilities, requiring vendors to whom data is entrusted to comply with a stringent data security policy and securely rendering data unintelligible once there is no longer a legitimate need to preserve it. Physical safeguards should be implemented that require secure storage of data, prohibit employees from keeping sensitive data in plain view, and restrict storage, access and transportation of such data outside of business premises without good cause. From the technical perspective, unique logins, secure passwords, and up-to-date and comprehensive antivirus and firewalls should be the norm along with encryption of data both at rest and in transit. Of course, establishing a robust data security program will be an individualized process that will address all known and anticipated risks that may be unique to a particular industry and company.

NPZ Law Group
By David H. Nachman, Esq., Managing Attorney

While there are many Americans who offer information technology (IT) and intellectual property (IP) expertise, there are also many talented IT and IP professionals from other countries. When these assets are identified by our business clients, the NPZ Law Group devises short-term and long-term strategies for these experts to enter the United States, train and remain here for specialized work assignments. For example, we were recently contacted by a top IT firm seeking to employ an Israeli IT security and encryption specialist who was to be deployed to numerous New Jersey and New York businesses to design systems to protect their electronic and other sensitive corporate data. Due to the candidate's academic and experiential background, NPZ rapidly secured an O-1, extraordinary ability, nonimmigrant visa for her. Now, she is using her skills on behalf of numerous local and national businesses to devise systems for protecting various forms of electronic and other sensitive company data. NPZ contributes to the protection of sensitive corporate data by helping companies and staffing agencies rapidly acquire the talents of IP and IT experts from around the world.

Pashman Stein P.C.
By Ryan J. Cooper, Esq., CIPP/US, Counsel, Privacy and Information Governance Practice Group

A very effective but relatively low-cost best practice for securing your intellectual property and other valuable corporate information is employee training on how to recognize malicious attacks. Phishing or spear-phishing attacks, where an intruder sends a malicious e-mail disguised as one originating from within the company in order to trick an insider into divulging log-in credentials, is a devastatingly effective means to defeat even elaborate digital security systems. When successful, these attacks give intruders access to essential intellectual property, confidential and proprietary corporate information and trade secrets, and customer and employee personal information. Training employees to recognize and defeat such attacks has proven to be among the most effective countermeasures. The case for training is even more compelling when the cost is compared to the expense of state-of-the-art digital security software and the staff needed to install, monitor and maintain it. The specific training should be customized for individual firms, and should balance information security with organizational objectives and operational realities. Most important, the training should be rigorous enough to be effective, but easy for new employees to