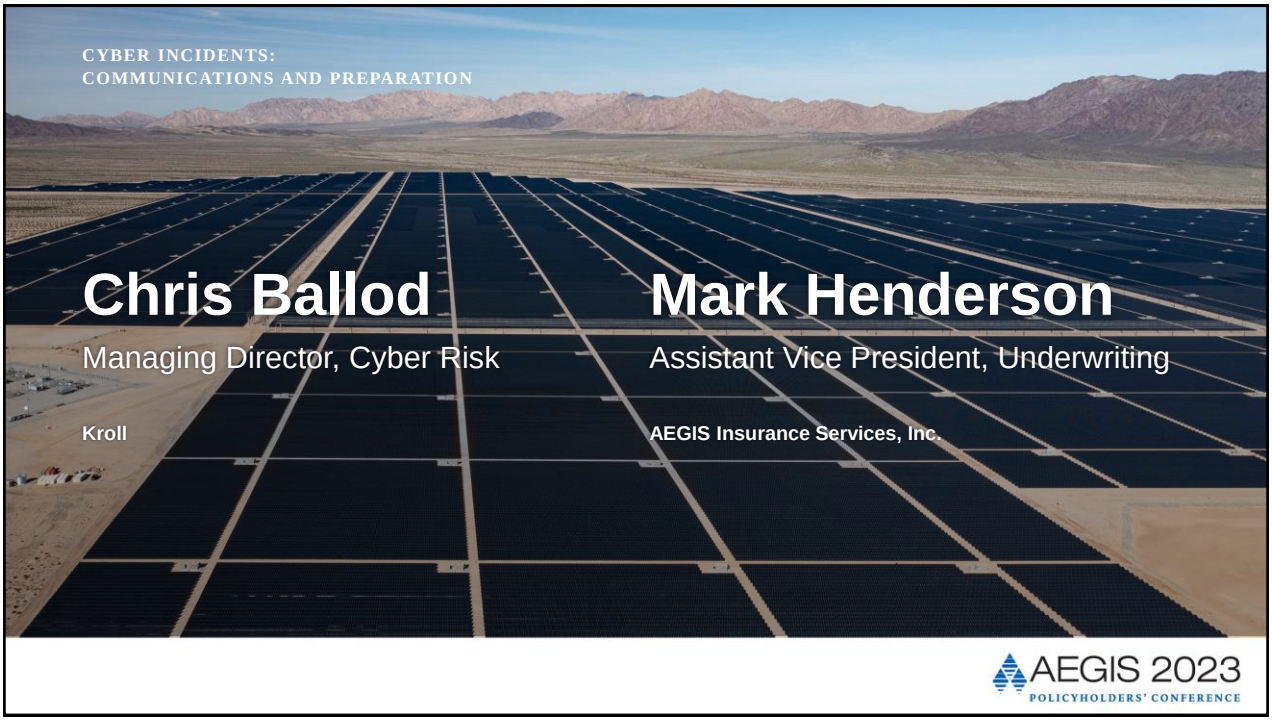


1

What to Prepare for

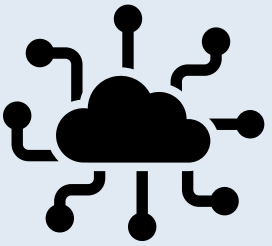
THE THREATS

AEGIS 2023
POLICYHOLDERS' CONFERENCE

2

WHAT ARE "CYBERSECURITY INCIDENTS" IN 2023?

- Extortionate Attacks
  - Active Intrusion - Ransomware (with or without data theft)
  - Active Intrusion - Data Theft
  - DDoS Attacks
  - Shaming Emails
- Social Engineering Attacks
  - Business Email Compromises
  - W-2 fraud
  - Tech support scams
- Others
  - Insider Threats
  - Hacktivists



AEGIS 2023 POLICYHOLDERS' CONFERENCE

3

THREAT ACTOR ACTIONS DURING ACTIVE INTRUSION INCIDENTS

ATT&CK Matrix for Enterprise

- Initial access methods
- Credential collection
- Network recon
- Lateral movement
- Persistence
- Data staging
- Data exfiltration
- Payload

AEGIS 2023 POLICYHOLDERS' CONFERENCE

4

THREAT ACTOR ACTIONS DURING ACTIVE ICS INTRUSION INCIDENTS

- Initial access methods
- Credential collection
- Network recon
- Lateral movement
- Persistence
- Inhibit Response Function
- Impair Process Control
- Impact

AEGIS 2023 POLICYHOLDERS' CONFERENCE

5

2023 ATTACKER PROFILES

Adapting to the Adaptations

- Attackers are bypassing MFA
- "Double encryption" to defeat new tools
- Weaponizing security tools
- Demands are up
- Spikes and dips seem to correlate to activities in Ukraine War

AEGIS 2023 POLICYHOLDERS' CONFERENCE

6

IMPACT OF ACTIVE INTRUSION ATTACKS

- Technical
  - Network downtime (24 hours to one week)
  - Data lost with backup destruction
  - Replacement/overhaul of security tools
  - Hardware replacement
  - Personnel burnout
- Costs
  - Business interruption (3 days to months)
  - Incident response costs ($100,000 USD to $2million USD)
  - Lost business and reputational harm
  - Regulatory costs
  - Potential litigation

AEGIS 2023 POLICYHOLDERS' CONFERENCE

7

IMPACT OF ACTIVE ICS INTRUSION ATTACKS

- ICS Specific Impacts
  - Loss of Protection
  - Loss of Safety
  - Physical Property Damage
  - Environmental Damage
  - Bodily Injury/Loss of Life

AEGIS 2023 POLICYHOLDERS' CONFERENCE

8

What it Looks Like and Why

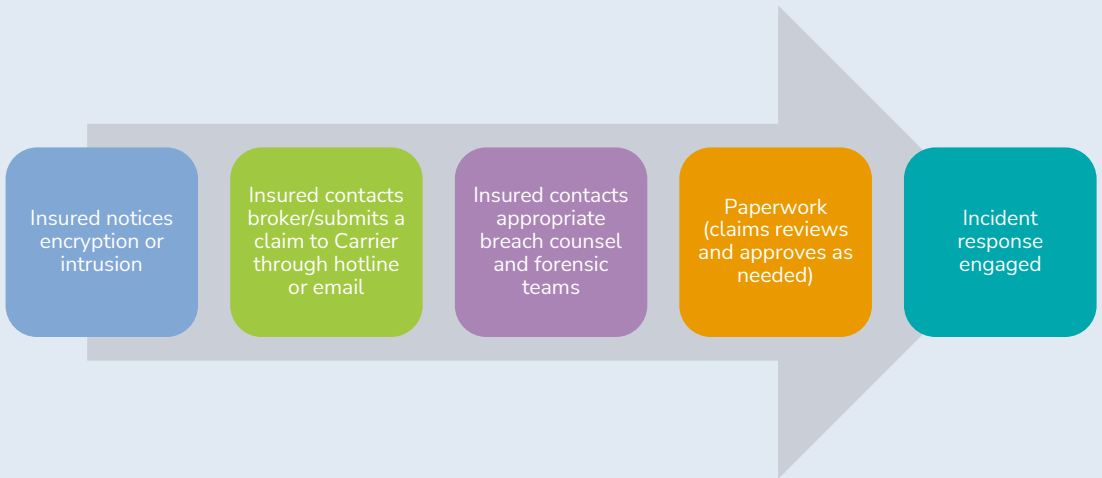
GOOD INCIDENT RESPONSE

AEGIS 2023 POLICYHOLDERS' CONFERENCE

9

OVERVIEW OF INSURED NOTIFICATION OF CLAIM TO ENGAGEMENT

The simple steps



AEGIS 2023 POLICYHOLDERS' CONFERENCE

10

OVERVIEW OF DETECTION TO ENGAGEMENT

Not so simple on closer look

Detection	Technical observation	Report to leadership	Identify support resources	
Claim	Convey the incident to Risk Management	Identify policy and contact information	Claim must be processed	
Scoping	Coordinate carrier, broker, counsel, forensics, and insured	"In crisis" triage of facts and actions taken	Plans developed	
Paperwork	Contracts generated and conveyed	Insurer approval	Client execution	Returned to vendor(s) through counsel
Response	Provisioning	Kickoff communications	Technical deployment	

AEGIS 2023 POLICYHOLDERS' CONFERENCE

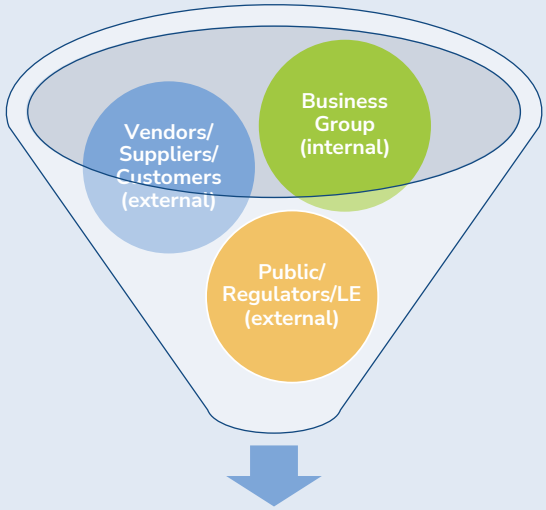
11

GOALS OF THE SCOPING CALL

- Gather facts
  - What happened and what have they already done?
  - What does this client's digital environment look like?
  - Who are they?
    - What are their internal needs?
    - What are their external concerns?
  - What solutions will work for them?
    - Time, money, reputation, internal dynamics
- Interview under pressure
  - Why would they want our help at all?
- Develop the response plan
  - Lay groundwork for consistent communications
- Manage the crisis
  - Set expectations
  - Instill calm

AEGIS 2023 POLICYHOLDERS' CONFERENCE

12



Consistent Actions and Communications

AEGIS 2023 POLICYHOLDERS' CONFERENCE

13

AEGIS 2023 POLICYHOLDERS' CONFERENCE

14

15