Ransomware: response and resiliency

Presentation by United States of America
Timothy J. Shimeall, Ph.D.
Software Engineering Institute
Carnegie Mellon University

UNIVERSAL POSTAL UNION

Presentation Markings

Overview

Ransomware

Identify

Protect

Detect

Respond

Recover

Decisions

Ransomware

Attack holding data from a compromised computer

- Encrypt data
- Threaten loss or disclosure
- Demand payment
- Repeated attack

Attacks growing against organizations, not individuals

In 2019, Internet Crime Coordination Center report:

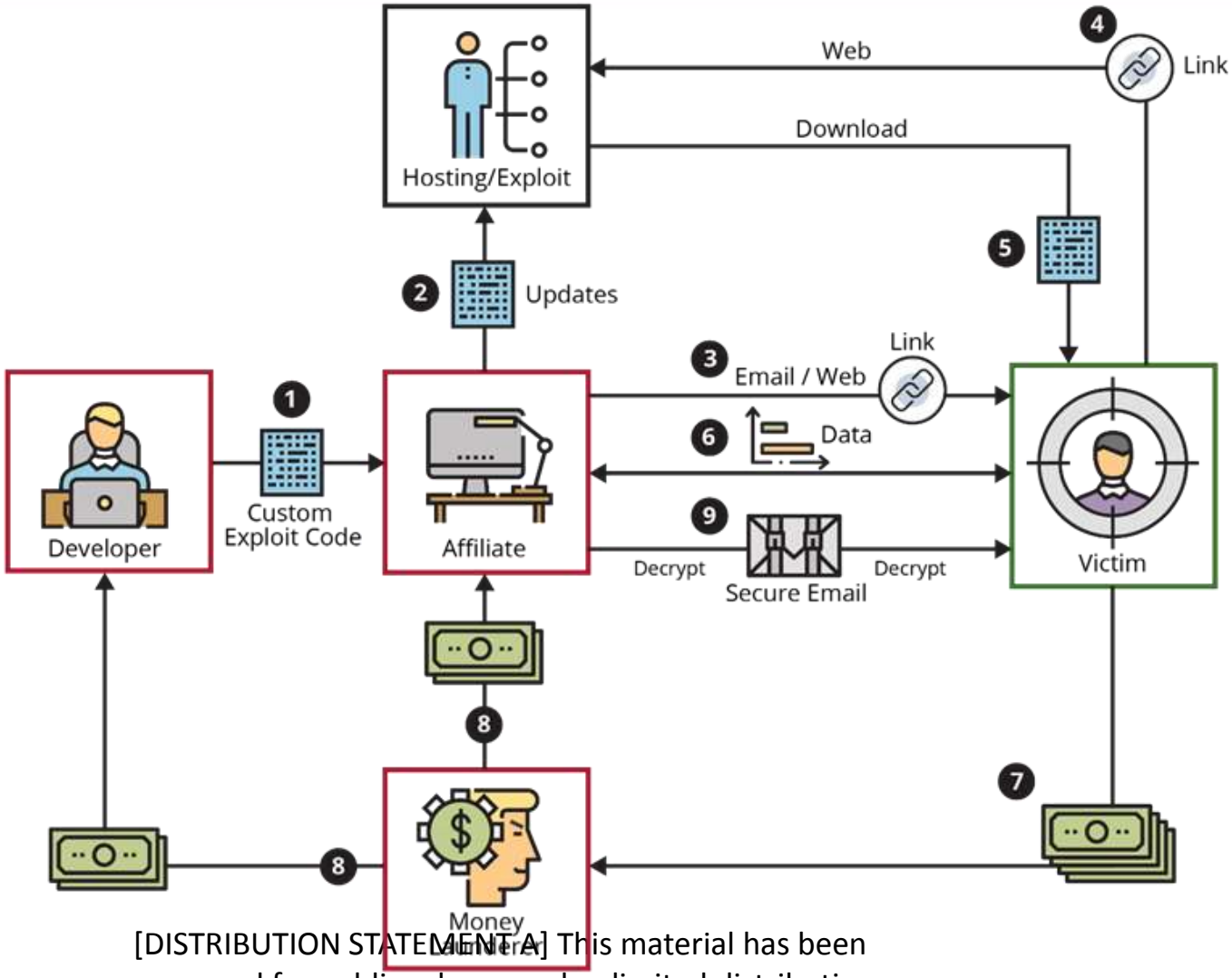
– 2,047 complaints

– US $8,965,847 losses

In 2018, SentinelOne (UK) report:

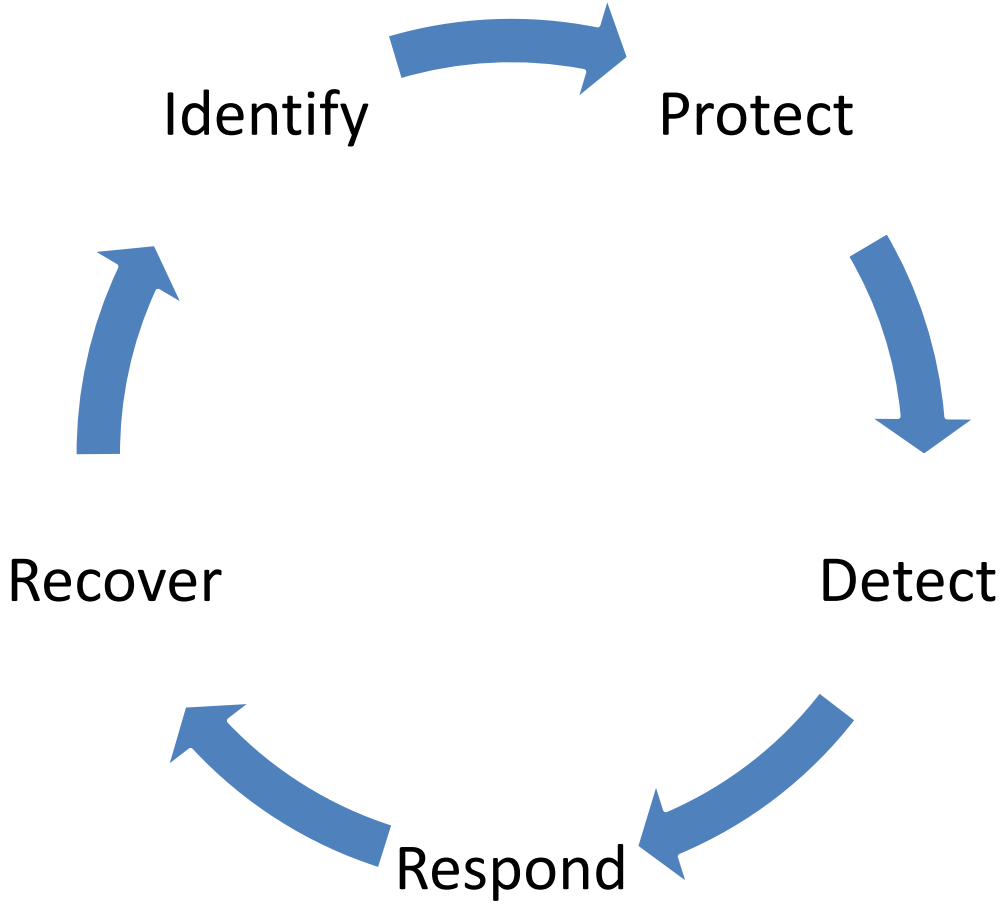
– Average attacked organization: 5 attacks in 12 months

Ransomware Attack



UNIVERSAL POSTAL UNION

Response and Resiliency



UNIVERSAL POSTAL UNION

Identify

Assets

- Devices, Clients, Servers, Data
- Processing platforms, Applications
- Documentation

Vectors

- Malware propagation methods, Access paths
- Downstream risk to assets

Priority

- Business value, criticality
- Allocate resources in line with risk, priority

UNIVERSAL POSTAL UNION

Identify Example

Corrupted software update

Infected

Identification is ongoing

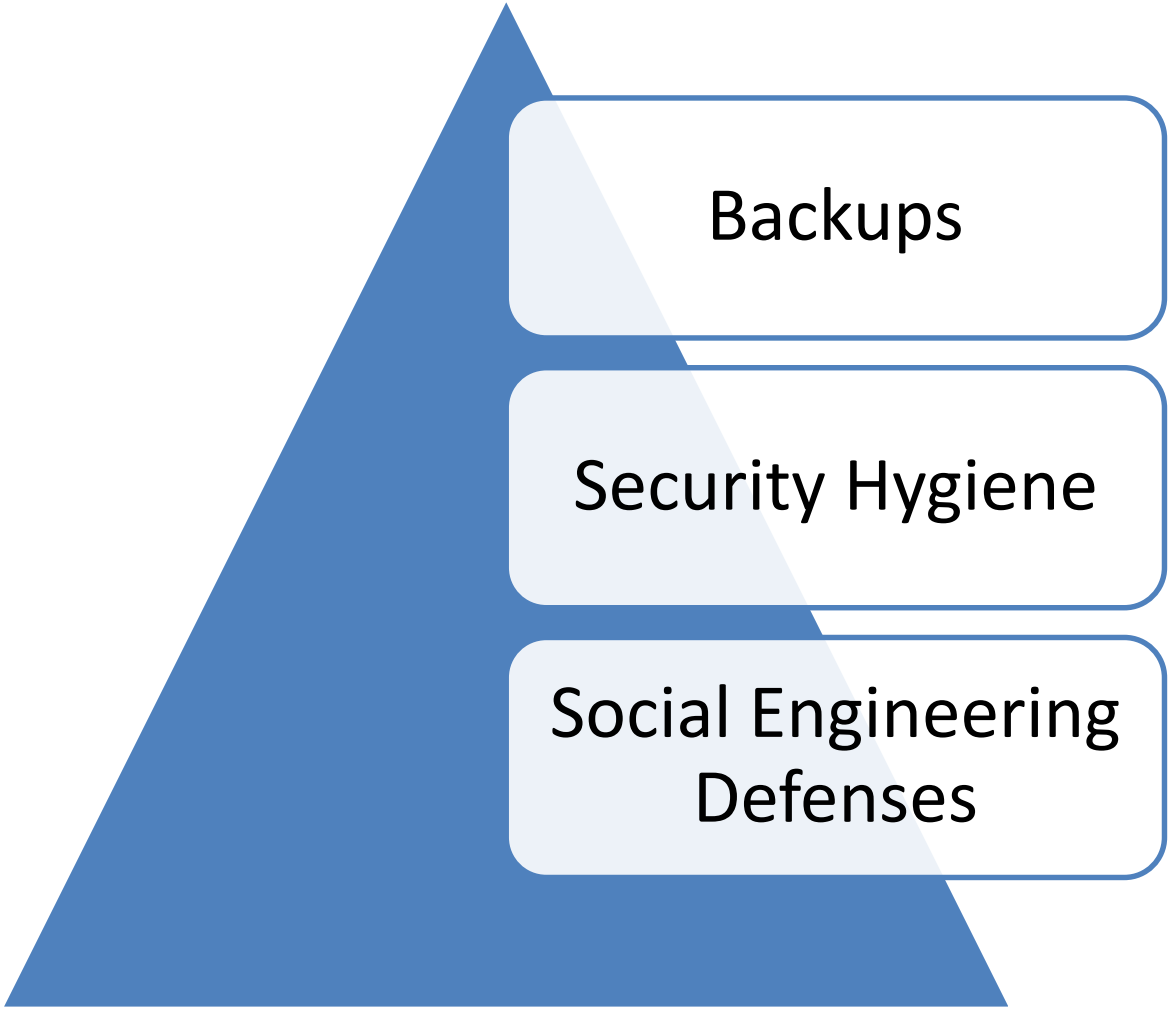
Include all paths to assets

Examine expected paths

Lost or redirected packages
US $300,000,000 loss
Reputation loss

UNIVERSAL POSTAL UNION

Protect



Protect Example

Phishing

To: Postal Agent
From: orders@example.com

Attached is the invoice for your shipment

Malware

Postal Agent

Did not open malware
Closed critical file shares

Reported message to Security

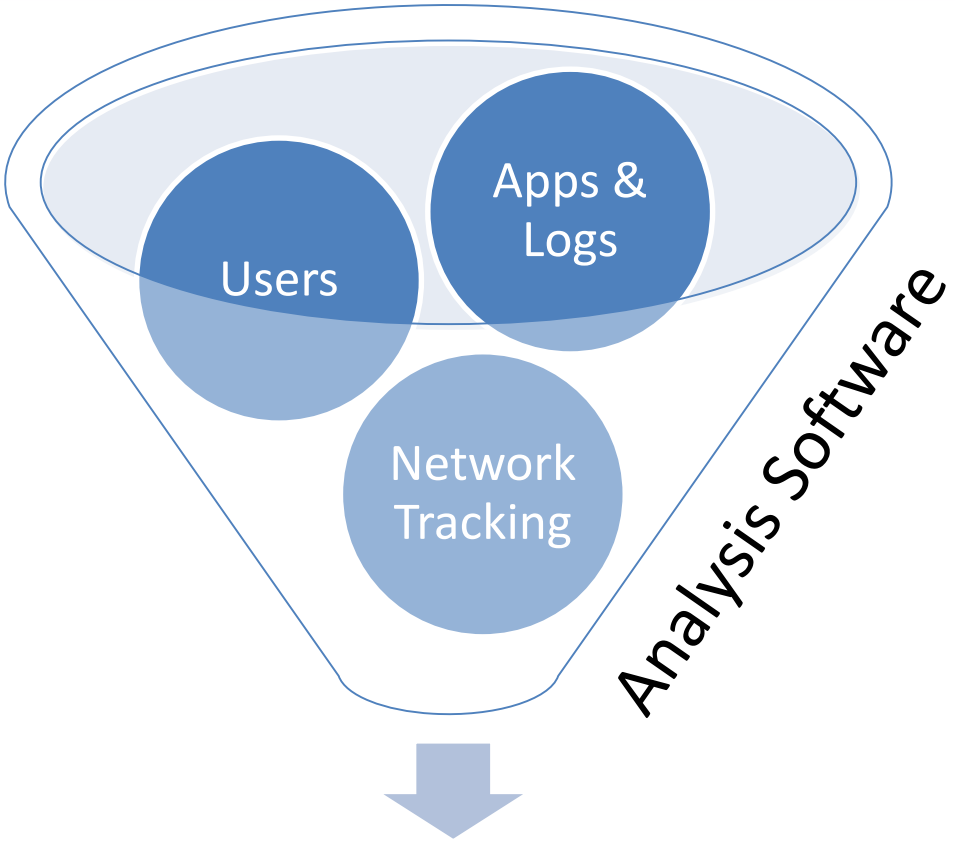
Data

Security

Analyzed malware
Warned clients and vendors
Updated defenses

Reported message to Law Enforcement

Detect



Rapid detection

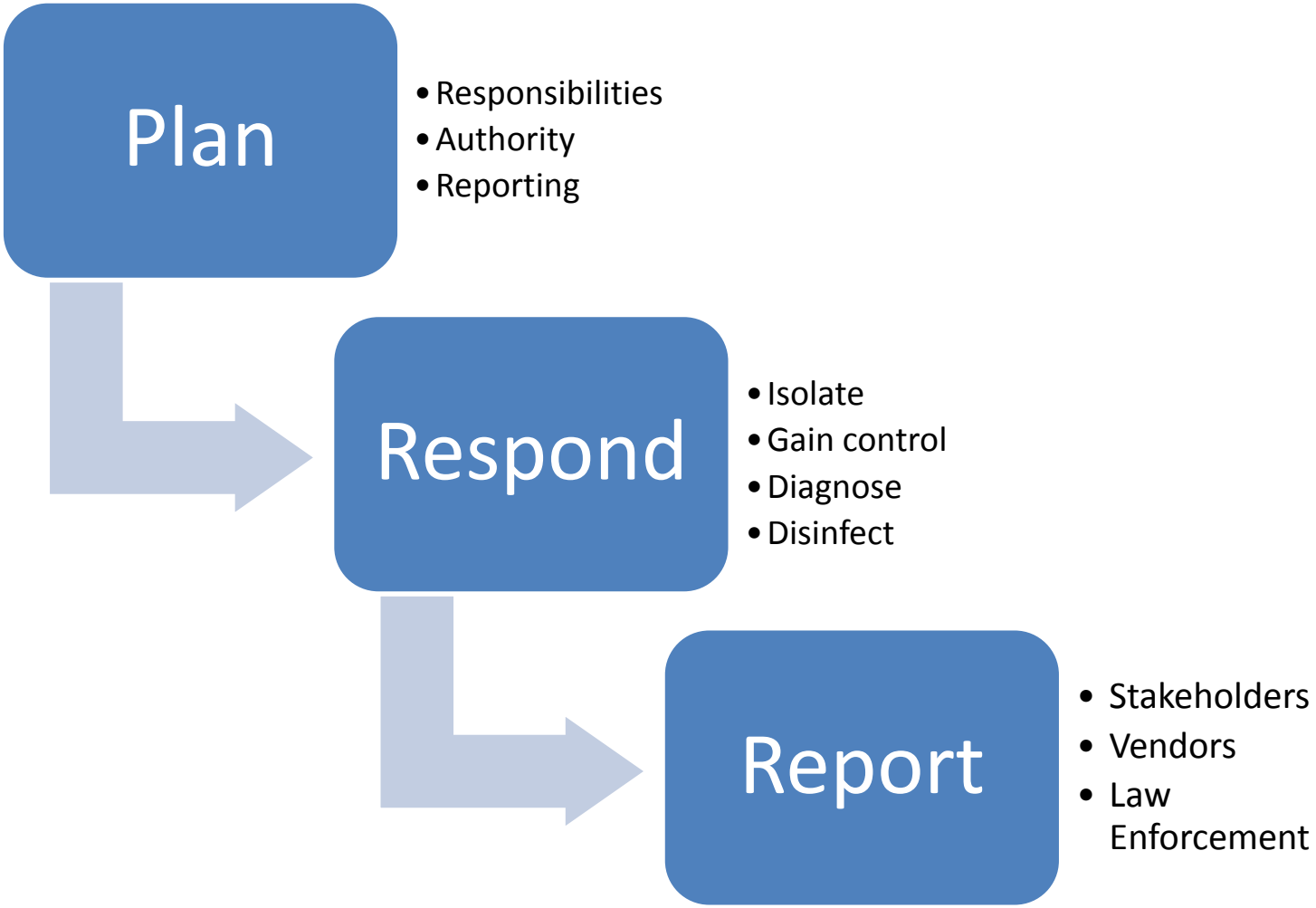
Detect Example

Ryuk
- Social engineering attacks (phishing or user click)
- Insecure web site attacks
- Invoke Trickbot and Emotet

Trickbot and Emotet
- Spread using PsExec or Group Policy update
- Drop Ryuk
- Gain RDP access
- Steal data
- Make network more vulnerable to later Ryuk attacks

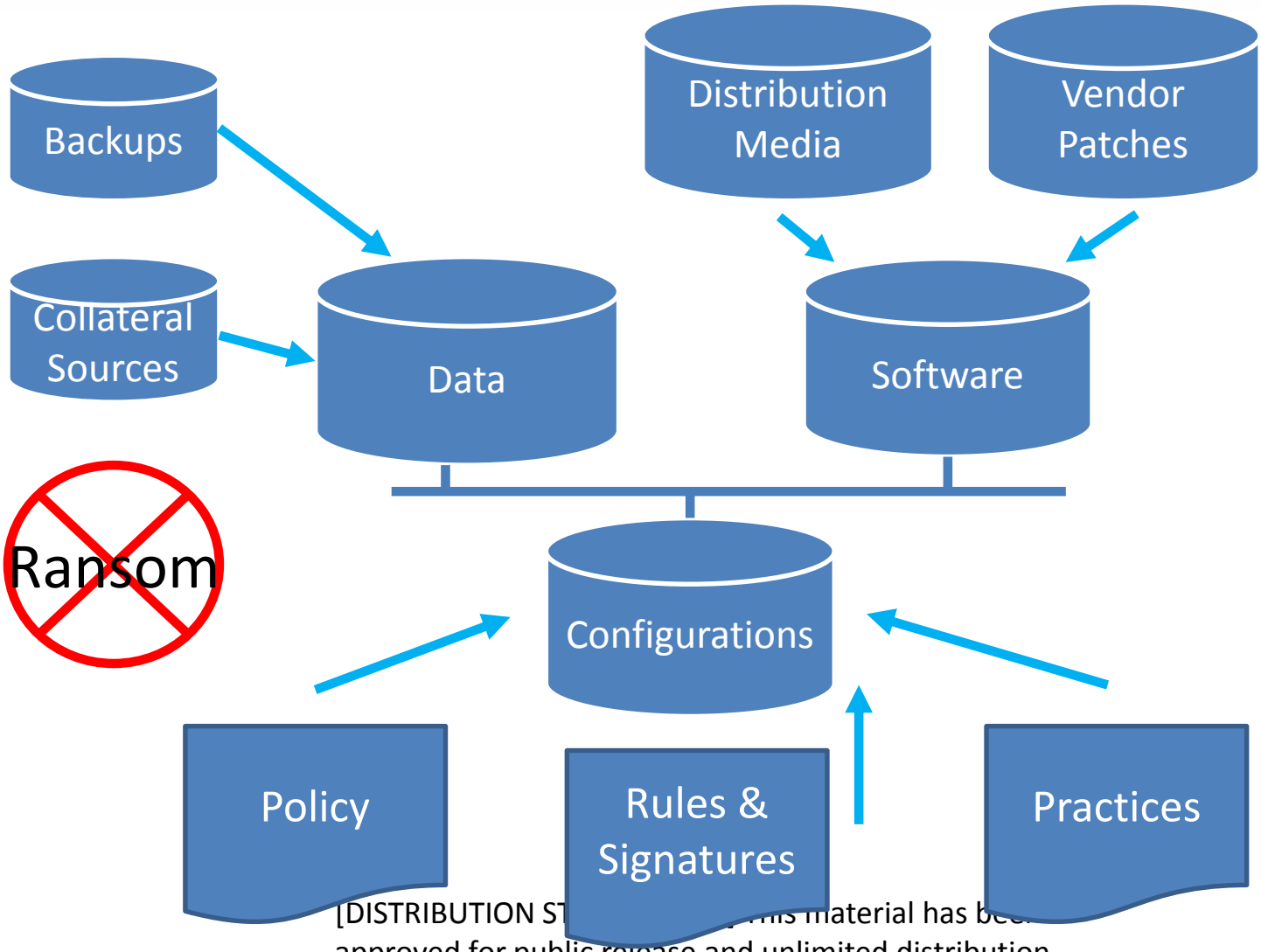
UNIVERSAL POSTAL UNION

Respond



UNIVERSAL POSTAL UNION

Recover



Decisions expected

- Allocating resources
- Emphasizing strategies
- Moving forward