2023 Dr. Diane M Janosek, Esq.
TOP CYBER NEWS

Resources for Cyber Compliance

In the *Top Cyber News Magazine, Aug 2022 issue*, I discussed "Effective Cyber Compliance" and the steps to achieve an effective compliance program. It is well accepted that in today's digital consumer and transactional environment, a top priority is to protect all sensitive business proprietary information. It is equally important to protect consumers' and partnering service providers' data. This data protection security expectation is now non-negotiable as data breaches continue to skyrocket globally. Businesses must demonstrate active cybersecurity compliance programs. Regulators, shareholders, and customers demand it.

The Cost of Cyber Noncompliance

If one thinks cyber compliance is expensive, try non-compliance. Estimates for the global average cost of a data breach keep increasing by order of magnitude.

International, U.S., and state regulations, as well as third party data sharing agreements, all mandate that businesses know what data they have, why they have it, if consent was given, where the data is stored, who has access to the data, and why they have access. A strong data governance and protection plan makes business, ethical, and common sense.

Cyber compliance regulations are now being imposed to ensure a proper level of investment. Businesses must have visibility into their systems to act proactively, not just react. On 30 January 2023, *The Washington Post Cybersecurity 202* confirmed for the businesses that operate in the United States stricter regulation is coming to include mandatory reporting and response plans. Companies will need to warrant or ensure with certainty they have an active program that is proportionately invested at the level necessary to protect the criticality of their data at rest and in transit.

One example of the cost of non-compliance is the State of New York fined an online clothing retailer almost $2M. Cyber fines on retailers are new. Zoetop is the owner of fashion brands SHEIN and ROMWE, and it was fined for failure to accurately and timely report a breach affecting 39 million customers. According to CyberSecurityHub, this monetary fine is in addition to the remedial costs the business had to take, to include follow-on, frequent, mandatory reporting.

Various research reports are available on the estimated cost to a business for just one breach; these reports suggest a breach can go from about $5 million to $8 million. That being said, the true costs and residual costs are not always known or included. For example, the cost to repair a technical issue across a business may be $5 million, but that may not include missed opportunity costs, loss of employee productivity costs, longer term decreased confidence in a company's reputation, also referred to as 'good will.' Longer-term costs can and may include the costs of enhanced safeguards, and more frequent vulnerability assessments and employee training.

Who are you going to call?

Cyber incident responders-

Cyber Incident Responder professionals are postured to assess *if* and *when* a privacy breach or cyber incident occurred. They are often cybersecurity engineers trained in digital forensics. Forensics will help pinpoint when and how an intrusion occurred. Their strongest strength is being able to investigate potential multiple layers of intrusions so that a root cause can be identified. Root cause analysis is one of most important assessments in establishing an entity's mitigation response. For example, an insider threat will be handled very differently than a failed firewall or patch. If it is not strictly a technical challenge or breakdown, it may be a training issue for employees, or even possibly just one employee. If it is an insider threat, consult with legal counsel and possibly law enforcement. When a breach occurs based upon an employee's access, a whole new set of considerations arises. Establishing a proper trail or chain of custody will be paramount.

Data Privacy Counsel and Privacy Professionals-

Privacy professionals are good resources that an entity can use to communicate directly to those impacted in a data breach. These professionals are best if they practice in the geographic area for which individuals were impacted as they will know the local privacy guidelines and reporting requirements. For example, if operating in the European Union, there are clear processes that must be followed. If operating in the United States, there are different rules based on the State. For example, the State of California has stricter rules for timely reporting and higher potential fines for not reporting or for a delay in privacy breach reporting and notification. California's privacy rules are based on the California Constitution which provides for privacy as an inalienable right. In California, a company or entity is required to inform a California citizen if sensitive information was exposed. (See CA SB 1386). Across all 50 States in the United States, there are federal HIPAA guidelines that must be followed in the arena of all healthcare practices. There are also privacy rules for consumers as part of credit reporting in the FCRA (Fair Credit Reporting Act). Data Privacy Counsel are the most helpful when a business crosses international boundaries, and in the key industries that are the most regulated, such as banking and finance.

Global Cyber Counsel-

Global Cyber Counsel are best positioned to assess the gravity and risk of the potential or actual cyber incident. Depending upon the entity of the situation or the impact on customers, cyber counsel generally have the best overall view of appropriate next steps. Once the gravity of the breach is assessed, a mitigation strategy will need to be identified. Cyber counsel will also have a recommended strategy to inform board members, stakeholders, business partners, as well as customers. The customer notification process can tend to be the trickiest. In some cases, a media strategy is also recommended, which includes a press release, social media and emails to key stakeholders and influencers.

Local Legal Practitioners-

Based upon the industry sector and country of breach, Legal Practitioners generally are well versed in legal reporting requirements and potential for legal fines. It also gets tricky when

a breach crosses multiple industry sectors and geographic boundaries. Local reporting also varies, and so local legal practitioners are the best bet to address impacts, reporting, communication, and mitigation. Local legal practitioners will stay helpful past the initial stage of the discovery of the incident. Often, follow-up periodic reporting to local jurisdictions will be required, and it can include an onsite inspection. Local legal practitioners are often the best resource to be the after-the-fact lead point of contact for overseers.

Oversight Professionals-

Oversight Professionals will appreciate the regulatory environment and/or oversight reporting that is required for your specific industry. Some industry sectors have more comprehensive reporting requirements, such as finance, healthcare, and energy (to include nuclear power). Once a potential or actual incident or breach has occurred, the oversight professional will know the proper steps in which to inform overseers, board members, stake holders, and potential cybersecurity breach victims. These oversight professionals will also know the method in which to inform the various entities.

Policy writers-

Every entity, whether they are non-for-profit or for profit, must have a privacy policy. Hiring and consulting with policy writers and professionals will be important. There is a niche in policy writing as it must be 'plain-speak' and easy to understand. It is the opposite of a legal disclaimer for example that may be in small print and barely read. Privacy policies need to be comprehended by consumers, partners, and employees alike. A privacy policy should clearly state the data being collected, the purpose of its collection and use, any subsequent uses, and an ability to opt out of collection and/or follow on use. All ages of varying educational levels should be able to understand the policy and an entity's privacy practices. Also, certain geographic areas and business sectors require a policy to be clearly identified on the first page of a website, upfront in a solicitation, and/or clearly visible in a publication or form collecting data. Any policies impacting employees should be clearly stated in an employee handbook to which an employee will attest to their adherence. Also, a company should have a well-known policy and standard process (SOP) for escalation and mitigation of a cyber incident or privacy breach. Policy writers are a key part of a defensible data governance and cybersecurity program.

Bottom Line:

Today's ubiquitous environment brings both challenges and opportunities. Don't wait to invest in a cybersecurity and data governance program until an incident occurs. The high costs of insecure cyber practices, underfunded privacy programs, or programs lacking rigorous compliance processes could signal the end of a company when the unexpected happens. Be proactive, and focus on program integrity and resiliency to be prepared. Don't fret though: there are qualified professionals at hand to help with cyber compliance and data governance. The cyber community is a supportive profession to ensure long-term success!