WILK AUSLANDER

Wilk Auslander LLP
1515 Broadway
New York, NY 10036

T 212-981-2300
F 212-752-6380
wilkauslander.com

December 21, 2020

RECENT DEVELOPMENTS IN CYBERSECURITY LAW AND THE STEPS THAT COMPANIES SHOULD TAKE TO LOWER THEIR RISK

The U.S. government recently suffered a major cyber-attack. Russian hackers appear to have infiltrated and stolen information from multiple government agencies, bypassing cybersecurity firm FireEye. While the scale of the theft is not yet clear, the attack demonstrates that even entities with some of the most sophisticated protections available may not be 100% safe.

Every organization that has trade secret, healthcare, financial, or any other kind of sensitive information should be taking immediate steps to assess its cybersecurity framework and reevaluate whether it is sufficient to meet the organization's risks. Cyberattacks can have wide-ranging effects that extend beyond theft of data, including customer litigation and government enforcement actions. Having the right policies and procedures can help organizations prevent an attack, mitigate harm during an attack, and contain post-attack fallout. This article focuses on recent developments in cybersecurity law and the concrete steps that companies should take to lower their risk.

Increased Threats Caused by COVID-19

Many Americans are now working from home due to the COVID-19 pandemic. The shift to working remotely has had major consequences for cybersecurity. Understandably, few organizations were prepared for a situation like COVID. Companies used to working in office spaces may not have set up reliable remote access systems that can handle the amount of traffic created when the entire workforce started working remotely.[i] Or, companies may not have provided a laptop to everyone who needed one, causing employees to rely on personal machines that may not have had the necessary safeguards, such as a secure remote login system or up-to-date antivirus software.

Now that employees are using more devices and different kinds of devices, including personal devices, malign actors' "attack surface," or the range of opportunities to steal data, has expanded. There are major vulnerabilities that did not exist before COVID.[ii] Not surprisingly, the rate of success of cyberattacks has increased as cybercriminals exploit opportunities created by the shift to remote work. As of September 1, 2020, in almost half of ransomware cases, the attackers gained access through the remote access systems, either through phishing emails or exploiting the system's vulnerabilities.[iii]

Business email compromise is almost as common as ransomware. Law enforcement agencies such as the FBI have warned that fraudsters are exploiting the uncertainty surrounding the COVID pandemic through business email compromise. For example, the FBI reported on April 6, 2020, that a bank received an email allegedly from the CEO of a company requesting that a previously-scheduled transfer of $1 million be moved up and the recipient account

changed due to the pandemic and quarantine precautions. The email address used by the fraudsters was identical to the CEO's actual email address, except for one letter.

Malign actors are also pursuing COVID-specific attacks. The government's efforts to respond to the pandemic have created new opportunities for bad actors, such as phishing attacks aimed at coronavirus stimulus check fraud. For example, on August 15, 2020, the Canadian government revealed that a cyberattack had stolen COVID relief payments out of almost 10,000 accounts. Other examples of COVID-specific attacks include malware that looks like COVID information or work-from-home resources. One strain of ransomware is using files with "coronavirus" in the name so that they look important. Or, hackers may send emails disguised as government emails or charity solicitations. Due to general interest in obtaining up-to-date information on the pandemic, people are more likely to click on links without checking the credibility of the source.

In short, it is more important than ever to make sure that your company's systems are secure. This means being familiar with various legal requirements, training staff properly, investing in security, and increasing awareness of cyber threats. Summarized below are some key points and issues that companies should consider when making cybersecurity decisions in the time of the COVID pandemic.

Duty to Employees

A trio of recent cases has made clear that companies owe a duty not just to their customers, but also to their employees, and should ensure that employee data is just as secure as customer data. In one case, *Dittman v. University of Pittsburgh Medical Center*, 196 A.3d 1036 (Pa. 2018), hackers broke into a hospital computer system in 2014 and stole the names, birthdates, Social Security numbers, salary records, and banking and tax information of 62,000 current and former employees. The hackers filed false tax returns in employees' names to receive refunds. The Pennsylvania Supreme Court held that the employer had a duty to act with reasonable care to safeguard its employees' sensitive personal information stored on an internet-accessible computer system. Specifically, the court found that because the hospital system collected and stored employees' information without implementing adequate security measures to protect against breaches, the breach was within the scope of risk created by the hospital system. The court remanded to the lower court to consider damages.

The *Dittman* case governs in Pennsylvania. Two other recent cases in New York and Kansas similarly found that employers have a duty to protect their employees' information. In *Sackin v. TransPerfect Global, Inc.*, 278 F. Supp. 3d 739, 748 (S.D.N.Y. 2017), a phishing attack in 2017 caused the release of employees' names, addresses, dates of birth, Social Security numbers, and bank account information. The court reasoned that employers are best positioned to avoid such incidents, because employees generally cannot protect information that is in the hands of their employers, and withholding their sensitive information is not a realistic option. Furthermore, in the event of a breach, employees (more so than employers) suffer the harm. In 2018 the court approved a class settlement that included identity theft protection valued at around $3.5 million. Similarly, in *Hapka v. CareCentrix, Inc.*, No. 16 Civ. 2372, 2016 WL 7336407 (D. Kan. Dec. 19, 2016), a breach led to the disclosure of employees' personal information; the court found that the employer had a duty to implement reasonable data security

measures because the harm was foreseeable. The court later approved a class settlement that included payments up to $5,000 per class member, credit monitoring services, and identity theft insurance.

What Companies Can Do to Meet the Cybersecurity Challenges of COVID-19

Every company that holds private information should make sure its cybersecurity program is designed to keep its data safe and comply with lawmakers' and regulators' expectations. The best way to meet the increased challenges and risks in the age of COVID-19 is to be prepared with a strong cybersecurity program, a written incident response plan, and a robust cybersecurity insurance policy. Even with these preparations, companies should expect to make ongoing efforts to foster a secure cyber environment.

A strong cybersecurity program will incorporate elements of zero-trust architecture. The guiding principle of zero-trust architecture is "never trust, always verify": treat every user as a potential threat and prevent access to data and resources until the user can be properly authorized and authenticated. The following are some of the key components of zero-trust architecture:

- Implement multi-factor authentication.
- Assess every device that accesses your company's network, whether or not it is a company device, to determine its trustworthiness. Devices that do not meet the minimum security and trust requirements set by your organization should be denied access.
- Users should be given access only to the extent needed to perform their jobs. Define, at a granular level, which users and devices can access particular applications, and under what circumstances.
- All activity must be logged and monitored, and any anomalies, including suspicious lateral movement, be immediately flagged.
- Network segmentation, where possible, can prevent a small breach from turning into a company-wide breach.
- Conduct regular penetration testing and risk assessments.
- Consider using a virtual desktop infrastructure (VDI) system for your remote workforce.

To complement these technological safeguards, every company with private information should have a written incident response plan. The plan should set forth the duties and responsibilities for every phase of response to a breach, from detection to communicating with law enforcement to recovery of the data. The plan should also provide for regular security reporting to the board and the CEO.

Fostering a safe cyber also entails ongoing work like continuously training employees on the threats they face. Phishing simulations can help employees understand best practices. Another ongoing task is to ensure the cybersecurity program is sufficiently funded to work as intended, and is considered part of budget planning.

As companies look towards returning to the office environment, they should consider their long-term cybersecurity needs. For example, having a remote workforce may make clear that certain devices, tools, and platforms need to be updated. Other companies that went remote due to the pandemic may have realized that they need to reevaluate IT staffing needs. Consider also what new vendors have been engaged to help respond to the pandemic, and whether these vendors are as protected as you are. For example, transitioning to cloud storage can improve security, but doing so also makes security a shared responsibility, so it is important to choose a vendor carefully.

Finally, if your company owns or licenses private information about consumers, consider cybersecurity insurance. While policies vary, many cover forensic investigation costs, business interruption costs, crisis management expenses, the costs of notifying clients, and the costs of PR firms and lawyers to address reputational and legal consequences. Some may also cover data restoration costs, the cost of the ransom (in the event of a ransomware attack), and regulatory penalties. Be aware that some policies may limit coverage if, for example, your company's software is not up to date. Insurers may also cover third parties only and not employees, have low limits, not cover fines, not cover prior acts, and have various other exclusions. Be aware of these limits when choosing a policy.

The SHIELD Act

Even before the pandemic, regulators and law enforcement were taking increased action to stop cyberattacks and protect consumer privacy. Enforcement efforts may increase given the cybersecurity concerns raised by COVID. The most notable development New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). The SHIELD Act is one of the most important data security to come into effect in recent years, and it applies to many companies – specifically, "[a]ny person or business which owns or licenses computerized data which includes private information of a resident of New York." All companies that own or license New Yorkers' private information should be aware of their duties and responsibilities under the Act, particularly given the new and unique risks posed by COVID-19.

The Act has two main parts. First, it made important changes to New York's pre-existing data breach notification law. These changes went into effect on October 23, 2019. Second, the Act imposed requirements on covered businesses to implement a data security program. The data security provisions went into effect on March 21, 2020.

Under the new breach notification rules, any covered business – meaning any business that owns or licenses private information of a New York resident, which includes most businesses with employees in New York – must provide notice to affected New Yorkers as quickly as possible if their data is breached. Notably, simply gaining unauthorized access to information, even if the information is not acquired, is enough to trigger the notification provisions.

Under the new data security provisions, the SHIELD Act requires that covered businesses have reasonable safeguards to protect the private information. The Act outlines the administrative, physical, and technical safeguards that are considered reasonable protections of private information. Examples of administrative safeguards include risk assessments and

employee training. Technical safeguards include regular testing and monitoring, and physical safeguards include properly disposing of private information after it is no longer needed.

While the SHIELD Act contains no general exception for small businesses, the law provides some relief for entities with fewer than fifty employees, less than $3 million in gross annual revenue in each of the last three fiscal years, or less than $5 million in year-end total assets. For such a business, the nature and extent of the security program can be reshaped as appropriate for the size and complexity of the business and the sensitivity of the information it collects. The SHIELD Act also has a narrow exemption for inadvertent disclosure by a person authorized to access the private information if the breach will not result in misuse of the information or financial harm. The business must make that determination in writing.

The Role of Sanctions in Cybersecurity

In addition, the Office of Foreign Assets Control (OFAC) recently set forth its views on how sanctions laws will be enforced in the cybersecurity context. On October 1, 2020, OFAC issued an advisory on the sanctions risks associated with ransomware payments. Hackers may be sanctioned or have a nexus to other sanctioned entities, so companies that facilitate payments to them (such as banks, cyber insurance firms, and companies involved in incidence response) may risk violating sanctions. While OFAC's advisory addresses companies that facilitate payments, as opposed to the victims of the attack, it appears to be directed to all parties – both victims and the companies that help victims deal with the attack. Because OFAC sanctions are a matter of strict liability, ransomware victims may face a difficult choice, but it remains to be seen whether OFAC will bring any enforcement actions against victims as opposed to the payment facilitators. OFAC encourages full and timely cooperation with law enforcement during and after an attack and considers cooperation as a "significant mitigating factor" when evaluating potential enforcement outcomes.

* * *

Wilk Auslander can help your company structure a cybersecurity program that will effectively lower your risk so that you can focus on your business. The firm advises on preparedness and legal requirements, and in the event of an attack, serves as a "first responder" by overseeing and coordinating with all relevant partners, from forensic experts to law enforcement. The firm also serves as legal counsel in the event litigation or an enforcement action follows. Contact Natalie Shkolnik for more information at 212-981-2294 or nshkolnik@wilkauslander.com.