Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Cybersecurity

Contributing Editor
Alan Charles Raul
Sidley Austin LLP

chambers.com

2020

INTRODUCTION

Contributed by: *Alan Charles Raul,* ***Sidley Austin LLP***

Governments around the world are increasingly imposing ever-more comprehensive and granular cybersecurity obligations, shorter-deadline data breach notification laws, and sizeable enforcement fines and penalties. None of this has proven sufficiently effective at reducing the epidemic of data breaches, hacks, cyber-intrusions and data breaches, including from recent trends in ransomware demands and business email compromises.

Since governments are not yet ready – or perhaps not even capable of – saving citizens and companies from cyber-criminals and nation-state hackers, here are some practical suggestions that companies could consider to reduce their likely vulnerabilities and help defend themselves from the legal, operational and reputational risks. While some of it is US-specific, much of it is of wider application, whether directly or indirectly.

Do This as Soon as You Can...
Enable effective system monitoring and a solution to analyse and meaningfully act upon the increased volume of information.

Impose multi-factor authentication for remote access to your networks and email systems.

Educate (and re-educate) employees to resist and report phishing attacks designed to access user credentials or sensitive data, or to trick personnel into clicking on malicious links.

Inventory or "map" your valuable data and systems, determine whether you have properly prioritised protecting them, and make sure your software patching program is up-to-date and sufficiently comprehensive.

Implement a "vendor management" program, and make sure you monitor and contractually bind service providers to adhere to your cybersecurity (and privacy) standards.

Conduct table-top simulations of cyber-attacks to practice your incident response protocols and educate employees as to what they would face in a real incident and how they need to work together.

In the USA, rely on the Cybersecurity Information Sharing Act of 2015 to monitor networks, implement cybersecurity defensive measures and share cyber-threat information "notwithstanding any other provision of law".

Implement and Be Prepared to Demonstrate Reasonable Security
Numerous US state laws (such as New York, California and Ohio) and federal agency enforcers (such as the Federal Trade Commission) require companies to provide "reasonable security" to protect sensitive personal information. The New York SHIELD Act specifies what constitutes "reasonable security" in highly specific detail. The Ohio law provides details and options for achieving "reasonable security" and provides companies with an affirmative defence against state tort actions for those that do.

More ominously, the 2018 California Consumer Privacy Act does not specify what constitutes "reasonable security", but does expose companies that suffer data breaches resulting from the failure to implement "reasonable security" to private litigation with potentially bankrupting statutory damages. In 2016, however, then California Attorney General Kamala Harris (who is now a US Senator and a former presidential candidate) issued a formal report providing some helpful guidance and perspective on "reasonable security". (Report issued by the California Attorney General in February 2016, available at https://oag.ca.gov.) Accordingly, companies would do well to take her commentary to heart and consider the following.

Companies should implement and maintain reasonable security practices and procedures appropriate to the nature of the personal information they collect, use, retain, transfer or otherwise process. A reasonable security process would be implemented and maintained in accordance with applicable law and relevant standards as outlined in the Attorney General Report. For example, as set forth in the 2016 Report, among other safeguards, a reasonable security process would implement the Center for Internet Security's Critical Security Controls for Effective Cyber Defense as identified in Appendix A of the California Attorney General Report.

Significantly, however, as also noted in that Report, "there is no perfect security". The Attorney General expressly acknowledged this, and stated that reasonable security is a process that involves risk management and risk reduction, rather than risk elimination. Therefore, companies should be prepared to defend against California data breach actions by pointing to their commitment to developing, implementing, maintaining, monitoring and updating a reasonable information security program, but explain to consumers that, as noted by the Attorney General, no such program can be perfect. In other words, all risk cannot reasonably be eliminated. Data security incidents and breaches

can occur due to vulnerabilities, criminal exploits or other factors that cannot reasonably be prevented.

As stated in the Attorney General Report, "implementing the [CIS] Controls will not prevent every attack, but it will significantly reduce the risk". Accordingly, while corporate reasonable security processes should be designed to manage data security risks and reduce the risk of data security incidents and breaches, it cannot be presumed that the occurrence of any given incident or breach results from a company's failure to implement and maintain a process for reasonable security.

In any event, companies would be well served to map their information security programs to the standards specified in the New York SHIELD Act and the 2016 California Attorney General Report, and other recognised cybersecurity frameworks (such as those of the National Institute for Standards and Technology).

Conduct a Cybersecurity Governance Review

Company counsel should review their company's cybersecurity processes, protocols and other significant documentation (eg, policies, reports to the Board, incident response plans, risk assessments, audits, etc) to identify potential governance or compliance gaps and areas for improvement and, potentially together with a cybersecurity forensic firm, review their cybersecurity program and risk assessments from a technical perspective as well. The purpose of this type of cybersecurity legal governance review would be to provide legal advice regarding the company's compliance obligations as well as to prepare for defence of potential claims, enforcement or litigation challenging the company's current practices – especially after a data breach has occurred. This governance review and cybersecurity assessment should be conducted pursuant to attorney-client privilege and attorney work product confidentiality protection.

Possible work products could include: (i) summaries of applicable cybersecurity legal requirements; (ii) comments on and proposals of possible revisions to the company's core documents; (iii) high-level assessments of compliance against industry accepted third-party standards and defensibility of the information security controls; and (iv) recommendations and next steps to further strengthen the company's program and governance posture.

Cybersecurity and Incident Response Assessment

In the spirit of practical guidance, the following are some elements that companies should focus on in assessing their cybersecurity program and incident response protocols.

Information collection

- Summaries or overview of information security programs;
- copies of written information security plan(s);
- recent cybersecurity risk assessments and audits;
- board presentations on cybersecurity;
- public filings and statements on cybersecurity;
- history/experience of cyber-incidents, including phishing and business email compromise;
- organisation charts noting personnel with privacy and cyber-responsibilities;
- analysis of legal, contractual and regulatory obligations on cybersecurity;
- prior or pending regulator examination letters or similar material, inquiries, litigation, and investigations regarding cybersecurity or data breaches;
- employee manual or handbook (or relevant sections);
- insider threat program;
- existing incident response plans or crisis management plans;
- cyber-insurance contract;
- agreements with key vendors and other third parties;
- vendor management and oversight program, and data security contractual requirements;
- training materials and table-top simulations regarding cybersecurity and privacy;
- audits and risk assessments of cybersecurity programs;
- penetration test reports;
- website security protocols and assessments;
- reports to and mandates from CEO, GC, CIO regarding cybersecurity;
- data leakage programs; insider threat programs; anti-phishing programs;
- other material identified as intrinsic to obtaining a fundamental understanding of the company's cybersecurity program.

Initial participant determination

Understand and identify the key participants in a scoping project, and conduct interviews of key personnel with the following responsibilities: relevant divisional or business unit leaders regarding cybersecurity and incident response; the chief information security officer; the legal/regulatory/compliance officer.

Analysis and recommendations

In the longer term, it is sensible to focus on the following:

- cybersecurity governance structure;
- board engagement and knowledge;
- documentation demonstrating "reasonable security";
- SEC and public filings on cybersecurity;
- employee training;
- information security regulatory compliance and management;
- incident response readiness;
- sufficiency of existing documentation, policies, and procedures;

- contractual obligations;
- vendor due diligence and oversight;
- posture of technical safeguards, tools, deployments, etc (as assessed with forensic experts);
- legal vulnerabilities;
- legal defensibility.

Get Ready to Act When You Are Attacked by Ransomware

In the immediate aftermath of a ransomware incident, the most important elements are containment and recovery, in other words to preserve forensic data, and plan to limit business disruption through work-arounds or alternative channels. Top priorities should be to consider bringing in a third-party forensic vendor to assess systems and malware – such a vendor may be able to identify the ransomware and the threat actor – and identifying the system vulnerability and what steps can be taken to close it.

Another important question companies face is whether to pay the ransom. The FBI advises against this, but recognises that companies sometimes have to do so. While there is no exact science on whether companies decide to pay, it is usually based on the importance of the ransomed data to their ongoing operations, whether there are usable back-ups, the amount of the ransom demand, and whether the attacker will actually follow through on decrypting the data (which the forensic vendor may be able to help assess). Any ransom payment should be discussed with the board of directors. To pay the ransom, a company will typically need a vendor with a bitcoin wallet; the forensic vendor may be able to provide this service.

Checking the OFAC list to establish whether a criminal is on the sanction list is another option, as indeed is negotiating with an attacker to lower the amount of the ransom demand and to have the attacker demonstrate that it is capable of decrypting the frozen system by doing so for a sample file. Other important topics include the following: notifying the insurer; notifying law enforcement (ie, the FBI); and considering any updates to SEC filing disclosures.

After the immediate focus on containment and recovery, the focus very quickly (ie, within 24-48 hours) should shift to external data breach notification needs. The key question is whether the ransomware malware is known or not known to seek to exfiltrate data. Is the ransomware a feint to cover another ongoing attack? The forensic vendor should be able to provide guidance on this, including by looking at the vector of attack, the nature of the malware, whether there was escalation, etc. If there was no exfiltration, it is less likely notifications will be necessary.

Nonetheless, it will be necessary to consider a number of different potential notification obligations, including at least the following: (i) state and (if relevant) international notification requirements for breaches of personal information; and (ii) notifying business partners or counter-parties.

Going Forward

Looking ahead, the longer-term project of assessing what steps should be taken to help prevent recurrence need to address the following issues: back-ups and resiliency; anti-phishing training; multi-factor authentication; anti-intrusion systems and safeguards as well as detection; restoring customer relations with business partners, counter-parties and customers; and detailing the lessons learned on minimising business disruption.

Every corporate cybersecurity program must, of course, fit the company's own risk profile and threat environment. Nonetheless, the steps recommended above should help provide corporate counsel with a practical framework to assess their company's state of cyber-preparedness on some key cyber topics. Anticipating and planning for these risks will also help the company defend itself in the event an incident triggers legal scrutiny.

INTRODUCTION

Contributed by: Alan Charles Raul, ***Sidley Austin LLP***

Sidley Austin LLP is a global law firm with 2,000 lawyers in 20 offices around the world. The firm's privacy and cybersecurity group has more than 70 professionals across offices in the USA, London, Brussels, Hong Kong, Singapore and Tokyo. Sidley Austin represents clients in a broad range of sectors, including financial services, life sciences and healthcare, communications and media, information service providers, professional services and internet companies. The firm undertakes highly sophisticated legal counselling and advocacy, and provides actionable legal advice on challenging and novel questions of privacy and information law. Sidley's lawyers focus on privacy, data protection, information security, internet and computer law, e-commerce, consumer protection, outsourcing, competitive intelligence and trade secrets, information management and records retention, and responding to cybercrimes and network intrusions. The team also handles litigation and government investigations; crisis management and incident response; compliance and regulatory counselling on all data protection laws, such as GDPR and CCPA; legislative and policy developments; and international data transfers.

Contributing Editor

Alan Charles Raul is a partner and the founder and leader of Sidley's privacy and cybersecurity practice. He represents companies on federal, state and international privacy, cybersecurity and digital technology issues. His practice covers global data protection and compliance programmes, data breaches, crisis management, consumer protection issues and internet law. Alan advises companies on cybersecurity preparedness and digital governance, and on litigation, regulatory defence, internal investigations and policy advocacy. He handles consumer class actions, enforcement matters and public policy involving the FTC, State Attorneys General, the SEC, the FCC, the DOJ, international data protection authorities and other government agencies. Alan is a member of the American Bar Association's Cybersecurity Legal Task Force, the Technology Litigation Advisory Committee of the US Chamber Litigation Center, the PLI's Privacy Law Advisors Group, the governing Board of Directors of the Future of Privacy Forum and the Center for Democracy and Technology's Advisory Committee.

Sidley Austin LLP

1501 K Street, N.W.
Washington, DC 20005

Tel: +1 202 736 8477
Email: araul@sidley.com
Web: www.sidley.com

SIDLEY