

FDCC CCS ANNUAL MEETING · SEPTEMBER 2026 · NEW ORLEANS

Prevent, Defend, and Recover

after a Cyber Incident

The Corporate Counsel Cyber Playbook



Presented by Jessica Eldridge · Jane Warring · David Vanalek · Kate Barecchia

Objectives

Pre-loss decisions drive post-loss outcomes — four counsel objectives across the incident lifecycle

PREVENT

01

Help prepare clients before a security incident

Align governance, IR plans, and insurance terms while leverage and time still exist.

MANAGE

02

Counsel-driven decisions in crisis

Make the calls — privilege, narrative, ransom, notice — under one coordinated counsel-led structure.

INSULATE

03

Reduce litigation and claims friction

Build a defensible loss narrative tied directly to policy language; avoid hindsight reconstruction.

LEARN

04

Convert lessons into preparedness

Translate every incident into IR plan revisions, tabletop scenarios, and renewed coverage alignment.

The Cyber Risk Landscape

Counsel must now assume cyber risk as a corporate-wide legal and business issue



OWNERSHIP HAS SHIFTED

Cyber risk is no longer owned solely by IT

Boards, legal, finance, operations, and risk management all share responsibility — and exposure — for cyber readiness.



EXPOSURES MULTIPLY

A single incident triggers four parallel crises

Operational disruption, financial loss, regulatory scrutiny, and litigation exposure unfold simultaneously, often within hours.



WHERE THE LOSSES LIVE

BI and supply chain losses exceed remediation costs

Business interruption, third-party harm, and contract penalties consistently outweigh forensic and IT recovery spend.

PART I

Before the Security Incident

How corporate counsel can help prepare clients



Aligning governance, response plans, and insurance — before they're tested.

Helping Clients Prepare Before the Security Incident

Four levers counsel can pull before an incident occurs



01

Governance & Board Oversight

Align corporate governance and board reporting with the cyber risk profile. Establish committee accountability and cadence. Have discussions with subject matter experts during tabletop discussions.



02

IR Plan / Policy Alignment

Ensure incident response plans satisfy cyber insurance policy conditions, notice triggers, and panel-counsel requirements.



03

Close Coverage Gaps Early

Purchase the right coverage for your business. Identify sub-limits, exclusions, and waiting periods that surface only at claim time. Close gaps while leverage exists.



04

Pre-Loss Communication Strategy

Pre-wire stakeholder, regulator, and insurer communications to reduce post-loss disputes and inconsistencies.

Building the Incident Response Plan

Best practices for security incidents and ransomware attacks — pre-defined authority, not improvised decisions



Decisionmakers Identified in Advance

Pre-define every decision authority before an incident — ransom payment, regulator notice, customer disclosure, vendor engagement. Eliminate ambiguity at the worst possible moment.



Detailed Lines of Authority

Document who decides what — and who decides if they're unavailable. Map authority to specific decision categories with named primary, secondary, and tertiary holders.



Appendix: Direct Cell Numbers

Maintain personal cell phone numbers for every decisionmaker and IR team member in a dedicated appendix. Corporate channels may be unavailable; personal contact is the failsafe.



PRINT THE PLAN. Distribute hard copies to every team member in advance — a ransomware lockout may make your digital plan inaccessible exactly when you need it most. Update the IR Plan regularly to include new contacts and revised procedures.

Cyber Insurance: Where Clients Get It Wrong

The most common mistakes that surface only when the claim is filed

01

Incomplete Policy Review

Reading the dec page is not reading the policy.

Endorsements, definitions, and conditions buried deep in the form drive coverage outcomes — not the headline limits.

02

Sub-Limits, Waiting Periods & Exclusions

Where coverage quietly disappears.

BI sub-limits, dependent BI carve-outs, war/cyber operations exclusions, and waiting periods routinely strand otherwise-valid losses.

03

IT Plans Misaligned to Policy Conditions

Operational reality vs. policy paper.

Forensic vendor selection, notice timing, and ransom decision authority must match policy conditions or coverage may be jeopardized.

Insurance: Triage Points and What to Look For

Beyond the cyber policy — every adjacent and excess layer counsel must check

ABOVE THE TOWER

Umbrella & Excess Coverage

- Does the umbrella attach above the cyber policy?
- Follow-form, or its own carve-outs and definitions?
- Identify gaps between primary cyber and excess layers
- Often-untapped capacity once the primary is exhausted

PRIMARY LAYER

The Cyber Policy

- Coverage triggers, notice provisions, retentions
- Sub-limits, waiting periods, dependent BI carve-outs
- War / cyber operations exclusions and endorsements
- Panel-counsel and approved-vendor restrictions

ADJACENT POLICIES

Other Coverage to Check

- Social engineering / fraudulent instruction (Crime)
- Computer fraud, fidelity, employee dishonesty
- D&O for board-level exposure; E&O for professional duty
- Property / GL for BI tied to physical or third-party harm
- Reputational harm, AR, upgrades

PULL THE ENTIRE TOWER. Recovery often lives in policies counsel didn't initially look at — review primary, excess, and every adjacent line.

PART II

When the Security Incident Happens

Counsel-driven decision points



Decisions made in the first hours shape every claim, dispute, and litigation that follows.

The First 72 Hours

Three tracks that must run in parallel — under one coordinated counsel-led structure

72
HOURS

*The window in which most
litigation outcomes are
effectively determined*



Narrative Control

Who speaks externally, when, and through what channel?



Privilege Preservation

Counsel-led engagement of forensics; segregate fact-finding from defense work product.



Track Coordination

Forensic, legal, and insurance workstreams run in parallel — but to a single playbook.



PRE-ENGAGE FORENSICS. Establish the forensic vendor relationship in advance — and consider engaging through outside counsel to preserve privilege from the start.

Ransomware, Payments & Business Interruption

Where legal, financial, and operational pressure collide



Ransom Payment Decision-Making

Sanctions exposure (OFAC), fiduciary duty, insurer pre-approval, and downstream litigation risk all converge on one decision under time pressure.



Downtime vs. "Resumption"

Policy definitions of "period of restoration" and "resumption of operations" rarely match operational reality. Document both definitions in real time.



Real-Time Loss Documentation

Financial reconstruction is far harder retroactively. Stand up contemporaneous BI workpapers from Day 1 — under privilege where appropriate.



PRE-DECIDE. Review ransom payment decision criteria with the CEO, outside counsel advisors, and the Board in advance of an attack — not in the heat of the incident.

Managing Executive & Board Expectations

Three counsel-led tensions to manage, in real time, in front of the board

Timing

VS.

Certainty

Speed pressure vs. accuracy of facts before regulator and customer disclosures.

Regulatory Notice

VS.

***Coverage
Preservation***

Notice obligations may collide with insurer cooperation conditions and privilege.

Decisive Action

VS.

Hindsight Bias

Decisions made under fog of war will later be judged by litigators with full information.

PART III

After the Crisis

Reducing litigation and claims friction



Disputes are rarely about bad faith — they are about ambiguity, valuation, and credibility.

Triggers of Cyber Claims Disputes

Even when both sides intend to perform — these are the friction points

Policy Ambiguity

Definitions of "covered loss," "period of restoration," and dependent BI vary widely — and rarely map cleanly to a real incident.

Loss Quantification Disagreements

Carrier and insured forensic accountants apply different methodologies to the same data, generating wide gaps in indicated loss.

Industry-Specific BI Methodologies

Manufacturing, professional services, and retail each demand tailored loss models — generic BI math creates credibility problems.



THE COUNSEL RESPONSE

Build a defensible loss narrative tied directly to policy language

- Map every claimed loss to a specific policy term
- Document methodology choices contemporaneously
- Avoid hindsight reconstruction; preserve credibility
- Engage industry-appropriate experts early

Industry-Agnostic Case Snapshots

Three patterns we see repeatedly — and what counsel could have changed



Manufacturing

Ransomware Shutdown

Production line halts; downstream customer penalties and contingent BI claims dwarf the IT recovery spend.



Professional Services

Data Exfiltration

Sensitive client data exposure triggers regulatory inquiries, professional duty issues, and reputational harm in parallel.



Retail & Logistics

Third-Party Vendor Compromise

Vendor compromise becomes the insured's incident — contract indemnity, contingent BI, and customer notification all activate.

EVERY CASE HIGHLIGHTS: Counsel decision points · Coverage implications · Missed opportunities to reduce exposure

The Corporate Counsel Cyber Playbook



Preparedness as Strategy

Cyber preparedness is core legal and risk strategy — not an IT line item. Treat it as such on the board agenda.



Early & Active Counsel

Counsel involvement at the start of the incident — not the claim — drives every downstream legal and coverage outcome.



Practical Preparation

Pre-loss alignment of governance, IR plans, and policy terms is the single most reliable lever for post-loss outcomes.

Tabletop Exercises

Best practices for testing the plan before it's tested for real



01

Cross-Functional Participation

Include legal, IT, finance, communications, executives, and the board — plus external counsel, forensics, and broker.



02

Realistic, Varied Scenarios

Rotate through ransomware, data exfiltration, vendor compromise, and insider threat. A repeated scenario tests muscle memory, not the plan.



03

Stress-Test the Plan

Inject curveballs — degraded communications, key personnel unavailable, conflicting customer demands. Surface gaps before an adversary does.



04

Document & Act on Findings

Every exercise produces a gap log. Convert each gap into a plan revision, authority change, or training need — and track to closure.

If the plan isn't tested, it isn't a plan.

Presenters

Forensic consulting · coverage litigation · in-house legal · insurance leadership



FORENSIC ACCOUNTING

Jessica Eldridge

SVP & Practice Director, Cyber

J.S. Held



COVERAGE LITIGATION

Jane Warring

Partner

Zelle LLP



INSURANCE LEADERSHIP

David Vanalek

SVP, Chief Legal & Compliance

***Richmond National
Insurance***



IN-HOUSE COUNSEL

Kate Barecchia

SVP, Legal

IntegriChain

Thank You

Pre-loss decisions drive post-loss outcomes.

