Data Breaches: Avoid Becoming a Headline

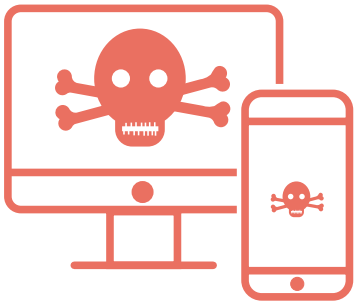
We Value Your Security | Vol. 1 No. 3

pfm

More than a decade ago, a data breach forced many organizations to realize the consequences of exposing protected data to unauthorized access and manipulation. Laws were established in response to this first "major" breach and sensitivity to cyberattacks heightened. Fast forward to today and that early breach seems practically insignificant compared to the recent Capital One data breach that exposed the personal data of more than 100 million people.

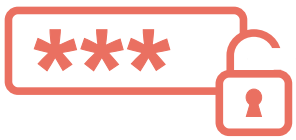
Bringing awareness to how data breaches can occur and the damage they can cause to the clients we serve is part of our turnkey approach to client service. Below, we discuss the current trend of data breaches and how you can be more prepared should a data breach happen to you.[1]

What is a Data Breach?



Unlike cyberattacks such as ransomware, a data breach is the result of a social engineering attack that provides unauthorized access to steal confidential personal or financial data.

Current data breach trends show that cybercriminals are mostly motivated by money to acquire personal information, many companies are still not properly prepared for breaches, and the number of breaches increases each year. Risk Based Security Inc.'s recent *Data Breach QuickView Report* noted that more than 1,900 breaches were reported in just the first quarter of 2019, exposing approximately 1.9 billion records. When compared to the first few months of 2018, data breaches are up 56.4%.



What is causing this upward trend?

COMMON RISKS RELATED TO BREACHES

- **Employee Errors:** The leading cause of data breaches around the world is employee error.[2] These errors come in the form of compromised credentials or lost or stolen devices like company cell phones and laptops, but also a lack of general awareness for how to handle, retain and dispose of sensitive data. Lack of education also leaves employees vulnerable to cybercriminals.
- **Phishing Attacks:** Hackers use social engineering tactics to capitalize on relationships and social behavior to manipulate people into providing access, supplying information or performing an action. Hackers use emails, texts or phones calls disguised as legitimate requests to trick employees into unknowingly providing protected information or unauthorized access.
- **Weak or Stolen Credentials:** Phishing attacks are often designed to obtain a user's credentials. In a study of 905 phishing attacks, 91% were found to be targeting usernames and passwords.[3] Password guessing software is also used to search for weak credentials — passwords that are repeatedly used or that contain personal or easily guessed information.

1 This report provides general advice to raise awareness about data breaches. It is not intended to provide specific advice on your situation.
2 National Conference of State Legislatures, *Taking Aim at Data Breaches and Cyberattacks.*
3 Return Path, *3 Top Insights from the 2016 Verizon Data Breach Investigation Report.*

- **Ransomware:** This is a type of malicious software that infects, locks or takes control of a system, or encrypts important data, then demands a ransom to undo it. Ransomware typically falls into two categories:
    1) **Locker Ransomware** - locks a user out of a system but typically leaves the underlying system and files untouched.
    2) **Crypto Ransomware** - encrypts files stored on a user's computer or mobile device, rendering them unreadable until the victim pays for the decryption key.

  Ransomware is typically installed through a malicious email attachment, an infected software download or a visit to a malicious website. Payment requests are made in bitcoins, wire services, or gift cards, all of which are hard to trace. Paying the ransom does not guarantee the encrypted files will be released. Ransomware has been used against local governments, preventing the delivery of critical services.
- **Spyware:** This type of attack often occurs when an employee unknowingly downloads spyware thinking they are performing a routine update or running a seemingly nonthreatening computer program. Instead, the malware infects a computer or network, seeking to steal personal information or other data.
- **Third-Party Vendors:** As trusted partners for your agency, vendors can sometimes become an unsuspecting accomplice to cyberattacks leading to data breaches. A survey by eSentire that interviewed 600 IT professionals determined that nearly half of the respondents experienced a data breach caused by a vendor, 26% of the breaches were caused by employee errors and stolen passwords, while the rest were the result of some form of malware, like spyware.[4]
- **Outdated Software:** Software companies routinely alert users to available updates that provide important software patches to fix identified vulnerabilities. When these updates are overlooked or delayed by employees, it leaves them open to hackers. For example, once a month, Microsoft sends out a notice of available updates. These notifications are sent to software users, but are often monitored by hackers too. Hackers will use this information to seek out users who have not yet applied the update, providing a window to gain access to data.

Data Breach Consequences: Beyond the Headlines

When a breach is discovered, the first course of action is typically to stop operations until the source is identified and the issue is resolved. Shutting down operations causes a decrease in production and ultimately a loss of revenue. For public agencies providing essential services, shutting down operations may not be an option. If it is, the consequences could be detrimental to the communities served.

According to one study the average cost of a data breach, at $3.86 million, far exceeds the cost to properly educate staff and implement the internal controls necessary to help protect your agency.[5] That said, the range of "costs" following a data breach can hurt more than just your budget.

- **Damage to Your Reputation:** Building and maintaining the reputation of your firm is something that takes a lot of work, and a data breach can quickly tarnish a good reputation that has taken years to build. Forty-six percent of organizations say they suffered damage to their reputation as a result of a data breach.[6] This damage is from lost trust and customer loyalty, and ultimately leaves the victim facing a decline in revenue. For example, in 2013, Target experienced a data breach that resulted in 40 million credit card records being stolen and saw profits fall by 46%.[7]

4 eSentire, Inc, *Nearly half of firms suffer data breach at hands of vendors,* https://www.esentire.com/blog/nearly-half-of-firms-suffer-data-breach-at-hands-of-vendors/.
5 IBM, https://www.ibm.com/security/data-breach.
6 Return Path, *3 Top Insights from the 2016 Verizon Data Breach Investigation Report.*
7 Krebs on Security, *The Target Breach by the Numbers*, https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

- **Loss of Proprietary Information:** Unlike data breaches involving personally identifiable information, which regulations generally require be publicly reported, most cases of breaches involving proprietary information have not received widespread attention. Hackers will target things like customer lists, financial models and pricing strategies, using these trade secrets to damage competitiveness by exposing the information to the public. Publicizing this information could mean losing a "first-to-market" advantage, loss of revenue or losing entire business lines to competitors.
- **Lost Customer Trust:** Sharing sensitive information with a vendor shows that a client trusts that their information will be kept secure. When a data breach occurs, clients may question the amount of trust they placed in that particular entity. Loss of trust does not only stem from a breach, but lack of follow-up after an incident can also be a contributing factor.

What Can You Do to Avoid a Data Breach?

Unfortunately there is no way to prevent hackers from targeting your organization; however, you *can* establish "data hygiene" protocols to help mitigate the risk of a breach happening to you.

"Unfortunately there is no way to prevent hackers from targeting your organization; however, you can establish "data hygiene" protocols to help mitigate the risk of a breach happening to your agency."

- **Employee Awareness, Training and Testing:** Not understanding security risks or the best practice measures to take in response is the root of vulnerability for public agencies. Teaching employees how to recognize signs of possible fraud and how to respond appropriately is the first step towards preventing cyberattacks that may lead to a data breach. Employees should understand appropriate data retention and disposal methods, utilize strong passwords and multi-factor authentication, understand the process for processing and responding to requests for sensitive information and know their role as part of their office's incident response plan.
    - Many data breaches are caused by improper disposal of company files and equipment. In 2010 an insurance agency in New York returned leased copy machines that contained the personal information of more than 344,000 individuals.[8] If proper disposal protocols had been in place this incident might have been avoided. Proper disposal can come in the form of employing a shredding service or properly "cleaning" machines before returning or disposing of them.
    - Requiring passwords to meet specific criteria and implementing multi-factor authentication for online account access can also help prevent a data breach. Best practice is for passwords to be between eight and 64 characters, contain a mix of upper and lowercase letters, numbers and special characters and should never include personal information like birthdays, street names or pets' names. Multi-factor authentication should also always be used when available. Though it is not fool-proof, multi-factor authentication can greatly decrease the chance of information being compromised and help to ensure only authorized individuals are accessing online accounts.
    - An incident response plan is an organized approach to addressing the aftermath of a security breach or cyberattack. Plans should address a situation in a manner that limits damage and reduces recovery time and costs. Without an incident response plan in place, an organization may not be able to detect an attack or follow the proper protocol to contain the incident and recover from it.
- **Apply Technical Controls and Protection Software:** Public entities should have a routine process for distributing and installing critical security patches. They should also have trained security professionals who understand the vulnerabilities of their system to take proactive steps to mitigate risks.

8 Data Breach Today, *$1.2 Million Penalty in Copier Breach*, https://www.databreachtoday.com/12-million-penalty-in-copier-breach-a-5991.

Utilizing intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help to detect unusual activity behind the scenes to alert IT staff to potential cyberattacks. When alerted to a potential threat, IPS can then deploy prevention tactics to fight against the attack and keep protected information secure.

It is also a best practice to run regular upgrades to outdated or unsupported software. Routine software upgrades apply new security patches to existing software to protect against newly discovered vulnerabilities. It is important to be aware of and to manage system vulnerabilities to ensure necessary upgrades are occurring. Vulnerability management helps to ensure software patches are in place.

- **Penetration Tests:** Employing security companies to "test" the security of your agency's network is another way to help prevent data breaches. Penetration testing, also known as ethical hacking, is the practice of testing a computer system or network to detect security vulnerabilities. These tests are performed to see if an agency's network is hackable. If an area of exploit exists, it can be quickly identified and resolved as a result of this type of testing.

Living in a digital society challenges us daily to stay one step ahead of cybercriminals who want to exploit our protected information. Attacks continue to become more sophisticated, which has required us to develop prevention measures that are equally sophisticated. Understanding how and why data breaches occur is the first line of defense. With the right mix of education, technical controls and prevention software, public entities can fight back to protect their information and reduce their chance of becoming the next major security breach headline in the news.