Sills Cummis & Gross P.C.

Client Alert **Cybersecurity**

Third-Party Aspects of Cybersecurity Protections: Beyond your reach but within your control

Data privacy and cybersecurity issues are ongoing concerns for companies in today's world. It is nothing new to hear. By now, every company is aware of the existence of cybersecurity threats and the need to try to protect itself. There are almost daily reports of data breaches and/or ransomware attacks. Companies spend substantial resources to try to ensure the security of their confidential information, as well as the personal and confidential information of their customers, employees and business partners. As part of those efforts, companies are faced with managing and understanding their various legal and regulatory obligations governing the protection, disclosure and/or sharing of data – depending on their specific industry and the type of data they handle – as well as meeting the expectations of their customers to avoid reputational harm.

Despite the many steps involved in developing wide-ranging cybersecurity protocols – such as establishing a security incident response plan, designating someone to be responsible for cybersecurity and data privacy, training and retraining employees, and requiring passwords to be changed regularly – it is not enough merely to manage risks internal to the company. Companies are subject to third-party factors not within their immediate control, in particular vendors and employee BYOD (Bring Your Own Device). If those cybersecurity challenges are not afforded sufficient oversight, they will expose a company to significant risks that will undo all of the company's hard work trying to secure and defend its data from unauthorized disclosures or cyberattacks. Although companies may afford some consideration to vendor management and BYOD policies, absent

July
2017

rigorous follow up, a company may too easily leave a gaping hole in its cybersecurity protections.

VENDORS

To accomplish business functions and objectives and to improve services, companies regularly rely on third-party service providers and vendors. To that end, vendors may get access to and get control over confidential or personal information to perform the contracted services. That information may belong to the company, employees of the company, the clients of the company and/or business partners of the company.

When information is placed into the hands of a vendor and/or onto its computer systems, stored in its facilities, or handled by its employees or business partners, the information is subject to unknown risks based on what could happen to the information while with the third-party. The possibility of a security breach or the unauthorized use or access to the information still exists but a company cannot be sure what the vendor will do to protect against or address those dangers if they arise. A company cannot rely on its vendors to maintain necessary security protocols and instead must be vigilant by exercising reasonable due diligence over its vendors and instituting appropriate protections. To achieve this task, a company needs to consider the type of information involved, the level of protection required, the risks at issue and how those risks can be managed and mitigated.

Due Diligence | A company must perform due diligence over the vendor and the services to be provided and should consider, among other things, supplying a questionnaire to the vendor to answer a host of cybersecurity related questions including:

- *What services will the vendor provide?* Gain an understanding of the services being provided by the vendor, including whether the vendor only gains access to, or actually takes possession of, any information. There is an important difference between a vendor (i) having access to a company's network to implement a third-party solution or provide a third-party service and (ii) taking possession of and/or storing information on its network or even the network of its own third-party vendors.
- *Who will have access to the information?* A company should know who at the vendor will have access to the information. Which employees? Will the vendor need assistance from other third-parties to provide the contracted-for services? Does the vendor perform background checks

of its employees? Do protocols exist to prevent employees who are not authorized from having access to the information?

- *What security controls does the vendor have in place?* A company should review the vendor's controls and procedures to make sure they comply not only with applicable legal and regulatory requirements but also with the company's own standards. Does the vendor have the financial wherewithal to manage cybersecurity risks? Does the vendor have cybersecurity insurance? Does the vendor have a security incident response plan? To what extent has the vendor trained with or used the plan? Has the vendor suffered a cyberattack? If so, it actually may be a good thing depending on how the vendor responded to the attack and what, if anything, it did to improve its security following the attack. What training is in place for the vendor's employees? How is the vendor monitoring itself to ensure compliance with its own procedures?

The Contract | A company should seek to include strong contractual language to obligate the vendor to exercise its own cybersecurity management and to cooperate with the company to ensure protection of the company's data. There are multiple provisions to consider when engaging vendors and drafting or updating contracts to afford the company appropriate protections. A one-size-fits-all approach for vendors will not work and clauses will need to be modified to take account of, among other things:

- *The sensitivity of the information at issue* – Does the information include only strictly confidential information, such as trade secrets or news of a potential merger? Does the information include personal information, such as names, signatures, addresses, email addresses, or telephone numbers? Does the information include what is considered more highly sensitive personal information, such as SSNs, financial account information, credit card information, tax information, or medical data?

- *The standard of care and obligations for the treatment of information* – A company should want its vendors to meet the same standards the company demands of itself. Vendors should be required to acknowledge that they will have access to or will take possession of information and that they will use reasonable care to perform their services, including the collection, access, use, storage, disposal, transmission and disclosure of information, as applicable. This can, and often should, include: limiting access to only necessary employees; securing business facilities,

data centers, paper files, servers and back-up systems; implementing database security protocols, including authentication and access controls; encrypting highly sensitive personal information; and providing privacy security training to employees. Contracts also should provide that vendors are responsible for any unauthorized receipt, transmission, storage, disposal, use, or disclosure of information, including the actions and/or omissions of their employees and/or relevant third-parties who the vendors retain.

- *Expectations in the event of a security breach at the company* – A company should include a provision requiring a vendor's reasonable cooperation if the company experiences a breach. A company should have a contact at each of its vendors, who is available 24/7 to help resolve a security breach. Compliance with a company's own obligations to deal with a breach (including notification or remediation) could be delayed if a vendor refuses to timely provide necessary information or copies of relevant documents. A company also can negotiate to include an indemnification provision requiring a vendor to reimburse the company for reasonable costs incurred in responding to and mitigating damages caused by any security breach related to the work performed by the vendor.

- *Expectations in the event of a security breach at the vendor* – A company should demand reasonable notification if the vendor experiences a security breach and require the vendor to take reasonable steps and use best efforts to remediate the breach and to try to prevent future breaches. A company should negotiate for a provision permitting the company to audit the vendor's security procedures and perhaps even to physically inspect the vendor's servers and data storage facilities if the data at issue is particularly sensitive.

Monitoring | Due diligence and contractual provisions are necessary steps in managing the cybersecurity risks that a vendor presents, but absent consistent and proactive monitoring of the vendor relationship, including periodic audits and updates to vendor contracts, all prior efforts to protect the company in this respect will be undermined. Determining who within the company is responsible for the relationship – HR? Procurement? Legal? – is critical to help manage the vendor relationship.

- *Schedule annual or semi-annual reviews of the vendor relationship* – A company not only should confirm that the vendor is following its

cybersecurity protocols but also should inquire if any material changes to those protocols have been instituted that impact the manner in which the vendor handles the company's data. Depending on the level of sensitivity of the data being handled by the vendor, a company may consider retaining a third-party reviewer to evaluate the vendor.

> *Update the vendor contract, as necessary* – A company employee should be responsible to review vendor contracts annually to determine if any changes are necessary in view of cybersecurity concerns.

BYOD

Ransomware – where a hacker demands a ransom to unencrypt a company's data caused by malicious software that the hacker deposited onto the company's network to hold it hostage – certainly is a heightened concern for all companies. It is the fastest growing malware targeting all industries, with more than 50% growth in recent years. Every company is wary of ransomware and is trying to do as much as possible to protect itself from hackers. The best practices against ransomware are to (i) periodically train and retrain your employees to be on the lookout for ransomware; (ii) constantly backup you data systems; and (iii) split up the locations where data is maintained to limit the damage in the event some servers fall victim to ransomware. One thing that easily is overlooked, however, or is afforded more limited consideration, is a company's BYOD policy and enforcement of that policy.

Permitting a company's employees to use their own personal electronic devices to work remotely will lower overhead costs and improve efficiency but will bring a host of security and compliance concerns. The cybersecurity and privacy protocols that the company established and vigorously pursues inside the company must also be followed by its employees when using their personal devices – home computers, tablets, smartphones – outside the company. Employees likely are more interested, however, in the ease of access to work remotely than in ensuring that proper cybersecurity measures are followed with respect to their personal devices. Are the employees using sophisticated passwords on their personal devices or any passwords at all? Do the employees' personal devices have automatic locks? Are the employees using the most current software and installing security updates?

These concerns are real. In May of 2017, the Wannacry ransomware attack infected more than 200,000 computers in over 100 countries, incapacitating companies and hospitals. Hackers took advantage of the failure to install a patch to Microsoft Windows, which Microsoft had issued weeks earlier. Even worse, it was discovered

that some infected computers were using outdated versions of Microsoft Windows for which the patch would not have worked regardless. Companies cannot risk pouring significant resources into establishing a comprehensive security program only to suffer a ransomware attack or otherwise to have its efforts undercut by an employee working remotely who failed to install appropriate security protocols on his/her personal devices.

The dangers to be wary of include, among others:

- Personal devices may not automatically lock or have a timeout function.
- Employees may not use sophisticated passwords to protect their personal devices.
- Employees may use unsecured Wi-Fi hotspots to access the company's systems, subjecting the company to heightened risk.
- Employees may access the company's systems using outdated software that is vulnerable to cyberattacks.

Combatting the Dangers | To address the added risks that accompany allowing BYOD, a company must develop, disseminate and institute a comprehensive BYOD policy. That policy should identify the necessary security protocols that the employee must follow to use a personal device to work remotely, including, among other things:

- Sophisticated passwords
- Automatic locks
- Encryption of data
- Installation of updated software and security apps
- Remote access from secure WiFi only
- Reporting procedures for lost/stolen devices

A company also should use mobile device management technology to permit the company to remotely access the personal devices of its employees to install any necessary software updates or to limit access to company systems. Of course, the employee must be given notice that the company may use such technology and the capabilities of that technology. Among other things, mobile device management technology can:

Client Alert Cybersecurity

- Create a virtual partition separating work data and personal data
- Limit an employee's access to work data
- Allow a company to push security updates onto an employee's personal device

Enforcement | Similar to vendor management, the cybersecurity efforts undertaken by having a robust BYOD policy in place, or even using mobile management technology, are significantly weakened unless a company enforces the policy it has instituted.

- A BYOD policy should be a prominent part of any employee cybersecurity training.
- The company should inform the employee of the company's right to access/monitor/delete information from an employee's personal device in the event of, among other things, litigation and e-discovery requests, internal investigations, or the employee's termination.

CONCLUSION

Implementing the above recommendations will not guarantee a company will not suffer a breach but will stem the threats created by third-party aspects of its cybersecurity program. Even if a company ultimately suffers a breach, having had these protections in place to administer the risks associated with vendor management and BYOD certainly will help safeguard the company from the scrutiny of regulators or the criticism of their customers, which would be worse!

If you have any questions regarding information in this alert, or if you need more information, please contact the following Sills Cummis & Gross attorney:

Joseph B. Shumofsky, Esq.
Chair, Cybersecurity and Data Privacy Practice Group
jshumofsky@sillscummis.com | (973) 643-5382