DATA BREACH STARTER KIT

ESSENTIAL CONSIDERATIONS TO REDUCE RISK

Maureen Frangopoulos and Colin Gainer SmithAmundsen

INTRODUCTION

Target, Home Depot, and Sony are just some of the corporations that have made headlines in the recent past not for their services, but for their exposure to large data breaches. Even with continuing advances in data security, data breaches remain a serious risk to companies, and the large breaches continue to make headlines.

From human error to cyber terrorism, there is a broad area of data risk that companies must traverse in order to defend against data breaches. Unfortunately, the risk appears to be proportional to data usage, and data consumption is not slowing down. The Internet, mobile devices, and cloud-based data storage are just some examples of technology that have spread rapidly in the corporate world, and these technologies all carry inherent data breach risks.

Moreover, the government is well aware of the risks posed by data breaches, and it often looks to businesses to carry the burden of protecting data disclosed or obtained from individuals. A company's failure to do so may not only result in regulatory action, it can also damage a company's reputation. Therefore, businesses need to implement data prevention plans, and they also need to be prepared to respond quickly to a data breach, if one occurs.

LESSONS FROM REGULATORY ENFORCEMENT AND DEFINING "REASONABLE SECURITY"

In the area of regulatory enforcement against companies, the Federal Trade Commission has emerged as the lead enforcer of privacy violations by utilizing its Section 5 authority. To those companies developing and revising their privacy plans, a common concern is the lack of an explicit set of standards from the FTC which outlines what the agency is looking for regarding "reasonable security." The lack of standards is a common discussion topic in the industry.

In lieu of a set of standards, the FTC points companies in the direction of its enforcement actions and resulting settlements for guidelines on what will *not* encompass "reasonable security" to try and then piece together what should constitute "reasonable security." Privacy professionals have started to compile a list of presumed standards pursuant to these enforcement actions from a comprehensive study of them.[1] We will not delve into an exhaustive overview of all a company should be doing in light of what the FTC has said in the past during enforcement actions, but below is a summary of the top "must haves" as we interpret them from data security settlements with the regulatory agency.

First and foremost, a company must develop a privacy program with designated leaders including a chief privacy officer to enforce a company's privacy policies within an organization. Privacy policies and data security should be considered and integrated into any new business product, model, plan, etc. rather than the afterthought of a business decision. A company should routinely audit its existing privacy and security practices, preferably utilizing a third-party auditor, for assessment of a company's compliance with its program. An organization's privacy and security leaders should continuously focus on risk considerations and keep adequate records of their assessments.

Second, a company must keep its privacy promises. We routinely see the FTC cracking down on companies when they break privacy

promises and fail to enforce their own privacy programs. The FTC also keeps a close eye on a company's business decisions that could implicate their privacy promises (i.e. Facebook's acquisition of WhatsApp). Advising consumers of policy changes and respecting user choices are a must.

Third, take a hard look at general security to safeguard data such as a company's password requirements, encryption procedures, unauthorized detection methods, and software use to comply with industry standards. For example, simple measures such as assigning unique passwords and login abuse detection systems prevent attacks against user credentials. Ensure antivirus software is updated and firewalls are active. Encryption and e-mail authentication on incoming and outgoing e-mail should be used. Mobile devices also need to be considered. Requiring authentication to unlock a device, locking out a device after a set number of failed attempts, using encrypted data, and remote wipes of lost or stolen devices are all prudent methods to minimize risk. The development of a data breach prevention plan is ongoing, and a business must regularly test its systems to check the vulnerability for breach. The plan must also be updated in response to the vulnerabilities exposed during these tests, as well as in response to changes in data breach security standards external to the company.

Furthermore, some basic guidelines for the collection of personal identifying information are only to collect/retain what is needed to complete the required task and allow minimum access to avoid inadvertent disclosure by employees. Retain information for a reasonable time period and destroy in a manner that renders personal identifying information undecipherable.

Lastly, it is absolutely clear in the industry that employee training on privacy policies and data security is a must. This training should be done routinely (at a minimum, yearly) and not just with an employee's on-board training. Employees should know about the type of data retained, the risks associated with it, detecting and reporting, and breach response. It is wise for a company to have a comprehensive privacy program, but this program is useless without adequate training to enhance compliance with it.

Looking forward, the next wave of security concerns will likely focus on the issues a company faces with cloud computing and we will probably see an increase in future FTC settlements dealing with enforcement in this area. Cloud computing presents a whole different set of privacy and security risks and a company must be aware of those in the contract stage so as to negotiate in its best interests.

THE INEVITABLE DATA BREACH AND THE POST-BREACH RESPONSE

Even with reasonable security, the inevitable data breach will occur. In the event of a breach, a response plan is necessary, as it enables a business to move quickly to assess the situation of the breach and mitigate damages. A written breach response plan needs to be developed and should identify the employees that will be handling each incident – the response team. Ideally, the response team should be comprised of employees knowledgeable in the company's technology infrastructure and its management, as well as employees involved in legal and public relations. The plan should also cover procedures on preserving evidence, limiting exposure, handling internal and external communications about the breach, and compliance with applicable regulations (e.g. data breach notification rules). The plan should be tested at least quarterly with the key breach response players to ensure everyone knows their role, should a breach occur. This testing can include running through different breach scenarios to see whether the team thinks a particular incident would trigger notification to law enforcement, the public, etc.

Preservation of evidence is a critical early step in responding to a breach. An employee, or consultant, with data forensic skills needs to be utilized to assess the details of the breach, such as the type of breach and its scope. Determining what types of data have been exposed will guide the course of the response. For example, a breach concerning protected health information will activate mandatory reporting requirements. It is recommended to have a working list of forensic experts, who have all been properly vetted, so you know the price scheme ahead of time and how you will work together post-breach. Often, these experts are a great tool to guide you through the steps, in conjunction with outside counsel, to handle a breach response.

A business needs to be knowledgeable with all applicable state statutes and federal regulations. As mentioned in the example above, a business may have a duty to notify individuals, law enforcement, and/or administrative agencies. Data breach reporting laws also vary from state to state, and multiple state laws or regulations may be involved, depending on the scope of the breach. In addition, credit monitoring services may also be required to be provided to affected individuals.

Insurance issues should also be addressed in the early stages of a breach. If a company has data breach coverage, it should contact its insurer immediately to report the claim and trigger coverage. Moreover, insurers are often experienced with data breaches and may provide additional assistance or guidance.

Depending on the circumstances, outside counsel should strongly be considered. Importantly, counsel can perform an investigation of the breach in a way that maintains confidentiality of communications with the attorney-client privilege. Outside counsel also can determine what regulatory compliance issues are involved, which may avoid or reduce fines, penalties, and audits.

CONCLUSION

As data breaches become more sophisticated, a company must be vigilant in protecting its data, and having a comprehensive data security and privacy program is a necessary component of the corporate world these days. No program exists that will make a business completely risk-free, but a successful program will equip a business with the knowledge and tools necessary to minimize the risk as well as the damage that can occur in the aftermath.

Colin Gainer is an attorney with SmithAmundsen in Chicago. A member of the Data Security & Breach team, Colin counsels health care entities on patient privacy concerns, electronic medical records and HIPAA and HITECH compliance.

Maureen Frangopoulos is an attorney with Smith Amundsen in Chicago. As part of the Data Security & Breach team, Maureen addresses privacy issues, helping her clients to implement sound data practices and work through the myriad of issues resulting from a breach.

[1] *See* Bailin, Patricia "Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices," International Association of Privacy Professionals, Sept. 19, 2014, *available at* https://privacyassociation.org/news/a/study-what-ftc-enforcement-actions-teach-us-about-the-features-of-reasonable-privacy-and-data-security-practices/.