# CFMA Cyber Security Luncheon Presentation

June 16th, 2022

Presented by:
Shawn Huffman - Cybersecurity Advisor
Coro Cybersecurity
Shawn.Huffman@coro.net

# Agenda

- The State of Cyber Security Today
- Key Cyber Domains Every Organization Should Protect
- Is There a Simple All-In-One Solution?
- Q&A / Open Discussion

CORO

# Cybersecurity in the News

*Cyberattack Forces a Shutdown of a Top U.S. Pipeline*

The operator, Colonial Pipeline, said it had halted systems for its 5,500 miles of pipeline after being hit by a ransomware attack.

**J&J experiences 15.5B cybersecurity incidents per day, CISO says**

Hannah Mitchell - Thursday, June 3rd, 2021 Print | Email

**Major meat producer JBS USA hit by cyberattack, likely from Russia**

By Rob McLean, Alexis Benveniste and Allie Malloy, CNN Business

Updated 8:59 PM ET, Tue June 1, 2021

EDUCATION

**Two Somerset County school districts report cyber attacks**

Mike Deak MyCentralJersey.com

Published 5:00 a.m. ET Apr. 14, 2021 | Updated 7:46 a.m. ET Apr. 14, 2021

POLITICS

**Ransomware attack hits ferry service to Cape Cod, Nantucket and Martha's Vineyard**

PUBLISHED WED, JUN 2 2021-12:07 PM EDT | UPDATED WED, JUN 2 2021-1:08 PM EDT

**Major DC insurance provider hacked by 'foreign cybercriminals'**

BY MAGGIE MILLER AND LAURA KELLY - 04/08/21 05:23 PM EDT 10 COMMENTS

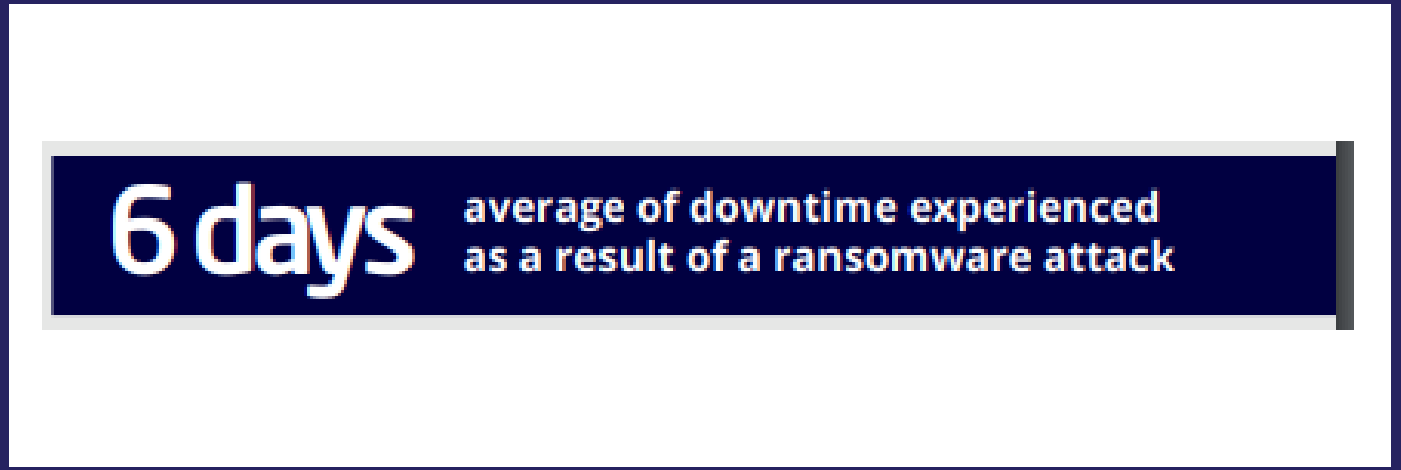
**Elliman's property management arm suffers data breach**

*Thousands of New York homeowners may be affected*

New York / By Erin Hudson

# Cyber Statistics

- 6 out of 10 companies have suffered from a ransomware attack
  - 66% recovered their data
  - 52% paid the ransom
- Employees are clicking on 3X as many malicious emails as they had before
- 63% increase in phishing attacks
- 70% of companies expect their business to be harmed by an email sourced attack
- 79% of companies were hurt by their lack of cyber preparedness
- 88% of Microsoft Office 365 users think their companies need additional email security



In the second half of 2021 alone, research found that ransomware incidents increased by 715% year-over-year. In July and August, an average of 60% of all emails received were fraudulent, according to the research from Bitdefender.

# What is Ransomware

- Ransomware starts with unsolicited email that victim clicks on a link or downloads an attachment.
- Ransomware runs an infecting Code
- Ransomware encrypts the data on the system
- Attacker demands ransom to decrypt the data
- Note: Some ransomware is designed to spread to other computers on the network.

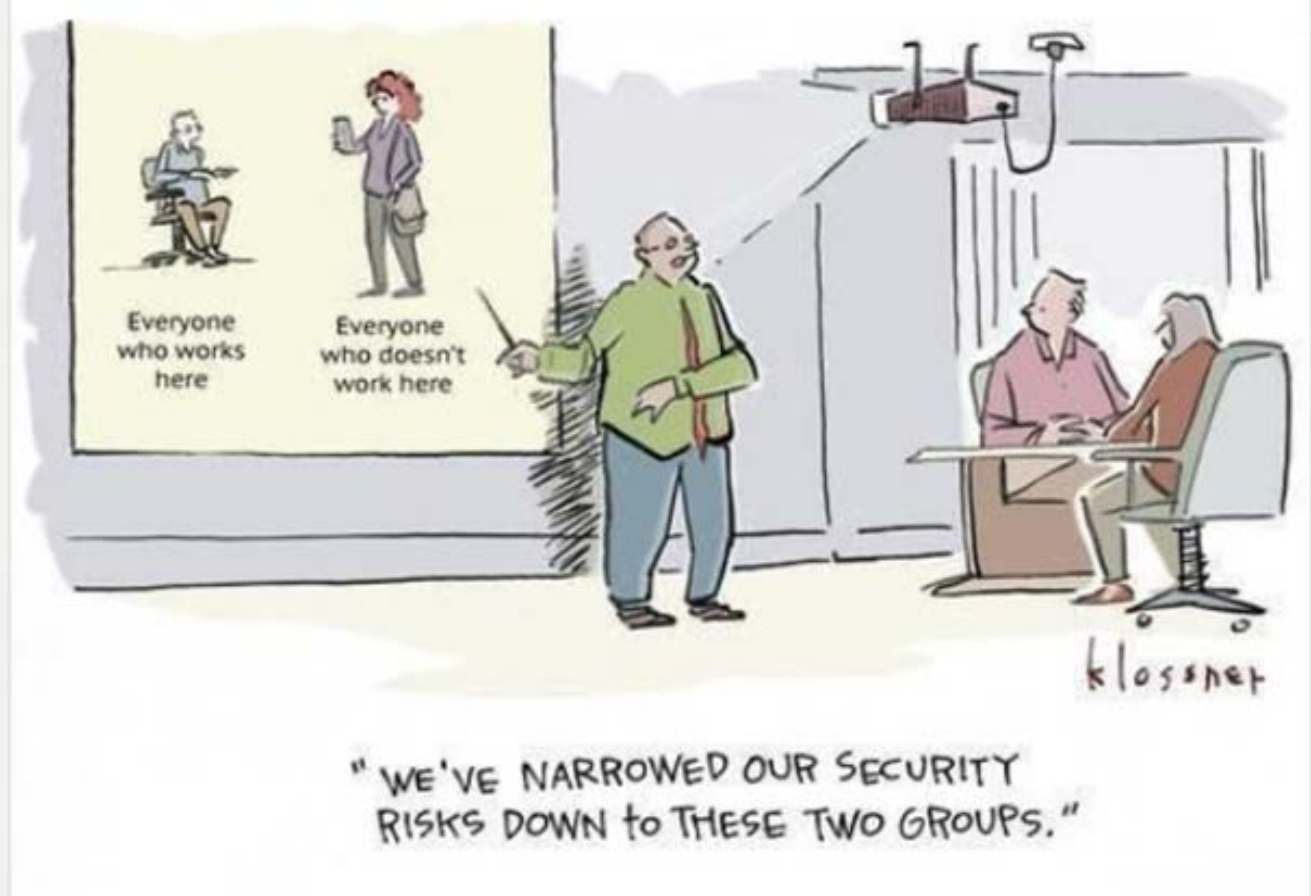


# A Successful Ransomware Attack Results in:

- Inaccessible files
- Threat to release or block such access indefinitely
- “Ransom” – asking for $$
- Brand reputation, loss of Bid Data, Plans, etc.
- 60% of all businesses that suffer a ransomware attach go out of business within 12 months

# How Ransomware is Evolving

- Attacks are becoming more sophisticated daily.
- Ransomware as a Service.
- Utilizing Phishing as entry-point, Phishing as a Service.
- Exploiting the weakest link of organizations – employees.



# Keys Cyber Domains Every Organization Should Protect



# Six Best Tools To Prevent Ransomware Attacks

# According to IDG, the top 4 domains that every business must protect in 2021

**Cloud Apps**

Office 365, Google, Salesforce etc.

**Email**

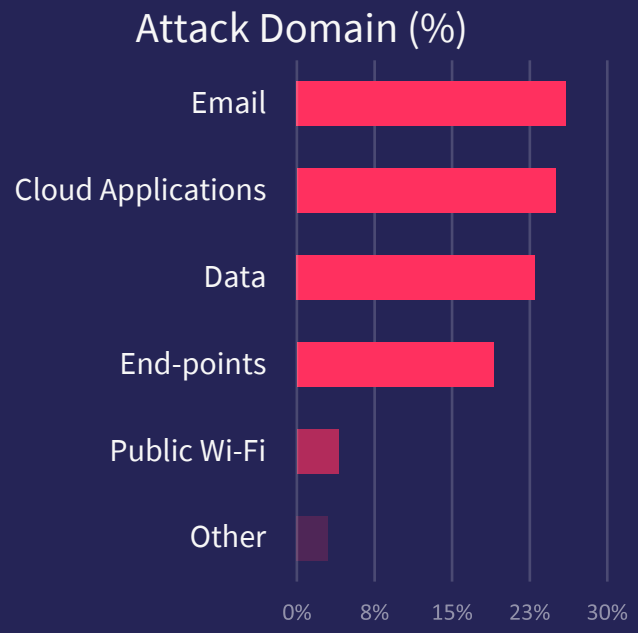
Attachments, body, addresses

**Endpoints**

Laptops, desktops, mobile, connectivity

**Data**

PII / PCI / PHI, business data




IDG, Cyber Insights report June 2021

# WiFi Phising

- Access to Wi-Fi has a cost
- Perimeter-less environments
- Compromised Wi-Fi networks
- Some types of Attacks
  - Rogue access points/Pineapple devices
  - Man in the middle attacks

# Typical limited mid-market coverage

Cyber security protection for mid-market is limited and does not provide sufficient coverage

| | Cloud Apps | Email | Devices |
|---|---|---|---|
| MALWARE & RANSOMWARE | | | ✓ |
| PHISHING | | ✓ | |
| HACKING & ACCESS CONTROL | | | |
| INSIDER THREATS | | | |
| DATA LOSS & GOVERNANCE | | | |

# Is there a simple All-in-One Solution?



CORO

# One platform that includes all you need to secure your business

Users Protection

Cloud Apps Protection

Email Protection

Devices Protection

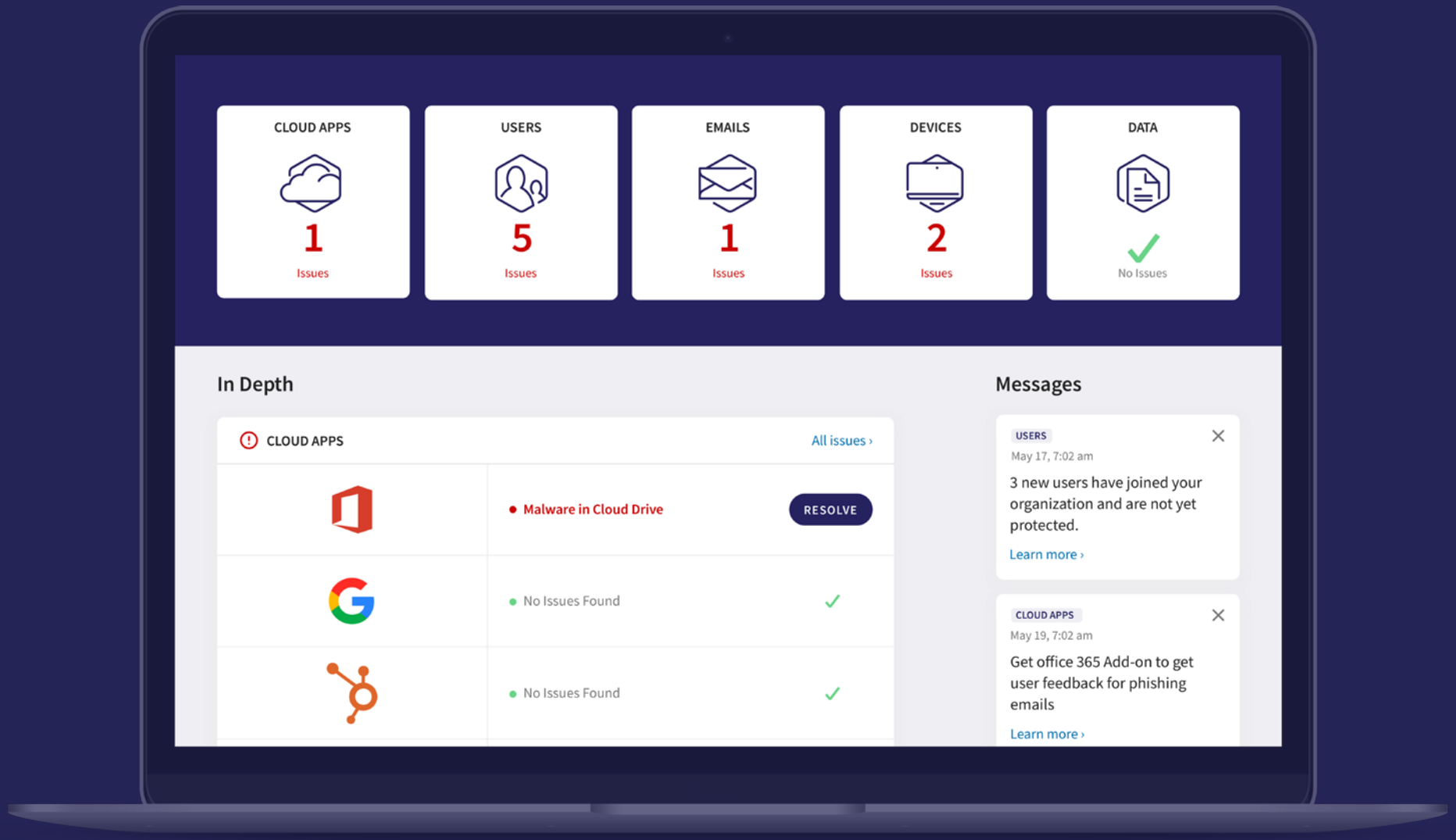
Data Protection

# Full security coverage with Coro

With Coro you get all the protection you need in one platform

| | Cloud Apps | Email | Devices |
|---|---|---|---|
| MALWARE & RANSOMWARE | ✓ | ✓ | ✓ |
| PHISHING | ✓ | ✓ | ✓ |
| HACKING & ACCESS CONTROL | ✓ | ✓ | ✓ |
| INSIDER THREATS | ✓ | ✓ | ✓ |
| DATA LOSS & GOVERNANCE | ✓ | ✓ | ✓ |

# Single Pane of Glass Console



# Coro is Designed for SMB and Mid-Size Businesses

**Why Coro?**

- Affordability
- Ease of use
- Consolidation

**Ideal Partner**

- Cost driven
- Seeking simplicity
- Consolidation of endpoint, email, and DLP tools

**Trusted Since 2014**

- 40,000 Users
- Cash Flow Positive
- Numerous Awards

***Protecting our economic backbone – the millions of growing businesses, empowering them to be resilient to cyber threats***




The Ultimate All-in-One Security
for Growing Companies

# Cyber Threats, Trends and Response

MICAH HOFFMAN, Managing Director & Counsel, Cyber Claim

# Agenda

- Cyber Threats and Cyber Claim Trends
- Cyber Claim Process
- Questions

# Disclaimer

*This presentation is for general informational purposes only. This presentation is about coverages generally available in the marketplace and is not based specifically on the policies or products of Travelers Casualty and Surety Company of America and its property casualty affiliates ("Travelers"). This information does not amend, or otherwise affect, the terms, conditions, or coverages of any insurance policy issued by Travelers. This information is not a representation that coverage does or does not exist for any particular claim or loss under any such policy. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy provisions, and any applicable law. The availability of coverages referenced in this presentation may depend on underwriting qualifications and state regulations.*

*This presentation does not cover all possible cyber threats that may exist, does not identify all potential controls for those risks, and does not constitute legal advice. This presentation is not intended as advice to you or your insureds about specific risk control practices. It is not designed to be comprehensive and it may not apply to your particular facts and circumstances. Consult as needed with your own attorney or advisor.*

# CYBER THREATS

Spam

Failure to Patch

Employee Negligence

Business Email Compromise

Human Error

Stolen Credentials

Vendor Breach

SOCIAL ENGINEERING

Skimmer

Malvertising

Cloud Provider Hacked

DDoS

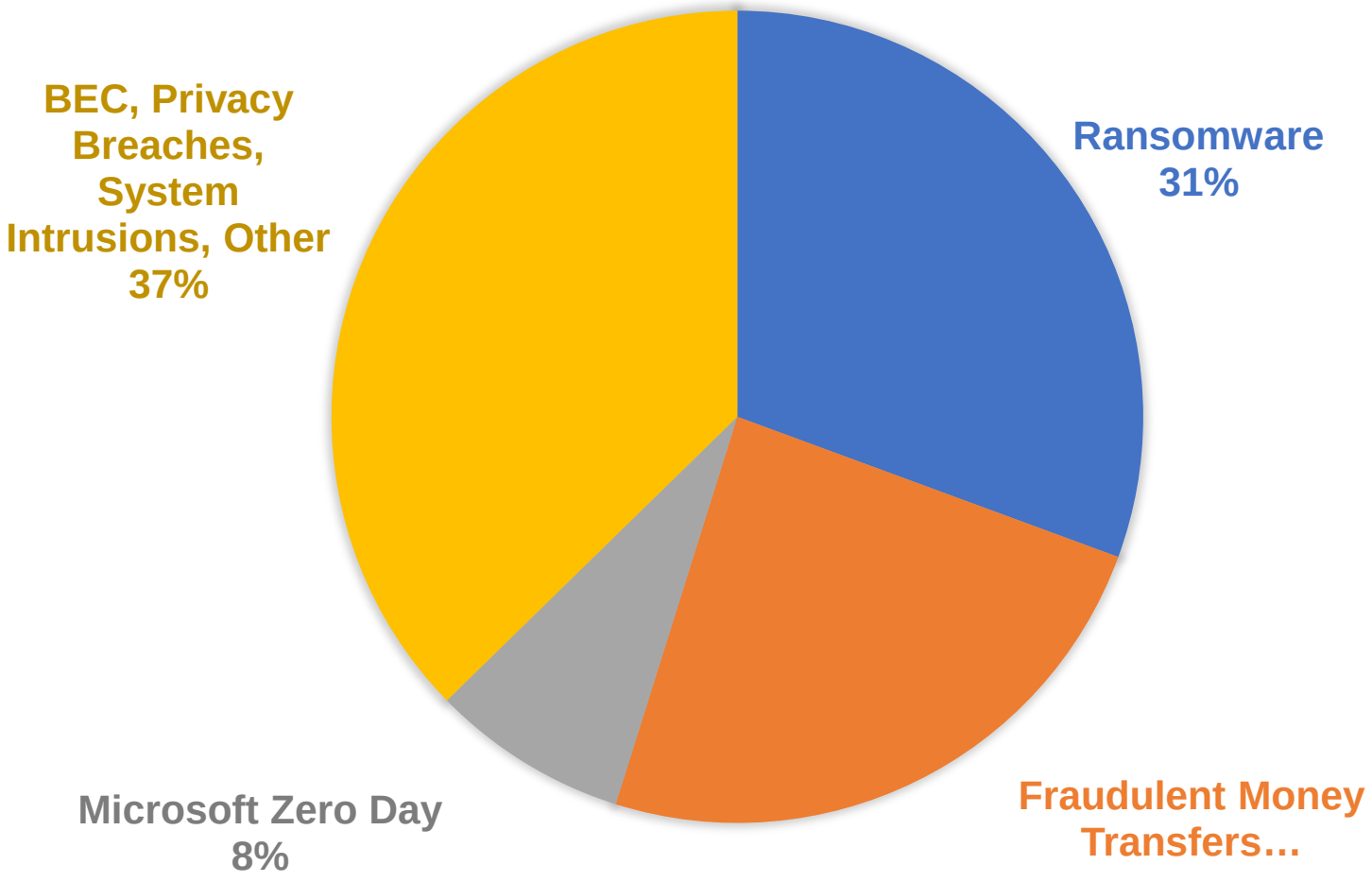
RANSOMWARE

SQL Injection Attacks

Lost Laptop

Environmental Event

# CLAIM TRENDS




In 2021, more than half of reported matters involved ransomware or social engineering fraud.

Source: Travelers Claim Data Year End 2021

# Cost Driver

Business Interruption

Post Breach Costs (Notification)

Increased Ransom Demands from Hackers

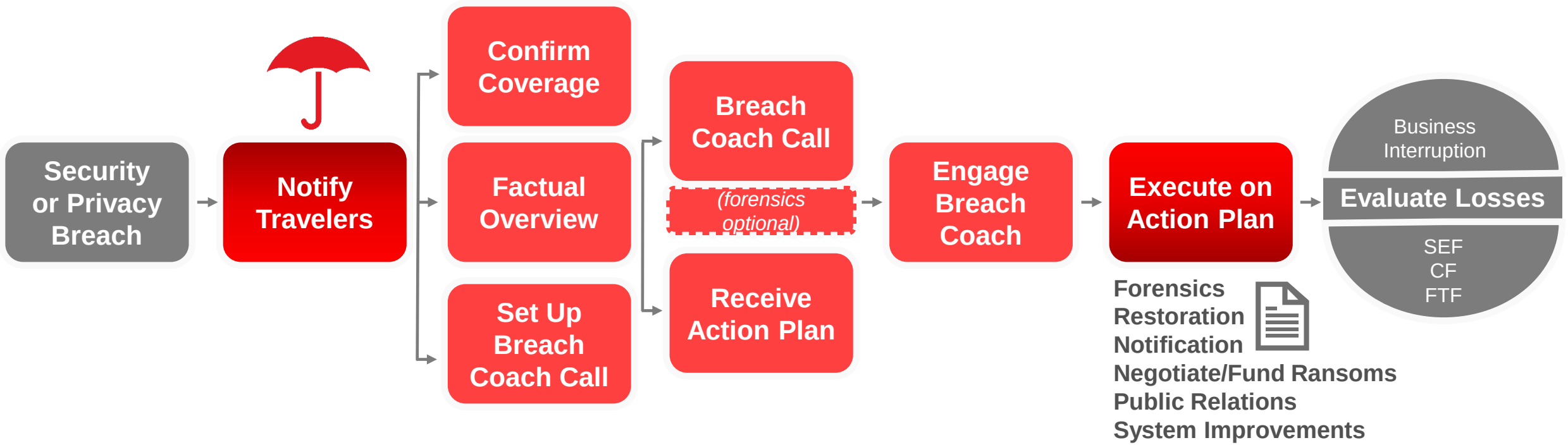
Time needed to identify & contain breach

Restoration Costs

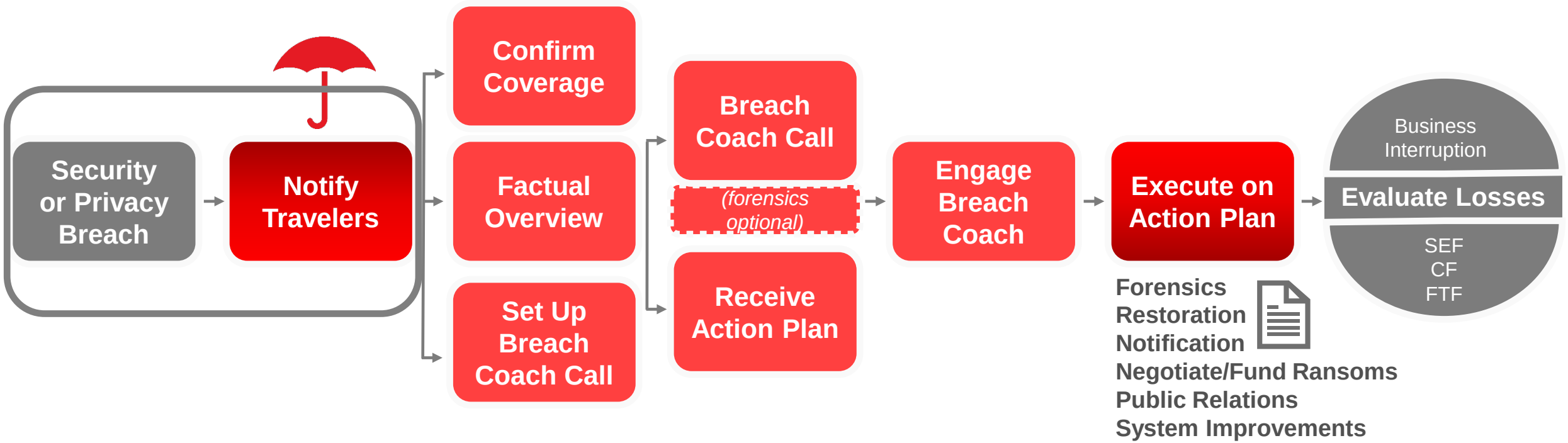
Costs for Breach Counsel and Forensics

Third Party Claims/ Loss of Customers

# CyberRisk Breach Response Continuum

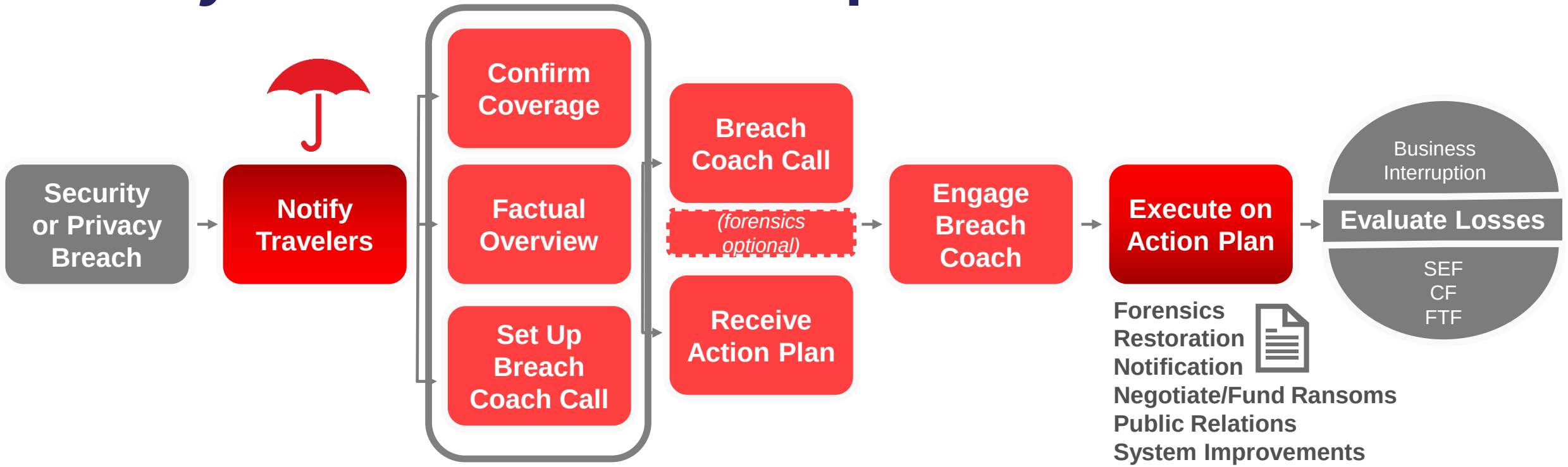


# CyberRisk Breach Response Continuum

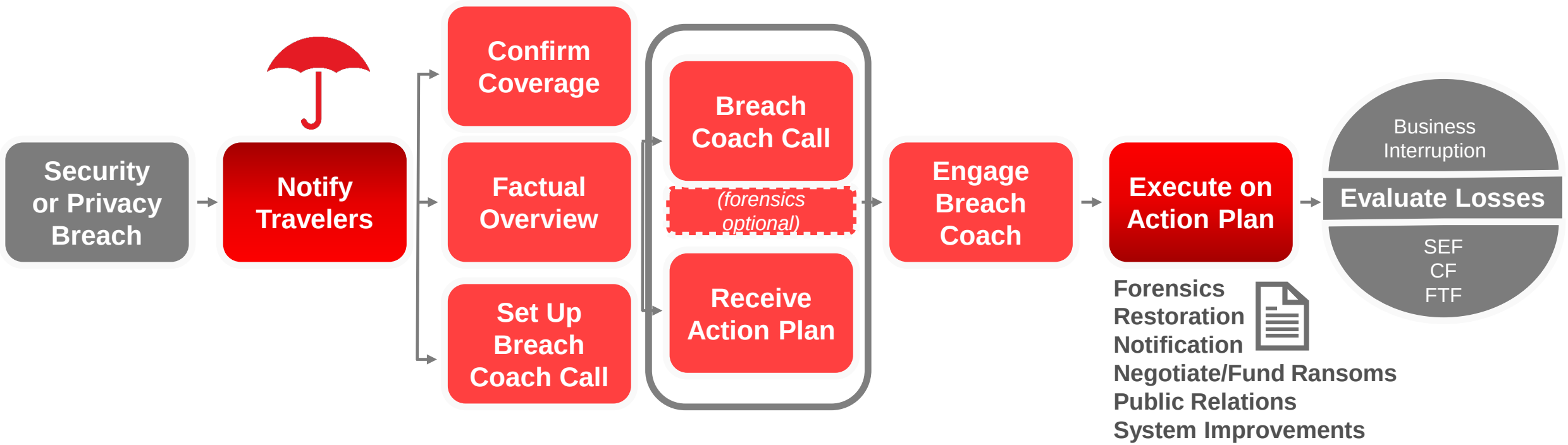



Incident Response → Remediation

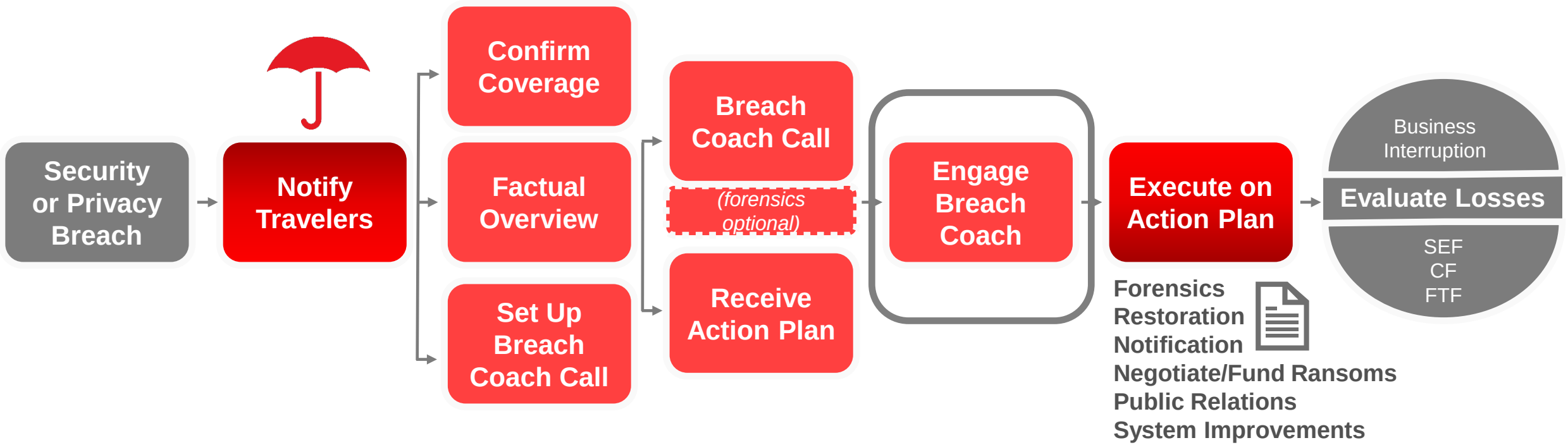
# CyberRisk Breach Response Continuum



# CyberRisk Breach Response Continuum

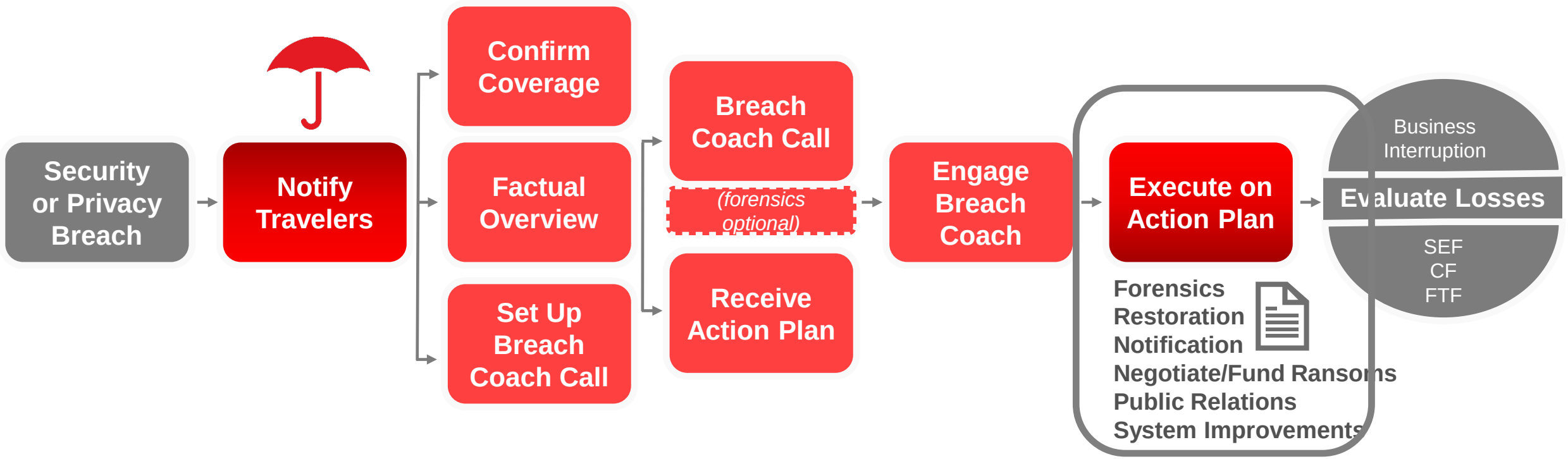


# CyberRisk Breach Response Continuum

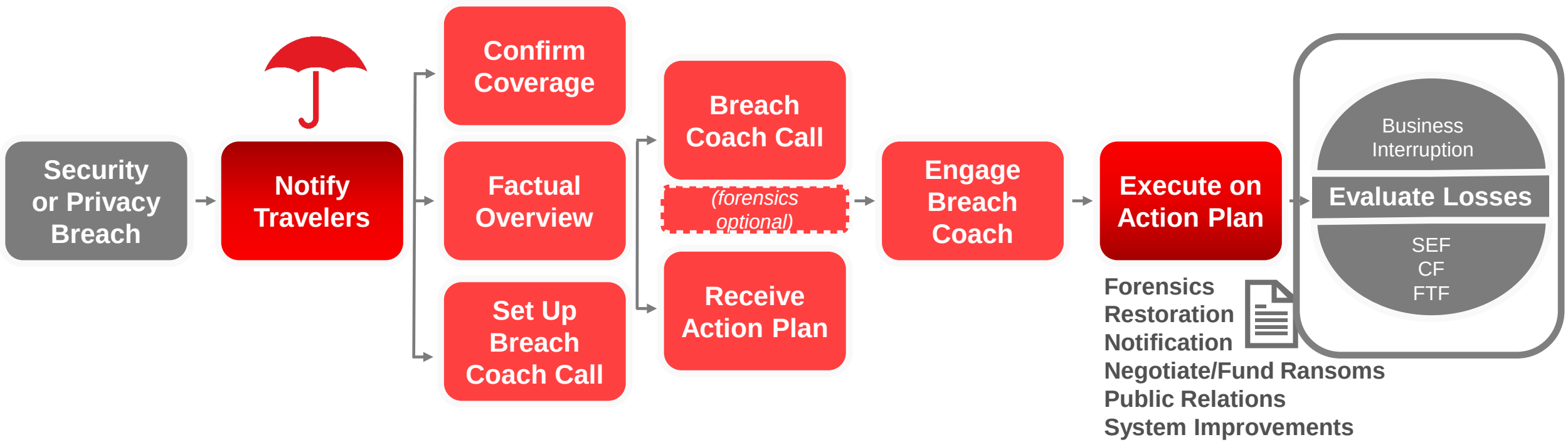



Incident Response → Remediation

# CyberRisk Breach Response Continuum



# CyberRisk Breach Response Continuum




Incident Response → Remediation


QUESTIONS ?