SEPTEMBER 25, 2024

UT LAW CLE

TEXAS Law
The University of Texas at Austin
School of Law

# TAKING YOUR INCIDENT RESPONSE PLAN TO THE NEXT LEVEL

**WILL DAUGHERTY**
Partner, Head of Cybersecurity, U.S.
Norton Rose Fulbright
Houston, TX

**JOHN ANSBACH**
Managing Director, Cyber Solutions
Stroz Friedberg, an AON company
Dallas, TX

1



# Cybersecurity Threat Landscape

## What do organizations need to prepare for?

- Ransomware Attacks Evolved
- Data Theft & Extortion
- High pressure tactics used by Threat Actors
- Attacks on Vendors that impact your Organization
- AI driven threats

2

# Cybersecurity Incident Response

Where do organizations struggle with in actual incidents?

- Project Management
- Lack of Strong Governance
- Communications (internal & external)
- Recovery and Restoration
- Business Continuity
- Preparedness

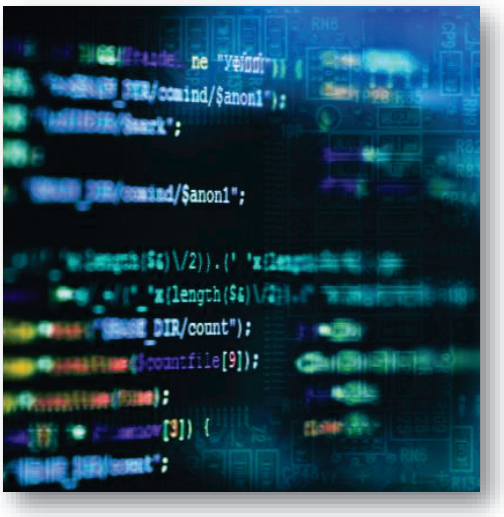




# Incident Response Plan

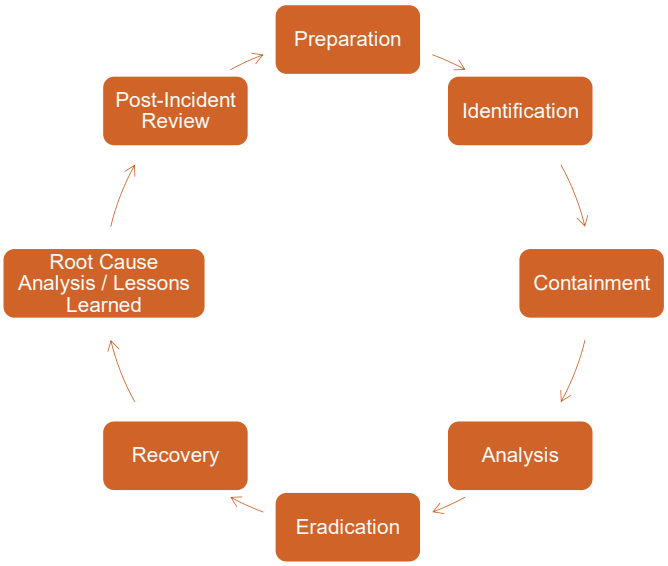
We have one, now what?

- Living document that should mature as the organization matures
- Common shortcomings of an IRP
- Where does the IRP fit within the organization's hierarchy of Plans?
- Harmonization across other organization plans?
  - Crisis Management Plan
  - Business Continuity Plan
  - Disaster Recovery Plan
  - Crisis Communications Plan



# A Living Document

- The IRP should mature as the organization matures








# Common shortcomings of an IRP

- Misidentification of IR team members, roles, and responsibilities (wrong-size, mismanaged)
- Absence of priority classification of Incidents
- Runbooks related to the IRP are not updated
- Lack of testing of the IRP
- Legal is not integrated into Security Operations Center (SOC) alerting processes

→ • Make sure the IRP aligns with the organization's hierarchy of Plans

# Title search: Taking Your Incident Response Plan to the Next Level

Also available as part of the eCourse
Hooked on CLE: May 2025

First appeared as part of the conference materials for the
2024 Essential Cybersecurity Law session
"Taking Your Incident Response Plan to the Next Level"