Cyberspace: Protecting Data is Serious Business

Bad actors—both foreign and domestic—make cyberspace one of the most dangerous neighborhoods, and yet security precautions remain inadequate to the risks.

COMPILED BY JOHN JOSEPH PARKER
CONTRIBUTING EDITOR

CYBERCRIME IS ON THE RISE, draining about $500 billion a year from businesses worldwide. In fact, bad actors—both foreign and domestic—make cyberspace one of the most dangerous neighborhoods, and yet security precautions remain inadequate to the risks that we now face. The answers to this challenge include creating a cybersecurity defense; software and technology; improved governance and policies; outsourcing to third parties; breach response drills; reorganization of IT; and more personnel.

COMMERCE asked experts at some of New Jersey's top accounting firms and law firms to offer some advice, as well as share some success stories.

ACCOUNTING

Citrin Cooperman

By Suzanne Miller, Ph.D., CHS-III, CISA, CISM, CRISC, QSA, Principal, Technology Risk and Advisory Consulting Group

Citrin Cooperman employs a cybersecurity awareness outreach program, whereby our clients can request an assessment to see if they are at risk of a cyberattack. Our client, a large automobile dealership, wanted to know if they were at risk of a data breach. They were using a dealer management system and their vendor assured them that they were "safe." However, once the owner learned that a data breach of their customer data is legally the dealership's liability, not their vendor's, they wanted to know how to protect themselves. The first thing we did was perform a data mapping to identify the flow of customer data through our client's dealership. This process identified multiple risks of exposure across their networks, and on workstations, laptops, tablets, and cell phones. As their data traverses, it is duplicated and stored throughout the dealership, as well as on Internet apps. We helped our client by building a roadmap to implement specific controls that would eliminate certain exposures and reduce the risks of a cyberattack—at the same time making it possible for the client to meet the compliance obligations of the Payment Card Industry (PCI) Data Security Standard and the FTC Safeguard Rule requirement.

KPMG, LLP

By Sarat Mynampati, Managing Director, Cyber Security Services

Media and entertainment organizations often find themselves at the sharp end of targeted cyberattacks in which ransomware is used to distribute Denial-Of-Service indications on organizations' physical and digital assets to gain intelligence about their customers, clients and third parties. In response, KPMG's Cyber team recently provided IT governance, risk and compliance (GRC) strategy and program design as well as an enterprise security roadmap for a large multinational media company concerned about the increasing cyber threats facing its business. Additionally, the firm provided business continuity and disaster recovery planning for the same company to help offset any potential threats posed by environmental and geopolitical risks.

Sax Technology Advisors

By Matthew Hahn, CTO

Sax Technology Advisors (STA), Sax LLP's Cybersecurity and Managed IT Practice recently onboarded a distribution company seeking cybersecurity services because their IT manager left the company. STA implemented a Business Continuity and Disaster Recovery (BCDR) solution to eliminate exposure and data loss in the event of a ransomware attack. After the implementation of the BCDR solution, the company was ultimately hit with a ransomware attack. An employee working remotely but connected to the company's server opened a corrupt e-mail that was disguised as a legitimate one, which then encrypted all of the company's shared data files. STA was able to restore the encrypted server to the most recent point, which was within 15 minutes of the attack, because of the BCDR solution STA

continued on page 24

continued from page 22

implemented—saving the client from data loss and the need to pay a ransom. STA also provided a cybersecurity training curriculum to the entire company to educate the staff on distinguishing between a phishing email and a legitimate email, password security best practices, threat response and device security. The Security Awareness Training program also included simulated attacks and drills and tests throughout the company on an ongoing basis so the mindset for identifying threats is constant and always measured.

SobelCo
By Rebecca Fitzhugh, CPA, CFF, CFE, MBA, CIT, CIGA, Member in Charge, Forensic Practice

SobelCo's professionals aided a young woman who became a victim of stalking and harassment as a result of her position with her company. An individual who had a complaint with the young woman's employer had contacted her to assist him. However, he soon began to send her threatening messages and even showed up at her office. She had a unique surname and was terrified he would identify her and continue harassing her, and possibly her family, by finding a photo of her or personal information on social media or other online sources. Our team performed an Internet risk assessment to identify publicly available information about the young woman that could enable her harasser to track her down, and methodically went through a process to remove as much information as possible from public access. This included having photos of her house obscured on sites like Google and Bing, as well as alerting her that her mother's Facebook page included photos of her but was not private. As a result of our team's work, this young woman was able to recover a sense of safety and security and be protected from future threats by her harasser.

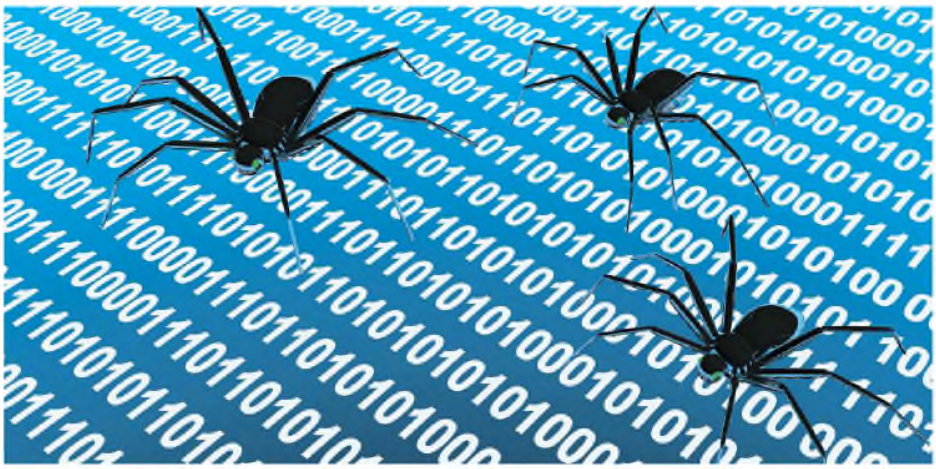
Withum
By Anurag Sharma, CISA, CISSP, CRISC, MBA, Principal, Cyber and Information Security Services

In a recent advanced penetration test for a healthcare client, Withum's cybersecurity team of testers uncovered a major vulnerability in the client's network. This vulnerability gave them access to data, which had been there for four years. If our team had been a group of hackers, this breach would have cost the company more than $103 million in PCI fines alone. The interesting fact about this study is that the company had been getting "penetration testing" performed quarterly for more than four years by various notable companies. That is a total of 16 penetration tests by 7 different vendors that missed the vulnerability. Each penetration test prior to ours had relied heavily on automated tools to identify vulnerabilities. The pen testing teams would run automated scans and then perform manual tests of the results. The problem with that is automated tools only look for publicly known vulnerabilities in systems—leaving vulnerabilities in custom applications or undiscovered "zero day" vulnerabilities unidentified. Similar to an iceberg, most vulnerabilities are hidden from automated and compliance-driven vulnerability scanning and penetration testing. Taking an enhanced team approach to advanced penetration testing finds risks "below the surface" by manually emulating the aggressive actions of a hacker.

LAW

Connell Foley LLP
By Karen Painter Randall, Esq., Chair, Cybersecurity and Data Privacy Group

As a Breach Response Coach, Connell Foley leads the response effort under the attorney-client privilege after a ransomware attack by managing and coordinating the overall response efforts with the incident response team. This includes: properly preserving evidence; working with law enforcement, forensic vendors, IT, insurance and public relations experts to investigate, contain/eradicate, and assess incident severity; negotiating with the attacker; evaluating notification requirements pursuant to 50 state laws and regulations; and remediating the situation. It is extremely important to prepare for a ransomware attack in advance, especially with proper backup of data onsite, offsite and in the cloud. Response options include restoring files from backup, attempting to decrypt, doing nothing, or negotiating and/or paying the ransom. In evaluating response options, the enterprise must decide quickly whether to pay a ransom to retrieve sensitive data. The response decision will be dictated by the organization's readiness as reflected in its incident response plan and ransomware playbook. Connell Foley analyzes efforts post-breach to remediate and better prepare the enterprise in the event another incident occurs, and we defend businesses in regulatory enforcement actions and litigation stemming from a data breach.



continued on page 26

continued from page 24

CSG

By Michelle Schaap, Esq., Member, Privacy & Data Security Group

A client's employee was on leave—and, in theory, not working—with unrestricted access to the firm's systems and company-issued devices in possession. The client came to us seeking to terminate the employee for poor performance. Our Employment Group advised on how to terminate an employee on leave, making the client aware of the need to have a witness to the call. The CEO went on to terminate the employee with a VP as witness to the discussion—but as the termination call proceeded, the VP suddenly realized that thousands of company files were being deleted. Upon learning of this incident, I immediately went into damage-control mode, engaging forensic experts on the company's behalf to maintain attorney–client privilege. I also dispatched a courier to the employee's home to recover company devices, the employee's spouse's devices, a personal hard drive and passwords to the employee's and spouse's cloud accounts. All devices were recovered; and the forensic team removed more than 30,000 records from the employee's and employee's spouse's devices and accounts. We have since worked with the client to implement a "least rights" approach to access. Additional technological, environmental and operational measures have been implemented and documented to better secure the confidentiality, integrity and accessibility of the company's critical assets.

Fox Rothschild LLP

By Mark G. McCreary, Esq., Partner, Chief Privacy Officer

The Children's Online Privacy Protection Act of 1998 is a federal law that applies to the online collection of personal information about children under 13 years of age. The law provides what must be disclosed in a privacy policy, and importantly when and how to seek verifiable consent from a parent or guardian. Our client is a mobile application publisher of educational games for children. Unknown to our client, their analytics company received the unique device identifier (UDID) from users. The UDID is a 40-character string of characters created by the device manufacturer and tied to a specific device. Our client never had access to, and never saw, the UDIDs transmitted to the analytics company. The analytics company also received screen-names of players. The screen-name was intended to be a first name. For example,

continued on page 28

continued from page 26

parents typically enter "George" as opposed to "George Washington" when creating a screen-name. In a first of its kind action in the State of New Jersey, our client entered into a Consent Decree with the Attorney General of the State of New Jersey, agreeing to cease sharing information with third parties without parental or guardian consent. No fine was paid by our client.

Gibbons P.C.
By John T. Wolak, Esq., Chair, Privacy & Data Security Team

Despite proper planning and preparation, data security incidents happen. For the last 10 years, Gibbons has worked with clients to respond to and mitigate the effects of malicious activities and personnel mistakes. We recently served as data breach counsel leading the security incident investigation and response activities for a regional healthcare provider headquartered in New Jersey. The incident resulted in the potential disclosure of extensive patient health information and personal information spanning multiple years and involving several hundred thousand patients residing in 50 different jurisdictions. Immediately after being notified, we retained an independent forensics team to identify the nature and scope of the incident and confirm that the incident was properly contained. We worked extensively with the client's staff to ensure that the client could continue daily operations and properly treat patients. We also interfaced with local law enforcement and federal authorities at the Office for Civil Rights to ensure that the client met all applicable regulatory obligations, and that each patient's privacy and individual rights were properly safeguarded. After extensive analysis of the notification obligations in all 50 jurisdictions and under applicable federal law, we concluded that, based on all available information, no additional notification was required.

NPZ Law Group, P.C.
By David H. Nachman, Esq., U.S. Managing Attorney

Establishing and maintaining digital integrity should be a paramount concern across all industries. Cybersecurity breaches are not limited to large scale corporations which we hear about in the headlines. In reality, small and medium size organizations are often more vulnerable to digital security and privacy concerns. As an Immigration and Nationality law firm, we represent numerous U.S. IT companies that hire foreign national cybersecurity experts to reduce their company's risk of intellectual property theft, privacy breaches and cyber espionage. NPZ Law Group brings cyber security experts to live and to work in the United States with Intercompany Transfer visas (L visa), H-1B non-immigrant work visas, O-1 visas for individuals with Extraordinary Ability, and Treaty Trader visas, depending on the country from which the foreign national

continued on page 30

continued from page 28

comes. Data breaches are a tremendous liability and corporations are potentially responsible for paying out settlements for sloppy security practices, which is why many insurance companies offer policies to cover cybersecurity issues. The onus of responsibility is ultimately on every business to hire qualified individuals to establish and maintain digital security through policies, procedures, technology updates and training of personnel.

Riker Danzig Scherer Hyland & Perretti LLP
By Michael P. O'Mullan, Esq., Co-Lead Partner, Data Privacy and Cyber Security Practice Group

An existing client discovered that a security vulnerability on its web site had permitted access to certain information. The security vulnerability had been successfully patched and the company's investigation confirmed that there was a very low risk of impact to any customer data. Nonetheless, the company's European Counsel had determined that the incident was reportable under the European Union's General Data Protection Regulation (GDPR). They asked us to analyze whether the incident was reportable under U.S. law. After reviewing the patchwork of U.S. laws relating to data privacy disclosure, we concluded that the facts of the incident did not give rise to a current reporting duty under applicable U.S. law. We were also able to advise the company regarding regulatory guidance and evolving developments that might impact such an incident in the future.

Wilentz, Goldman & Spitzer, P.A.
By Brett R. Harris, Esq., Shareholder, Business, Nonprofit and Technology Attorney

We focus our legal services on cyber preparedness for the "not if, but when" being proactive rather than reactive in assisting clients in carrying out best practices for cybersecurity. Strategies include creating a "security culture" through employee training on practical common-sense policies for careful use of technology in the business. We support clients in assessing and implementing administrative, technical and physical security measures to manage risk of data breaches and malicious intrusions. Companies must act decisively and effectively to protect customers, employees and their brand from the potentially devastating impact of data breaches. We work with clients to develop incident response plans in advance, soliciting input from management, human resources, public relations, IT and legal perspectives to help minimize overall breach response costs and reputational harm and to ensure business continuity. ■