Best Practices for Data Privacy Breach Response Lessons Learned from Social Media Case Studies

Anne Connell (Carnegie Mellon University, US)
Lauren Cooper (Carnegie Mellon University, US)

Speakers

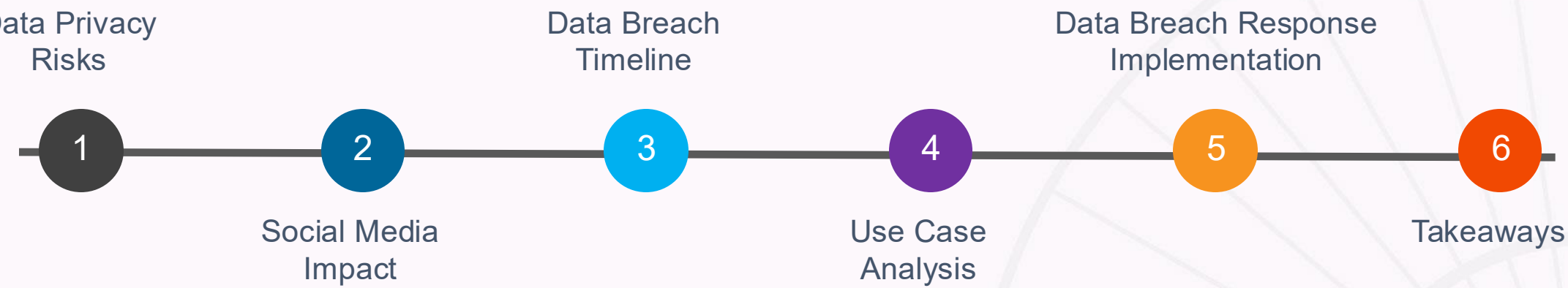
Anne Connell
CISSP, CIPM, CIPP/US

- Member of the technical staff at Carnegie Mellon University (CMU)
- Experience in software development, resilience management, privacy program development, and instructional design
- Research interests include privacy, social cybersecurity, security by design, and human computer interaction
- Adjunct Professor of Privacy in the Digital Age at the CMU Heinz College of Information Systems and Public Policy
- Active speaker on youth online safety and social media

Lauren Cooper, CISSP

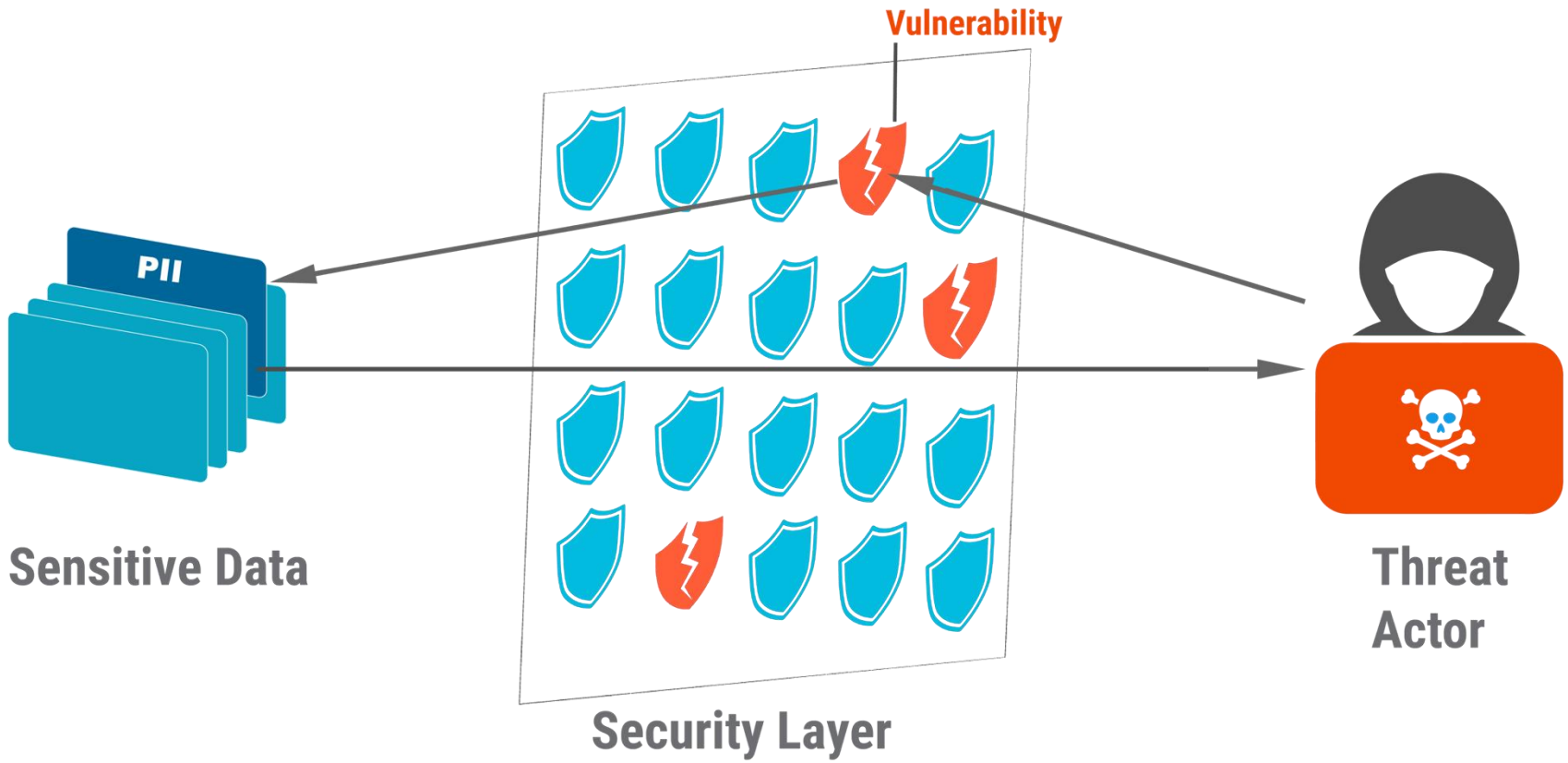
- Member of the technical staff at Carnegie Mellon University (CMU)
- Experience in IT operations, information security, and privacy
- MS in Information Security Policy and Management from CMU
- Research interests include privacy, community approaches to cybersecurity, security by design in complex systems, and human factors

Agenda


Data Privacy Risks
1
2
Social Media Impact
Data Breach Timeline
3
4
Use Case Analysis
Data Breach Response Implementation
5
6
Takeaways

Data Privacy Risks

DATA BREACH


Vulnerability
PII
Sensitive Data
Security Layer
Threat
Actor

Almost 98% of organizations have a relationship with at least one 3rd party that has experienced a data breach.

Source: IBM Cost of a Data Breach 2024 Report, https://www.ibm.com/reports/data-breach

The average cost of a data breach, globally

$4.88 M

Source: IBM Cost of a Data Breach 2024 Report, https://www.ibm.com/reports/data-breach

The notification costs of a data breach, a 19.4% increase

$570 K

It takes organizations an average of 204 days to identify a data breach and 73 days to contain it.

Source: IBM Cost of a Data Breach 2024 Report, https://www.ibm.com/reports/data-breach

The most common link in data breaches is the human element.

74%

Source: Verizon 2025 Data Breach Investigations Report, https://www.verizon.com/business/resources/reports/dbir/

Social Media is a Key Communication Vehicle

Social media is a ***tool*** used during a data breach

- Provides 2-way communication
- Requires a shorter lifecycle
- Allows re-sharing of new information compared with traditional media
- It is for ***crisis communication***, **not** “just PR”

Social Media Impact

It has become more accepted that data breaches happen, and organizations are more comfortable disclosing they have been victim of an attack.

It has become more accepted that data breaches happen, and organizations are more comfortable disclosing they have been victim of an attack. ***However, organizations are being judged more by how they manage a breach.***

Today in the age of social media, if your organization is in the center of a crisis, if it doesn't say anything, somebody else will.

Disconnect: people getting information and organizations sharing information

Social Media Use Gap

In an interconnected world, social media is often the first place people turn to for information during a crisis.

- Almost **68%** of adults get news from social media platforms and that number is increasing

- Approximately **45%** of organizations use social media platforms for communication purposes, disseminate news, and increasingly use to combat misinformation

Note(s): Worldwide; February 2025; social networks and messenger/chat app/voip included; figures for TikTok does not include Douyin

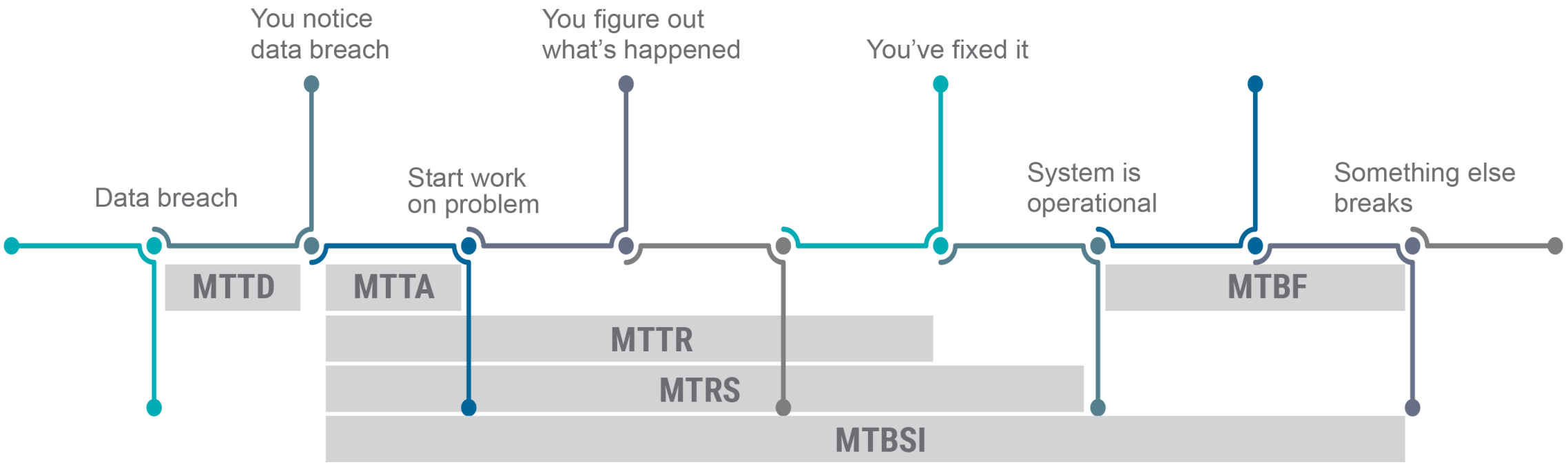
Source(s): We Are Social; DataReportal; Meltwater; ID 272014, https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/

Data Breach Response

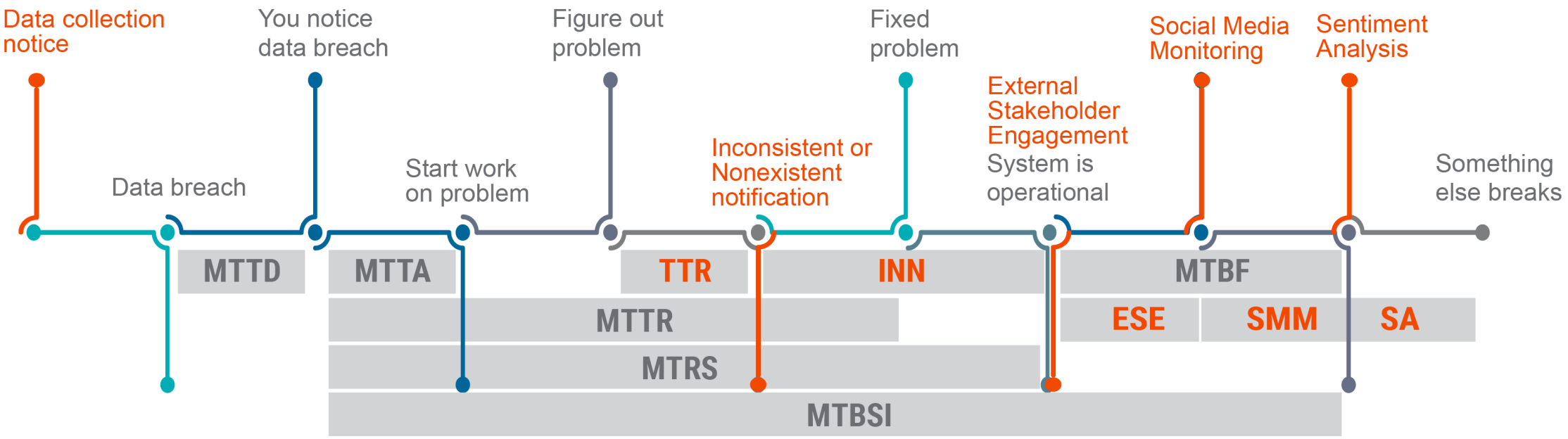
Data Breach Response (DBR)

- *Scope*: A specific type of security incident involving the unauthorized access, disclosure, or acquisition of sensitive data
- *Examples*: Loss or theft of customer data, ransomware attacks where data is exfiltrated
- *Goal*: Not only minimize damage, restore systems and manage legal and reputational risks
- *Response*:
  - Investigation: Determining the scope and impact of the breach, identifying the compromised data and systems.
  - Notification: In many jurisdictions, data breaches require mandatory notification to affected individuals, regulators, and law enforcement within specific timeframes.
  - Legal Compliance: Adhering to data breach notification laws and regulations (e.g., GDPR, DORA, HIPAA, CCPA).
  - Public Relations: Managing communications with the public to maintain trust and minimize reputational damage.
- *Potential for Severe Consequences*: Financial penalties, legal action, and significant reputational damage

Standard IR Timeline



DBR Timeline



How Does DBR augment an IR?

In other words, what to do if you get hacked

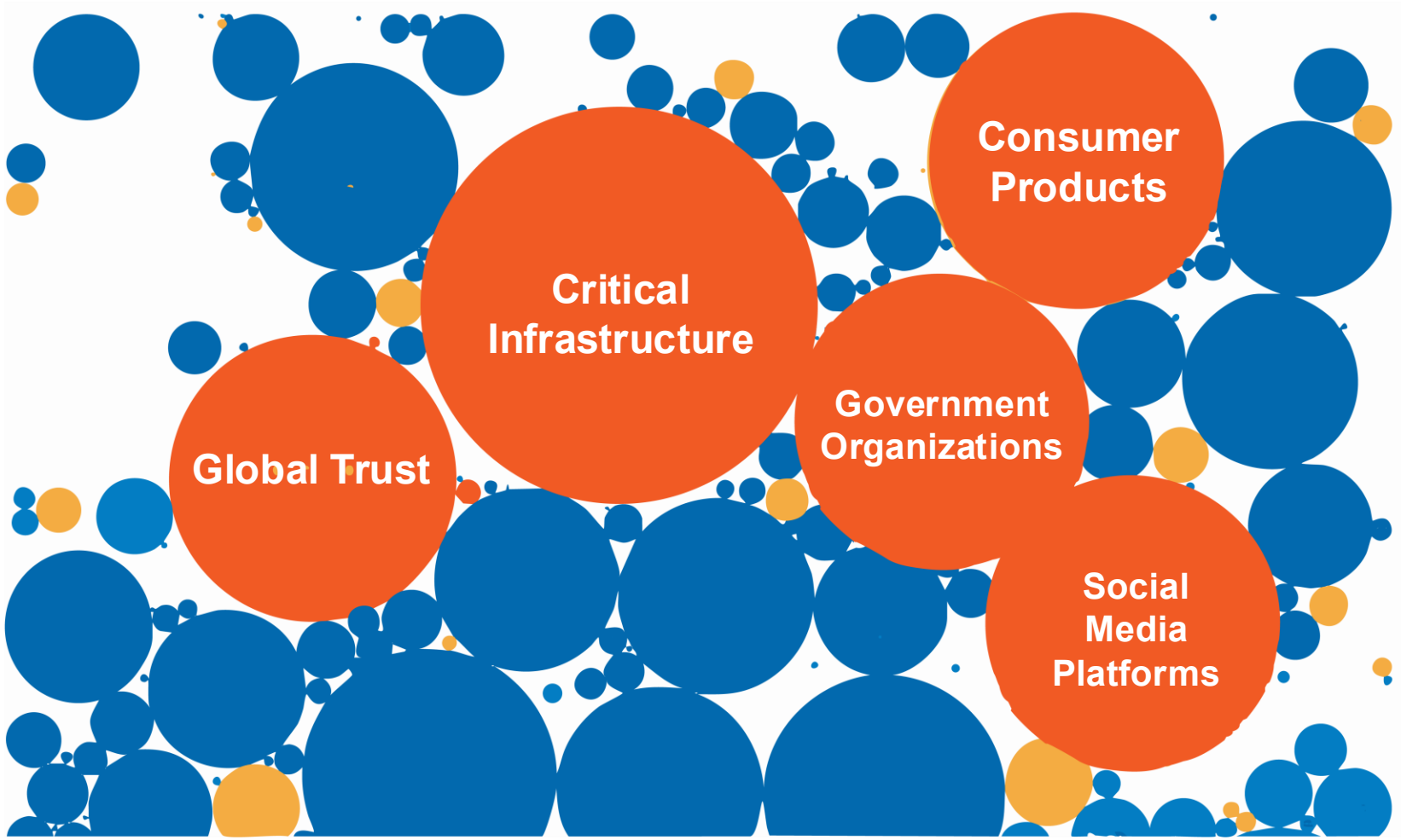
- Data breach response plan is essential
  - Preferably separate from the IR plan
- Defines the policies, team members with defined roles and responsibilities, steps, and training for managing a data breach
- Team needs to includes a leader, lead investigator, ***communicator***, and legal representative
  - DBR Communicator role has *different* responsibilities from the standard IR communicator
- Critical to conduct tabletop exercises and regular training

DBR Steps

- ***Provide data collection notice when to all new data subjects***
- Identify critical systems and categorize data by sensitivity
- ***Prepare and implement of a data breach policy and response plan***
- ***Inform personnel what a data breach is, how to identify one, and escalation procedures***
- ***Create clear communication protocols before and during data breach***
- ***Notify when and how for suspected data breaches including internal and external partners (legal and compliance authorities, 3rd parties, service agreements, etc.)***
- *Detection and analysis with advanced monitoring tools (SIEMs,* ***sentiment analysis***, etc.)
- Containment to prevent further data loss and investigate source
- Conduct ***Assessments, Tabletop exercises, and Training specifically for DBR***

Use Case Analysis

Social Media Use Case Categories



Analysis Results – Criteria

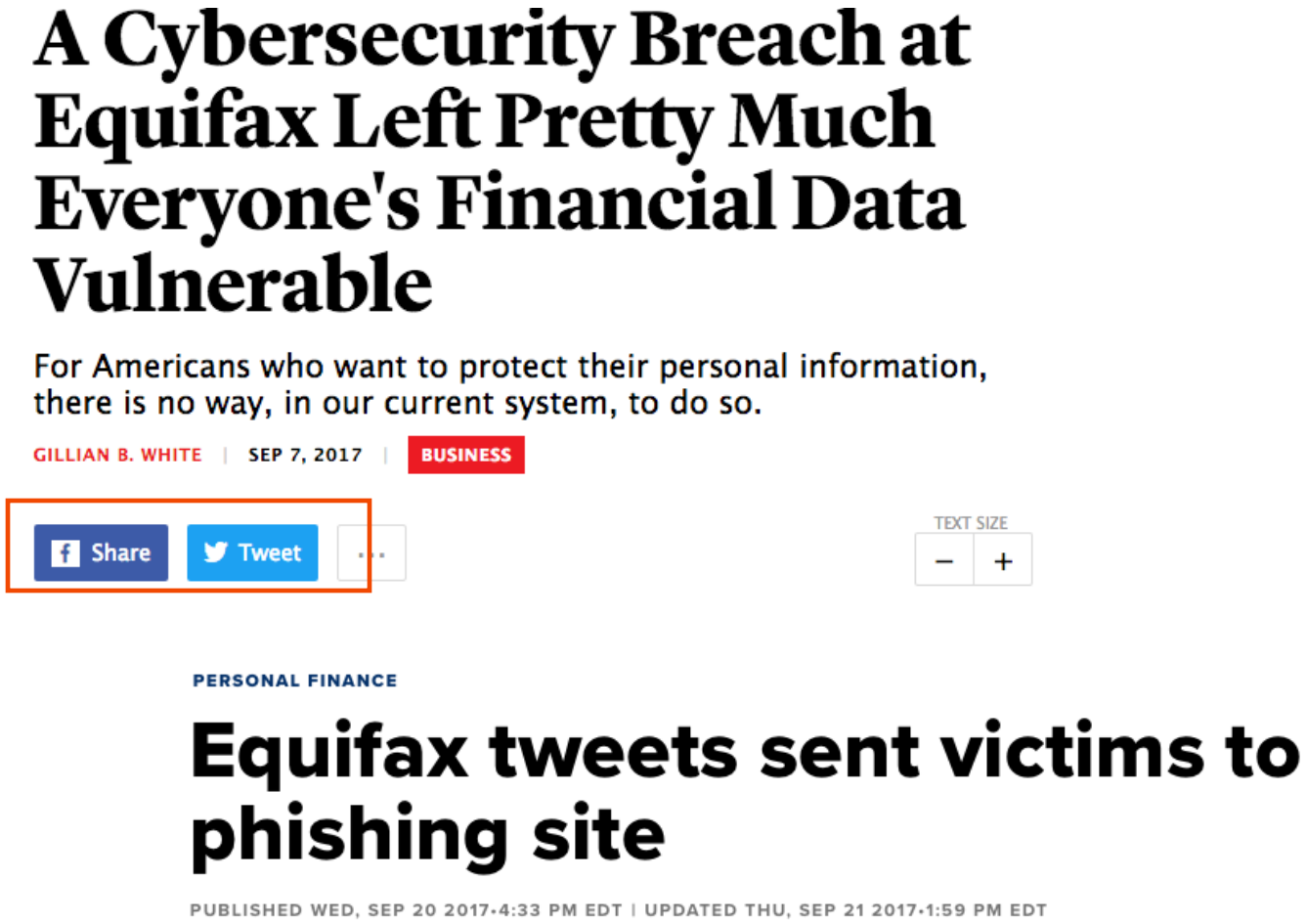
- Type of breach/Vector
- Region
- Sector
- Org/Company Name
- Data Collection Notice
- Data Breach Response Plan
- Problem/Violation
- Duration
- Affected data
- Affected entities
- Harms and potential harms
- Incident Report Time
- Time to Official Notification
- Response Time Effectiveness
- Regulatory Requirements (EU, US, ASIA, DORA)
- Right to Be Forgotten
- Penalties
- Social Media Posting Platforms
- Post-Breach Engagement
- Media Sentiment Analysis
- Customer Retention
- Customer Trust Indicators (provide trusted information)

Equifax – 2017

https://www.cnbc.com/2017/09/20/equifax-tweets-sent-breach-victims-to-phishing-site.html

Equifax

- *Data subjects* – 143m
- *Regulatory impact* – US FTC Act GLB Act's Safeguards Rule
- *External parties* – 3rd party phishing site
- Failure to monitor on Twitter
- *Outcome* – Penalties $700m, congressional hearings



A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

For Americans who want to protect their personal information, there is no way, in our current system, to do so.

GILLIAN B. WHITE | SEP 7, 2017 | BUSINESS

Share Tweet ...

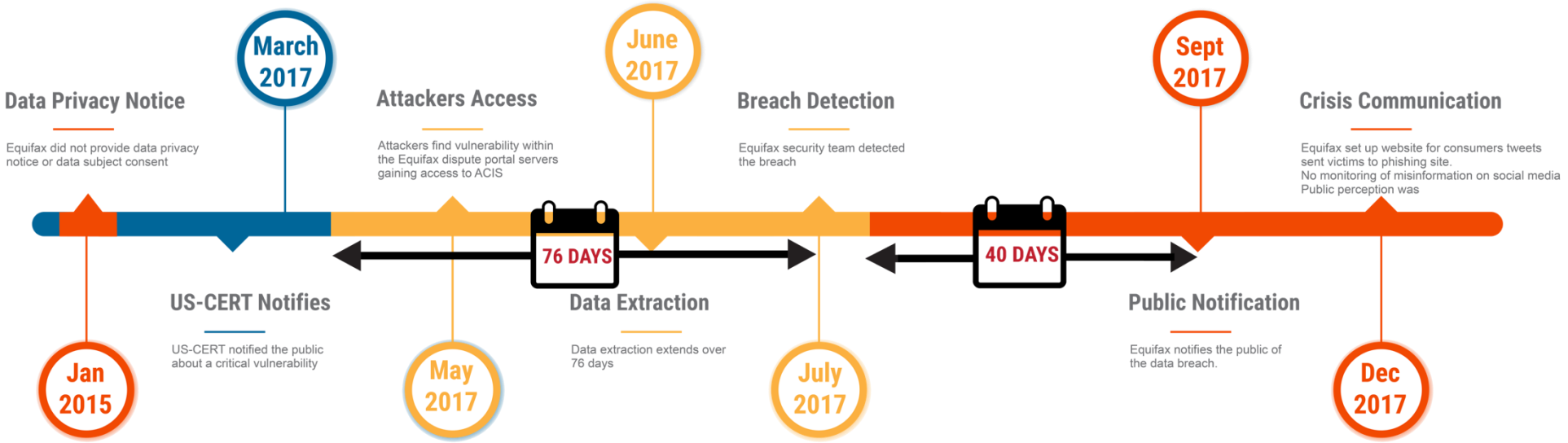
TEXT SIZE – +

PERSONAL FINANCE

Equifax tweets sent victims to phishing site

PUBLISHED WED, SEP 20 2017·4:33 PM EDT | UPDATED THU, SEP 21 2017·1:59 PM EDT

EQUIFAX BREACH



Takeaways from this use case:

- **No notification or acknowledgement of breach after detection for 40 days**
- **Crisis communication failures – No social media monitoring**
- **More people affected by incorrect information via social media (phishing site)**
- **Company profiting from the breach (selling LifeLock before breach notification)**

Social Media Platforms

Facebook – 2019

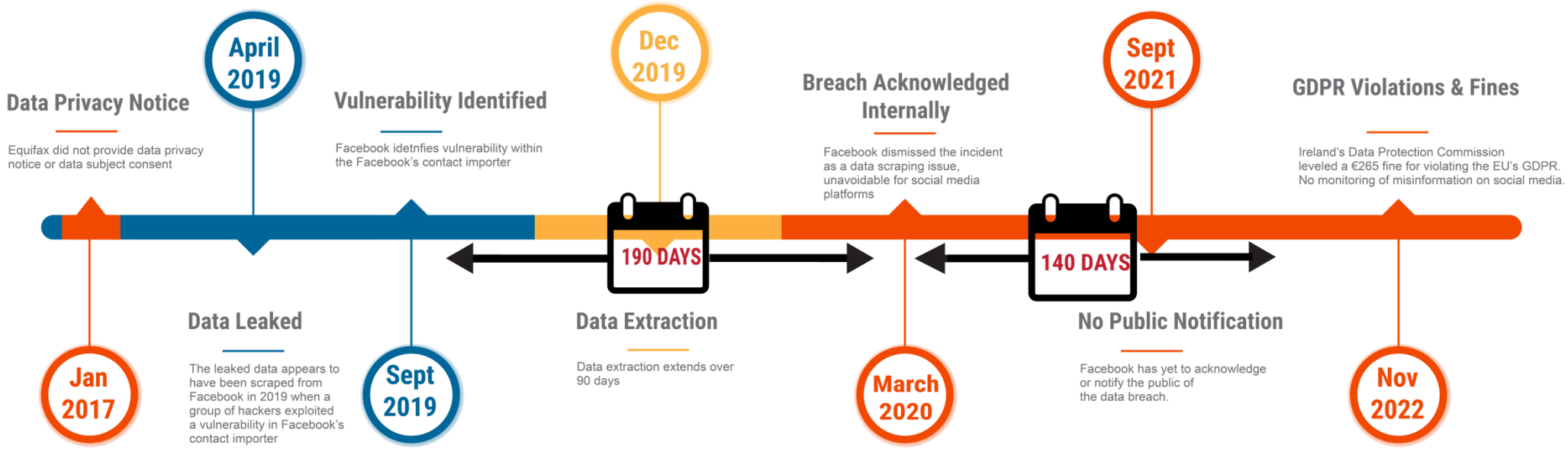
https://www.bbc.com/news/technology-56815478

Facebook

- *Data subjects* – 533 million
- *Regulatory impact* – EU's GDPR
- *External parties* – database was leaked on the dark web for free adding more criminal exposure
- *Outcome* – Penalties from Ireland's Data Protection Commission leveled a **€265m** fine against Meta and **€405m** fine for privacy violations by Instagram

https://www.bbc.com/news/technology-56815478
https://firewalltimes.com/instagram-data-breach-timeline/

FACEBOOK BREACH



Takeaways from this use case:

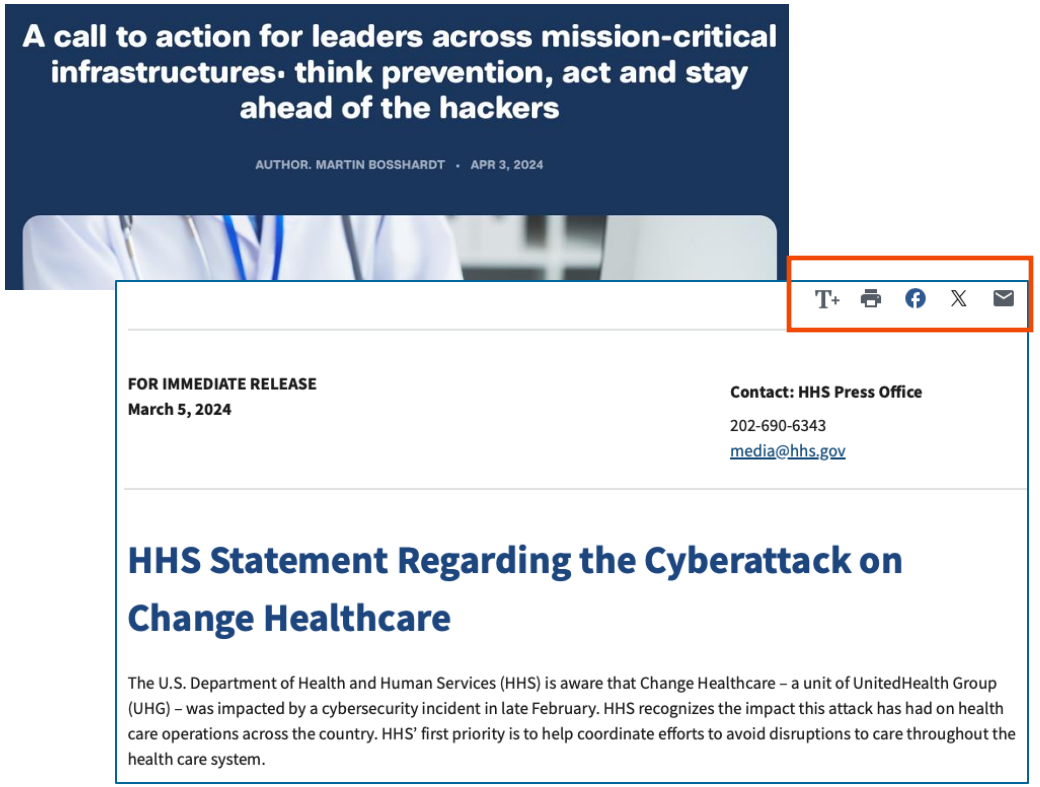
- **Internal notifications can easily become public**
- **No notification or acknowledgement of breach**
- **Lacked coordination with 3rd parties delaying remediation**
- **Data subjects further affected by platform failing to protect their information**

Change Healthcare - 2024

https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html

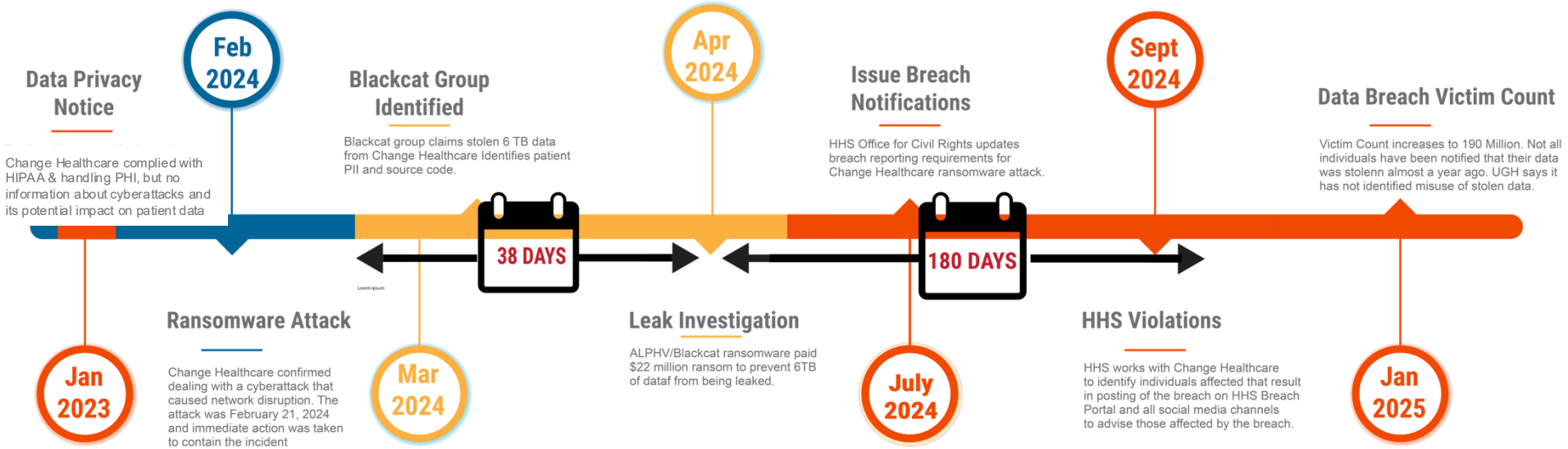
Change Healthcare

- *Data subjects* – 190 million
- *Regulatory impact* – US Health Insurance Portability and Accountability Act (HIPAA); US Health Information Technology for Economic and Clinical Health Act (HITECH Act); US Federal Trade Commission (FTC); US Securities and Exchange Commission (SEC)
- *External parties* – Ransomware by Blackcat/ALPHV threat group
- *Outcome* – Multiple lawsuits leading to settlements with affected individuals and providers; United Health Group Anticipates $1.6 Billion Loss to Ransomware Attack



https://www.anapaya.net/blog/a-call-to-action-for-leaders-across-mission-critical-infrastructures-think-prevention-act-and-stay-ahead-of-the-hackers

CHANGE HEALTHCARE BREACH



Takeaways from this use case:

- **Delayed notification of breach, lack of data privacy notice and data subject consent**
- **Widespread disruption due to breach without corresponding communication**
- **Lack of recourse for data subjects whose PHI was published during breach**
- **Crisis communication failures – No social media monitoring**

Associated Press & Twitter - 2013

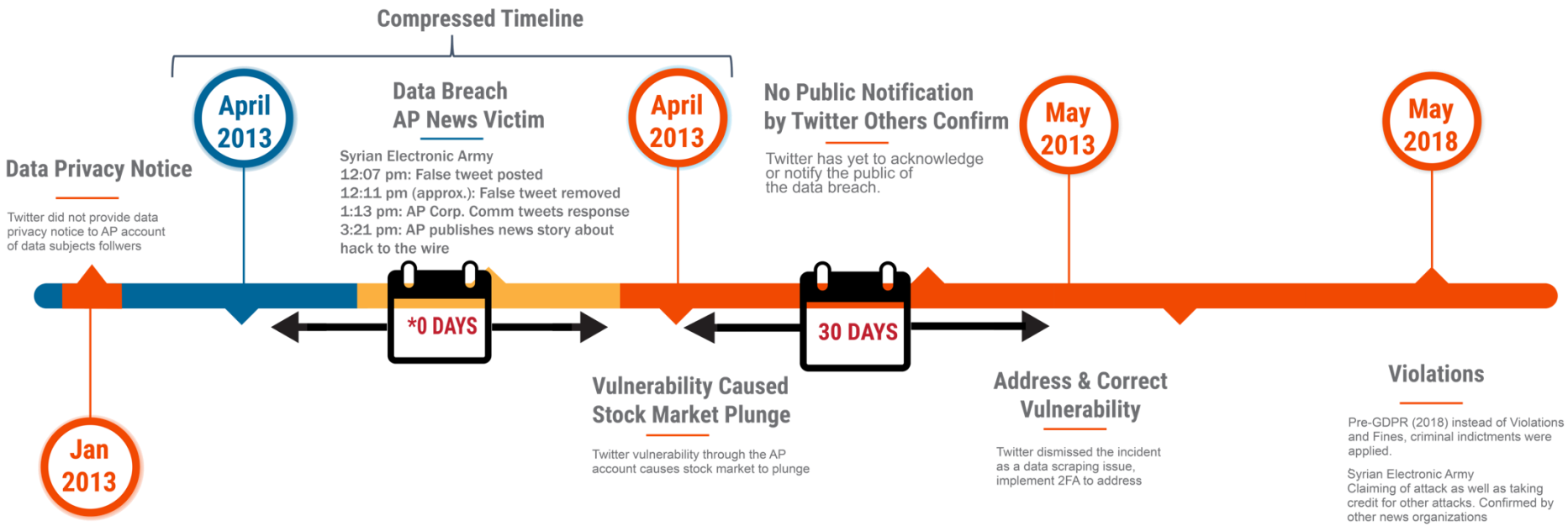
https://web.archive.org/web/20130423211938/http://bigstory.ap.org/article/hackers-compromise-ap-twitter-account

The Associated Press & Twitter

- *Data subjects* – 1 account, 1.9 million followers
- *Regulatory impact* – Multiple criminal indictments against threat actors (2016 & 2018)
- *External parties* – Syrian Electronic Army threat group
- *Outcome* – Stock market lost approximately $136.5 billion in market cap, but quickly recovered

Source: https://www.justice.gov/usao-edva/pr/two-members-syrian-electronic-army-indicted-conspiracy

AP & TWITTER BREACH



Takeaways from this use case:

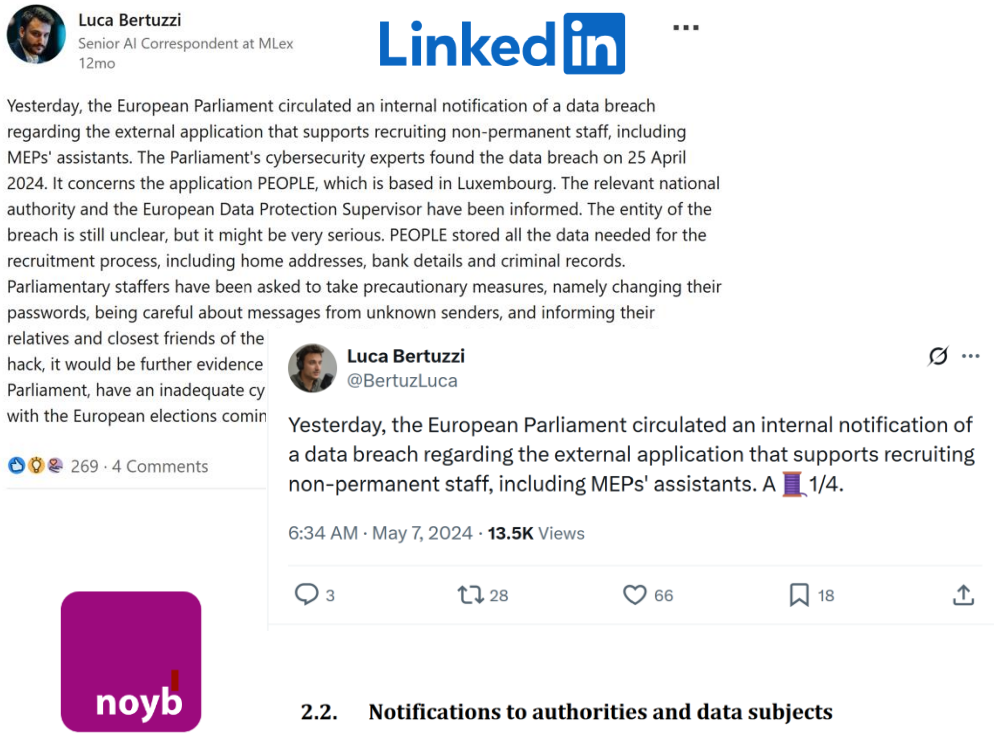
- No notification or acknowledgement of breach by Twitter
- Breach response complicated by platform and 3rd party challenges
- Criminal charges may take years to manifest

European Union Parliament (EU) - 2024

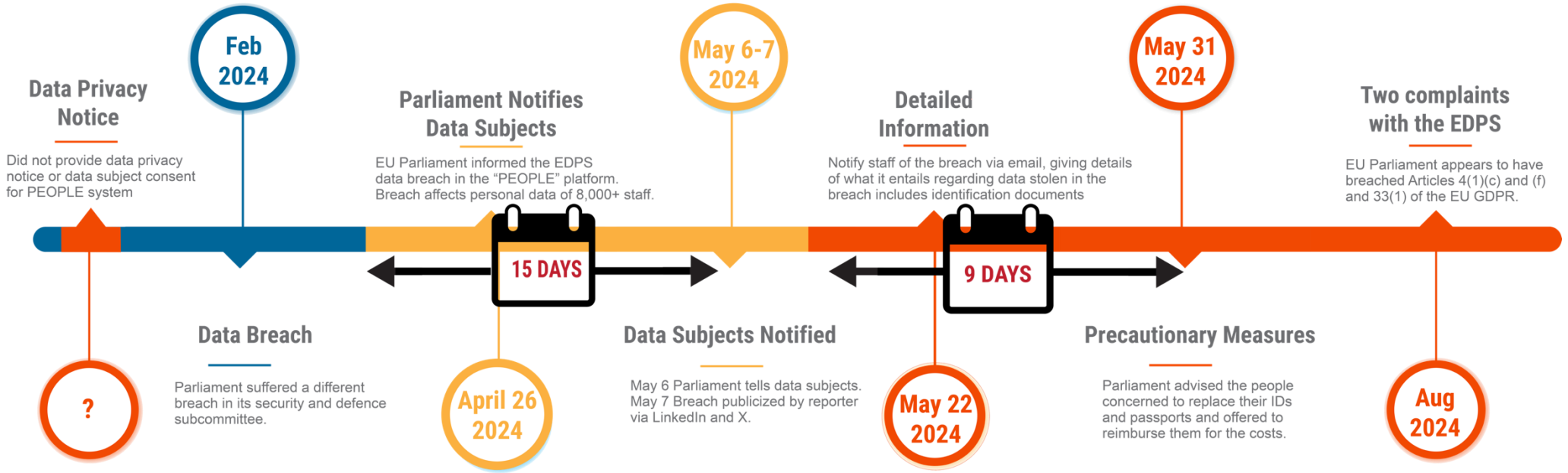
https://www.politico.eu/article/eu-parliament-id-cards-personal-records-data-breach-chamber-apa-victims/

EU Parliament Breach

- *Data subjects* – 8,000 +
- *Regulatory impact* – GDPR EU Parliament informed the European Data Protection Supervisor (EDPS) about data breach in PEOPLE
- *External parties* – Unnamed threat actor and unclear motivation for the breach
- *Outcome* – Every record in the PEOPLE system compromised, including ID cards, passports, criminal record extracts, residence documents, marriage certificates



EU PARLIAMENT BREACH



Takeaways from this use case:

- **No public notification or acknowledgement of breach until after media reports**
- **Internal notifications can easily become public**
- **Multi-language environments require multi-language communications for including social media channels**

75% of the increase in average breach costs in this year's study was due to the *cost of lost business and post-breach response activities.*

The lesson: investing in post-breach response preparedness can help dramatically lower breach costs.

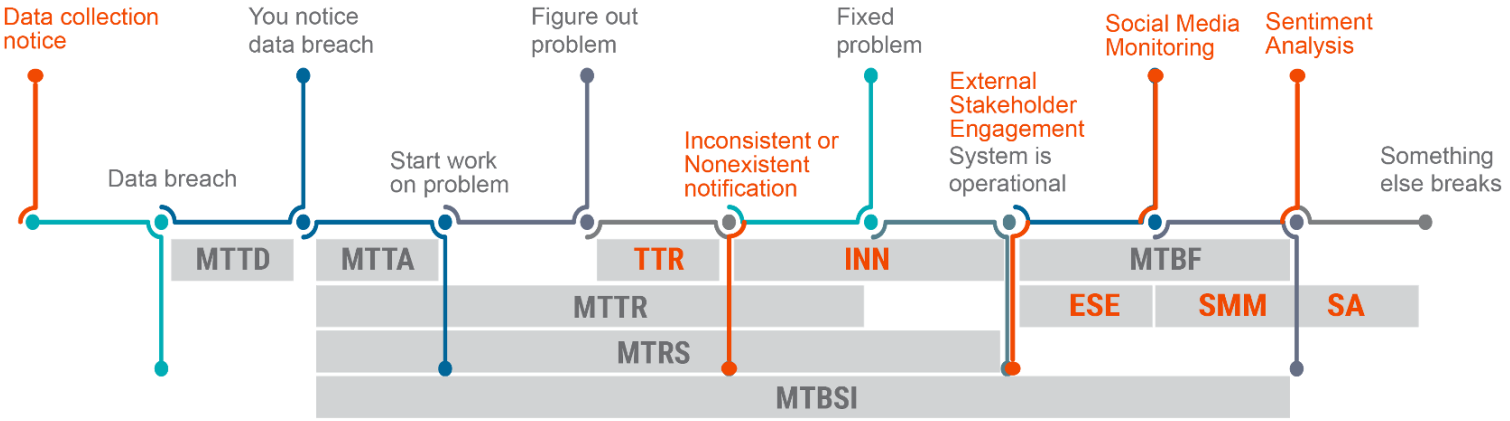
Source: IBM Cost of a Data Breach 2024 Report

Implementation

Gaps exist throughout the execution of an incident response plan, especially for communication of the data breach. Data subjects may not be aware of data collection.

Data Breach Response Timeline

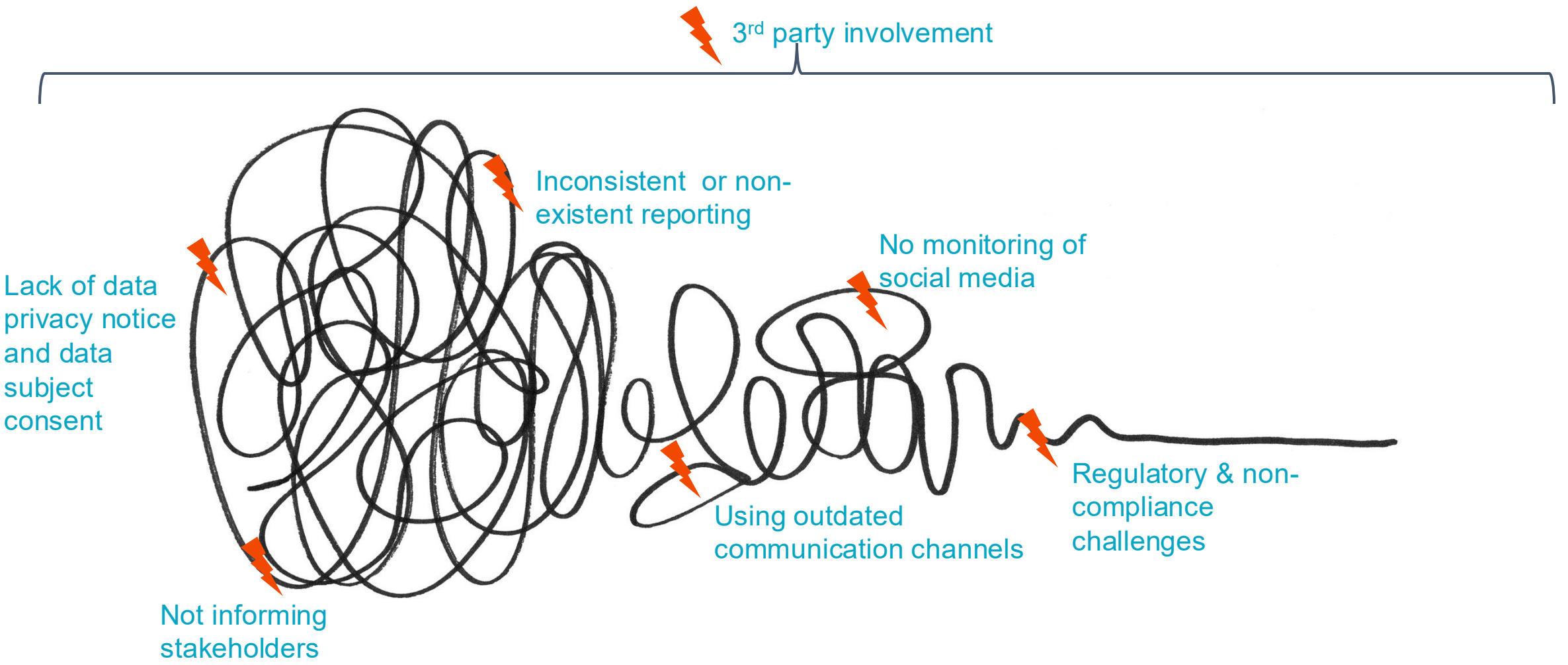
The Plan



vs.

The Reality

Major Breakdowns



Problem: Third-Party Involvement

- Third-parties often serve as a critical path in incident response
- Crisis communication plan should include provisions for third-party involvement
- Third-parties may be involved as data subjects, vendors, platforms, or other entities
- Third-parties may be involved before, during, and/or after a breach
- ***Consider all relevant third-parties as potential data subjects, potential sources of breaches, and as potential customers or suppliers***

Success Factors

- *Data Collection Notice*
- *Data Breach Response Plan*
- *Time to Official Notification*
- *Regulatory Requirements (EU, US, ASIA, DORA)*
- *Right to Be Forgotten*
- *Customer Trust Indicators (provide trusted information)*

Problem: Lack of data subject notice & consent

- Crisis communication starts at the ***first*** point in the information life cycle where data is collected using the privacy notice
- Communication plan should include notice of information collection that is consistent with the privacy notice
- Transparency is key to ensure you're using data for the purpose stated
- ***Prioritize the use of plain language***

Success Factors

- *Data Collection Notice*
- *Data Breach Response Plan*

Problem: Not informing stakeholders

Inform stakeholders simultaneously

Not just these…

Internal

- **IT**
- **Staff**
- **Board**

But also, these

External

- Partners & MSPs
- Suppliers
- APIs
- Customers
- Regulators
- PII holders
- ICO
- Inter-jurisdictional entities
- Data Subjects

Success Factors

- *Data Breach Response Plan*
- *Time to Official Notification*

It does not matter how wonderful the incident response plan is if it is unknown

Problem: Inconsistent or non-existent reporting

- Set up a dedicated cross-functional cyber crisis comms team with ***clear roles & responsibilities***
  - IR team leads; marketing team should **not** take lead during crisis
  - Identify the spokespersons; determine who will publicly represent the company
- Create process for **approving** social media crisis communications
- Swift, consistent, and transparent statements

Success Factors

- *Data Breach Response Plan*
- *Time to Official Notification*

Problem: Using outdated communication channels

- Define use cases for each platform
- Be aware of platform inconsistencies between organizations and individuals
- Avoid a communication vacuum by selecting the correct communications channels
- ***It is essential to include information posted on all social media platforms about next steps for data subjects***

Success Factors

- *Data Breach Response Plan*
- *Right to Be Forgotten*
- *Post-Breach Engagement*
- *Media Sentiment Analysis*
- *Customer Trust Indicators (provide trusted information)*

No monitoring of social media

- Social media response metrics can be used for process improvement (“lessons learned”)
- Have a proactive plan to answer *or* not answer comments, including ***response templates***
- Define the signal to avoid the noise
- Embrace the human factor: use a known face of the company on social media to enhance trust and demonstrate accountability
- ***Crisis communications should not be a one-way broadcast of information***

Success Factors

- ***Post-Breach Engagement***
- ***Media Sentiment Analysis***
- ***Customer Retention***
- ***Customer Trust Indicators (provide trusted information)***

Problem: Regulatory and non-compliance challenges

- Must include inter-jurisdictional reporting requirements in crisis communication plan
- Consider laws, regulations, and frameworks such as:
  - EU General Data Protection Regulation (GDPR)
    - Incident Response Plan (IRP)
    - Article 4(12) and Articles 33 and 34 and Recitals (85) to (88) of the GDPR
  - NIST Cybersecurity Framework 2.0 (NIST CSF)

Success Factors

- *Data Breach Response Plan*
- *Data Collection Notice*
- *Time to Official Notification*
- *Regulatory Requirements (EU, US, ASIA, DORA)*
- *Right to Be Forgotten*

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Takeaways

Key Takeaways

- Data breaches are a ***crisis***.
- Failure to communicate about them in a timely manner makes organizations look like they're potentially incompetent or hiding something.
- Information will fill a communication vacuum; quickly mobilizing a coherent messaging strategy will help to control the narrative.
- Social media can get the message out faster and more effectively.

Embrace Social Media

- The role of social media in crisis management continues to evolve alongside platform changes and new use cases
- Organizations should regularly assess their use of social media as part of their crisis response plan
- ***Social media can be a powerful tool for communicating about data breaches while maintaining trust and transparency***

Questions?

Presenters

Anne Connell
Senior Cybersecurity Engineer
Email: aconnell@cmu.edu

Lauren Cooper
Cybersecurity Engineer
Email: lcooper@cmu.edu

37TH ANNUAL
FIRST
CONFERENCE

COPENHAGEN
DENMARK

#FIRSTCON25

JUNE
22 • 27
2025

FORTRESSES OF THE FUTURE - BUILDING BRIDGES NOT WALLS