evident

AVOID **CYBER ATTACKS** AND SAVE **MONEY** BY HOLDING LESS **DATA**

THE COMMODITIZATION OF DATA: AN **ASSET** AND A **LIABILITY**

Now more than ever before, data is at the heart of every organization. Whether it's used to offer more personalized services or provide increased security for the business, data is inherently necessary to run businesses today.

Data, especially Personal Identifiable Information (PII), is considered an asset because it has universal applications, like helping businesses to better understand their customers, but, because it's difficult to secure, too much of it is considered a liability. **Cyber criminals target data because it's both monetarily lucrative and easier to steal than actual dollars**, which is why prevalence of data breaches continues to grow, in magnitude, year-over-year.

The threat of cyber attacks has existed since data went digital, but there's been a recent spike in cyber attacks resulting in high-profile data breaches like **Marriott** (500M records compromised in November 2018), **Quora** (100M records compromised in December 2018), and **Collection #1** data breach of at least 773M unique email addresses and 21M unique passwords posted to a hacking forum in January 2019.

These breaches are proof that data is being commoditized, and thus, a bigger target for theft. Generally speaking, data theft is a prolific problem that impacts everyone, and it’s getting worse every year. No matter the scale or depth, a cyber attack that results in a data breach is sure to have a negative impact on a company’s brand reputation, credibility, and customer and employee trust, among other things.

In this white paper, learn more about why cybercriminals prioritize data hacking for financial gain, how your company can protect itself from a breach, and how data minimization practices can reduce the risks of cyber attacks and save you money.

WHY DO CYBER CRIMINALS TARGET **DATA** OVER **MONEY**?

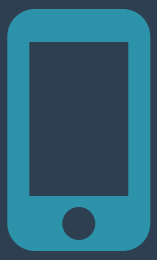
Cyber criminals can easily monetize the data they're stealing, either by leveraging it themselves for fraudulent activity, or selling it to a third party. Digitally savvy hackers also find it easier to steal data, like financial or medical records, than actual money, which further contributes to the value of personal data.

The opportunity to profit from stealing data is enormous, because companies are collecting and handling more personal data than ever before.

A hacker only needs to find a single lapse or vulnerability, and they can potentially access large volumes of sensitive data. Once it's stolen, it's easy to sell through dark web marketplaces to anonymous users that are willing to pay (likely with some form of cryptocurrency) for hundreds of millions of personal data records.

The threat of a cyber attack will always exist, as cyber criminals conduct more elaborate and innovative schemes to access large volumes of data with minimal effort. Organizations with ample cybersecurity are lucky to stay one step ahead of fraudsters, but those without adequate cyber defense or Privacy by Design policies are far more likely to fall victim to cyber attacks.

How Do Cyber Criminals Profit from Stolen Data?



Phone call scams

SMS spam or unsolicited marketing

Email spam or unsolicited marketing

Gain access to online accounts

Initiate ransomware or phishing attacks

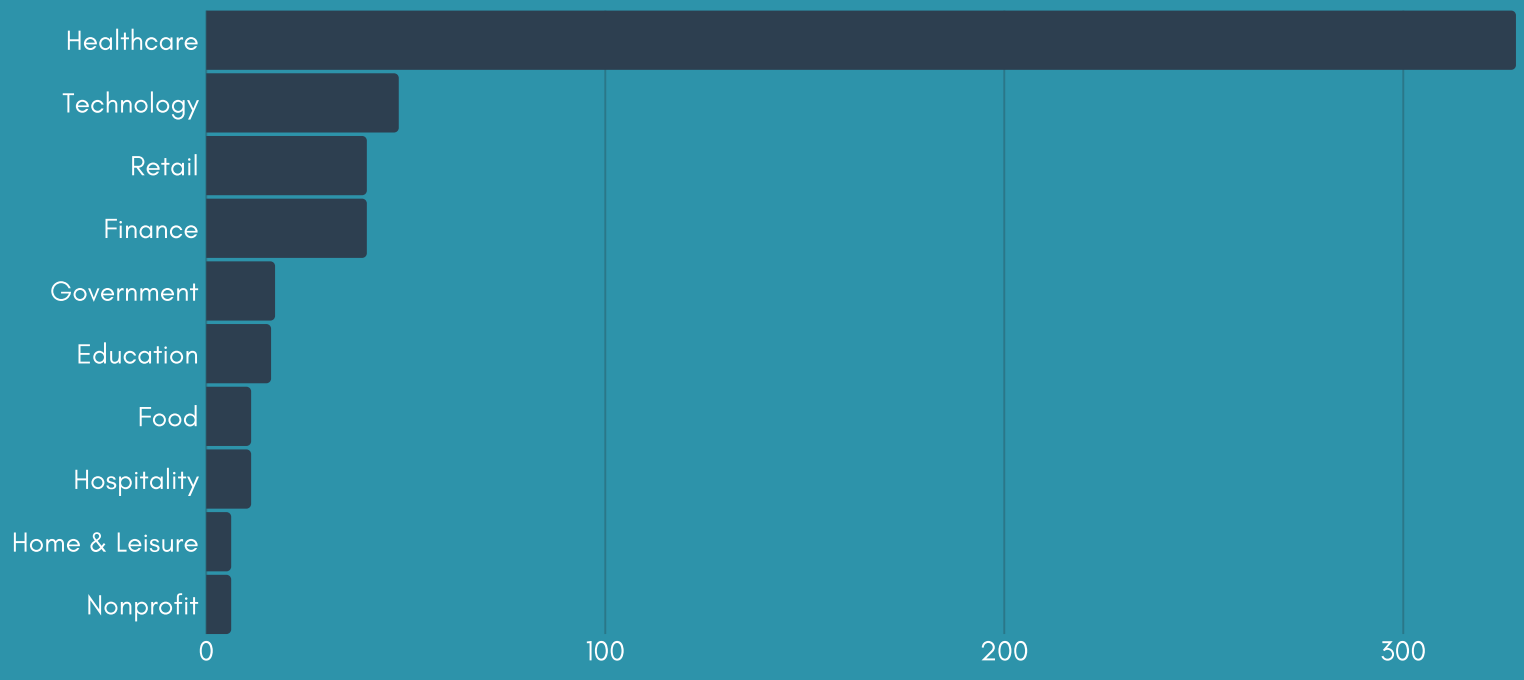
File fraudulent tax returns

Transfer money illegally

Apply for loans and credit cards

Threaten extortion, blackmail, or bribery

Top Industries Affected by Data Breaches



Source: https://www.fastcompany.com/40527767/these-industries-are-the-most-vulnerable-to-data-breaches-in-the-united-states

THE **TRUE COST** OF A DATA BREACH

The aftermath of a cyber attack can be an expensive undertaking for any organization. In 2018, the average cost of a data breach outside the U.S. reached $3.86M, but in the U.S. alone, data breaches averaged $7.91M – more than double the cost for other global organizations – with "mega breaches" costing businesses hundreds of millions of dollars or more.

$3.86M

Average cost of data breach to a global organization

$7.91M

Average cost of data breach to a U.S. organization

Source: https://www.forbes.com/sites/niallmccarthy/2018/07/13/the-average-cost-of-a-data-breach-is-highest-in-the-u-s-infographic/#23f3fa0a2f37

In addition to monetary loss, organizations undergo remediation, investigation, notification, and post-mortem analysis to swiftly diffuse the attack. While it's tempting for companies to measure the full impact of a data breach in actual dollars lost and remediation, the true cost of a breach also includes intangible repercussions that have lasting effects, like:

1. **Negative impact on brand image or reputation**
2. **Lack of trust in the business** (customers and/or employees)
3. **Loss of intellectual property** (if product data is compromised or stolen)
4. **Diminished market value from the perceived vulnerability**
5. **Elevated marketing and PR costs to neutralize public perception of breach**

Individually, these consequences are somewhat negligible, but simultaneously, they can be a serious hindrance to growth and profitability. What's more, the cost to protect data and minimize risks are often higher when an organization has already experienced a breach of significance. Cyber insurance rates go up, IT and cybersecurity costs increase, and lots of time and money is spent on company-wide security training and winning back customer detractors.

EASY WAYS TO **PROTECT** DATA ASSETS

Establishing strong security protocols, educating employees and workers about the necessary processes, and minimizing exposure and access to sensitive personal data to only those that absolutely need it are all important ways that companies can protect themselves and their data. While this is not an exhaustive list, here are some straightforward data protection tips to help prevent significant breaches.

Restrict Data Access

In 2015, 60% of cyber attacks **were inside jobs**, with 44.5% of the insiders being identified as "malicious." From an Identity and Access Management (IAM) standpoint, restricting the identities and devices (and even certain networks) that have been granted access to data can derail potential fraud.

Putting the right controls in place so that only the appropriate people and/or devices have access to the data immediately puts up barriers and makes it harder to transfer data outside of the environment.

This short list outlines a few easy strategies to safeguard data from malicious employees:

Run comprehensive employee background checks

Establish secure Access Control Lists to determine who has access to what data

Don't give employees more access than what they need to do their jobs

Set restrictions on file sharing

Log all network activity to deter an attack

Verify Employee Identity and Credentials

Employee background checks can provide important insight into an individual's past behavior, and can be a potential indicator of future actions, but a background check is just the first step. Verifying that an employee or applicant is who they say they are, has the credentials and education that their resume claims, and meets any regulatory requirements necessary for their role can also help minimize the risk of a cyber attack.

Secure Mobile Devices

As society moves into a mobile-first world, nearly every business employee and user expects constant access to an application. Whether they're working at the airport or at a hotel, or even at home, individuals naturally use a wide range of modalities and form factors to access data they need, and how organizations protect that data is important.

Businesses should have a secure approach for mobile access (BYOD, enterprise devices, etc.), the right set of security devices, controls, and segmentation, and the knowledge of endpoint security or access based on location to protect devices and their access to data. Some strategies for this might include:

A 2016 Tech Pro Research survey found that BYOD practices were used at **59%** of organization respondents, with another **13%** planning to allow it.

Source: http://www.techproresearch.com/article/byod-iot-and-wearables-thriving-in-the-enterprise/

1. **Creating a strong password for unlocking a device and routinely changing it**
2. **Using auto-wipe to automatically delete sensitive data if a device is stolen**
3. **Protecting mobile devices from malware and viruses**

Use a Strong Firewall

Investing in a quality firewall helps to heighten overall security, quickly detect suspicious activity, and identify which of your data assets is most susceptible to an attack. Strong firewalls are quintessentially advised, but they're only as effective as the rules they have in place. If the segmentation rules are too relaxed, malicious attackers can easily find their way into a system via internal or external access.

Tighten Physical Security

With such a large percentage of attacks being instigated by employees and other insiders, physical security is just as important as restricted access. Some examples of physical security measures might include: video surveillance, access control cards, biometric access control, and intrusion detection sensors, among others.

LESS **DATA**
LESS **RISK**

Holding any amount of data is risky, especially if you're doing minimal work to protect it. Companies may want to consider a layered approach to security as a more effective way to protect their data assets, rather than relying on a single method.

Administering **Privacy by Design** and **Data Minimization** policies from the beginning (or as soon as possible) helps organizations identify vulnerabilities before they ever fall victim to attackers, and can be far less expensive (and frustrating) than navigating post-breach damage control. Start by evaluating what information is really needed, how the organization is collecting, transferring, and storing data, and then conduct a cost/benefits analysis to determine which risk is greater:

1. A data breach, which can lead to significant monetary loss and potential damage to brand reputation, or

2. The upfront costs of putting security and privacy measures into place to demonstrate accountability and protect data before it's compromised.

Here's a list of sample questions to help determine appropriate security methods:

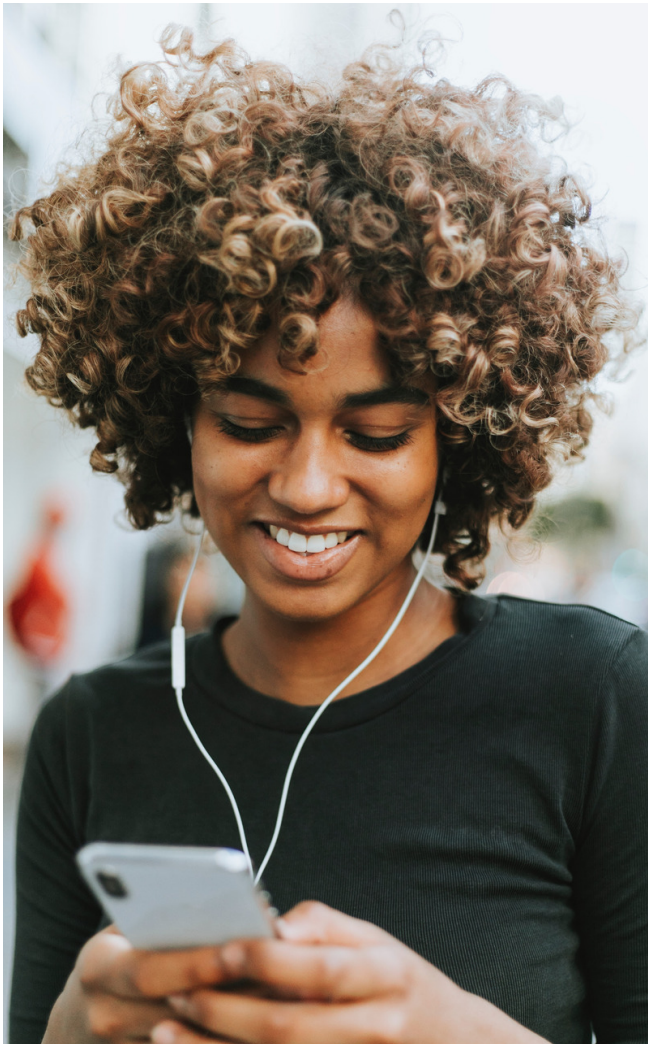
- What is the data's persistence?
- How is the data stored at rest?
- How is the data stored in transit?
- What are we doing to protect access to data?
- What are we doing to monitor who has access to data?

Consider your customers: Protecting customer data goes hand-in-hand with customer service. Secure their PII, and you'll have loyal customers for life.

Consider your employees: Protecting employee data demonstrates your commitment to them and their safety. Employees perform best when they feel like their employers care about them.

THE PROBLEM WITH **CENTRALIZED DATABASES**

Most companies store and manage millions of consumers' personal data records in centralized databases, but holding this much data all in one place isn't necessary or advisable. Companies that choose between data provision and data protection – instead of leveraging existing tools that do both – are at greater risk for a cyber attack.



Even if a company isn't actually storing the data, they're still being exposed to the data they're processing. This creates significant issues, since log files – typically generated from online form submissions, or data from suppliers and vendors – aren't always considered absolutely necessary to secure, leaving the door open for cyber criminals to easily steal that information.

In lieu of a centralized database, leveraging a distributed data model (especially one that has end-to-end encryption in place, like **Evident**) enables companies to limit their exposure to only the data that's necessary to conduct their business, helping them circumvent culpability for holding sensitive data entirely.

Verifying an individual's identity or credentials to participate in a platform without ever having to hold their personal data is an organization's best security measure. Companies can obtain a greater level of assurance and get the value of using personal data without incurring the risk of handling it. Evident helps customers differentiate their products and services by giving their end-users the control over who sees their data and when.

DON'T SET IT AND FORGET IT... CYBER CRIME IS **ALWAYS EVOLVING**

As the digital economy grows, so, too, does the prevalence of data breaches. Data is easier to monetize and move across international boundaries than ever before, which is why cyber attacks are becoming more sophisticated over time.

It's unrealistic for a business to operate without personal data, but it's important to have a healthy internal dialogue about how your organization is managing it so you can put the right security measures in place to protect it. Every organization is ultimately responsible for choosing how it interacts with personal data, but the threat of cyber attacks will never go away.

The cost of a data breach goes beyond losing your customers' trust or your intellectual property––it can also include regulatory penalties. The multiple millions of dollars that global companies spend annually on managing the impact of data breaches can help justify your organization's investment in cybersecurity measures to protect data assets.

An organization's best and most realistic approach to data security is to only use (or act) on data that is absolutely necessary to meet its business goals.

This can be accomplished by:

Executing thoughtful data protection and security processes

Questioning the collection of data that's invaluable or potentially risky

Balancing the value of the data with the potential liability of holding it

Understanding that when it comes to personal data, less is more

Technology exists to help businesses get the verified personal data they need without having to hold or manage PII in one place. Any centralized database that holds personal information will certainly be vulnerable to a breach, and the only way to prevent this is to find a streamlined solution that enables businesses to access the data they need to operate without requiring them to be responsible for holding and protecting that data within their infrastructure.

About Evident

Evident is revolutionizing the way personal data is shared. Evident's simple, secure Identity Assurance Platform lets businesses confidently know who they're dealing with without handling sensitive personal data. With connections to thousands of authoritative sources through a single API, Evident is the only platform that enables comprehensive, accurate, and up-to-date identity and credential verifications without the risk and liability of holding personal information. For more information, visit **evidentid.com**.