Shape the future with confidence

Safeguarding advanced technology from insiders

Forensic & Integrity Services comprehensive insider risk solutions

September 2025

Organizations developing and distributing critical and emerging advanced technology face significant "insider" risk relating to the protection of this intellectual property.

Advanced technology disciplines at greatest risk include:

- Artificial intelligence and machine learning software
- Semiconductor and microelectronics technology
- Communications and networking technology
- Biotechnologies
- Position, navigation and timing services technology
- Robotics
- Weapons systems
- Advanced manufacturing
- Digital identity infrastructure and distributed ledger technologies
- Clean energy generation and storage
- Quantum information technologies
- Cryptocurrency and other financial products

The better the question.
The better the answer.
The better the world works.

Adversary nations, non-state actors, malicious cyber groups, transnational organized crime groups and even some companies are executing strategies to secure the cooperation — witting or unwitting — of employees and other "insiders" who have access to these types of critical technologies. These strategies take a number of forms, including:

- Sophisticated "recruitment" efforts managed by intelligence professionals and co-optees
- Social engineering and other schemes designed to dupe a subject into turning over valuable information
- Cyber penetrations aided by insiders

Insider cooperation can be voluntary, driven by a diverse range of motivations (from greed to disgruntlement), as well as ideology-based or forced scenarios involving blackmail, extortion and threat.

It is difficult to underestimate the importance of these critical technologies to various threat actors and they are deploying tremendous resources to obtain it by any means necessary. Also, these adversaries are regularly adapting, changing and enhancing their methods and practices, and incorporating the latest, cutting-edge technology into these approaches.

Realities of adversary competition in the current geopolitical environment strongly suggest these trends will continue and even escalate. Many of the technology disciplines in play have overt national security implications.

Taking ownership

- In this rapidly developing environment, organizations must take ownership of these insider risks and develop robust programs and countermeasures designed to protect advanced technology intellectual property (IP).
- While law enforcement and intelligence agencies can provide advice and support, security responsibility rests with the organization.
- Failure to effectively manage IP security can have serious downsides beyond loss of IP, including reputational damage, risk to contracts, litigation, regulatory penalties and involvement in criminal and national security investigations.
- Many organizations, including technology companies and academic institutions, struggle with this responsibility.
  - Companies are focused on thriving in their highly competitive markets.
  - Academic institutions want to establish environments characterized by the free movement of information and collaboration.
- Companies and academic institutions must balance the security and compliance needs associated with managing critical technologies with optimizing business efficiency. Creating a culture of security is an ongoing process. The challenge, therefore, is to design and execute these programs in ways that are consistent with the culture, objectives and resources of the client organization.

Enter Ernst & Young LLP

- The EY Crisis Management and Investigations practice has established an Insider Threat program designed to help companies, academic institutions and others manage insider threats related to these technologies.
- The program is administered by a multidisciplinary team of professionals that includes former federal law enforcement and intelligence officers, and others with experience in technology, organizational management, investigations, open-source research and cybersecurity.
- The team is focused on delivering solutions that produce strategically significant outcomes. Too often, "insider risk" programs focus on the process of investigating individual allegations or implementing check-the-box procedures. Our programs aim to implement integrated and proactive solutions to help mitigate the problem.
- Our solutions also focus on optimized collaboration with government agencies where necessary. Team members have spent careers in federal law enforcement and intelligence organizations. These EY personnel can leverage their understanding of federal and state programs, objectives and personnel to help a client develop a consistent and productive collaboration with relevant agencies within applicable legal frameworks.

Offerings

The EY Crisis Management and Investigations practice provides several specific offerings related to advanced technology insider threats, as follows:

- Security program assessment — a holistic assessment of an organization's security program with a focus on the high technology IP intended to protect against threats from insiders.
- Threat intelligence program and assessment — an analysis of an organization's threat environment and program from an advanced technology insider risk perspective.
- Cybersecurity program assessment — an assessment of an organization's cybersecurity program, also focused on advanced technology insider risk.
- Training program assessment — an analysis of an organization's insider threat training program focused on these risks.
- Employee investigation — onboarding, periodic evaluation and offboarding investigative measures and protocols.

EY teams assess organizations' existing security program elements against industry-leading practices, including the National Institute of Standards and Technology (NIST) guidelines, International Organization for Standardization (ISO) standards, ASIS International Risk Management Guidelines and various US government insider risk practices, including the National Insider Threat Task Force (NITTF) framework.

Contact information

Jeffrey Sallet
Partner, Boston, MA
Ernst & Young LLP
jeffrey.sallet@ey.com

Ryan Dobson
Principal, Boston, MA
Ernst & Young LLP
ryan.dobson@ey.com

Chris McCavitt
Managing Director, Boston, MA
Ernst & Young LLP
chris.mccavitt@ey.com

Brian Wolfe
Managing Director, Chicago, IL
Ernst & Young LLP
brian.wolfe1@ey.com

Christine St. Pierre
Senior Manager, Dallas, TX
Ernst & Young LLP
christine.st.pierre@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. More than 4,000 EY forensic and technology professionals help leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. EY teams consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned professionals for you and your legal advisors. They strive to bring you the benefits of leading EY technology, deep subject-matter knowledge and broad global sector experience.

CSG no. 2505-11149-CS
ED None

ey.com/forensics