Is Your Legal Team Staying Ahead of Cyber Risks? Consider These Tips from ACC's Updated Cybersecurity Toolkit

Compliance and Ethics

Information Governance

Technology, Privacy, and eCommerce

Banner artwork by Icons8 / Envato

Cybersecurity risks constantly evolve. In boardrooms and general counsel offices worldwide, it consistently ranks among the top organizational risks. To meet the needs of the moment, cyber defenders, and the tactics we employ, must also evolve.

To help counsel better adapt to this evolving landscape, ACC recently released the second edition of its popular Cybersecurity Toolkit for In-house Lawyers. This article highlights the toolkit's four major updates, and includes my personal thoughts on how they can contribute to the development of an effective in-house cybersecurity program.

The growing cyber risks from AI and how organizations can fight back

The first update is a summary of the AI security landscape. As an increasingly important and ubiquitous new tool, AI introduces new risks and opportunities. In addition to the AI security checklist that was included in the toolkit's first edition, the update now includes a brief overview of common and emerging attack methods such as:

- Enhanced attacks: AI used to supercharge phishing and social engineering.
- Attacks on AI systems: such as data poisoning and adversarial inputs.
- AI-generated attacks: deepfakes, identity fraud, and automated malware.

Equally important, the update also outlines mitigations, such as suggesting enhanced phishing training designed to counter AI-level deception.

How will this new article benefit counsel? Its goal is not to turn you into overnight AI experts. Instead, it provides a practical foundation for counsel to better understand AI-related risks. In turn, this knowledge can help you ask sharper questions and build more effective partnerships with your security teams.

*(**Author's note:** Many readers may be new to AI and looking for guidance to structure AI education for themselves or for the teams they lead. For a deeper dive on structuring one's AI education, see my ACC Docket article, Roadmapping AI Education for the Enterprise, which outlines practical steps for building AI literacy)*

Download the **Cybersecurity Toolkit for In-house Lawyers, Second Edition**, today!

Contributing to the software development lifecycle (SDLC)

The next update consists of a checklist listing tasks designed to assist counsel secure the development of software products. I'm particularly enthused about this one because I authored it.

Why update the toolkit to include software development? Traditionally, cybersecurity programs have focused on protecting enterprise assets like email systems and servers. But recent, high profile, supply-chain compromises such as the 2020 SolarWinds attack highlighted the need to also secure software products provided by vendors.

Because SolarWinds "Orion" software product was widely deployed across government and industry, the successful compromise of this single product enabled hackers to gain footholds into prominent organizations worldwide, Widely viewed as a tectonic security event, the SolarWinds incident triggered increased operational and legal scrutiny into securing the software development process (e.g., see Harvard Law School forum's article on SEC claims against SolarWinds).

To meet this evolving risk, I contributed a new checklist for the toolkit that maps the role of security counsel across the stages of the software development lifecycle (SDLC) — a framework used in the software development industry for designing and implementing software.

How can this knowledge benefit counsel? While technical SDLC checklists for engineers and

developers are common, few (if any) exist with a focus on security counsel. This version fills that gap. It identifies key security, legal and compliance tasks for each stage, helping attorneys embed "security by design," "privacy by design," and "compliance by design" principles from the outset. By doing so, counsel can reduce regulatory risk, avoid costly redesigns, and strengthen their credibility as partners in the development process.

(***Author's Note:*** *The ACC version of my SDLC security checklist is intentionally concise. I am developing an expanded "director's cut" edition, with additional context and commentary, for broader distribution. Stay tuned for details.)*

Protecting the attorney-client privilege

The attorney-client privilege and work-product doctrine (collectively "privilege") can be difficult to preserve in the cybersecurity context. Even newly minted cybersecurity counsel have likely heard of the "Capital One" line of caselaw, which has tightened application of the privilege in incident response investigations (e.g., JD Supra collection of Capital One-related articles).

Despite this trend, the need for privileged communications remains as vital as ever — to enable free and frank discussions between attorneys and clients.

In response to this evolving landscape, the updated toolkit now includes a checklist detailing a list of practices intended to help counsel structure their communications and reports in response to an incident.

No checklist can guarantee results, and the content of the toolkit doesn't constitute legal advice. But following these practices might strengthen counsel's position in litigation and regulatory proceedings. As a former front-line practitioner in this area, I welcome any informative guidance that can help counsel to preserve this important legal protection.

> Cyber risks will continue to evolve. With this updated toolkit, counsel can help their organizations respond with foresight and resilience.

Updating the board on cybersecurity risks

The updated toolkit is, at its heart, intended for operators: the security legal professionals who "work in the trenches." However, in my opinion, engaged leadership is the cornerstone of effective cybersecurity.

Boards of directors set the tone from the top, approve budgets, and provide crucial, strategic oversight over an organization's operations. Regulators worldwide increasingly expect boards to be engaged in cyber governance (e.g., SEC 2023 press release).

For that reason, I particularly welcome this final update to the toolkit: a call-out box with sample board-level questions, such as:

- When was our last tabletop exercise or simulation?
- What is our stance on paying ransom, and how is that decision governed?

Why is this update important? There are two reasons. The first one is tactical: to provide a list of questions that board members can consult in exercising their oversight function.

Second: the presence of this call-out box focuses attention on the need for organizations to include board members, and other senior leaders, into an organization's security function.

For those reasons, I encourage you to share this resource with your leaders. I believe it will help them engage in meaningful conversations with your organization's managerial and operational personnel, and to maintain effective oversight.

Register for the ACC **Executive Cybersecurity Risk Credential** to learn more about overseeing cybersecurity risks

Concluding thoughts

When I began practicing in cybersecurity in 2009, the field was viewed as a niche interest. "What does an in-house cybersecurity counsel even do?" was a question I heard often. Today, it is universally recognized as a top business, legal, and regulatory concern.

The 2025 edition of ACC's Cybersecurity Toolkit for In-house Lawyers equips in-house counsel with practical guidance to meet these evolving challenges. Whether navigating AI-driven threats, embedding compliance into the SDLC, safeguarding privilege, or supporting the Board of Directors, this Toolkit remains a valued resource.

Cyber risks will continue to evolve. With this updated toolkit, counsel can help their organizations respond with foresight and resilience.

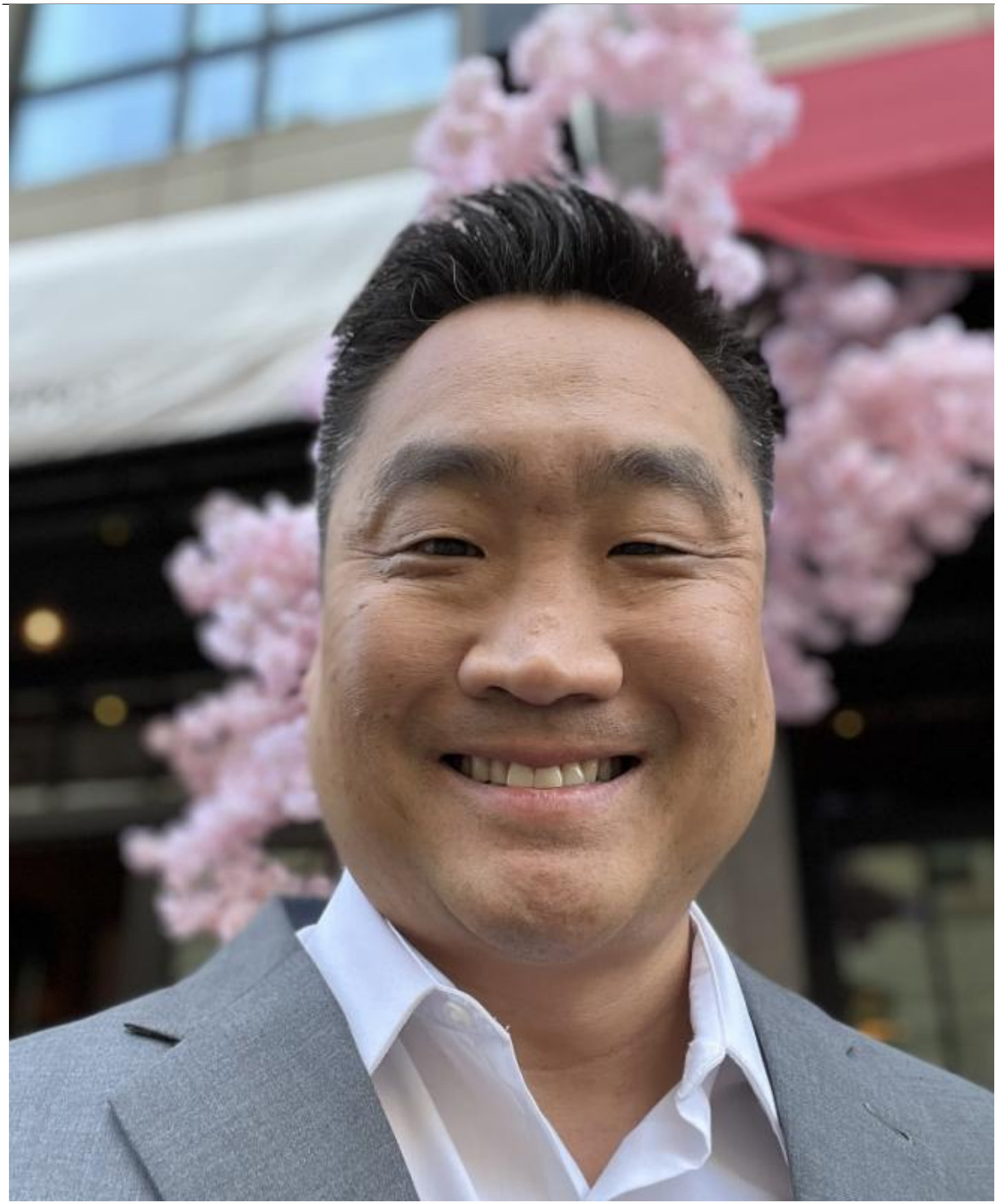
Acknowledgements

The author and ACC Docket thank the dedicated professionals of Jackson Lewis P.C., and the in-house counsel members, who contributed to the updated toolkit, including Abha T. Romkey, Vice President, Legal & Privacy, Emera; Bunny Smith, Global Cybersecurity Counsel, Yahoo; Jennifer K. Mailander, Vice President, Deputy General Counsel, Fannie Mae; Kenny Goh, Senior Legal Counsel, Changi Airport Group; Kristine Zipf Green, Cybersecurity Legal Counsel, Hitachi Energy; Lavonne Burke, Vice President Legal - Global Security & Resiliency, Digital (IT) and AI, Dell Technologies; Stephen H. Baird, Associate General Counsel SITA; and Wei Loong Siow Legal Counsel & Data Protection Officer Changi Airport Group.

Join ACC for more cybersecurity resources!

Disclaimer: The information in any resource in this website should not be construed as legal advice or as a legal opinion on specific facts, and should not be considered representing the views of its authors, its authors' employers, its sponsors, and/or ACC. These resources are not intended as a definitive statement on the subject addressed. Rather, they are intended to serve as a tool providing practical guidance and references for the busy in-house practitioner and other readers.

Robert Kang



Adjunct Professor

Loyola Law School, Los Angeles & USC Viterbi School of Engineering

Professor Robert Kang serves as adjunct faculty at the foregoing institutions. His role includes training the next generation of attorneys, CISOs and business leaders in meeting emerging technology and national security needs. He also provides corporate training. He is also a former in-house legal executive focusing on technology, cybersecurity and national security. Robert serves as a member of the ACC Foundation's Cybersecurity Advisory Board.

Visit his LinkedIn page.