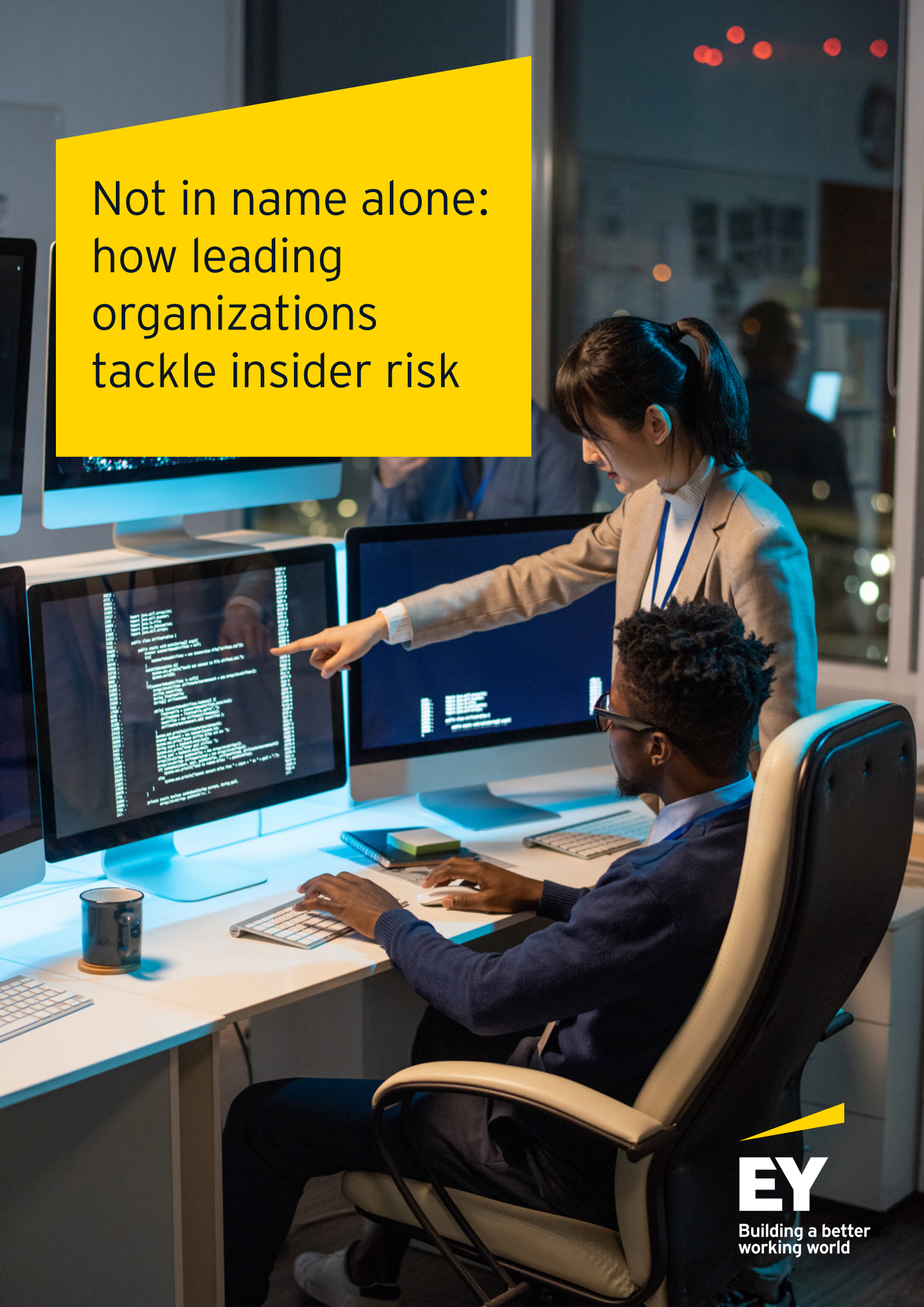
# Not in name alone: how leading organizations tackle insider risk



EY
Building a better working world

Insider risk comes in many guises. At one extreme are state-sponsored programs focused on obtaining, legally or otherwise, technology and intellectual property (IP) from foreign companies and governments. Harvard University chemistry professor Charles Lieber participated in just such a program, to his cost.

In December 2021, he was convicted in federal court of illegally concealing his links to the Thousand Talents Program, a Chinese government initiative to recruit people to obtain IP and foreign technology for China.[1] Prosecutors said Lieber hid from federal authorities the money China paid him to publish articles, organize international conferences and apply for patents on behalf of Wuhan University of Technology. Lieber is pursuing an appeal.[2]

At the other end of the spectrum — and occurring with much greater frequency than malicious exploits like the one described above — are employees who have been working remotely since the onset of the COVID-19 pandemic and may not realize that their laptops, tablets or smartphones may be storehouses of their employer's proprietary information, even after their term of employment has ended. Or they may feel entitled to retain data they helped to design or implement. They might not consider that information in their possession could be misused by a malicious actor in a way that negatively impacts the confidentiality, integrity and availability of critical company data assets.

[1] "In a Boston Court, a Superstar of Science Falls to Earth," *The New York Times*, Dec. 21, 2021.
[2] https://www.thecrimson.com/article/2022/2/9/Lieber-moves-for-retrial/.

Any current, temporary or former employee, contractor or business partner who has or had authorized access to an organization's IT system, data or premises is a potential insider risk. If the information they possess or control is improperly exploited, it could negatively impact the confidentiality, integrity and availability of the organization's critical data assets, with potentially catastrophic consequences for an organization's finances, reputation and relationships with regulators. And all too often, the specific risk is identified only after the damage has been done.

With insider risk incidents growing 44% since 2020,[3] the need is clear for businesses, especially those whose strategies rest on a foundation of IP and proprietary data, to actively protect themselves from damage that insider risks can inflict. To help companies defend themselves, EY teams have developed a comprehensive approach to insider risk. EY professionals provide clients with the industry insights, leading practices and technology solutions needed to implement enhanced security programs effectively, and uses digital tools from vendors such as Microsoft and adopts innovative technology solutions such as user and entity behavioral analytics (UEBA).

Those methodologies and digital tools support experienced IT professionals, HR managers and compliance officers in identifying data usage patterns and behavioral anomalies that warrant a closer look.

For example, EY insider risk professionals recently worked with investigators at a global financial services company on the case of an IT executive whose behavior had grown increasingly erratic and hostile toward his employer. Having inventoried the company's IP assets and identified who in the organization had access to it, the investigators then applied analytics technology to study the executive's system interactions. They concluded that the IT director was likely preparing to sell proprietary company data to a competitor. The investigators took steps to gradually reduce the employee's access to sensitive data and minimize the potential damage he could cause while the company moved to terminate his employment.

[3] 2022 Cost of Insider Threats Global Report, the Ponemon Institute, 2022.

# How closely does your organization track insider risk?

The first step toward managing insider risk is to cultivate awareness of potential insider risks across the full spectrum of an organization's activities. That awareness promotes a proactive stance toward such risks — a stance that most businesses already take toward external risks.

Several recent developments have intensified the urgency of broadening business' approach to insider risk. One is the growth of programs organized by some governments to obtain IP by fair means or foul; the Thousand Talents Program is an example of such an effort. Another important development is the influx of employees shifting from traditional, longer-term tenure expectations at a single employer to a workforce with less organizational loyalty. They may take a more casual view of IP integrity and information security. But the most significant development is the COVID-19 pandemic and the resulting massive shift to remote work, which has introduced a wide array of new vulnerabilities for risk managers to address. For example, remote work has sharply reduced the number of face-to-face interactions in the workplace, which often is where possibly significant changes in an employee's behavior or attitude first appear. In place of such interactions, risk professionals have stepped up their reliance on technology-assisted behavioral assessment, applying the techniques of external security programs to insider risk.

Just as with external threats, companies cannot mitigate internal risk simply by out-designing or out-developing malicious actors. Instead, a growing number of organizations are setting up dedicated insider risk teams to aggressively address insider risk before it strikes. Typically, such teams consist of stakeholders from across the organization — including representatives from Legal and Compliance, HR, IT, Finance and other departments — collaborating under the leadership of a single lead, who owns the program and is accountable for its performance. To an increasing extent, such dedicated organizations are responsible for acquiring the technology necessary to do their job.

Or not acquiring it, as the case may be: many organizations are discovering that some of the security tools they already have in place can be adapted to addressing insider risk. In most cases, however, organizations lack the complete array of necessary tools. Many need to supplement their existing technology with components designed expressly to detect insider risk, such as UEBA; enhancements to physical security (workplace violence, after all, remains a salient form of insider risk); and capabilities such as CCTV coverage of photocopiers and other office equipment. Veterans of insider risk engagements note that while many companies are effective in some aspects of insider risk management, few possess the full spectrum of necessary capabilities, skills and technology.

More important than any single technological component is a system that links different devices and forms of data, such as Microsoft Purview, a recently released legal and compliance platform that includes, among many other features, an insider risk module. Such systems do more than simply track an employee's interactions with the organization's IT assets; they yoke together diverse forms of data to assemble a panoramic view of insider risk. When, for example, an employee who typically downloads five files a week suddenly starts downloading 500 files a week, the system flags the anomaly. The systems can also monitor physical movement, for example, extracting from badge data that an employee recently entered a secure location that they ordinarily would have no reason to visit. In addition, advanced systems such as Purview can organize and direct the entire case management workflow, from opening a case file to the particulars of an investigation all the way through to the case's resolution.

An effective insider risk program, however, is more than the sum of its technological features. It is a comprehensive framework that leverages technology to address insider risk along multiple dimensions. The framework enables an organization to prioritize risk mitigation activities to protect an organization's most valuable and vulnerable data assets and apply human judgment to distinguish between genuine threats to IP assets and "false positives" generated by random variations in data flows.

Merely establishing an insider risk program is no guarantee of success. A common complaint among former law enforcement agents recruited to develop such programs is that that they often begin and end with the appointment of an executive to lead the effort. To be effective, experienced insider risk professionals say that insider risk programs require visible support from senior leadership and the funding, talent and technological infrastructure needed to succeed. The digital tools, data and expertise needed to counter formidable state-backed adversaries form the core of that infrastructure.

The professionals further recommend that insider risk managers take a full inventory of their organization's IP assets, and work to ensure that management can see every feature of the IP landscape. They should also shape their program along the contours of the company's culture, recognizing that the high-security, surveillance-intensive environments typical of defense contractors may be ill-suited to more informal, entrepreneurial organizations. And of course, while protecting their data assets, companies also need to remain within the bounds of data-privacy laws and regulations.

# Have you taken these steps to counter insider risk?

- Don't just appoint a director of insider risk. Give the director the organization, funding, performance metrics and visible support from the top.
- Continuously assess your insider risk technology stack to identify gaps in coverage and operational areas where visibility is limited.
- Educate the board about current risks and provide tangible industry examples.
- Don't just respond to specific incidents — study them to learn how to prevent them from happening again.
- Do an IP assessment — by taking inventory of a firm's IP, you can begin to pinpoint who is likely to threaten it and shift processes with IP developments.

Just those steps alone can set an organization on the path toward establishing an effective, proactive insider risk program. Is your organization fully prepared or is there doubton how to fortify your business is against these types or risks?

# For more information please contact


Lou Bladell
Managing Director,
EY Forensic & Integrity Services LLP
lou.bladel@ey.com

Brenton Steekamp
Forensic Leader, Netherlands and WEM (Western Europe and Magreb Region),
Forensic & Integrity Services LLP
brenton.steenkamp@ey.com

Joseph Pochron
Senior Manager,
EY Forensic & Integrity Services LLP
joseph.pochron@ey.com

## **EY** | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



EYG no. 005334-22Gbl
BSC no. 2205-4042368
ED None

**ey.com**