A screenshot of a computer

AI-generated content may be incorrect.

Step

I chose project 1-1: Examine Data Branches – Visual

Screenshot labeled Step 1 represents my first visit to the Information is beautiful website.

Step 2-6

The above bubbles are some interesting breach stories I read the quick version of. I especially was intrigued by the AOL attacks!

A close-up of a paper

AI-generated content may be incorrect.

A white background with black text

AI-generated content may be incorrect.

1. Organized Threat Actors

* ShinyHunters is a known cybercriminal group, which means this wasn’t random, it was strategic and deliberate.
* It introduces you to the concept of Advanced Persistent Threats (APTs) and cybercrime syndicates.

2. Global Reach

* With hundreds of millions affected worldwide, this breach shows how international companies face global risks.
* It’s a reminder that data protection laws vary by country, complicating response and liability.

3. Payment Data Exposure

* Even partial credit card details can be used for fraud or phishing.
* You could explore how attackers combine breached data with social engineering to bypass security.

4. Brand Reputation

* Ticketmaster’s brand is built on trust and convenience; this breach undermines both.
* It’s a great example of how cybersecurity is a business issue, not just a technical one.

A blue circle with white text

AI-generated content may be incorrect.**1. Operational Disruption**

* Unlike breaches focused on personal data, this one directly impacted business operations.
* It shows how cybersecurity isn’t just about protecting data; it’s about keeping systems running.

**2. Incident Response**

* Clorox detected and contained the breach within a month, which is relatively fast.
* This highlights the importance of monitoring, detection tools, and incident response plans.

Step 8-10

3. Financial Consequences

* A 2% stock drop shows how cybersecurity incidents affect investor confidence and brand reputation.
* You could explore how companies communicate breaches to the public and stakeholders.

4. Transparency Challenges

* The lack of detail about affected files raises questions about disclosure policies.
* A screenshot of a computer

  AI-generated content may be incorrect.It’s a good example of how organizations balance security, legal risk, and public trust.

1. **Third-Party Risk**

* GovPayNow.com wasn’t a government agency itself, but a vendor used by agencies.
* This highlights the importance of vendor vetting and supply chain security, a growing concern in cybersecurity.

**2. Web Browser Vulnerabilities**

* The breach occurred via a standard browser, suggesting poor access controls or insecure URLs.

Step 11-14

* It’s a reminder that front-end security (like HTTPS, authentication, and session management) is just as critical as backend defenses.

**3. Payment Data Sensitivity**

* Exposure of credit card digits raises the stakes, this isn’t just about identity theft, but financial fraud.
* You could explore how PCI compliance standards are designed to prevent this kind of breach.

**4. Public Trust**

* Because this service was tied to government agencies, the breach could erode citizen trust in digital government services.
* It’s a great example of how cybersecurity intersects with public policy and ethics.

**15-16. Does this graphic convey a compelling story of data breaches? How does this visualization help you with the understanding of threats?**

This graphic helped me see just how different breaches can be, not just in size but in how they happen. Being able to filter by method or data type made it easier to spot patterns, like how poor security keeps showing up in certain industries. It’s not just a visual, it helped me understand the bigger picture of threats and how they evolve.