TRIAGING DATA BREACHES

By Mark Antalik

A data breach is one of the worst things that can happen to nonprofit organizations, their clients, donors and volunteers. When malicious perpetrators gain unauthorized access to financial information or other personal data, they can steal identities, exfiltrate intellectual property and can cause reputational damages that will affect the organization for years to come.

Information sharing is fundamental to virtually every aspect of business. As an organization grows, information sharing grows along with it—with vendors, contractors, partners and customers. And every one of these relationships present a new set of potential vulnerabilities.

Data breaches are increasing in frequency and can be potentially catastrophic to an organization; therefore, the need for data protection, as well as the way in which it is implemented, must be balanced thoughtfully against strategic and operational needs.

However, given that data breaches are virtually impossible to stop, it is imperative for organizations to build, maintain and follow a sound breach response program. To accomplish this, BDO developed a two-part series with step-by-step methodology to effectively respond to incidents and maintain a program that allows the organization to respond in the wake of crisis.

Series One

1. **Identify, Understand and Communicate** – Processes to identify the potential threat, gain an understanding of the threat and its potential impact, and communicate with the appropriate agencies and other involved or impacted parties.

2. **Respond and Contain** – Responses and efforts to contain or limit data breaches can have significant impacts on an organization's ability to recover from the incident.

Series Two

1. **Perpetuation** – Preservation of evidence will assist in remediating the current breach and may aid in identifying future attempted breaches.

2. **Notification and Identity Monitoring** – Through internal or third-party services, affected parties can be notified of any activity related to their personal information and efforts to remediate and reduce potential impact.

In this article we address the first series. We discuss identifying, understanding and communicating during a breach situation and how breaches should be managed. In the second series, we will elaborate on perpetuation through digital forensics, as well as outlining approaches to notification and identity monitoring. While it is impossible to eliminate all risk of a data breach, a well-designed program will minimize the negative impact on both short- and long-term business goals.

IDENTIFY, UNDERSTAND AND COMMUNICATE

There are numerous ways data breaches can occur. An organization's data governance architecture is important for providing the most resilient defenses. When reviewing priorities of a network security program, one must understand that breaches can occur in the following formats:

- Criminal act by outsider (hacking; portable device theft; cloning; burglary)
- Technology failure (firewall or server compromise)
- Insider threat (theft; embezzlement; unauthorized disclosures; collusion; retaliation)
- Human error (lost mobile device; misdirected email or fax [yes…faxes are still in use]; improper configuration of security systems; improper trash disposal; failure to secure physical premises)
- Vendor error (misdirected data, packages or mail)

Given the interconnected nature of our business and personal environments, data breaches can be relatively simple for the persistent malicious perpetrator or discontented insider. Every computer, cellular device, networked system and unsecured Wi-Fi connection represents a potential point of entry.

Unfortunately, most organizations are unaware of how vulnerable they really are; some understand the threat landscape, but they may be focused on other revenue-generating areas of the business. IT professionals, with support from senior leadership, must understand that data breaches are responsible for $400 billion in global losses every year. The problem will only get worse, especially as individuals migrate more of their lives to online systems and resources.

Data breach threats are on the rise for organizations of all sizes and in all industries. Regulators, industry associations and the federal government have begun to act, issuing attestation guidelines and regulatory mandates surrounding organizational cybersecurity programs.

With concern growing among stakeholders, there is building pressure for organizations to prove they have effective controls in place. Organizations must be able to detect and mitigate data breaches that have the potential to disrupt business operations, damage their brand and cause significant financial losses.

Undertaking a comprehensive data protection and cyber risk assessment allows an organization to understand the current state of its program, identify potential gaps and risks and, ultimately, implement and operationalize an effective framework. At a minimum, risk assessments should evaluate:

- **Application Security.** Are your applications protected from outside threats?
- **Data Protection.** Do you know where your sensitive data is stored and how it is protected?
- **Identity and Access Management.** How well do you control who accesses your systems and data?
- **Infrastructure Management.** How well is your network protected?
- **Event Management**. Do you know what to do if there is a cyber breach?
- **Vendor Management.** What are the security practices of third-party vendors who have access to your systems and data?
- **Training.** How aware is the employee population about their cyber responsibilities?

RESPOND AND CONTAIN

Having a plan to respond and contain a breach is a critical step in the breach preparation process. A well-planned response will provide explicit guidance for response resources, reduce emotional conflicts in tense breach situations and demonstrate to clients, donors and volunteers that organizations are in control of the situation and are concerned about protecting personal information.

Consider the following key data breach response-and-contain plan elements:

- **Stay calm.** The steps in dealing with a data breach are mostly common sense. A well-crafted data breach response plan helps avoid reckless decision-making.
- **Assembling a team.** Choose an organization spokesperson in advance such as the general counsel, chief executive officer or another senior leader. Identifying and training backup resources for each role is essential as well.
- **Understanding of the law.** Organizations are sometimes unaware that their public statements, including media appearances and communication with clients, donors and volunteers, may be admissible in court if a lawsuit is filed. Consulting with a privacy attorney and media relations expert can guide language and strategy while also helping to address regulatory and fiduciary responsibilities.
- **Keep the risk within the organization.** Organizations that have been breached can, in turn, unintentionally compromise other organizations by transmitting infected files or malware links. To prevent this, organizations should choose to spend resources and time to fully evaluate the risk and determine measures to reduce it. Measures to reduce risk may include soliciting the expertise of cybersecurity experts that can evaluate and address current and future risk levels for the organization.
- **Deploying a cyber forensic team.** A cyber forensic team will analyze the data breach and determine how the organization was breached, what areas of the enterprise were affected and what information may have been compromised. They can further investigate if the data breach was initiated by an insider, either unknowingly or by nefarious means.
- **Involve legal counsel.** Either internal or external counsel should be engaged for legal guidance and to maintain privilege through the breach response process. Assume that clients, donors, volunteers or other third parties may take legal action against the organization related to the data breach.
- **Notifications.** For data breaches that require notification, a communications plan should include call center guidelines and training. The training might include the tone and message for responding to calls and how any frequently asked questions will be scripted. There will likely be additional notification obligations to regulators or other authorities where counsel and data privacy subject matter experts should be consulted.
- **Communicate on all available channels.** Use the organization's corporate social media channels to frame the story rather than waiting for it to unfold in the media. The media may misinterpret or embellish facts, where the organization can control the narrative. Additionally, organizations should use plain language for these communications rather than potentially confusing technical and legal terminology to express what remediation efforts are being conducted to protect their information.
- **Employee communications.** Communicate with employees so they are aware of the data breach before they hear about it in the media. With knowledge of the breach, employees, with the appropriate approvals, can provide informed communications to their business contacts.
- **Transfer risk to another entity.** This is primarily done through obtaining insurance coverage that specifically addresses the impacts of a data breach. An insurance broker specializing in cyber risk, along with the expertise of forensic accounting and claims consultants experienced in measuring losses, is essential. Keep in mind that communications with insurance agencies do not typically fall under privilege. (See the **Spring 2021 Issue of the Nonprofit Standard** for an article on cybersecurity insurance.)

Even though customers and individuals are increasingly aware that organizations are at risk for data breach, a breach can be a real test of resiliency. Organizations must plan for a breach and be clear and transparent to clients, donors, volunteers and other third parties about what the organization is doing to protect data. Organizations who meet the crisis head on may even be able to emerge stronger, with a closer connection to their constituencies.