Revamping Your Cybersecurity Policies and Procedures: Tips and Tricks

As each year passes and technology advances, businesses face an increasingly difficult task to maintain adequate security measures to protect their organizations' assets and data. With this in mind, it is important to review your cybersecurity policies and procedures at least annually to ensure they are up to date and reflect advancements in technology and the changes in the law. There is no better time than Cybersecurity Awareness Month to review your organization's policies and procedures. Below, we outline the importance of having proper cybersecurity policies and procedures in place and some best practices.

Importance of Policies and Procedures:

Cybersecurity policies and procedures are important administrative safeguards that help to prevent cybersecurity incidents and mitigate harm resulting from a data breach. These policies and procedures, including incident response plans, data breach policies and information security procedures, help employees and organizational leaders better understand how to maintain the security of the organization's network, applications and data, and provide a plan detailing how to respond in the event of a cybersecurity incident. Cybersecurity policies and procedures also play a critical role in an organization's credibility. Customers, partners, investors, shareholders, prospective employees and others want evidence that the organization can protect sensitive and personal data. Without proper policies and procedures, an organization may not be able to provide such evidence. Further, a data breach, if not handled properly, can cause reputational damage to an organization. As a result, having proper policies and procedures allows companies to react expeditiously to mitigate any reputational harm that may occur as the result of a breach. Similarly, organizations may face legal action after a data breach occurs. Proper policies and procedures assist in counteracting potential litigation claims and action from state authorities.

Incident response policies, written information security plans, business continuity plans and data governance procedures are especially important for organizations that operate in heavily regulated industries, such as health care, finance or higher education. For example, the Gramm-Leah-Bliley Act (GLBA), the New York Department of Financial Services Cybersecurity Regulation (NY DFS), Health Insurance Portability and Accountability Act (HIPAA), consumer privacy laws and many other laws, regulations and standards outline policy and procedural requirements that regulated entities must meet to ensure compliance. These types of organizations not only run the risk of a costly data breach, but also large regulatory penalties, loss of funding or reputational harm if they do not have adequate policies and procedures in place that meet regulatory requirements.

Even organizations operating outside of highly regulated industries often have a minimum standard for cybersecurity they are expected to maintain. For example, many states, including but not limited to New York and Massachusetts, have instituted mandatory minimum security requirements for organizations conducting business and handling the personal information of individuals located

within their states. Many of these laws, such as the New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD Act), govern all types of businesses, even small businesses, requiring security that is proportional to their size and risk. If an organization fails to properly implement these minimum standards and experiences a data breach, the organization could be deemed negligent and investigated and fined by state attorneys general.

Best Practice Tips:

Unfortunately, no single procedure or policy alone can ensure protection. As such, it is critical for organizations to implement multiple policies that work together and encompass legal requirements and best practices to maintain a comprehensive cybersecurity program. Below are some best practices that organizations should consider when implementing or revising cybersecurity policies and procedures.

One of the most important steps an organization can take to protect itself is to implement regular and continuous training of employees. In 2023, 68% of data breaches that occurred involved a human element, such as a person falling victim to a social engineering attack or making an error.[1] Your employees are often your first line of defense. As a result, having a policy that requires employees to complete adequate training in relation to suspicious emails and general cybersecurity is imperative. Additionally, promoting the use of strong passwords, software updates and other "tech hygiene" practices is also important.

Furthermore, it is imperative to ensure policies regarding security, such as access control policies and information security policies, are consistently reviewed and revised – taking into consideration changes in the business, new circumstances or new best practices or legal requirements. Identification of reasonably foreseeable internal and external risks is also important. Regular reviews to identify risks through practices such as risk assessments, penetration testing, vulnerability scans or other reviews will allow for policies and other safeguards to be updated to protect against any identified vulnerabilities or risks. The frequency, duration, and type of reviews should be outlined in an organization's information security plan.

In addition, 2023 saw a large increase of data breaches affecting organizations' vendors that store or process information on the organizations' behalf, such as hosting or infrastructure partners or data custodians.[2] As a result, having a proper vendor due diligence policy and process in place, including review of their cybersecurity practices and contracts, is imperative to ensure proper security and remedies in the event of an incident.

Finally, one safeguard that is often neglected is disposing of personal and other sensitive information when it is no longer needed for business purposes. Proper disposal of unnecessary information and having an up-to-date data retention and destruction policy, is a key way that organizations can reduce risks of a large data breach occurring.

Cybersecurity Awareness Month is a great time to review your organization's policies and procedures to ensure they are up to date and reflect best practices. Bond attorneys regularly assist

1 Verizon Business 2024 Data Breach Investigation Report
2 Verizon Business 2024 Data Breach Investigation Report

and advise clients concerning drafting and revising policies and procedures, and on an array of other data privacy and cybersecurity matters. If you have any questions about the information presented in this memo, please contact Amber Lawyer, CIPP/E/US or Shannon Knapp, CIPPA/A/US.

Special thanks to associate trainee Leah Dawit for assisting with this memorandum.