PREVENTING & MITIGATING A DATA BREACH

HOW TO MITIGATE & RESPOND TO DATA BREACHES

LIGHTEDGE

TABLE OF CONTENTS

HOW TO MITIGATE AND RESPOND TO DATA BREACHES

Cybersecurity crimes and data breaches are on the rise, and it's estimated that these crimes will cost $6 trillion annually by 2021. Small to medium-sized businesses (SMBs) are more likely to fall victim; oftentimes, SMBs don't think they are large enough to target and lack the proper technology and processes to protect their network.

CLOUD ONLY ACCOUNTS FOR 28 PERCENT OF IT SPEND.

In fact, 87% of SMBs surveyed by Symantec's Security Threat Report said they didn't feel like they were at risk for a breach. And when confronted with the daunting task of developing a cybersecurity strategy, many IT, security, and compliance leaders are not sure where to begin (We get it—there are a lot of moving parts, as shown in figure 1). Taking a framework approach to risk management offers a structured way to identify, protect, detect, respond, and recover from any security incident your business may face. Although there are many components to risk management, this guide will focus on data breaches in particular.

WHAT IS A DATA BREACH?

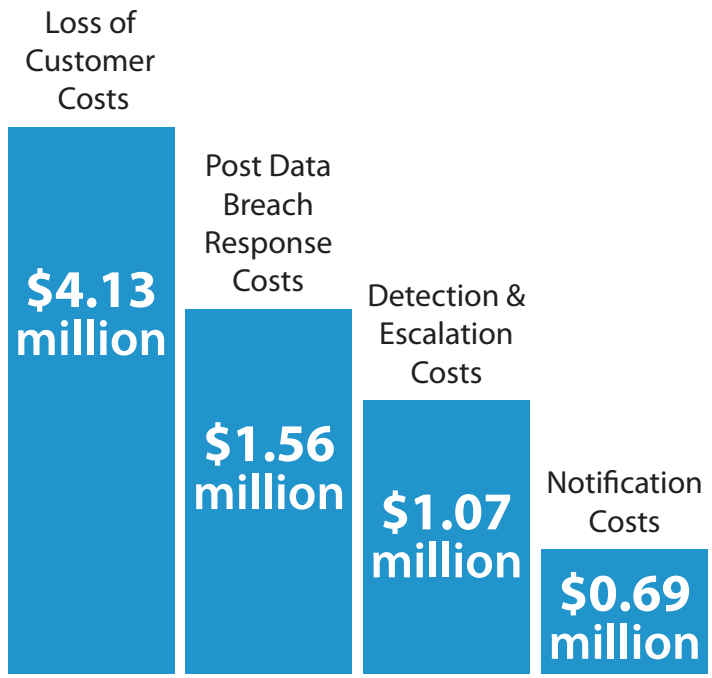
It's important to differentiate data breaches from other cybersecurity attacks. According to The Identity Theft Resource Center, a data breach is "an incident in which an individual's name, social security number, driver's license number, medical record, or financial record is potentially put at risk because of exposure." In short, it's an incident wherein information is taken or stolen from a system without the authorization of the owner.

WHAT IS THE IMPACT OF A DATA BREACH?

Although no two data breaches are the same, they all have negative consequences, ranging from legal fines to having to close your doors for good. For businesses where sensitive data—like personal customer information, is exposed— the result is broken customer trust, loss of existing or new business, and lawsuits that result in hefty fines.

By November of 2017, there were 1,172 data breaches for the year, with an estimated 171,687,965 records exposed. The average cost of a data breach in the U.S. according to The Ponemon Institute is nearing $7.35 million. These numbers may seem high to you, but you must consider both the direct and indirect costs associated with a breach. For instance, post data breach response requires help desk activities, special investigations, regulatory mandates, and legal assistance.

COST OF DATA BREACHES IN THE U.S.



Source: IBM and Ponemon Cost of a Data Breach Study

Figure 2: Source: Cost of a Data Breach Study, Ponemon Institute (in millions)

TYPES OF DATA BREACHES

What are the most common types of data breaches? What can you do to prevent a breach and, if a breach occurs, how you contain its impact? Let's review.

There are many types of breaches. Some are a result of employee error within an organization, and some are targeted attacks from external sources. Most breaches fall under these categories:

1. HACKS

Hacking accounted for over 60 percent of attacks by mid-2017 and included attempts of phishing, spear phishing, ransomware, and skimming.

Traditional phishing is characterized by an email from a perpetrator. Those who receive the email assume the communication is from a trusted source, such as a bank. The email often will guide the reader to click on a link to a malicious website. If the receiver clicks on the link, the hacker can infiltrate the user's computer and steal their username and password.

Spear phishing is more targeted—emails are sent to fewer but highly researched individuals or organizations. The attacker creates a customized message that appears credible so that the victim will unsuspectingly divulge critical information. Companies are highly susceptible to these types of hacks.

Ransomware, probably the most common type of hacking, uses cryptovirology to take control of a victim's data and block access to it until the victim pays a ransom.

Skimming, or card skimming, is the illegal copying of debit and credit cards. A store clerk might have a customer swipe a card more than once so that the magnetic strip can be copied, or an ATM might be rigged with a card skimmer.

Several well-known companies were targeted in 2017 in attacks that proved extremely costly both in terms of revenue and reputation. Some of the most notable events include:

Equifax

Equifax, one of the three main US credit agencies, discovered a breach in July 2017. Because the data stolen included the social security, drivers' license numbers, and other sensitive information of individuals, this could be the worst breach ever with 143 million consumers potentially affected. Hackers exploited a weak point that they discovered in the company's system.

Gmail

In May 2017, a sophisticated phishing scam succeeded using a worm that posed as an email. The emails appeared to come from a trusted contact and enticed the victim to share a Google Doc via a link to a fake app, which took over the management of the Gmail account. Quick action by Gmail shut down the attack within an hour, but approximately 1 million users may have been affected.

InterContinental Hotels Group (IHG)

IHG, also known by the brands Crowne Plaza, Holiday Inn, Candlewood Suites, and Kimpton Hotels, announced in February 2017 that 12 of its hotel properties had experienced a data breach. In this case, malware was discovered on servers that processed hotel restaurant and bar payments, and the malware stole data from August to December 2016.

Sensitive cardholder information was compromised. However, the company caused even more damage to its reputation when it announced that 1,200 hotels had been affected, not just the 12 originally reported.

Forever 21

The popular clothing retailer suffered a breach between March and October of 2017. After receiving an alert from a third-party, Forever 21 investigated and found that some point-of-sale (PoS) devices were compromised.

Although the company claimed that it had implemented encryption and tokenization solutions in 2015, that encryption had not been functional in some PoS devices. To date, the company does not know who was responsible or the number of people who may have been affected. This is often the case with PoS attacks.

2. EMPLOYEE ERROR

Approximately 30 percent of all attacks are a result employee error. These errors range in action, like not following proper security protocol or accidentally sharing sensitive information. Most errors happen without a malicious intent. Everyone is human, after all, and people make mistakes.

Cases in point, in 2016, an employee of the Federal Deposit Insurance Corporation accidentally downloaded sensitive data to a personal storage device without malicious intent. Also in 2016, someone impersonating Snapchat CEO Evan Spiegel emailed an employee asking for payroll information of hundreds of employees.

"81% of hacking-related breaches leveraged either stolen and/or weak passwords." – Verizon Data Breach Investigations Report, 2017

3. ACCIDENTAL EXPOSURE

In 7 percent of breaches, sensitive information is given up by accident, but by the company not an employee. It can be hard to differentiate the two without proper research. For example, Saks 5th Avenue accidentally exposed customer information on their website via a plain text link. It was never determined if that was an employee error or just a glitch in the system.

4. PHYSICAL THEFT

Theft of equipment or documents is another way that data breaches occur. This is a less subtle method of a data breach because someone would have to steal a server or documents from a company. No major company has reported any physical theft in the past few years most likely due to cloud storage.

5. THIRD-PARTY SUBCONTRACTORS

According to a Price Waterhouse Coopers survey conducted among 10,000 executives in 127 countries, almost 70 percent of companies use cloud-based cybersecurity services. However, third-party providers can be a source of security breaches.

Thousands of HIPAA-protected medical records were exposed from Bronx Lebanon Hospital Center in a data breach. A Rsync backup server hosted by a third party, iHealth, was misconfigured.

In a separate incident in Maine, the names, addresses, and social security numbers of parents who received foster care benefits were inadvertently posted to a public website by a third-party contractor as part of a technology upgrade.

While the breaches did not happen directly to the companies, their customers were still impacted.

HOW TO PREVENT A BREACH

Breach prevention in the digital age requires advanced technology solutions such as network firewalls, file and hardware-based encryption, backup, malware protection, intrusion detection and protection, vulnerability scanning, and log management.

It's also critical that your company have a proactive approach to security and employs the most knowledgeable security team available.

In addition, there are basic security policies that need to be in place for the ultimate data breach protection.

FOUR POLICIES FOR PROACTIVE IT SECURITY

Compliance requirements state various policies that companies should follow, but they are often uncorrelated and confusing. The following areas are considered pillars of a robust information security strategy.

1. RISK MANAGEMENT

When it comes to data breach and security. Risk management is paramount. Statistics show that 60 percent of companies that lose data in a disaster shut down within six months. All risks should be identified and assessed in terms of cost and prioritized according to operational criticality. Once identified, the level of resources needed to mitigate each identified risk can be allocated according to priorities. This analysis will form the basis for all other security-related decisions.

2. ASSET CLASSIFICATION

Classifying assets defines the appropriate level of protection. It will determine the cost of securing assets based on their value, the impact they have on the organization and its reputation, along with business opportunities that may be lost if the assets are gone. Classifying assets is fundamentally prioritizing to determine which ones to protect first.

3. INFORMATION SYSTEMS SECURITY

The Information Systems Security Policy defines which security controls should be executed for various information systems such as physical security, access management, and network security. The policy should be updated as new risks arise and technology is updated.

4. INFORMATION SYSTEMS ASSESSMENT & AUTHORIZATION

The Information Systems Assessment and Authorization Policy is key to securing operations. This policy ensures that any new systems adopted are properly protected. It also requires all users to understand the defined standards and any deviation from those standards. This policy should provide transparency and clarify who is responsible and how individuals will be held accountable for certain operations. The Information Systems Assessment and Authorization Policy links the three previous policies.

Developing these policies are exemplary of the Deming Cycle improvement process – plan, do, check, and act—which is a proven strategy for operational success.

Companies who experienced breaches in the past skimped on encrypted storage and multi-factor authentication security measures to save time and increase productivity.

The breach that affected Deloitte in 2017 is a prime example—their emails did not use encryption, the compromised administrator account was not protected by two-factor authentication and required only one password.

Round-the-clock, real-time monitoring is essential to preventing data breaches. Companies can only prevent data breaches if they have visibility into their environment. Outsourcing to a security operations center to monitor activity 24/7 can be a good option, along with automated intrusion detection and prevention solutions.

Tools, like a security information and event management platform (SIEM) provides actionable insights from advanced analytics and data forensics to mitigate risks and speed up your incident response. SIEM systems consolidate logs from devices throughout your network to detect patterns in data over time; this intelligence allows you to categorize issues according to their severity, so you can prioritize actions and make informed security decisions.

Employee expertise is vital, and security personnel should receive regular training so that they are aware of policies, expectations, and data security standards.

As IT technology advances, so too should employee training so that staff are equipped with the latest tools and know how to apply them. Training is an investment that will pay dividends in the long run.

MITIGATING AND RESPONDING TO A SECURITY BREACH

If a breach happens, there are certain steps that can mitigate and contain an incident. Recently, we've seen several major companies including Yahoo and Uber try to conceal the depth of a breach. Companies must do everything in their power to protect customers and shareholders, and be transparent about their efforts to build trust.

1. ORGANIZE AN EXPERT RESPONSE TEAM

A response team should include forensic, legal, IT, HR, operations, communications, investor relations staff, and management experts. This team will be in charge of dealing with the aftermath of a breach in all aspects of your business.

2. SECURE THE PHYSICAL AREA

Stemming the loss requires securing the physical area as well as systems. Equipment should be taken offline or replaced (depending on the situation), access to your logical and physical environment should be monitored and frozen as necessary, and passwords and access codes for authorized users should be updated.

3. CHECK WEBSITES AND ONLINE SOURCES

Any misplaced information should be removed from public sources. Internet search engines can cache information, but you can directly contact a search engine to make sure they do not archive personal information. Other websites should be contacted and asked to remove any exposed data that they may have obtained from a compromised site.

4. REMOVE VULNERABILITIES

Check the network segmentation with forensic experts and see who gained access to what using the data from your SIEM agents and logs, and you may uncover the source of the issue. Investigate whether or not the proper procedures and technology were used and review your access logs for clues. When identifying vulnerabilities, consider that they may originate from your third-party providers.

Verify which data, applications, and systems were compromised prior to taking action, and determine the number of individuals affected. Next, you'll want to contact stakeholders to let them know a security incident has occurred and what steps you're taking to recover.

5. CREATE A COMMUNICATIONS PLAN

Now is the time for transparency and communications both internally and externally. Companies that try to bury the extent of their breach, like Uber, often experience much worse consequences in customer backlash.

Consider all stakeholders in the plan, including business partners, investors, employees, and customers. Deliver a clear statement that is open and thorough without divulging information that could add risk. Organizations should report all data breaches to law enforcement, and follow other state and federal legal requirements—including compliance mandates.

The Federal Trade Commission offers a detailed guide on how to mitigate a security breach including a model letter to send to customers and stakeholders.

SECURITY THREATS IN 2018

Security trends show that companies of all sizes should expect an increase in attempted breaches in the coming years; hacking has become a profitable field for criminals.

According to QuickStart, some of the more likely threats include those aimed at the IoT, the cloud, and multi-cloud environments. According to QuickStart, part of the reason for increasing cyber security threats is that digital transformation has placed unreasonable expectations on IT executives.

Adding to the pressure is that spending on IT security will reach $93 billion and will include spending on IT outsourcing, consulting, and implementation, according to Gartner.

HOW LIGHTEDGE CAN HELP

The best way to handle a data breach is to prevent it, but this is not always possible. LightEdge has a full array of technology solutions, policy templates, and staff to help the overwhelmed IT security professional who simply doesn't have enough resources. Use a combination of these services to reduce risk and lean on our expertise along the way.

MANAGED SECURITY SOLUTIONS

24/7/365 Virtual Security Operations Center (vSOC). Detect, mitigate, and remediate risks with real-time insights from our virtual security operations center (vSOC). LightEdge vSOC monitors and assesses incoming cyber security threats 24/7/365, alleviating the strain on your employees and budgets.

- In partnership with CarbonHelix, a top IBM SOC/SIEM partner
- Staffed in U.S. by analysts with top security clearance
- Analysts provide interpretation & advice on security events generated by SIEM

Data encryption. Leverage LightEdge's data encryption services to ensure that your data is protected no matter where it's process or stored.

- Data at rest encryption on all storage (hardware-based, AES 256-bit)
- Centralized access control, granular auditing, and encryption key management for customers
- Encryption of data at rest & in transit
- Hardware, file, and image-level back and DR

Malware Protection.

Virus and malware protection keep systems and data secure from evolving threats. LightEdge's advanced anti-virus/anti-malware solution works in real time to detect and remove malware and protect IT infrastructure and sensitive data from malicious activity.Hackers exploited a weak point that they discovered in the company's system.

Intrusion detection and prevention.

Strict industry regulations require companies to identify suspicious network traffic and respond quickly to stop attacks. LightEdge has a standard solution for clients who already have security engineers monitoring and responding to alerts in-house. An advanced solution provides threat management functions in real time 24/7 for organizations that require full, round-the-clock protection.

Vulnerability Management.

Vulnerability management protects computer systems and critical applications by performing in-depth inspections of systems to identify security weaknesses.

- Regularly scheduled vulnerability scanning (IBM QRadar)
- Automated mitigation & patching (IBM BigFix)
- Audit-ready compliance reports

Load Balancing & Web Application Firewalling.

Load balancing optimizes the distribution of workloads to maximize throughput, minimize response time, and avoid overloading any computing resource. Web application firewalling identifies application-specific exploits missed by traditional firewalling techniques.

- Industry-leading Citrix NetScaler
- Quickly scalable & virtualized Infrastructure as a Service (IaaS)
- End user desktop & app delivery over encrypted SSL sessions

Next Generation Firewalling.

Network firewalls are your first line of defense against security threats, improving your ability to control traffic, applications, and users. Our talented engineers will work with you to define firewall rules and policies that permit or deny network traffic based on security, compliance, and business needs.

- Industry-leading Fortinet firewalling
- Integrated IDS/IPS, AV/malware & URL filtering
- High performance, data center-oriented architecture
- Physical & virtual, redundant options
- FIPS 140-2 compliant IPSEC & SSL VPNs
- Token-based & MFA authentication options

File integrity monitoring.

This solution monitors the changes to files, folders, and registry settings. It also monitors software, processes, and directories for any unplanned activity and sends out alerts when any unexpected activity is detected.

Multi-factor authentication.

As a general rule, more layers of protection are always better. Multi-factor authentication has the flexibility of a software token and requires two layers of authentication for validation of a smartphone or mobile device user.

Security Information and Event Management (SIEM).

Our security information and event management (SIEM) platform, powered by QRadar, collects and analyzes data from multiple sources to provide actionable insights so you can mitigate risks and speed up your incident response.

- Provides 24/7/365 network security and proactive alerts on emerging threats, and recommend security policy changes to allow you to best optimize staff resources.
- Increased visibility with a centralized IT operations and monitoring platform
- Integrates LightEdge's Colocation, Cloud, and managed hosting environments
- Reporting and data archival that meets compliance standards
- Developed & backed by IBM security labs

The SIEM also meets HIPAA-HITECH, PCI DSS, and other compliance needs. The platform is managed to HITRUST standards, allows you to customize reports for security and compliance management, and offers the log retention your compliance requires.

SECURITY IS AT OUR CORE. OUR CERTIFICATIONS PROVE OUR EFFORTS.

LightEdge has a range of certifications including HIPAA, HITRUST, PCI DSS, EU-US Privacy Shield, SOC 1 Type II, SOC 2 Type II & SOC 3, ISO 20000-1 and ISO 27001 which proves that our technology, people, and processes meet these high standards. We also offer security consulting expertise in NIST, FISMA, FedRAMP, CJIS, and NERC-CIP (to name a few) through direct access to our experienced CISO.