HINSHAW

From Protection to Readiness: What Today's Cyber Landscape Demands of Organizations

Cybersecurity, Privacy, and Compliance Considerations You Need to Know

Privacy, Cyber & AI Decoded Alert | 3 min read
May 6, 2026

By: Cathy Mulrow-Peattie, Laura Flanagan

3iCO and Hinshaw & Culbertson LLP recently hosted a webinar on the evolving cybersecurity landscape and what it means for firms today. The discussion was led by Cathy Mulrow-Peattie, Partner at Hinshaw & Culbertson LLP, and Laura Flanagan, Founder and CEO of 3iCO, and focused on how organizations can better prepare for, respond to, and navigate cyber incidents.

Below is a summary of the key themes explored in the webinar.

Cyber risk is evolving… and accelerating

Cyber threats are not just increasing; they are changing in kind.

Attackers are no longer focused on "breaking in." Increasingly, they are logging in, using stolen credentials obtained through phishing, social engineering, and highly convincing impersonation of you and your organization's personnel.

AI is accelerating this shift. Voice cloning, deepfakes, and emails that replicate tone and authority are making these attacks harder to detect and easier to act on.

The result: The risk has escalated; you can no longer wait to be prepared.

"Shadow AI"—the use of unvetted tools without standard due diligence and procurement practices—means sensitive data may already be compromised on external platforms, where appropriate cybersecurity and compliance controls may be lacking.

Regulatory expectations are intensifying… and moving faster.

Regulators are not standing still, and neither are enforcement actions.

Federal agencies and states are increasingly aligned in their focus on cybersecurity, with expanding privacy laws and coordinated enforcement efforts across jurisdictions.

The expectation is clear:

- Document where your data is;
- Protect it with appropriate cybersecurity controls and policies;
- Assess your cybersecurity risk regularly and as business circumstances change; and
- Be able to demonstrate that your policies are operationalized, not theoretical.

Organizations are not penalized for being breached.

They are penalized for being unprepared.

The cost of getting this wrong is high.

Cyber incidents are no longer isolated IT events…they are business events.

Financial impact can be substantial, but equally important are:

- Regulatory scrutiny
- Post data breach class action litigation exposure
- Long-term compliance oversight
- Reputational damage

In many cases, the downstream effects extend well beyond the initial breach.

Incident response readiness is where many firms fall short.

Most firms have an incident response plan. Far fewer have one that works.

Many plans remain high-level, focused on rudimentary documentation rather than execution. What's required is a detailed, operational plan with clearly defined roles, escalation paths, and customer and regulatory requirements.

And it needs to be: tested!

If a plan has not been exercised through simulations or real-time drills, it is unlikely to perform under pressure.

If you have not practiced it, you do not have it.

Cybersecurity is now a legal and reputational strategy.

How an organization responds to a cyber event can carry as much risk as the event itself.

Early involvement of cybersecurity counsel helps:

- Protect communications under privilege;
- Guide investigative and reporting decisions; and
- Reduce exposure to regulatory and litigation risk.

At the same time, communication must be tightly managed.

In a breach, organizations are not just reporting facts; they are protecting trust and credibility.

Third-party risk remains one of the largest exposure points.

Vendors continue to be a primary pathway into organizations, including AI platforms.

A common refrain, “we clicked accept,” is no longer sufficient.

Organizations are expected to:

- Conduct due diligence;
- Understand and test vendor security practices;
- Maintain appropriate contractual protections; and
- Monitor risk on an ongoing basis.

Your vendors’ cyber weaknesses will become yours.

Cyber insurance requires active management.

Cyber insurance can mitigate financial exposure, but only if properly understood and aligned with internal practices.

Organizations should:

- Evaluate what is--and is not--covered
- Ensure compliance with policy requirements
- Consider flexibility around counsel and vendor selection

Insurance can support response, but it is not a substitute for preparation.

Final Practical Considerations

The landscape has shifted from “protect your systems” to “assume a breach and be ready to respond.”

With the average cost of a data breach at $10M and climbing, proactive cybersecurity measures are not only a regulatory-sound practice but a financial necessity.

Organizations are expected to demonstrate that their approach to cybersecurity is:

- Operational,
- Tested, and
- Executable under pressure.

Because ultimately, the defining moment is not the breach itself… it is how the organization responds when it happens.

We are here to help.

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Related Capabilities

Data Breach

Data Privacy, AI & Cybersecurity

Regulatory & Compliance

Website Data Privacy

Related Insights

When a Cyber Breach Hits: Cybersecurity, Privacy, and Compliance

Cathy Mulrow-Peattie Warns of Escalating Cyber Threats Following Iranian Wiper Attack