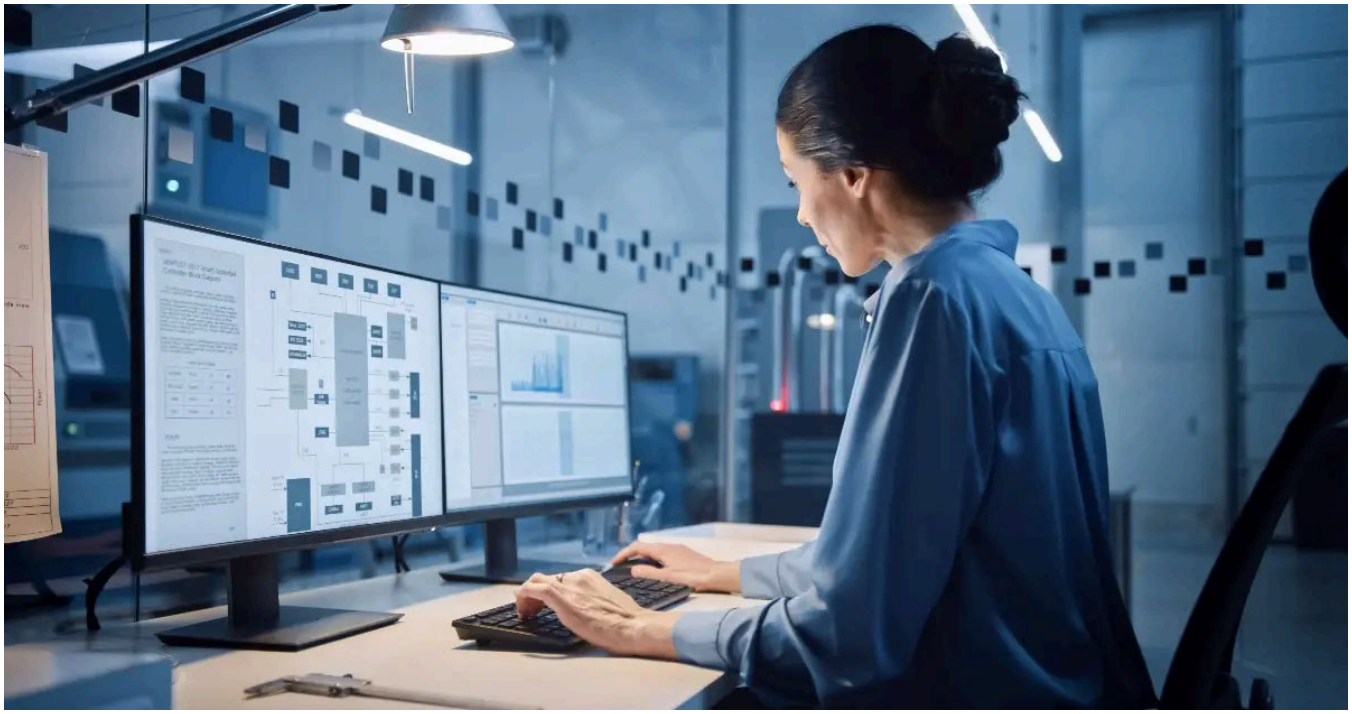
What kind of data costs most in a breach?



Light Dark

September 14, 2022

By George Platsis

4 min read

Data Protection

Cookie Preferences

operations, analytics and behavior recognition are all driven by data and the desire to possess it, regardless of what those who possess it want to do with it. We set out to answer the question "What kind of data costs the most in a breach?" As it happens, that's a complicated question. We'll need to factor in many variables depending on the specifics of your business.

Want to generate some revenue? You need some data to create a business plan, develop intellectual property and conduct a sales campaign. Want to commit a crime? Lock up some data, hold it for ransom and prey on the emotions of the owner. Want to stir up some geopolitical tensions? Manipulate some code to disrupt an industry.

Every one of these acts comes downstream from data generation, regardless of its origin or type: personal information, health information, intellectual property, financial – you name it, the list goes on and on.

Think about it: if you have no data, there is likely no cost to you. Conversely, without data, you can't generate a return, honest or illicit. Therefore, it's important to remember the life cycle of data, from inception to destruction. The steps along the life cycle allow you to determine what the costs of a breach may be to you.

Read the Report

What determines value?

In the movie "Indiana Jones and The Raiders of the Lost Ark," Indy's nemesis, Belloq, pulls out a pocket watch and says: "It's worthless. Ten dollars from a vendor in the street. But I take it, I bury it in the sand for a thousand years, it becomes priceless ... like the Ark. Men will kill for it. Men like you and me."

If you are not looking at factors that drive value, you will likely misappropriate the value of the data you could lose during a breach, in either direction (too high or too low). Within your operation, value may be derived through customer data, trade secrets, policy documents or business plans. Figuring out that value is a crucial first step.

Don't miss this boat. Everything downstream will likely be incorrect if the initial valuation is incorrect.

Who determines value?

Another key factor drives value: who is setting it? The exact same data set may be of extreme value to you, but utterly meaningless to me. After all, one person's trash is another person's wealth. Keep in mind a third party may be setting the price, too. For example, a regulator might deem certain types of data to hold some inherent or increased value (or risk). Depending on which industry you operate in, you may be bound by it. In your mind, you may not see the data as valuable. However, a governing agency may state that if you want to do business in this field you need to protect that data.

What is the value to you?

Of course, personal data has been a big juicy target for most of the major breaches recorded, but whether it has been the most costly is unknown. Many of the organizations that suffered these breaches are still up and running today. Larger groups can generally replace some personnel who take the fall and reach a settlement, even when millions of records are involved. But a smaller company, which may be responsible for less data being breached, has a greater likelihood of going out of business if there are disruptions to cash flows or legal bills it can't cover. That's just one at drives valuation.

What's in your vault?

Assume for a moment that you have been able to determine, with high confidence, what drives value. Now, the important action item is knowing if you hold that valuable data. Think of these three states:

- Known knowns: I know what type of data I hold, and I know where it is.
- Known unknowns: I know what type of data I hold, but I don't know where it is.
- Unknown unknowns: I don't know what type of data I hold, so I can't know where it is.

See the problem? Data discovery and classification are very important to find the cost of a breach. There are multiple proactive steps you can take if you have determined value, classification and location. Here is just a small list of some of the benefits:

- You can plan your infrastructure and architecture around data requirements, such as jurisdictional requirements, provenance, residence, segmentation compliance and so on.
- It is easier to follow requirements for encryption standards, access controls and group policies.
- You have access to response actions and requirements, and financial disclosures versus personal health information disclosures. Remember, part of the cost of a breach is the expertise you will require to respond. You might need a privacy lawyer, a Securities and Exchange Commission specialist or somebody familiar with regulations.
- Gain the ability to perform risk quantitative calculations. (For example, if I hold this type of data in this region, and it is breached and I lose x amount of records, the anticipated cost will be y.)

Simply put, you cannot determine the impact – or the cost – of a breach unless you know what factors feed into that. But once you do, your downstream actions end up being a whole lot easier.

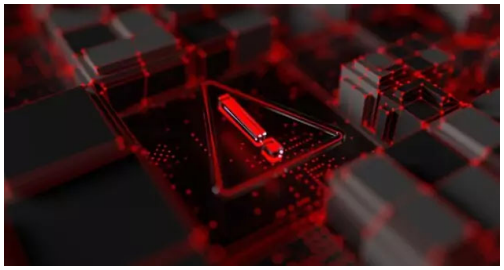
Who discovers and maintains what's in the vault?

If there was ever a team game for data classification and handling, it is data discovery and maintenance. The legal, finance and R&D teams may tell you what is valuable and what is a liability to hold or if lost. The security and developer teams may tell you how and where to protect the valuable data. The risk, resilience and incident response teams will likely be the ones who tell you what has been impacted by the breach. The infrastructure and compliance teams may be the ones determining what needs to be off-boarded, destroyed or maintained, both as a natural course of business and as data storage comes at its own cost.

What does it all mean? Simple: know your business. There is no single sweeping answer here. Just like 'the best food' is the food you like best, the most costly data is the type that is most costly to you.

Security breaches | cost of data breach | Breach | Cost of a Data Breach | Data Breach | Data Breaches

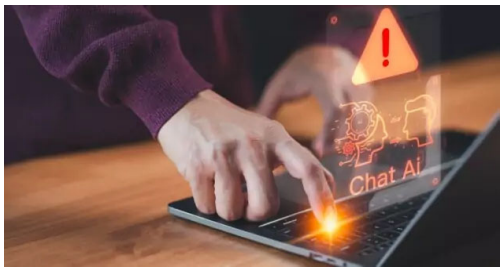
POPULAR



ARTIFICIAL INTELLIGENCE | April 30, 2024

AI cybersecurity solutions detect ransomware in under 60 seconds

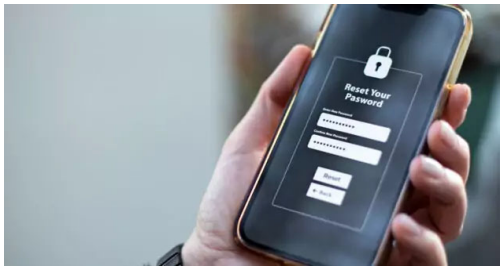
2 min read - Worried about ransomware? If so, it's not surprising. According to the World Economic Forum, for large cyber losses (€1 million+), the number of cases in which data is exfiltrated is increasing, doubling from 40% ...



RISK MANAGEMENT | April 24, 2024

Researchers develop malicious AI 'worm' targeting generative AI systems

2 min read - Researchers have created a new, never-seen-before kind of malware they call the "Morris II" worm, which uses popular AI services to spread itself, infect new systems and steal data. The name references the original...



IDENTITY & ACCESS | April 23, 2024

Passwords, passkeys and familiarity bias

5 min read - As passkey (passwordless authentication) adoption proceeds, misconceptions abound. There appears to be a widespread impression that passkeys may be more convenient and less secure than passwords. The reality is...

MORE FROM DATA PROTECTION

March 27, 2024

3 Strategies to overcome data security challenges in 2024

3 min read - There are over 17 billion internet-connected devices in the world — and experts expect that number will surge to almost 30 billion by 2030.This rapidly growing digital ecosystem...

March 12, 2024

How data residency impacts security and compliance

3 min read - Every piece of your organization's data is stored in a physical location. Even data stored in a cloud environment lives in a physical location on the virtual server. However, the data...

March 5, 2024

From federation to fabric: IAM's evolution

15 min read - In the modern day, we've come to expect that our various applications can share our identity information with one another. Most of our core systems federate seamlessly and bi-...

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.

Subscribe today →

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.