FIREWALL DOWN: The Countdown Begins

The First 48 Hours of a Cyber Incident

RISK MANAGEMENT

PRESENTED BY

KAILEY FLANNELLY
BEAZLEY SECURITY

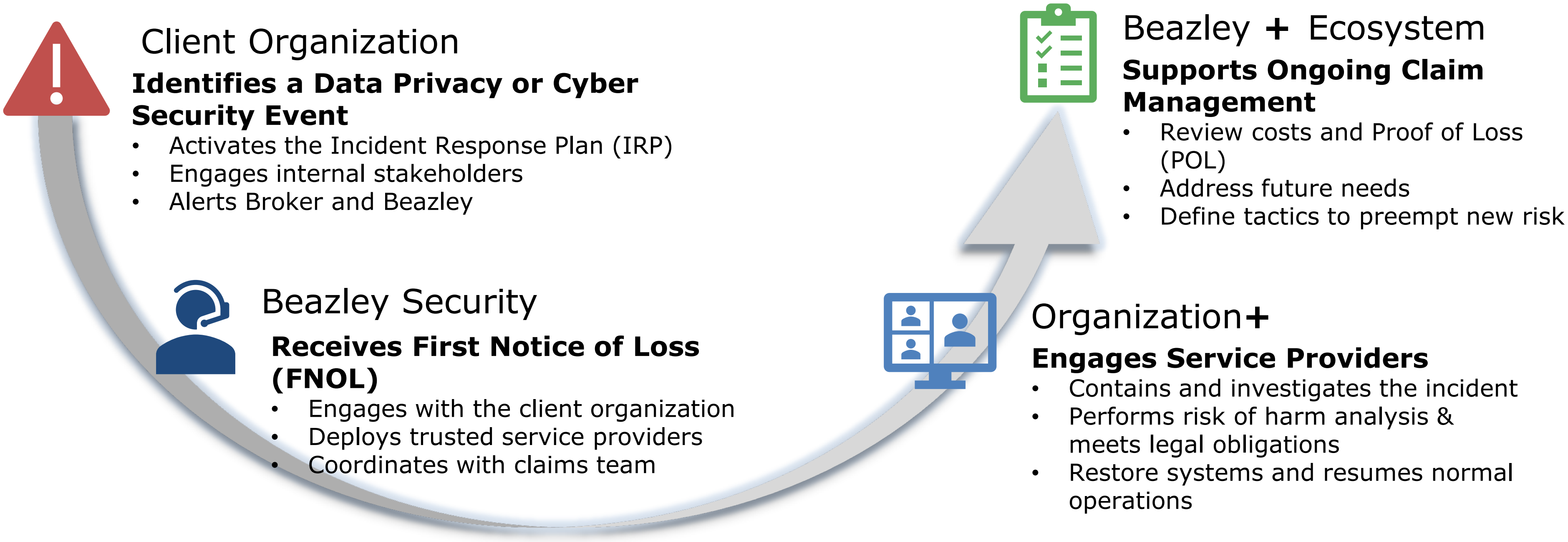
THOMAS JOYCE
ALLIANT

Report an Incident

Incident Notification

When?	Actual or suspected cyber security or data incident
	Does not trigger the policy
	Before you engage vendors. The sooner you notify, the sooner we can help
How?	Email / online form / phone
	Notify a breach | Beazley
	https://www.beazley.com/en-US/cyber-customer-centre/notify-a-breach/
What to include?	Brief description of the incident
	No sensitive data (PHI/PII)
	Don’t use the term “breach”
What to expect?	Cyber Services manager will schedule a call, coordinating vendors as needed
	You decide whether to engage vendors or open a claim

Lifecycle of a Cyber Incident



Client Organization

Identifies a Data Privacy or Cyber Security Event

- Activates the Incident Response Plan (IRP)
- Engages internal stakeholders
- Alerts Broker and Beazley

Beazley Security

Receives First Notice of Loss (FNOL)

- Engages with the client organization
- Deploys trusted service providers
- Coordinates with claims team

Organization+

Engages Service Providers

- Contains and investigates the incident
- Performs risk of harm analysis & meets legal obligations
- Restore systems and resumes normal operations

Beazley + Ecosystem

Supports Ongoing Claim Management

- Review costs and Proof of Loss (POL)
- Address future needs
- Define tactics to preempt new risk

Who is Involved?

IT / SECURITY

INTERNAL LEGAL COUNSEL

EXECUTIVE LEADERSHIP TEAM

COMMUNICATIONS

HUMAN RESOURCES & PAYROLL*

Securing the Right Providers

2026 AOA
ANNUAL CONFERENCE

Privacy Counsel

Roles of Privacy Counsel:

- **Establishes attorney-client privilege and directs the investigation**
- **Determines regulatory and notification obligations (FERPA, HIPAA, state breach laws, etc.)**
- **Approves external communications before release**

Digital Forensics & Incident Response (DFIR)

Roles of DFIR:

- **Determines how the threat actor (TA) gained access**
- **Determines what systems and data were accessed or encrypted**
- **Supports safe containment and recovery of evidence**

Threat Actor Communications (TAC)

Roles of TAC:

- **Manages controlled communication with the TA**
- **Assesses the credibility of the threat**
- **Supports intelligence gathering and ransom negotiations if approved**

Additional Service Providers

Restoration
&
Recovery

eDiscovery
&
Data Mining

Crisis
Communications
(PR)

Notification & Call Center

Credit Monitoring

Common Mistakes

- Engaging service providers prior to notification
- Rebooting or wiping systems
- Restoring backups immediately
- Over-communication early on
- Communicating with the Threat Actor

Best Practices

Incident Response

1

Restrict all inbound & outbound internet traffic before making exceptions for EDR tooling

2

Disable or limit all VPN and remote access

3

Audit all administrative accounts and all accounts created within the last 30 days to ensure they are legitimate

4

Reset passwords, including all administrative accounts, service accounts, and financial/banking accounts

5

Audit for maliciously created group policies (GPOs)

How to Prepare

1

Develop and annually review your organization's Incident Response Plan (IRP)

2

Determine if your organization needs to pre-vet any incident response vendors (i.e., Privacy counsel, DFIR)

3

Review carrier's list of panel vendors to maximize coverage during an incident.

4

Test your organization's IRP on an annual basis via a tabletop exercise. Consider testing different teams and leadership.

5

Regularly update your organization's IRP with relevant contact information and guidance to ensure timely response.

Scenario: Ransomware

Day 1

Monday, 6:00am

- Several faculty members at a university have reported to the Helpdesk that they found a strange file open on their PC’s this morning when they logged in.
- Word is starting to spread among faculty that this note was found.

Monday, 10:30am

- The internal IT team begins look through logs and checking with the SOC on any alerts coming from these specific user devices.
- The SOC identified suspicious sign-ins alerts coming from these user accounts 5 days ago but did not see any other unusual activity on those accounts.

Monday, 11:30am

- The SOC and internal IT teams confirm that at least 10 systems including some critical infrastructure, some of the school's operational technology (OT) environment, and some teaching devices were encrypted.
- The CIRT decides it is necessary to take systems offline as all 10 systems have encryption at the file level.

Day 1

Monday, 3:30pm

- In accordance with their IRP, the university's Risk Manager reaches out to Beazley Insurance using the bbr.claims@beazley.com email address.
- A Cyber Services Manager from Beazley Security contacts the risk manager to better understand the incident and make sure any necessary resources are coordinated for a scoping call.
- A meeting is set up between the university's CIRT, external Privacy Counsel, Digital Forensics & Incident Response, Restoration & Recovery, and Threat Actor Communications firms.

Day 2

Tuesday, 10:30am

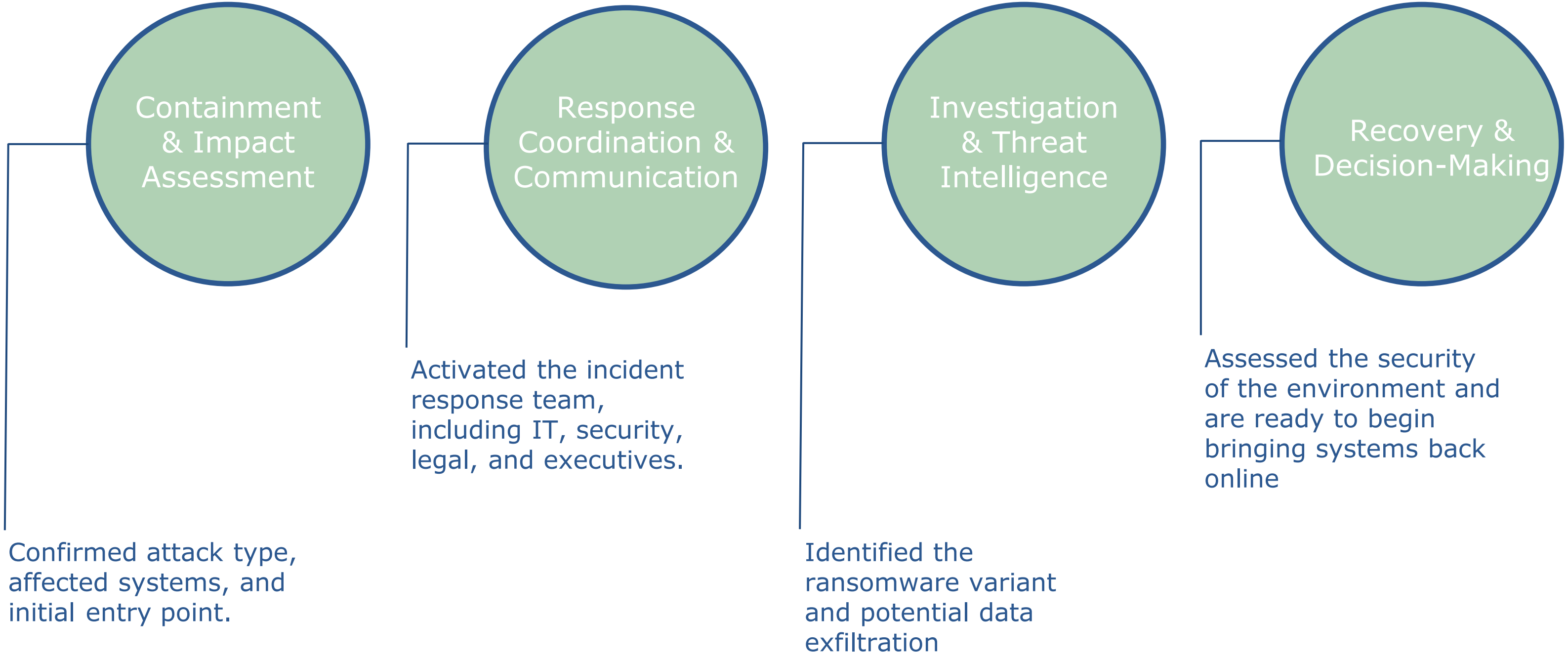
- During the first update call, legal has provided Silver Pine with a ShareFile to upload any relevant contracts which might need review.
- Legal also provides an initial summary of how the current facts relate to the regulatory landscape.
- DFIR/Resto teams now have visibility across the Silver Pine environment and have begun offline triage collections of any systems showing signs of unauthorized access.

Tuesday, 3:30pm

- During the second update call, the university executives approve reaching out to the threat actor for information gathering and research purposes only at this point.
- Based on previous interactions with the TA group, the TAC team estimates that negotiations can range from 6-12 days before the TA posts the data they have on their leak site.
- The TAC team is going to initiate contact with the TA within the next hour to start the process.

Context: Key Milestones

Typically achieved going into day 3 of a ransomware attack



Containment & Impact Assessment

Confirmed attack type, affected systems, and initial entry point.

Response Coordination & Communication

Activated the incident response team, including IT, security, legal, and executives.

Investigation & Threat Intelligence

Identified the ransomware variant and potential data exfiltration

Recovery & Decision-Making

Assessed the security of the environment and are ready to begin bringing systems back online

Questions?

2026 ANNUAL CONFERENCE OAKLAND, JANUARY 11 - 13

AUXILIARY ORGANIZATIONS ASSOCIATION

THE NEXT ERA OF AUXILIARIES
SHAPING TOMORROW

THANK YOU!