Stay Current

PAUL HASTINGS

September 2025

Follow us on LinkedIn

Compliance Update

Chinese Cyber Actors Impersonate House Committee Chair: Key Risks Companies Must Understand

By Ronak Desai, Renato Mariotti, David Coogan, Keith Feigenbaum and Marguerite Harris

Earlier this month, Chinese-linked cyber actors launched a spear-phishing campaign impersonating Representative John Moolenaar, chairman of the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party. Fraudulent emails sought "input" on draft sanctions legislation and were sent to U.S. officials, multinational companies, law firms, trade associations, think tanks and even at least one foreign government.

The campaign's sophistication lay not in the technical aspect of the subterfuge but rather in its credibility. Congressional committee offices routinely circulate draft language and solicit quick reactions from outside stakeholders. Exploiting that routine, the attackers created a scenario in which busy professionals might instinctively click, reply or forward, handing over credentials or opening the door to malware. The FBI and Capitol Police are now investigating.

The Broader Pattern

This episode is not an isolated case. It fits a wider panorama of adversary tradecraft targeting Congress, policymakers and affiliated communities:

- **Congress Under Direct Fire**: In 2017-18, Russian GRU unit APT28 spoofed Senate email domains to harvest staff credentials. Other Russian and Chinese campaigns have sought to compromise House and Senate systems for both espionage and influence.
- **Iranian Impersonation**: Iran-aligned actors (known as TA453 or Charming Kitten) routinely pose as journalists or scholars, sometimes even creating multi-persona conversations, to coax sensitive information from foreign-policy targets.
- **North Korean Campaigns**: North Korea's Kimsuky group has targeted think tanks and academics by posing as reporters seeking comment on topical issues, harvesting credentials that later fuel broader espionage.
- **China's Wider Toolkit**: Beyond phishing, China-nexus actors have abused cloud tokens (as in the 2023 "Storm-0558" incident that accessed senior officials' email) and embedded themselves in U.S. critical infrastructure using administrative tools to avoid detection.

The common thread: credibility and access. By masquerading as trusted policymakers, journalists or partners, adversaries shortcut skepticism and capture intelligence at the source.

Key Lessons

For companies, trade associations and law firms that regularly engage with Congress, the risks extend far beyond information technology:

1. **Congressional Investigations Risk**: A compromised email exchange with a committee can expose sensitive strategy, testimony drafts or lobbying positions, which can invite further scrutiny from investigators or regulators.

2. **Sanctions and Export Controls**: If adversaries gain advance knowledge of your positions on sanctions or supply-chain issues, they can anticipate and counter your moves. Even selective leaks of internal views could complicate negotiations or damage credibility.

3. **Reputational Harm**: Being identified as part of successful foreign cyber campaign, even as an unwitting victim, can undermine trust with Congress, regulators and the public.

4. **Disclosure Obligations**: Depending on what information is compromised, companies may face state breach-notification requirements, contractual notice clauses or, for issuers, potential Reg FD exposure.

5. **Third-Party Vulnerability**: Trade associations, external advisers and law firms are attractive targets because they aggregate sensitive information across many clients. A breach at one can ripple across the ecosystem.

Key Takeaways

While technical defenses remain essential, this campaign highlights governance and process vulnerabilities that legal and executive teams must address. Companies should be asking:

- Do we have a protocol to verify Hill outreach? Can our government relations (GR), policy and executive teams confirm legitimacy quickly without derailing urgent workflows?

- Who owns the response if an impersonation attempt succeeds — Legal, GR, IT or all three? Have roles been rehearsed?

- How are our policy positions stored and shared? Would their exposure trigger legal, contractual or disclosure obligations?

- Do our incident response plans contemplate congressional impersonation, including privileged notifications to committee staff, law enforcement and insurers?

- Are we prepared to run a tabletop exercise simulating a fake “request from Congress” hitting our GR team at a sensitive moment?

These questions are not hypothetical; they are the exact issues adversaries are probing today.

Strategic Response: What Companies Should Do Now

1. **Out-of-Band Verification**: Treat non-.gov emails claiming to be from Congress as suspicious by default. Establish a one-page verification protocol with pre-vetted staffer numbers and committee office lines.

2. **Preserve and Escalate**: Retain original suspicious emails and escalate through a legal-first process to preserve privilege. Counsel should coordinate any contact with committees or law enforcement.

3. **Harden Identity and Mail Security**: Ensure phishing-resistant multifactor authentication is mandatory, SPF/DKIM/DMARC policies are enforced and look-alike domains are monitored.

4. **Educate Frontline Teams**: Train GR, Legal and executives on impersonation risks and quick verification practices.

5. **Test and Drill**: Conduct tabletop exercises blending congressional outreach, legal obligations and technical containment.

Conclusion

This latest campaign is a reminder that cyber threats are no longer confined to servers or data centers. They now reach into the very heart of policymaking and congressional oversight. By impersonating trusted lawmakers, adversaries exploit the credibility that underpins our democratic processes.

For companies engaged in trade, sanctions and congressional engagement, the lesson is clear: prepare as though your inbox is part of the battlefield. Legal, GR and technical teams must align now before the next email arrives.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Washington, D.C.

Ronak D. Desai
+1-202-551-18265
ronakdesai@paulhastings.com

Keith Feigenbaum
+1-202-551-1929
keithfeigenbaum@paulhastings.com

Marguerite Harris
+1-202-551-1771
margueriteharris@paulhastings.com

Chicago

Renato Mariotti
+1-312-499-6005
renatomariotti@paulhastings.com

Dave Coogan
+1-312-499-6059
davidcoogan@paulhastings.com