

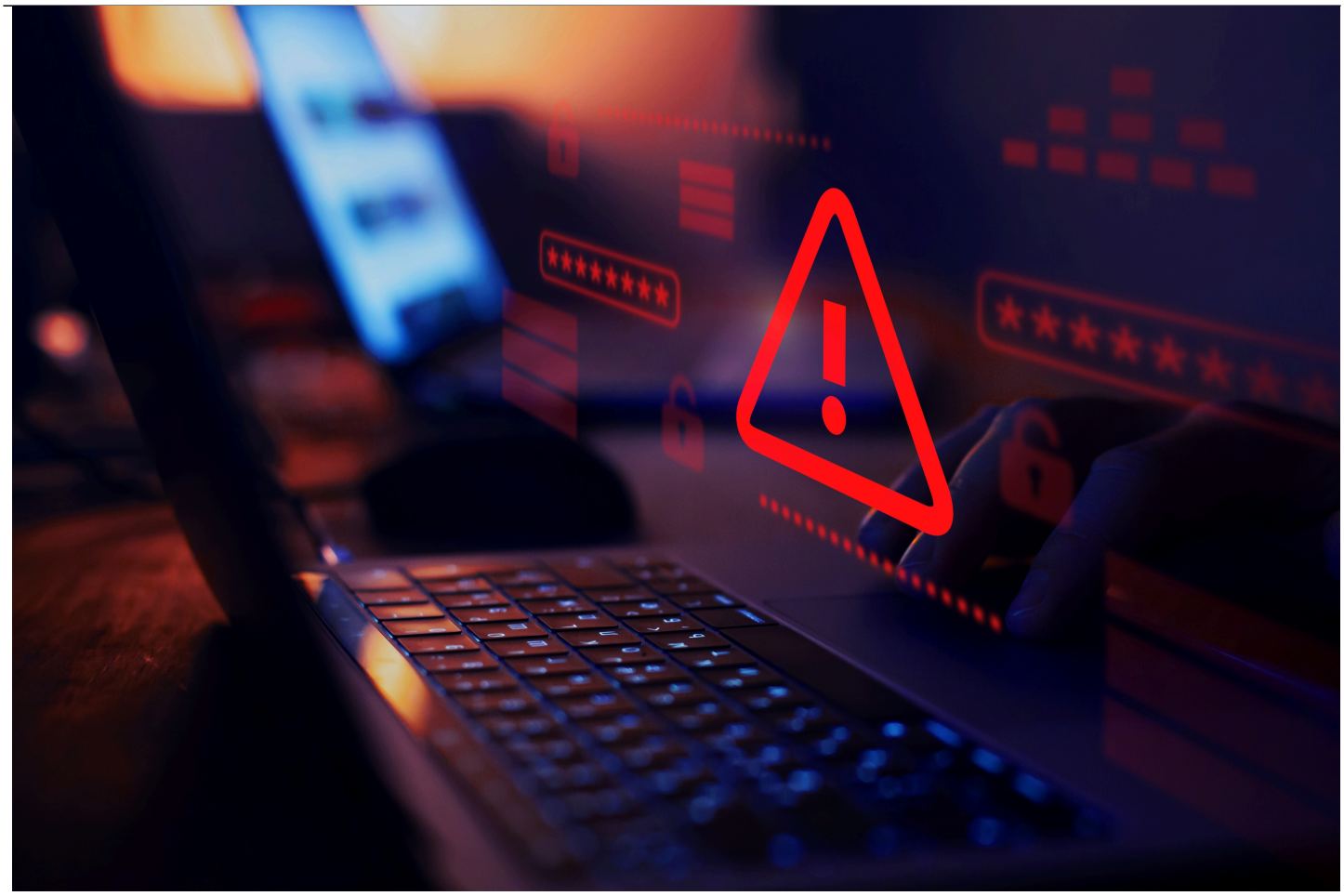
Binance Hack: 3 Lessons for In-house Counsel

Corporate, Securities, and Governance

Information Governance

Law Department Management

Technology, Privacy, and eCommerce



Banner artwork by / *Shutterstock.com*

What do in-house attorneys need to know in the wake of the Binance crypto heist?

On October 29, 2026, cybercriminals stole over $6 billion [USD] from Binance, a cryptocurrency exchange.

Blockchain intelligence firm TRM Labs called it the largest crypto theft on record. To put it in perspective: That is about four times the $1.5 billion [USD] Bybit hack of February 2025.

The massive heist was pulled off in just 20 minutes. The FBI has confirmed TraderTraitor, North Korea's elite hacking unit, was responsible for the theft.

The Binance breach is only a few days old, but there are still some lessons in-house counsel can take away (and they go well beyond crypto).

3 Lessons for In-house Counsel

1. **Check your insurance to determine if nation-state attacks are covered.**

Does your cyber policy have an exclusion that could block coverage?

Consider whether a “war exclusion” would apply. Depending on the country from which the cyber-attack originates, this could negate the policy.

Additionally, a policy may require you to timely report incidents. Review your policy to evaluate definitions and potential exclusions.

2. **Establish relationships before you need them.**

Binance reported that it immediately engaged with law enforcement and blockchain intelligence partners after the breach. Around $3 billion [USD] of affected assets had been frozen shortly after the attacks, the company said.

A rapid coordinated response is critical in the wake of a cyberattack. Keep a current list of contacts at law enforcement, regulators, key counterparties, and information-sharing groups.

Write down who in the company is authorized to contact each of them. Consider incorporating this information into your incident response plan.

3. **Prepare for increasingly sophisticated attacks.**

TRM’s assessment is that Binance’s hot-wallet signing infrastructure was compromised. In other words, the transactions looked legitimate because, technically, they were signed. Binance has not yet published a root cause.

However, as of publication, TRM has not confirmed that AI was used in the Binance attack. But the incident shows the conditions AI is making more common: attacks are being prepared in advance, can happen fast, and look like normal activity to the controls meant to stop them.

As Robert Kang wrote in a previous Corporate Counsel Now article, AI is “accelerating both the scale and sophistication of attacks, compressing the time organizations have to detect and respond.”

That cuts both ways for legal departments:

- **AI in remediation.** Security teams increasingly use AI to spot anomalies, triage alerts, and speed containment. In-house counsel should know what these tools are allowed to do automatically, such as freezing transfers or isolating systems.
- **AI can help cybercriminals evade controls.** Attackers can use AI to make malicious activity look routine, from convincing phishing to transactions that pass automated checks. A control that only asks, “is this signed?” or “does this look normal?” may not be enough.
- **Prepare before an incident occurs.** When funds can leave in 20 minutes, escalation paths, authority to freeze or halt, and evidence preservation protocols must be set before the incident.

ACC resources to help you prepare

ACC members can use the following resources to tighten AI and cyber readiness now:

- **The Hardest AI and Cyber Problems Aren't Technical. They're Decisions** *(Corporate Counsel Now)*. Robert Kang's recap of the 2026 Summit lays out four shifts for counsel: clarify ownership, define escalation, build evidence, and train people.
- **Cybersecurity Toolkit for In-house Lawyers, Second Edition** *(ACC Toolkit*). Nine checklists, including an **Artificial Intelligence and Cybersecurity** checklist, plus Responding to Cyber Incidents, Preparing for Data Breaches, and Protecting Attorney-Client Privilege.
- **Beyond the Battlefield: Recalibrating Enterprise Cyber Risk in an Era of Geopolitical Escalation** (*Corporate Counsel Now*). Practical steps for state-linked threats: confirm logging and monitoring, review incident response plans, check insurance for "act of war" exclusions, and strengthen MFA.
- **Navigating Risk and Opportunity in Digital Asset Treasury Strategies** *(ACC Resource)*. Covers regulatory, accounting, governance and custody issues for companies holding crypto, with an action checklist.
- FBI Cyber Collaboration: A Guide for In-house Counsel *(ACC Checklist)*. From July, this resource discusses how organizations can collaborate with the US Federal Bureau of Investigations (FBI) when responding to or preparing for a potential threat.
- **Data Breach! A Playbook for The First 72 Hours** *(Corporate Counsel Now)* Stephen Baird and Simon Elliott outline critical steps in-house counsel should make in the first hours of a data breach and why preparation is key.

Join the ACC Foundation in Los Angeles for the annual Cybersecurity + AI Summit

The threats are moving faster. The decisions behind your response cannot wait for the next incident.

The ACC Foundation 2027 Cybersecurity + AI Summit takes place **March 15–16, 2027, in Los Angeles**. Over two days, in-house leaders will work through the intersection of cybersecurity, AI, privacy, and legal risk, alongside the peers and experts shaping the response.

Register now: 2027 Cybersecurity + AI Summit

Association of Corporate Counsel



Staff

ACC