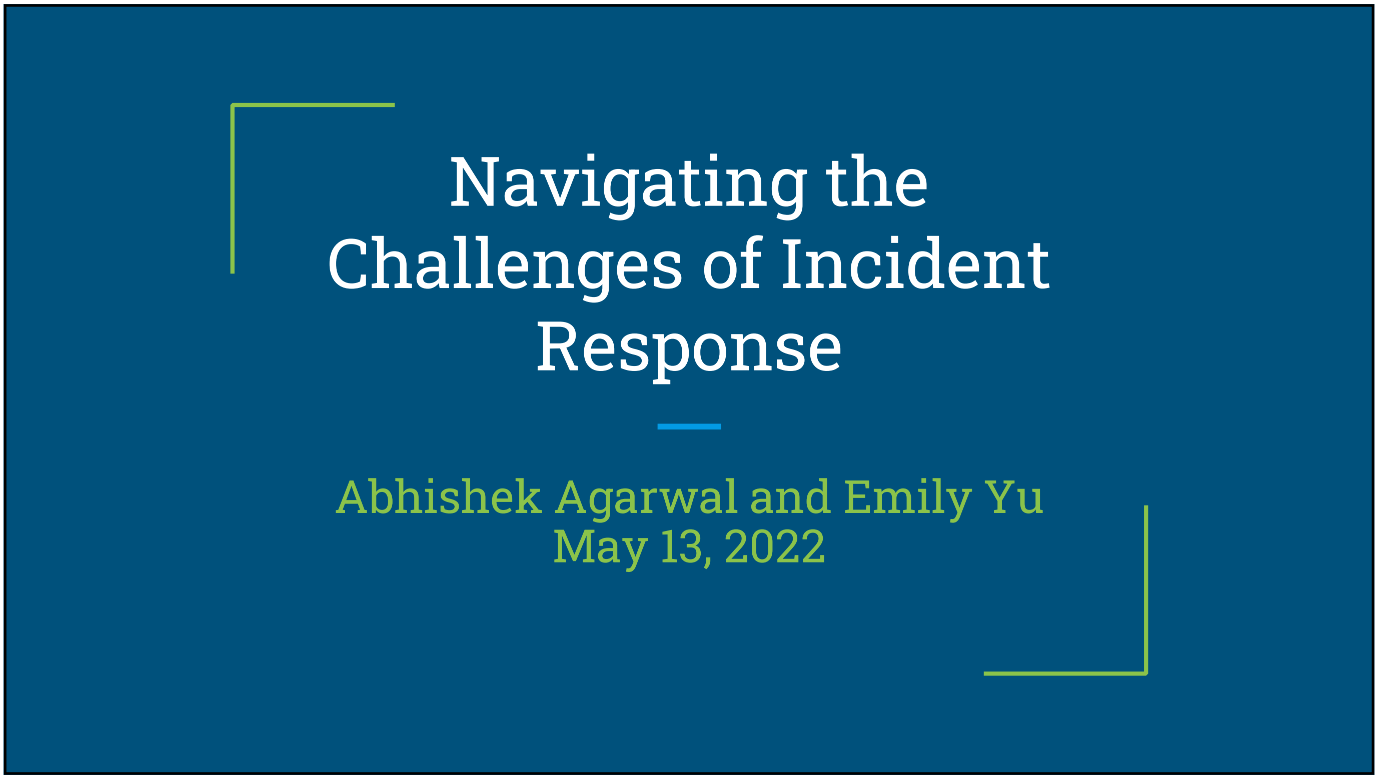
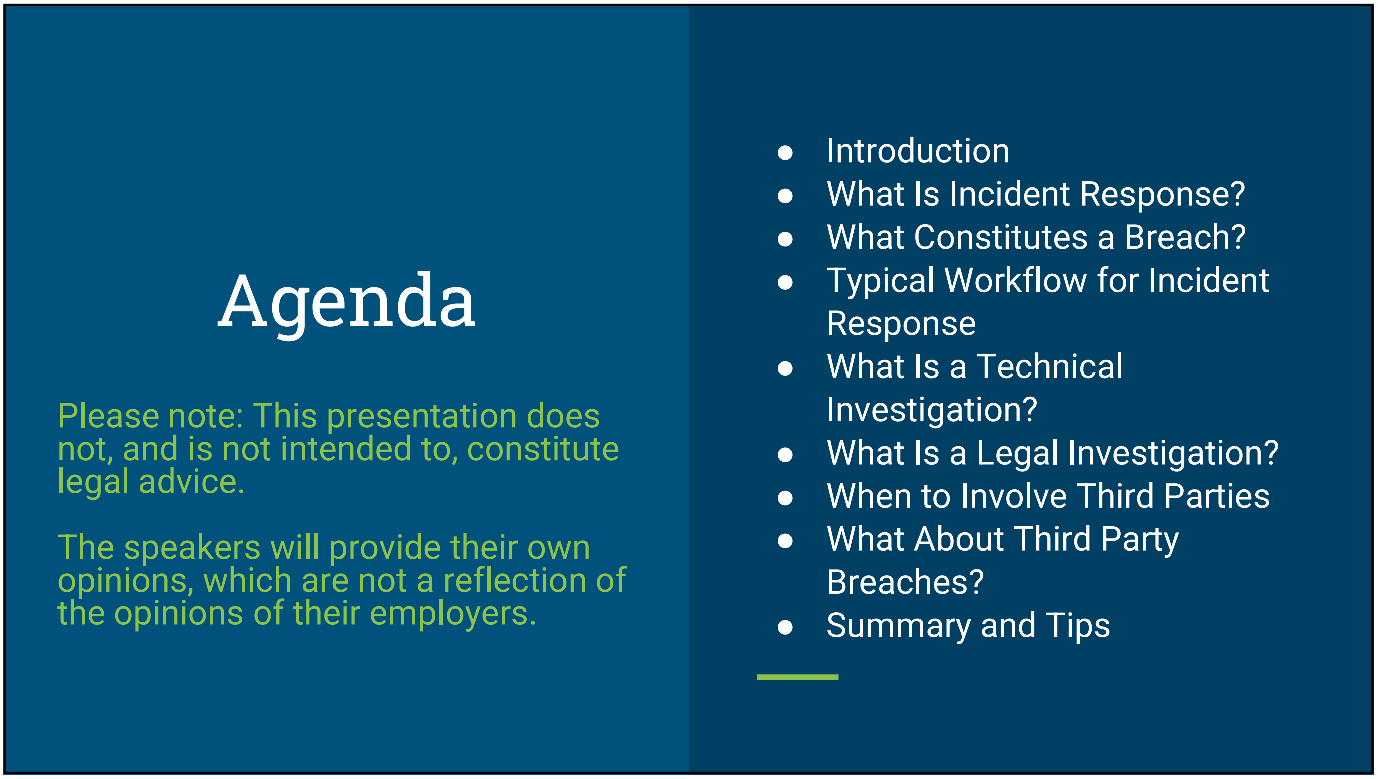


Navigating the Challenges of Incident Response

Abhishek Agarwal and Emily Yu
May 13, 2022

1



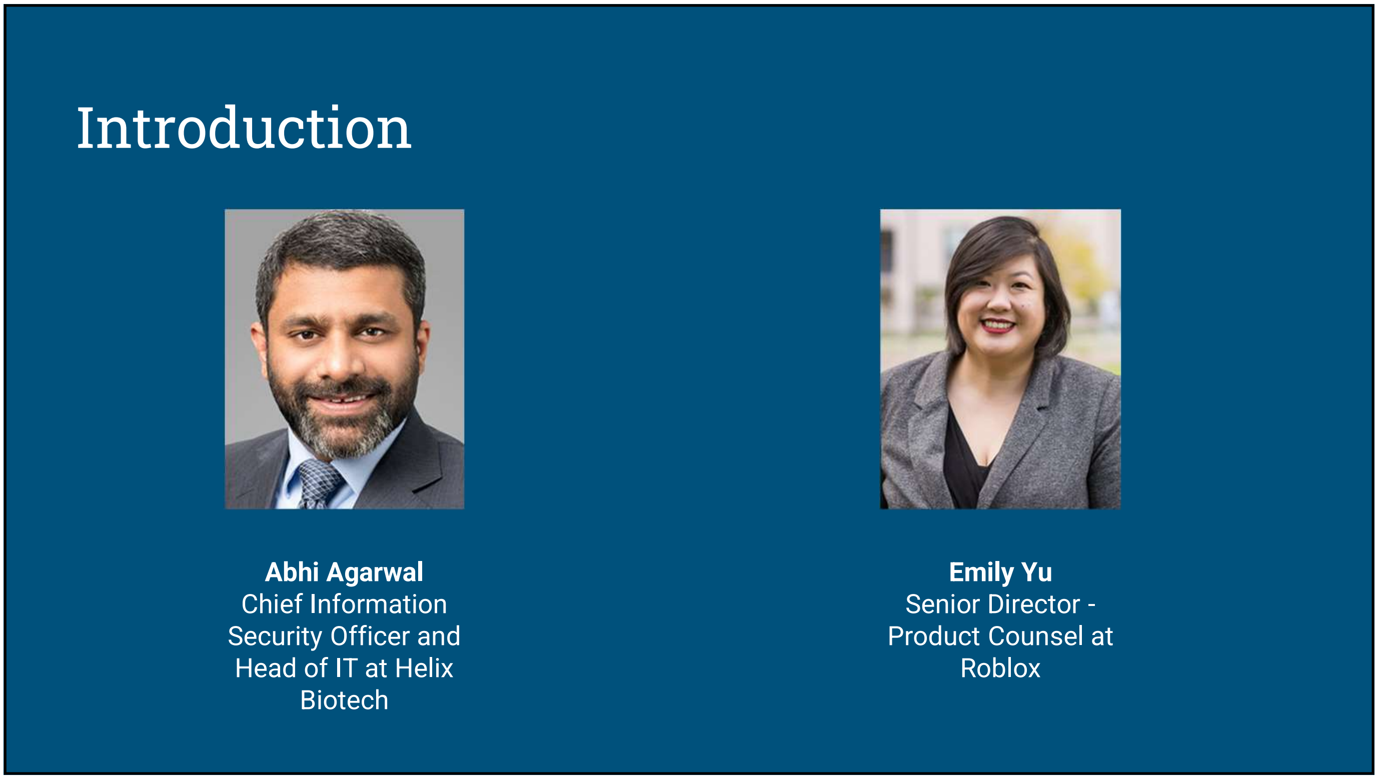
Agenda

Please note: This presentation does not, and is not intended to, constitute legal advice.

The speakers will provide their own opinions, which are not a reflection of the opinions of their employers.

- Introduction
- What Is Incident Response?
- What Constitutes a Breach?
- Typical Workflow for Incident Response
- What Is a Technical Investigation?
- What Is a Legal Investigation?
- When to Involve Third Parties
- What About Third Party Breaches?
- Summary and Tips

2

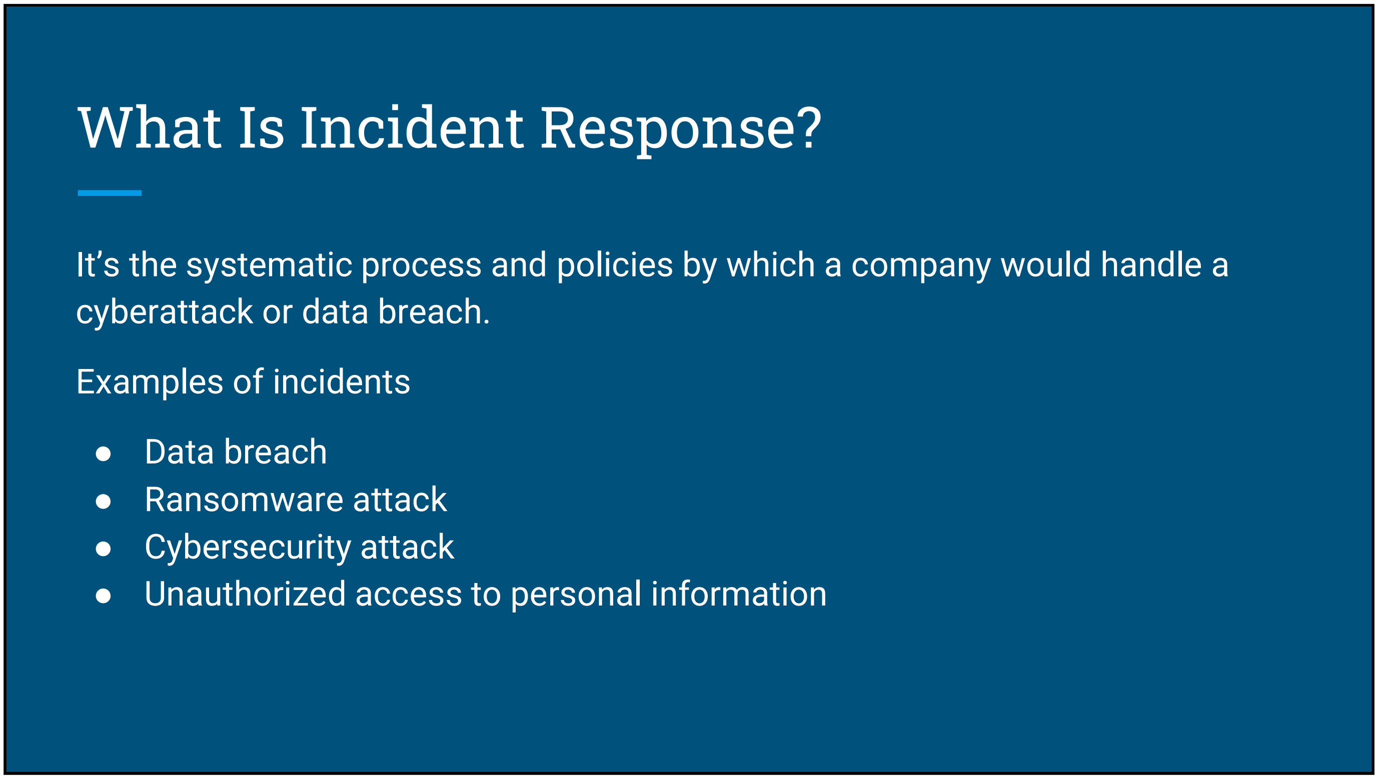


Introduction

Abhi Agarwal
Chief Information Security Officer and Head of IT at Helix Biotech

Emily Yu
Senior Director - Product Counsel at Roblox

3



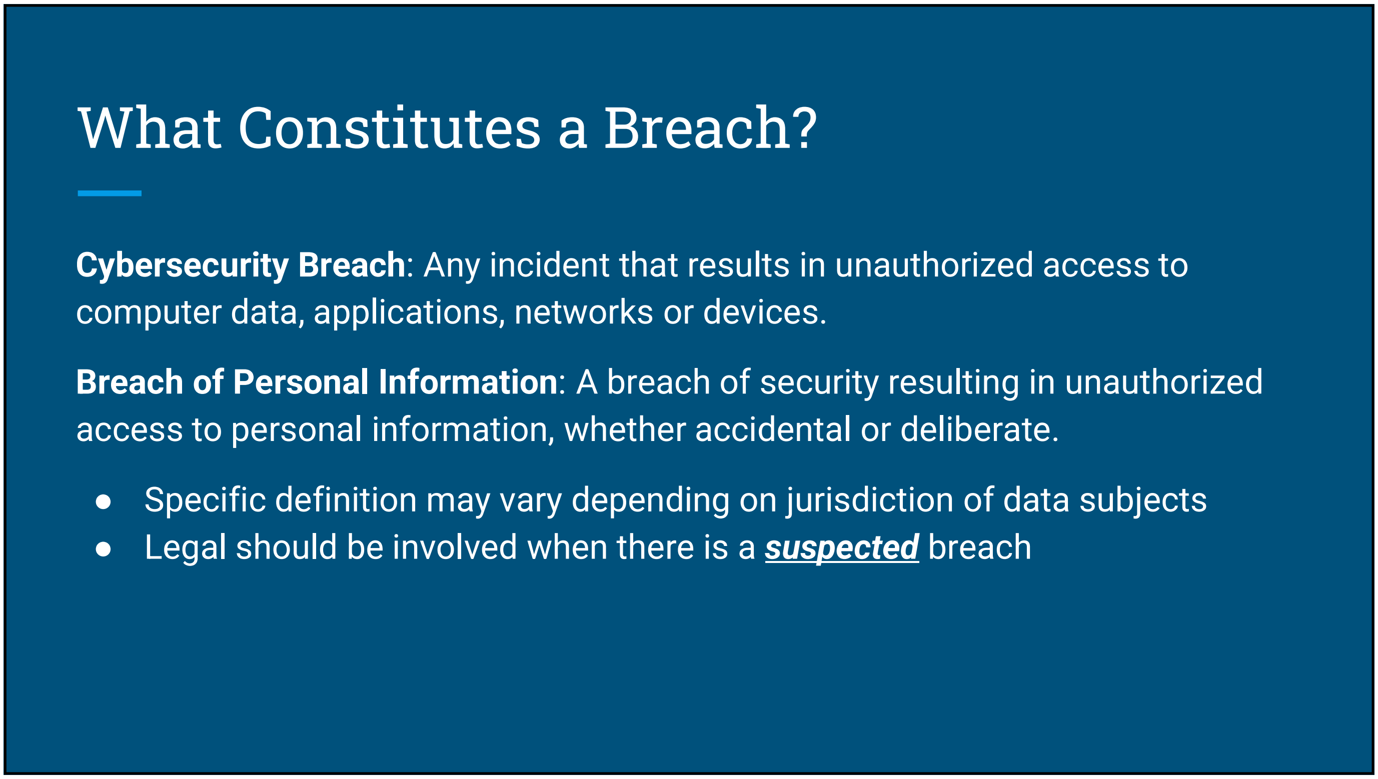
What Is Incident Response?

It’s the systematic process and policies by which a company would handle a cyberattack or data breach.

Examples of incidents

- Data breach
- Ransomware attack
- Cybersecurity attack
- Unauthorized access to personal information

4

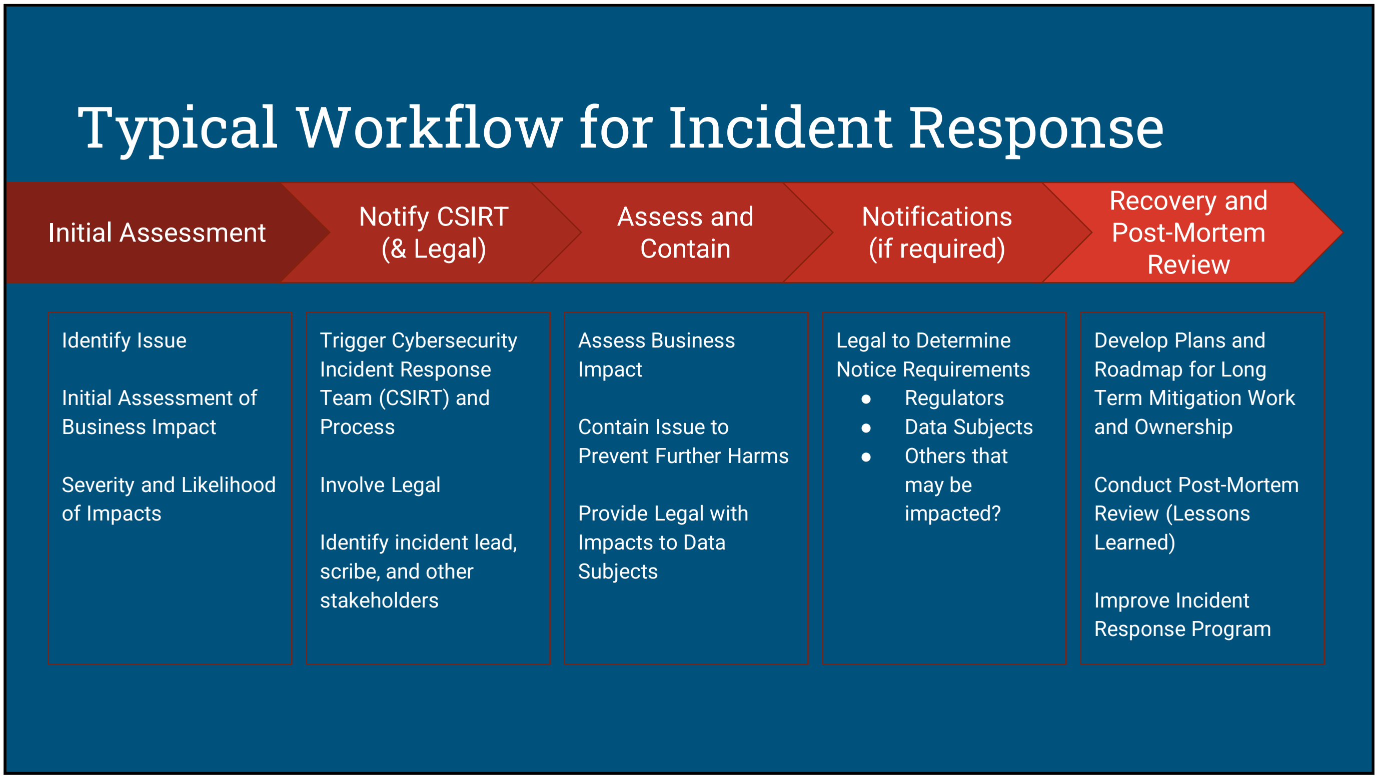


What Constitutes a Breach?

Cybersecurity Breach: Any incident that results in unauthorized access to computer data, applications, networks or devices.

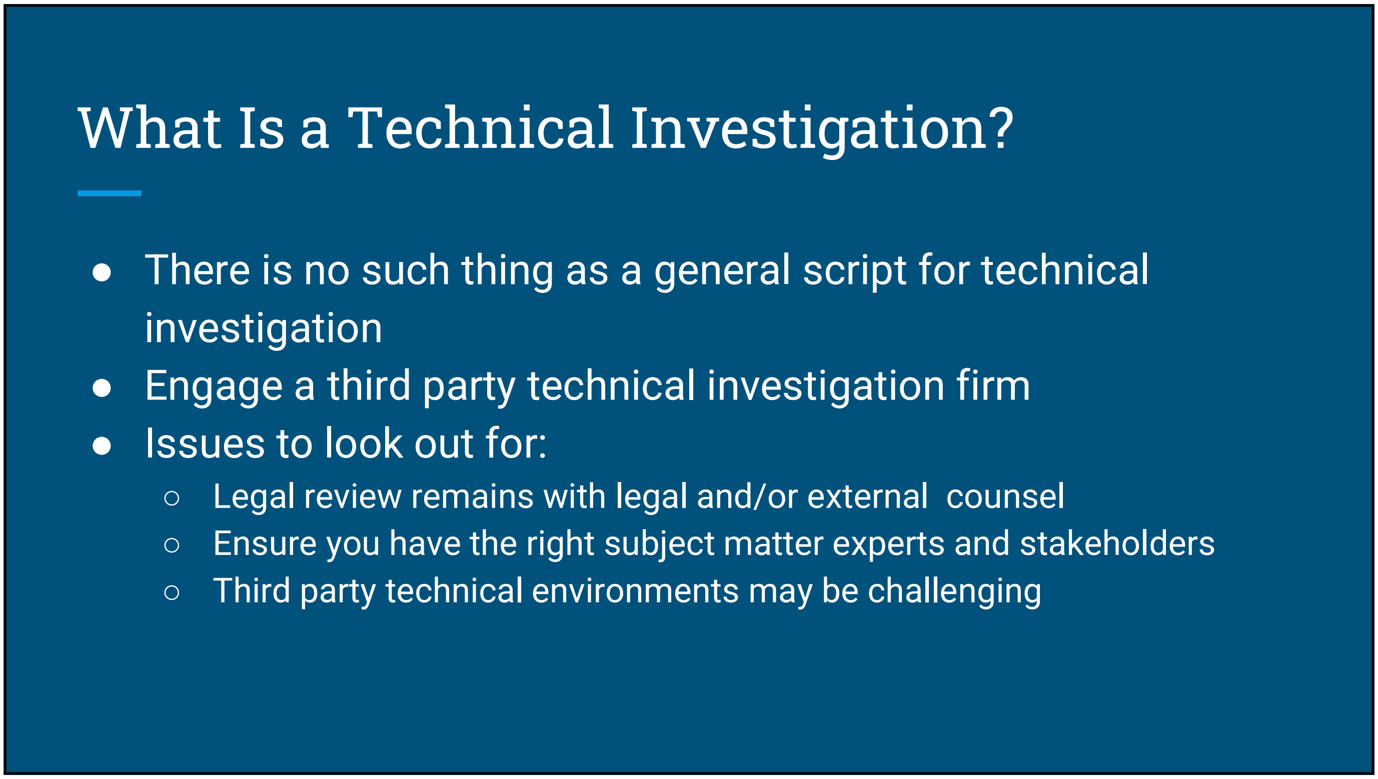
Breach of Personal Information: A breach of security resulting in unauthorized access to personal information, whether accidental or deliberate.

- Specific definition may vary depending on jurisdiction of data subjects
- Legal should be involved when there is a ***suspected*** breach



Typical Workflow for Incident Response

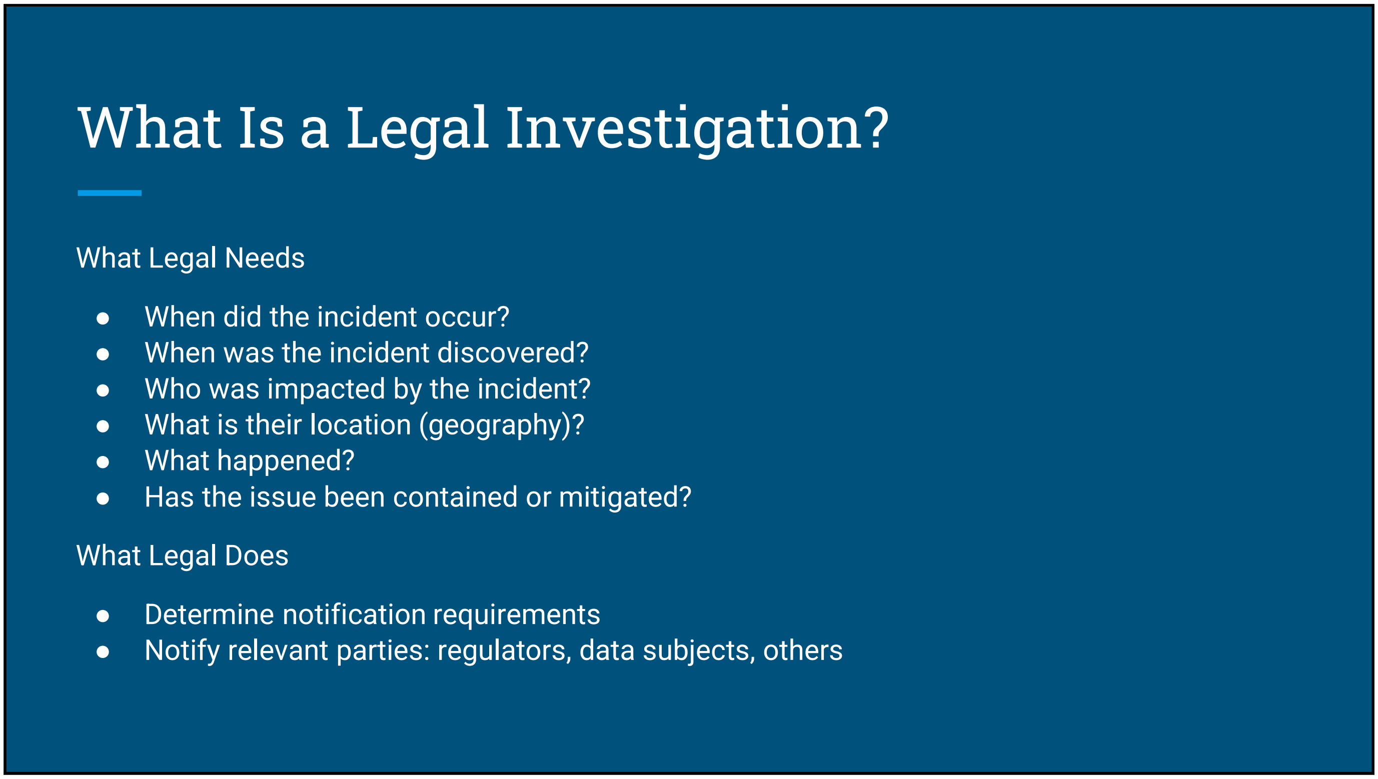
Initial Assessment	Notify CSIRT (& Legal)	Assess and Contain	Notifications (if required)	Recovery and Post-Mortem Review
Identify Issue Initial Assessment of Business Impact Severity and Likelihood of Impacts	Trigger Cybersecurity Incident Response Team (CSIRT) and Process Involve Legal Identify incident lead, scribe, and other stakeholders	Assess Business Impact Contain Issue to Prevent Further Harms Provide Legal with Impacts to Data Subjects	Legal to Determine Notice Requirements ● Regulators ● Data Subjects ● Others that may be impacted?	Develop Plans and Roadmap for Long Term Mitigation Work and Ownership Conduct Post-Mortem Review (Lessons Learned) Improve Incident Response Program



What Is a Technical Investigation?

- There is no such thing as a general script for technical investigation
- Engage a third party technical investigation firm
- Issues to look out for:
  - Legal review remains with legal and/or external counsel
  - Ensure you have the right subject matter experts and stakeholders
  - Third party technical environments may be challenging

7



What Is a Legal Investigation?

What Legal Needs

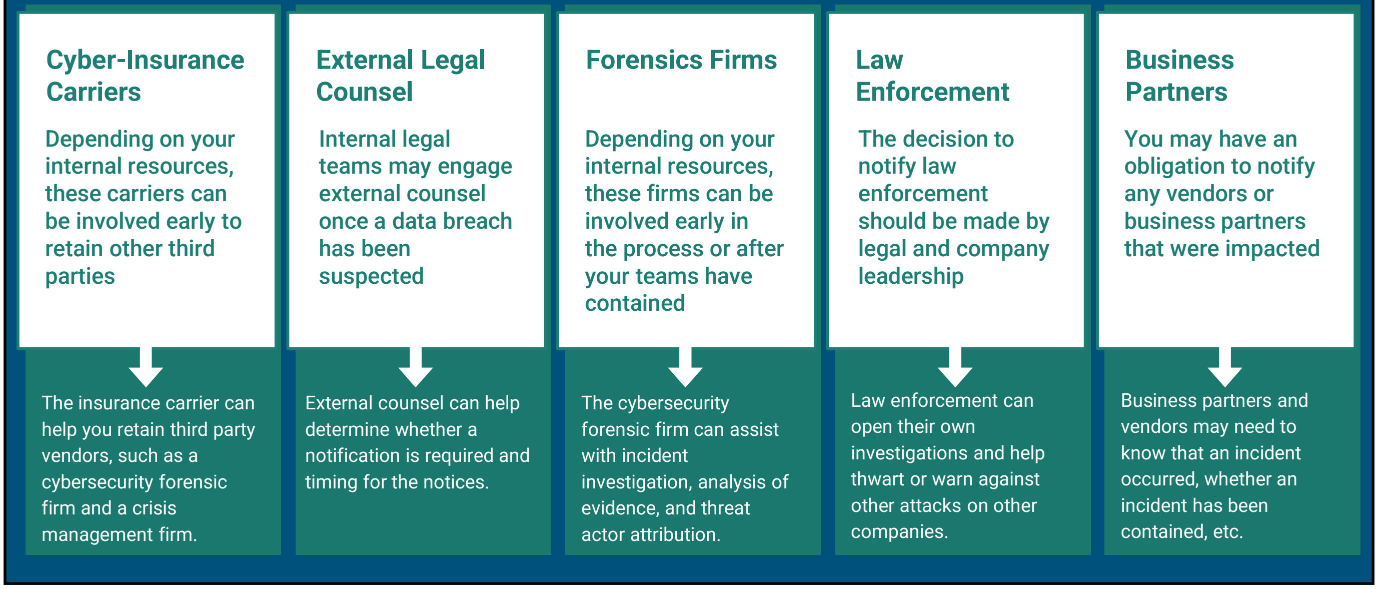
- When did the incident occur?
- When was the incident discovered?
- Who was impacted by the incident?
- What is their location (geography)?
- What happened?
- Has the issue been contained or mitigated?

What Legal Does

- Determine notification requirements
- Notify relevant parties: regulators, data subjects, others

8

When To Involve Third Parties



Cyber-Insurance Carriers

Depending on your internal resources, these carriers can be involved early to retain other third parties

The insurance carrier can help you retain third party vendors, such as a cybersecurity forensic firm and a crisis management firm.

External Legal Counsel

Internal legal teams may engage external counsel once a data breach has been suspected

External counsel can help determine whether a notification is required and timing for the notices.

Forensics Firms

Depending on your internal resources, these firms can be involved early in the process or after your teams have contained

The cybersecurity forensic firm can assist with incident investigation, analysis of evidence, and threat actor attribution.

Law Enforcement

The decision to notify law enforcement should be made by legal and company leadership

Law enforcement can open their own investigations and help thwart or warn against other attacks on other companies.

Business Partners

You may have an obligation to notify any vendors or business partners that were impacted

Business partners and vendors may need to know that an incident occurred, whether an incident has been contained, etc.

9

What About Third Party Breaches?

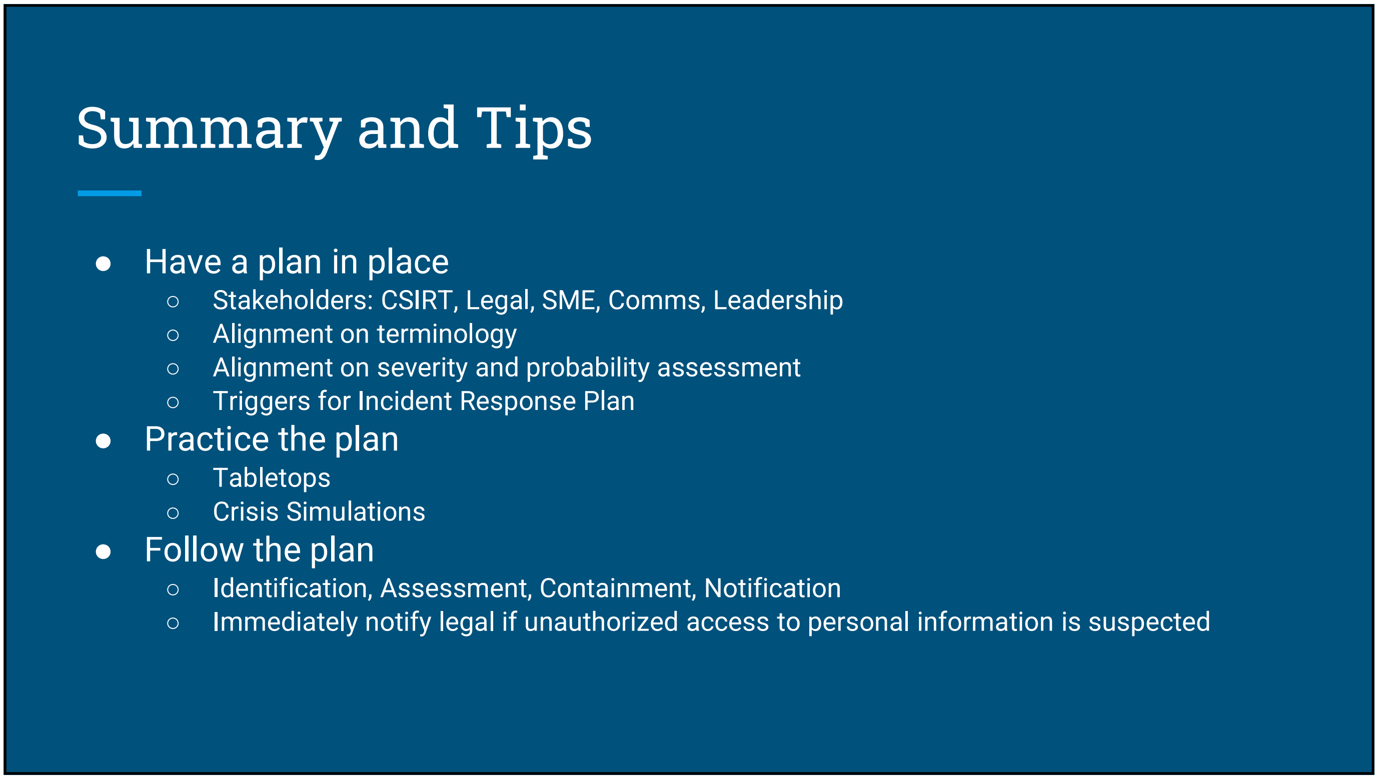
Before an incident

- Review cybersecurity and privacy practices of the vendor
  - SOC II reports
  - Privacy Policy
  - Privacy Impact Assessment
- Negotiate appropriate terms with vendor
  - Breach notification
  - Indemnification
  - Confidentiality
  - Liabilities

During an incident

- Notify Legal (Privacy Counsel)
  - Determine notification requirements
- Questions to ask the vendor
  - Scope and type of incident
  - Where they are in the investigation
  - Who is responsible for notification and costs to notify
  - Remediation and/or mitigation efforts to reduce risk in the future

10



Summary and Tips

- Have a plan in place
    - Stakeholders: CSIRT, Legal, SME, Comms, Leadership
    - Alignment on terminology
    - Alignment on severity and probability assessment
    - Triggers for Incident Response Plan
- Practice the plan
    - Tabletops
    - Crisis Simulations
- Follow the plan
    - Identification, Assessment, Containment, Notification
    - Immediately notify legal if unauthorized access to personal information is suspected