Monday, December 1, 2025

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next.

In a regulatory context, to predict means to use data, models, or past behavior, in order to estimate or forecast a future event, outcome, or condition before it occurs.

In psychology, to predict means to use observed data, psychological theory, or prior patterns, to estimate or forecast a person's future behavior, thoughts, or emotions.

In romantic relationships, prediction is the unreliable act of anticipating a partner's thoughts, emotions, or future actions, having incomplete information, and with a high likelihood of misinterpretation.

In the context of hybrid risk, to predict is the ability to anticipate, model, prepare, and forecast the behavior, decisions, vulnerabilities, and operational patterns of threat actors across multiple domains (cyber, physical, cognitive, legal, economic, informational, and societal).

Adversaries succeed because they can predict what we normally do. Repeated paths, fixed schedules, and routine interactions are opportunities for them to anticipate and exploit. Predictability is an attack surface. Threat actors weaponize routine.

In mathematics, the shortest distance between two points is a straight line. For adversaries who study their targets patiently, a straight line between intention and action is an invitation.

In a world where sophisticated threat actors model corporate behaviour with data mining, machine learning, and long-term surveillance, the straightest, most obvious route is not the safest. A longer, adaptive, and less predictable route often leads to far greater resilience.

Why did adversaries go to safari parks?
To study how lions wait at watering holes for thirsty executives.

In a watering hole attack, adversaries:

1. Identify websites or online services that a specific target group (employees of a company, members of an industry, government officials) regularly visit (their watering holes).

2. Compromise one or more of these trusted sites by injecting malicious code or hosting malware there.

3. Wait for the targets to visit the infected site, so the malicious code can exploit browser or plug-in vulnerabilities, install malware, or steal credentials.

Time and again, I have heard that a watering hole attack is difficult to execute. It is not. In fact, how difficult it is, depends on the following:

1. Choosing and compromising the site. It is easy if the attacker can find a poorly maintained blog, a small partner portal, or an outdated CMS with known vulnerabilities. It is harder if the target only visits well-secured, regularly patched, high-profile sites.

2. Delivering a working exploit. Zero-day exploits are expensive, but not for state-sponsored groups. Using known but unpatched exploits is easier, cheaper, and it works too.

3. Evading detection. Malicious code must stay hidden from the site owner. Is it easy? It depends on the site.

People always try to reduce uncertainty and feel safe. Predictability gives a sense of control and safety. When events feel predictable, people experience lower anxiety and greater perceived control.

Predictability also allows us to automate routine responses. Habits form because the brain identifies reliable cues and outcomes, reducing the need for conscious effort.

In developmental psychology, predictable behavior leads to a sense of security. Consistent and reliable responses foster secure attachment, and inconsistency contributes to anxiety.

Prolonged unpredictability correlates with chronic stress and can worsen mental health. But predictability can also lead to boredom, and vulnerability, where others can anticipate and manipulate one's behavior.

Predictability is comforting, except when you're the deer and someone's studying your path to the watering hole.

The old warning "curiosity killed the cat" is a good metaphor for how many watering hole attacks succeed.

Providing safe, verified mirrors for critical content means giving employees a controlled, internally managed source for the external material they need, instead of sending them to the open internet. By controlling the mirror, the organization can scan for malware and exploits, ensure that the content has not been tampered with, and prevent employees from relying on potentially compromised third party sites. This approach preserves access to needed information while removing the risk that attackers have injected malicious code into the original source.

Isolating browsing sessions from sensitive networks creates a deliberate separation between where curiosity happens and where critical systems reside. Employees can research, read, and experiment in an environment that has no direct path to production networks or to systems holding sensitive data.

Keeping user endpoints hardened ensures that even if curiosity leads to a compromised website, the attacker has difficulty exploiting the device. Hardening includes maintaining up-to-date operating systems and browsers, removing unnecessary plug-ins and legacy runtimes, applying strong endpoint detection and response tools, and operating with least-privilege accounts so a single browser exploit cannot escalate to full system control.

Curiosity may have killed the cat, but the cat has eight more lives. We don't. We just end up on the front page, with audit findings and sleepless nights.

Best regards,

George Lekatis
President of the IARCP

Introducing an Advanced Specialization in Hybrid Risk and Resilience management, exclusively for CRCMPs.

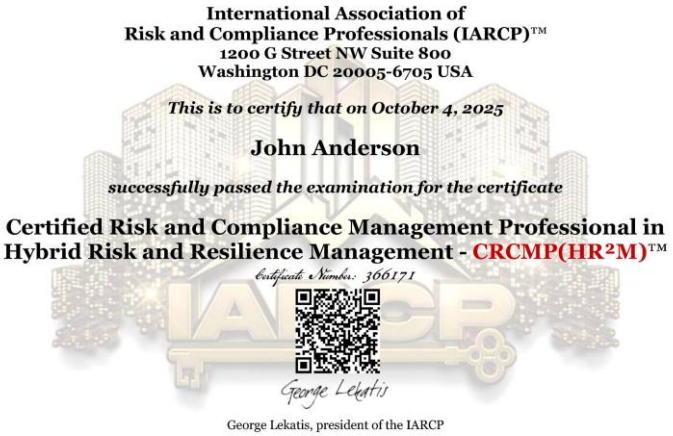
We are thrilled to announce the launch of the Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program.

It builds on the solid foundation of the CRCMP designation and equips participants with cutting-edge knowledge to understand, identify, assess, and effectively manage complex hybrid risks.

The program prepares CRCMPs to strengthen organizational resilience across interconnected domains, including geopolitical and regulatory risk, counterintelligence, and supply chain resilience, while advancing capabilities in hybrid threat psychology, hybrid stress testing, and crisis management, ensuring readiness for an increasingly complex risk landscape.

Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the CRCMP exam. To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

Learn more and view the full course synopsis:
https://www.risk-compliance-association.com/CRCMP_HR2M.htm


International Association of
Risk and Compliance Professionals (IARCP)™
1200 G Street NW Suite 800
Washington DC 20005-6705 USA

This is to certify that on October 4, 2025

John Anderson

successfully passed the examination for the certificate

Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M)™

Certificate Number: 366171

George Lekatis

George Lekatis, president of the IARCP

Number 1 (Page 8)

AI and central banking

Michael S Barr, Member of the Board of Governors of the Federal Reserve System, at the Singapore Fintech Festival, Singapore.

Number 2 (Page 13)

Building Tomorrow's Audit: Four Strategies for a Tech-Forward Future

Christina Ho, Board Member, 69th World Continuous Auditing & Reporting Symposium Rutgers Business School, Newark, New Jersey

Number 3 (Page 19)

FSI Insights on policy implementation No 70

Smart supervision: sound capacity development approaches for techsavvy supervisors

Financial Stability Institute | BIS

Number 4 (Page 22)

Resilient banks through effective supervision: a pillar of Europe's competitiveness

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at the ECB Forum on Banking Supervision 2025, Frankfurt

Number 5 (Page 25)

Global Economic and Trade Resilience and China's Contribution
Keynote Speech by PBOC Deputy Governor and SAFE Administrator Zhu Hexin at the Annual Conference of Financial Street Forum 2025, Beijing, China

Number 6 (Page 29)

United States Government Accountability Office
INFORMATION ENVIRONMENT
DOD Faces Risks with Publicly Accessible Information
Testimony Before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate, Statement of Joseph W. Kirschbaum, PhD
Director, Defense Capabilities and Management

GAO

Number 7 (Page 32)

ENISA Threat Landscape 2025

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

Number 8 (Page 36)

Disrupting the first reported AI-orchestrated cyber espionage campaign

ANTHROP\C

Number 9 (Page 37)

Google vs. "Lighthouse."

Google

Number 10 (Page 41)

Defending the cloud: Azure neutralized a record-breaking 15 Tbps DDoS attack

Microsoft

Number 1

AI and central banking

Michael S Barr, Member of the Board of Governors of the Federal Reserve System, at the Singapore Fintech Festival, Singapore.

Thank you for the opportunity to speak to you today. It is an honor and a pleasure to be here with you in Singapore, a crossroads for global trade and finance, to discuss the transformational nature of artificial intelligence (AI).

Like other central banks around the world, including the Monetary Authority of Singapore, we at the Federal Reserve have been exploring the use of AI in our operations for quite some time as well as considering the implications of AI's adoption for the financial sector and the broader economy.

At the Fed, we've been interested in the effects of AI on the economy and its role in the financial system for decades. Remarkably, in 1997, Governor Susan Phillips delivered a speech noting the use of AI in consumer loan underwriting. In the past year, no fewer than seven speeches by Fed Governors have had "AI" in the title.

Today I'll discuss the opportunities presented by AI relevant for central bankers as well as the risks it may pose that policymakers should consider. I will leave you with three main takeaways.

The State of AI Innovation and Deployment

My first main point is that while AI is a big deal that will transform economies, there are a range of outcomes for how it could do so.

AI—algorithms that mimic human thought, communication, and choices—has been with us for decades, but AI entered a new era with the launch of ChatGPT in late 2022.

Generative AI (GenAI) captured our imagination with convincing conversations in which it is possible to go deep on a wide range of topics. Earlier forms of AI were often the bailiwick of digitally native companies, but GenAI is spreading rapidly through the economy. As of 2024, three in four large companies were using GenAI, though some report it has yet to improve their bottom line.

Smaller companies have been slower to adopt GenAI, with adoption rates reported in the high single digits, albeit with a high degree of heterogeneity among sectors. Also, one could surmise, based on other surveys of individuals, that work-related use is more widespread among employees than their CEOs realize.

A recent survey by the Federal Reserve Bank of New York showed that firms plan to retrain their workforces to take advantage of AI to enhance productivity, with widespread layoffs limited.

But survey respondents also report that AI has led firms to scale back hiring, a development that may be contributing to the recent low levels of job creation in the U.S. economy, a concern for many workers and particularly for newer entrants to the job market.

Taking a step back, as I have noted in the past, I see two basic scenarios for how AI can transform the economy.

In the first scenario, there is incremental adoption of GenAI that augments existing tasks and jobs. In the second scenario, a revolution occurs. GenAI transforms the nature of work and leisure, boosting the efficiency of research and development, remaking industries, and creating firms with new—perhaps radically new—business models.

Right now, it is difficult to predict which scenario (or perhaps one or more intermediate scenarios) will come to pass.

We can already see incremental change as GenAI is increasingly integrated with standard workplace software. With its natural language interface, GenAI is inherently user friendly, so few workers need special skills or unusually onerous training to use it. At the same time, some start-ups have a more revolutionary flavor because they are centered on AI from the outset.

One indicator of how the labor market is evolving toward deeper integration with AI is the skills mentioned in job postings. While overall the share of job listings that mention AI-related skills is small—about 5 percent—in the information sector, it is about 20 percent. The financial sector, where firms are always looking for a technological edge, is not far behind, with 1 in 10 job postings mentioning AI.

So we can see that the skills needed in some key sectors are already changing. The speed of that change is likely to increase. If the AI changes happen gradually, workers and firms will have time to adjust, but if they happen rapidly, there may be significant dislocations in the short term.

A massive wave of data center investment has begun, pointing to signs of confidence among leading AI companies that the use of AI at scale throughout the economy is just around the corner.

If they're right and AI is useful enough to keep what is currently projected to be $3 trillion of new data center capacity utilized effectively, we can expect significant changes in economies.

Investment in capital generally raises labor productivity and offers the potential for higher output growth without pressure on inflation over the longer term. As I have discussed in previous remarks, if these changes are significant, they can also affect the conduct of monetary policy.

Of course, it may be the case instead that investment exceeds short-term demand, in which case there may be losses and adjustments to the AI sector.

AI and the Financial Sector

The second key point I would like to make is that the financial sector is adopting AI quickly, and while there are many benefits to this adoption, the risks will need to be managed carefully.

So far, AI adoption in the financial sector appears to be most concentrated in areas that can enhance operational efficiency, including applications that involve text analysis, classification, and information search inside the firm, as well as customer-facing functions. These incremental improvements to common business functions are a key reason to be hopeful about AI raising labor productivity in that sector.

At the same time, there is significant investment in experimentation with AI for core functions for financial services. Data-driven financial-sector-specific tasks, including credit decision support, fraud detection, and trading are using AI-specific tools. Ensuring that AI is used appropriately for these functions faces appreciable challenges.

First, the amount of organizational change needed by financial services firms to utilize GenAI may be substantial. History suggests progress may be slow. Adoption of machine learning, an AI technology that preceded GenAI, was concentrated in firms that were highly digitized from their founding—and even in those cases, adoption was a long process.

Fintech firms organized to exploit AI from their founding can play a key role in driving efficiency forward in the sector, providing services to the incumbent firms.

But productivity may even decrease in the short term, as heavy investments in business-process improvements take time to play out to productivity gains.

A second challenge is the practical constraints of rushing into AI for core business activities in the financial sector, as firms need to ensure that the resulting processes and outcomes are consistent with relevant laws and appropriate risk management. Large institutions are exploring the use of GenAI, including agentic AI, in their financial models—but doing so requires care.

To successfully leverage the potential of GenAI on a sustainable basis, decisions based on those models must be well controlled, numerically and legally precise, explainable, and replicable. AI developers still struggle to some extent with all of those criteria.

We need to reduce the risk that AI reinforces biases in consumer lending. And we also need to guard against the risks that could result from the use of AI in financial markets. For example, profit maximization by AI-powered trading algorithms may result in tacit collusion, market manipulation, or trading strategies that result in significant market volatility or even systemic risk.

We will need innovation that is responsive to these risks to see additional advances in the use of AI for a broad array of core financial services functions.

AI and Central Banking

A third and final point I would like to leave you with is that central banks, including the Fed, need to keep up with AI by increasing our speed of adoption for our own operations.

The nature of central banking work is inherently careful, considered, and measured when evaluating anything new. This is particularly true for any new technologies.

But it seems clear already that the many advantages offered by AI could assist central banks in at least some of their operations, and the speed at which this technology is moving makes it appropriate to proactively engage in using AI for our own operations. That is why the Federal Reserve is using AI, where appropriate, to increase staff efficiency and effectiveness. My view is that GenAI is a transformative technology that central banks need to remain engaged with to ensure an ability to execute as technology evolves.

As we push ahead on efficiency gains, it is important that we leverage the right tools for the task at hand, recognizing that GenAI is not always the best choice. Some of the challenges that we face can be addressed by robotic process automation or traditional AI methods. These are the same kinds of questions that every business and organization considering AI should be weighing.

At the Federal Reserve, we have focused on ensuring we can leverage AI capabilities by establishing an AI program and governance framework for the use of AI technologies.

We are taking an enterprise-wide approach of learning-by-doing and broadly adopting high-value uses of GenAI, such as writing, coding, and research activities. We have taken a "hands on keys" approach to having staff engage with it. We are identifying the business processes that can be improved and transformed with the technology.

One internal application of GenAI I am particularly excited about that helps us achieve all these goals is technology modernization. We are applying GenAI-enabled tools within clear guardrails to translate legacy code, generate unit tests, and accelerate cloud migration. So far, the result of this usage is faster delivery, improved quality, and enhanced developer experience. And it will likely mean better outcomes in support of the American people.

Given AI's current and prospective role in economic activity, we are devoting the necessary resources to understanding it, including by analyzing not only AI's economic and financial implications, but also exploring how AI can enhance our financial stability work, strengthen supervisory and regulatory capabilities, and ensure the smooth functioning of our payment systems.

These are just some of the ways that the Fed, like other organizations, is using AI to make us more productive and capable. These efforts may also help us understand the effect of AI on the economy, the banking system, and the payment system. That task will be a major job for central banks in the years ahead. AI has the potential to fundamentally change the economy and society. And as central bankers, we need to keep up.

Thank you.

To learn more:
https://www.federalreserve.gov/newsevents/speech/barr20251111a.htm

Number 2

Building Tomorrow's Audit: Four Strategies for a Tech-Forward Future

Christina Ho, Board Member, 69th World Continuous Auditing & Reporting Symposium
Rutgers Business School, Newark, New Jersey

Thank you for that kind introduction. I'm delighted to be here at the 69th World Continuous Auditing & Reporting Symposium.

This conference brings together some of the brightest minds in the accounting and auditing profession—academics, practitioners, and technologists—all focused on a question that keeps me up at night: How do we build tomorrow's audit?

First, the views I express today are my own and do not necessarily reflect the views of the Public Company Accounting Oversight Board, other PCAOB Board Members, or PCAOB staff.

Let me start with a fundamental question: What if the audit of tomorrow isn't just better— what if it's fundamentally different? That's not just a hypothetical. That transformation is happening right now, and the decisions we make today will determine whether our profession leads or is left behind.

The TIA Journey

It was one of the greatest privileges of my time at the PCAOB to chair the Technology Innovation Alliance Working Group, or TIA. Here's a remarkable coincidence: on November 30, 2022, the PCAOB officially launched TIA—the very same day that OpenAI released ChatGPT to the public.

While we didn't plan that timing, it turned out to be prophetic. That single day – November 30, 2022 - marked the beginning of the AI revolution that would reshape how we think about technology in auditing.

From November 2022 through May 2024, our ten-member TIA working group—comprising external professionals specializing in emerging technologies and auditing—collaborated extensively with stakeholders across the audit ecosystem. We engaged with audit firms large and small, preparers, investors, academics, and technologists. Our objective was clear: develop a strategic vision for how the PCAOB and the profession can harness technology to improve audit quality and protect investors.

The TIA delivered its recommendations in May 2024, and they were publicly released by the PCAOB only recently in September 2025. But here's the reality: AI has exploded since the TIA finalized its recommendations. We've seen the rapid

advancement of agentic AI systems, more sophisticated large language models, and AI capabilities that seemed like science fiction just 18 months ago. If anything, the urgency underlying the TIA's recommendations has only intensified. Today, I'll share the four strategic priorities that emerged from this work—priorities that I believe will lead us toward a tech-forward future.

The Foundation: Data and Trust

But before I dive into those four strategies, let me be clear about something fundamental: we are in the trust business. Accounting and auditing are the foundation of trust in our capital markets. And in a world where truth is increasingly difficult to discern—where misinformation spreads faster than facts—our role becomes even more critical.

This is why I see a tremendous opportunity for AI assurance. If our profession adapts quickly, we will lead. We can define the standards, shape the frameworks, and help ensure that AI systems used in financial reporting and auditing as well as other domain areas are trustworthy, transparent, and accountable. But if we resist this transformation—if we cling to the status quo—we risk losing this precious opportunity.

Let's embrace innovation. Let's evolve. Let's lead. Because the future of trust depends on it.

Strategy #1: Promoting Structured Data Creation and Dissemination in Public Company Audits

The first strategic priority is to promote the creation and dissemination of structured data. This was TIA's first recommendation because without quality, structured data, none of the other innovations can succeed. Data is the fuel that powers AI, and the quality of that fuel determines the quality of the output.

Let me give you a concrete example of why this matters. Imagine an audit firm that has standardized its audit documentation structure across all engagements. An AI agent could continuously monitor workpapers across hundreds of audits, identifying patterns, flagging inconsistencies, and learning from high-quality work. The use of AI could predict risks of material misstatements.

Now imagine that same firm operating today, where every audit uses different structures, different naming conventions, different taxonomies. The AI has no foundation to build on. That's the difference between innovation that scales and innovation that stalls.

AI transformation is well underway—one that will reshape the accounting and auditing profession as we know it. In particular, agentic AI will be changing how we work. Professor Miklos Vasarhelyi recently provided me the opportunity to hear about some of his students' and researchers' work. One involved the use of agentic AI in auditing and it gave me a better appreciation of its potential and mechanics. Agentic AI is an AI system that can set goals, reason through multiple steps, and make decisions autonomously.

Unlike conventional AI that follows predetermined functions, agentic AI operates with proactive independence—it can plan and execute complex workflows with minimal human oversight. This makes it particularly well-suited for audit workflows.

Now, audits may or may not become cheaper, but I believe they will become more comprehensive, more insightful, and more accessible—especially for smaller firms and investors who stand to benefit most from these advancements.

To create this foundation, we can start with a standardized taxonomy for audit documentation. The concept of the audit documentation taxonomy is not new. In fact, Eric Cohen who is a TIA member and is speaking later today, presented the idea at the WCARS 20 years ago in 2005.

With the advancement of AI, we can now appreciate the significant value of his idea. Several advantages arise from standardization: First, superior data improves AI learning capabilities. Second, standardization supports smaller firms by enabling third-party software providers to develop efficient, off-the-shelf solutions. Third, a uniform structure simplifies auditor transitions and potentially lowers initial audit costs.

Looking ahead, AI could even contribute significantly to creating this comprehensive taxonomy. These systems could initially be piloted within an innovation lab, where anonymized audit workpapers from various firms are analyzed to develop standardized structures. Once established, AI agents would benefit from enhanced autonomy, learning from higher-quality data and increasing trust in their outputs.

Now, let me touch on a second component of this first strategy: digital signatures. Currently, audit reports and signatures included in SEC filings are submitted by issuers—not by auditors themselves. This creates a trust and accountability gap. Issuers can make substantive mistakes when copying and pasting audit information, such as adding the wrong auditor name or uploading the wrong audit report. This lowers the quality and trustworthiness of the audit information itself—a particular problem when we're trying to adopt technology that depends on reliable data.

Digital signatures can solve this problem. They provide digital logs that archive when and where a document was signed and by whom. When auditors digitally sign their audit reports, it enhances accountability, traceability, and trust. It also reduces the surface area for cyberattacks, because bad actors can no longer simply alter audit information in filings.

Additionally, digital signatures can streamline the audit reporting process, reducing redundant steps between filing an audit report in a Form 10-K and reporting that same information to the PCAOB in a Form AP. This efficiency allows audit firms to shift time and resources from administrative compliance to higher-value audit procedures—which ultimately improve audit quality.

Strategy #2: Using AI in Audit

The second strategic priority is the responsible integration of AI into audit practices. Improving audit quality and protecting investors requires fostering innovation and responsible technology adoption. For too long, the auditing profession has relied on linear, manual, sampling-based methods that have remained largely unchanged for decades.

But let me ask you this: Does continuing to rely solely on decades-old methods best serve investors in 2025? I believe the answer is clear. With the advancement of agentic AI, we now have the tools to move toward continuous auditing and full-population coverage. This shift will dramatically enhance audit quality.

Here's a hypothetical to illustrate the urgency. An audit firm uses an AI tool to test 100% of journal entries, as opposed to taking the traditional manual sampling approach. One scenario is that regulators recognize 100% testing as an improvement because it provides more audit coverage.

The second scenario is that the lack of clear standards results in regulators seeking unreasonable levels of detail about the AI model. By requiring the firm to "turn over every rock," the firm decides to return to manual sampling because manual sampling is less risky from a compliance standpoint.

So I ask you: Does going from 100% testing to a sampling approach advance investor protection? I believe the answer is a clear "no." And under this scenario, is the regulator an anchor weighing down innovation or an engine catalyzing it? Again, the answer is clear.

The PCAOB can best advance its investor protection mission by laying the groundwork that catalyzes innovation. We must explicitly support firms in adopting new technologies that improve audit quality—not just by permitting innovation, but by actively encouraging it. Regulations should not merely be check-the-box compliance rules; rather, they should enable progress toward elevating audit quality.

To date, the PCAOB has not issued useful guidance regarding AI. The rapid development of AI highlights an urgent need for regulatory action. TIA recommended forming an AI Task Force to examine use cases using an agile methodology, with the aim of developing a principles-based AI framework. We do not have to start from ground zero—we can build upon established models like ISO 42001 and NIST's AI risk management framework.

In sum, if we truly want to promote audit quality and protect investors, we must embrace technological innovation in auditing. It's a strategic imperative and, more importantly, it's what investors deserve and what the capital markets need.

Strategy #3: Regulatory Innovation Capacity Building

The third strategic priority is to build regulatory innovation capacity to drive ongoing improvements in audit quality. This is an opportunity for the PCAOB to

deepen its understanding of AI's use by audit firms through structured experimentation and information sharing.

Specifically, the PCAOB could establish an Innovation Lab to conduct structured experimentation by engaging with audit firms, preparers, technologists, and other stakeholders. A sandbox within the Innovation Lab would provide valuable collaboration and generate insights into developing agile, technology-driven standards through AI experimentation and data-driven insights.

I envision a future where the regulator is at the forefront of developing technology standards that are nimble and remain relevant as technology continues to evolve. The UK's Financial Reporting Council launched their Innovation and Improvement Hub in September 2025 to create an exploratory space for collaborative problem solving.4 This is the time to catch up!

I spoke extensively about the Innovation Lab concept at the MindBridge Vision 2025 conference5, so I'll only touch lightly on it here. But let me emphasize this: doing nothing is not a viable option. Talk is cheap and time is expensive, and we have already lost too much time.

Strategy #4: Encourage Technology Literacy in Auditor Skillsets

Finally, promoting technology literacy among auditors is critical. The rapid advancement of technology demands increased engagement and learning opportunities for all auditors—seasoned professionals and those new to the profession alike.

For those entering the profession, I continue to encourage institutions of higher education to incorporate advanced data analytics, computer science, and AI into their accounting curricula. Auditor proficiency needs to extend beyond traditional accounting and auditing to include technology and data literacy to elevate auditors' effectiveness.

Here's a question we must ask ourselves: Are we preparing the next generation of auditors for the profession as it is, or for the profession as it needs to become?

As we look to the future, it's clear that technical expertise alone will not be enough. The next generation must cultivate two essential qualities: courage and problem-solving ability.

Let's start with courage. Accounting is fundamentally built on truth. We are defenders of truth, and truth is the foundation of trust. As I mentioned in the beginning, in today's increasingly complex and information-saturated world, truth is harder to discern. The proliferation of misinformation challenges our ability to stand firm. Sometimes, telling the truth comes at a cost. I believe courage is not optional, it's essential.

This profession should be seen as bold, innovative, and focused on the greater good. Instead of saying auditors merely follow procedures, we should highlight how they build trust in capital markets. To uphold trust, we must be brave enough

to speak the truth even when it's difficult—even when it makes us the "contrarian."

Now, let's talk about problem-solving. The challenges ahead will be more complex and multi-faceted than ever before. Our future accountants and auditors must be equipped not just to follow procedures, but to think critically, learn continuously, and work innovatively. We must show them how their work drives problem-solving, and improves lives and our world.

The profession must transition from a perception of strict, compliance-focused auditing to one that appeals to younger generations by providing flexibility and opportunities for problem-solving. AICPA's 2025 Trend report shows a 6.6% decrease in accounting graduates for 2023-2024.6 While this is lower than previous declines, it still raises concerns about the profession's future. We need to reshape the profession to attract future talent.

Together, courage and problem-solving form the pillar of a profession that does not merely respond to change—it leads it.

To learn more:
https://pcaobus.org/news-events/speeches/speech-detail/building-tomorrow-s-audit--four-strategies-for-a-tech-forward-future

Number 3

FSI Insights on policy implementation No 70
Smart supervision: sound capacity development approaches for techsavvy supervisors

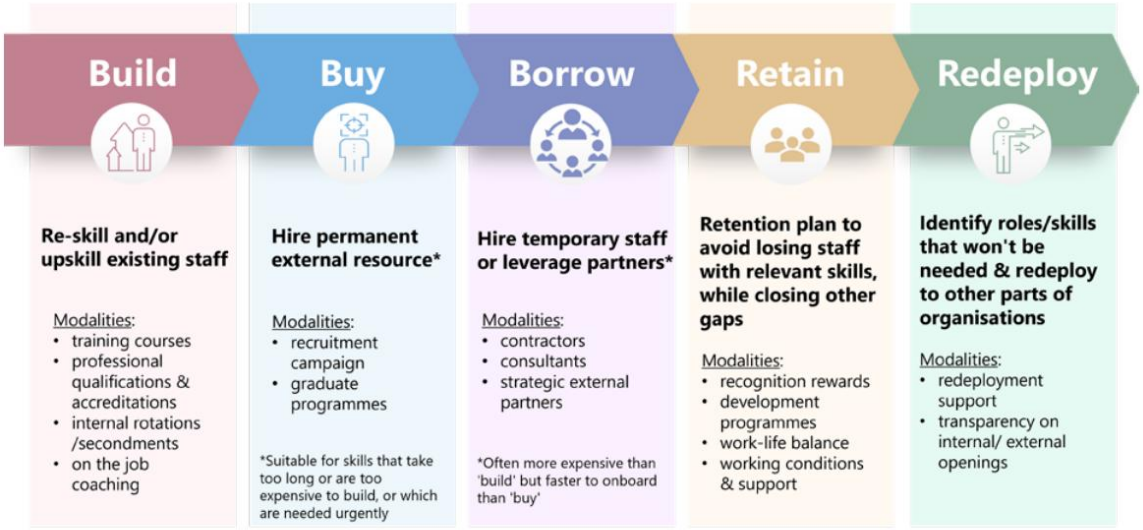
Financial Stability Institute | BIS

Executive summary

The rapid and continual advancement of technology is transforming the financial industry, requiring financial sector supervisors to keep pace. From a supervisory perspective, technological advancements present both risks and opportunities.

On the risk front, technologies such as artificial intelligence (AI) can introduce new risks or amplify existing ones as firms leverage these tools to develop innovative financial products, enhance services and improve internal operations. Breakthroughs in quantum computing, while still on the horizon, could significantly impair cyber resilience of firms in the future, with potential systemic implications.

Options to close technology skills gaps — Graph 2



All these developments require supervisors to stay on top of the underlying technology to be able to understand and address potential risk implications for supervised financial institutions and the financial system as a whole.

At the same time, supervisory technology (suptech) presents opportunities for supervisors to improve the efficiency and effectiveness of their processes.

Technology can automate processes, cutting down the processing time and resources needed to supervise firms effectively while augmenting supervisory capabilities to achieve better supervisory outcomes.

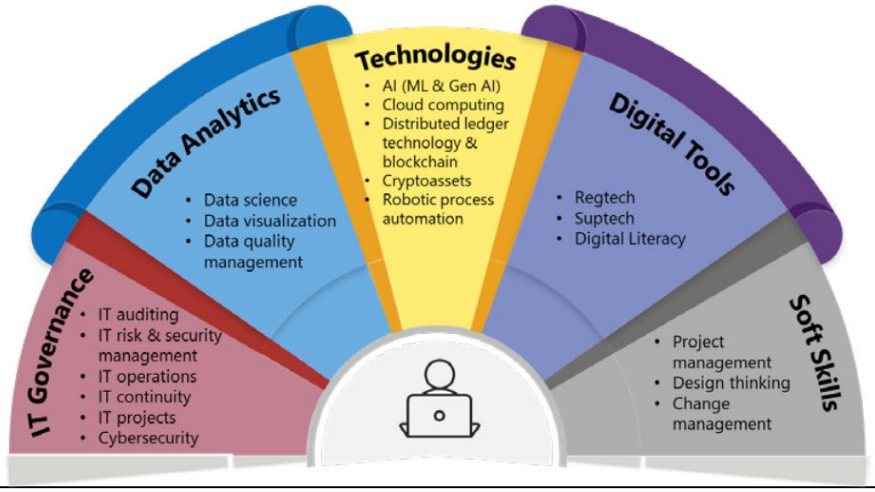
For example, AI has the potential to disrupt regulatory/supervisory functions, redeploying resources to high-value activities such as real-time supervision.

To achieve these benefits, supervisory staff need to have not only the necessary knowledge but also confidence on the responsible use of AI in supervision.

Both the risk and opportunity dimensions of technology require authorities to cultivate tech-savvy supervisors who can understand the technology and use suptech effectively.

Stylised example of topics in technology-related capacity development programmes

Graph 3

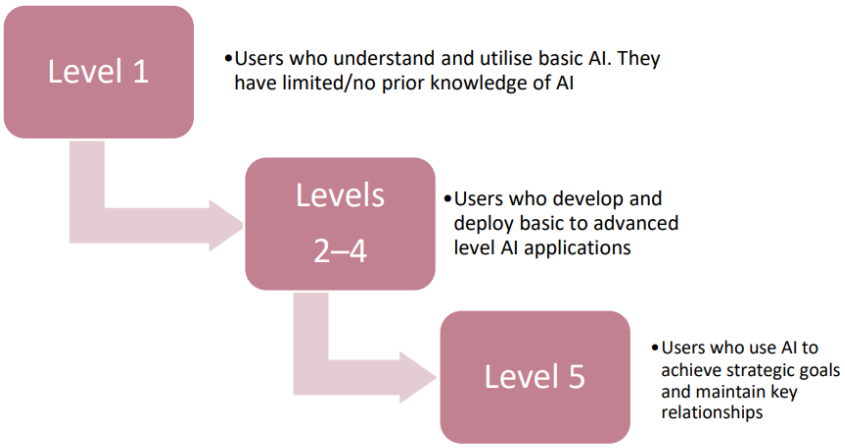


An effective capacity development (CD) framework on technology should be steered by a clear strategy that is well aligned with an authority's strategic objectives and priorities.

The framework should be operationalised through a structured process and be adaptable to technological developments. Given the rapid pace of technological advancements, authorities need to institutionalise a flexible framework that can be adapted and adjusted to remain relevant.
This requires flexible CD processes, which should be iterative, identifying training needs, delivering training and assessing outcomes to improve the identification and delivery of CD activities.

External factors such as technological advancements, policy changes and evolving business models should be continuously taken into account, shaping the CD framework as needed.

Example of an artificial intelligence (AI) proficiency ladder — Graph A1



To support technology adoption and enhance organisational efficiency and effectiveness, authorities can foster an innovation-friendly culture as part of their technology-related (techrelated) CD strategies.

Authorities with an innovation-friendly culture will find staff who are technologically adaptable and open to embracing new technology responsibly to augment their capabilities and improve their efficiency. An innovation-friendly culture requires promoting crossfunctional collaboration and embedding innovation in organisational values.

Having an institutional digital or technology policy can help to reinforce top-down steer on an authorities' level of ambition and, thus, clarify the necessary tech-related skills needed to achieve the ambition.

To learn more: https://www.bis.org/fsi/publ/insights70.pdf

Number 4

Resilient banks through effective supervision: a pillar of Europe's competitiveness

Frank Elderson, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at the ECB Forum on Banking Supervision 2025, Frankfurt

It is a pleasure to deliver the last keynote speech of this year's banking supervision forum. Over the past two days, we have discussed what resilience means in times of challenge, complexity and disruption – and why resilience should be broad based.

As the Chair mentioned yesterday morning, broad-based resilience is about strong financials, but equally about operational resilience, sound governance and good risk management.

During this period of profound change, a debate on European competitiveness has emerged with full force. Many are asking what the key impediments and main enablers might be for a more competitive European economy. How can we tackle the former and improve the latter? And what role does the banking sector play in shaping the competitiveness of the real economy?

The good news is that over the past decade, much has already been achieved to make banks more resilient, and this resilience remains the indispensable foundation to support the real economy throughout the economic cycle. I will therefore start by illustrating this very welcome healthy state of the banks under our supervision.

At the same time, discussions about the complexities that are having an impact on European banks' competitiveness have gained prominence.

Today I would like to highlight how we are tackling undue complexities in the regulatory and supervisory framework in order to help banks operate efficiently within a predictable, proportionate and risk-based framework.

I will then illustrate how banks' competitiveness crucially hinges on structural and macroeconomic factors that will require a concerted effort from a wide range of stakeholders.

In this way, Europe's banking system can be both innovative and strong, competitive and resilient. So, let me first start by looking at the resilience I mentioned at the start.

Bank resilience is crucial to withstand shocks and support the economy at all times

Resilient banks are a vital precondition for a thriving real economy. Why is this so?

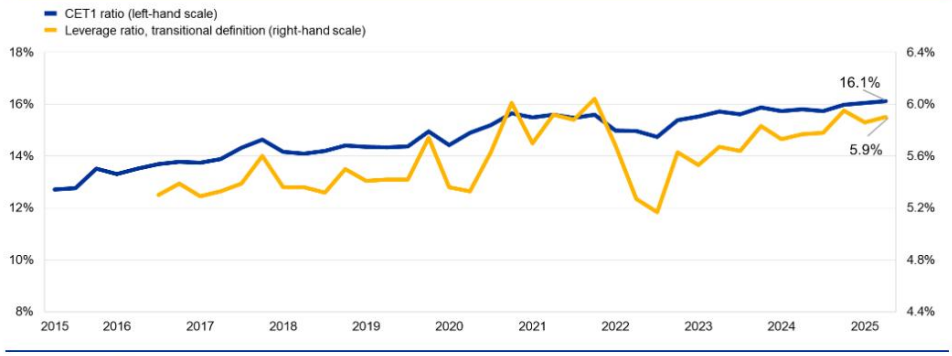
Well-capitalised and resilient banks are better placed to channel funds from savers to borrowers to enable businesses to innovate, households to buy homes and governments to finance public goods. Banks must therefore be well regulated and supervised.

European banking supervision was established in 2014 in response to the global financial crisis and subsequent European sovereign debt crisis. Now, almost to the day 11 years later, banks under our supervision are significantly stronger. Thanks to regulatory guardrails, rigorous supervision and continued improvements in banks' risk management, the banking sector is now in a much better position to fulfil its essential function of supporting the economy at all times.

Today's euro area banks have solid capitalisation levels, with a Common Equity Tier 1 (CET1) capital ratio of 16% compared with 12.7% a decade ago.

Chart 1

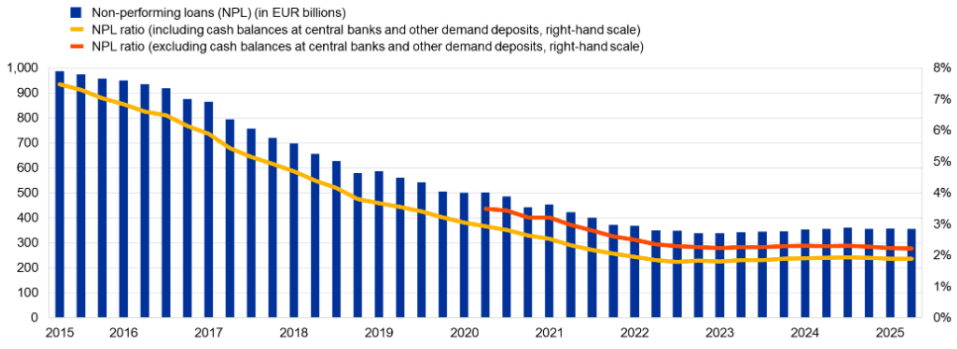
Capital adequacy



Source: ECB supervisory banking statistics.

Chart 2

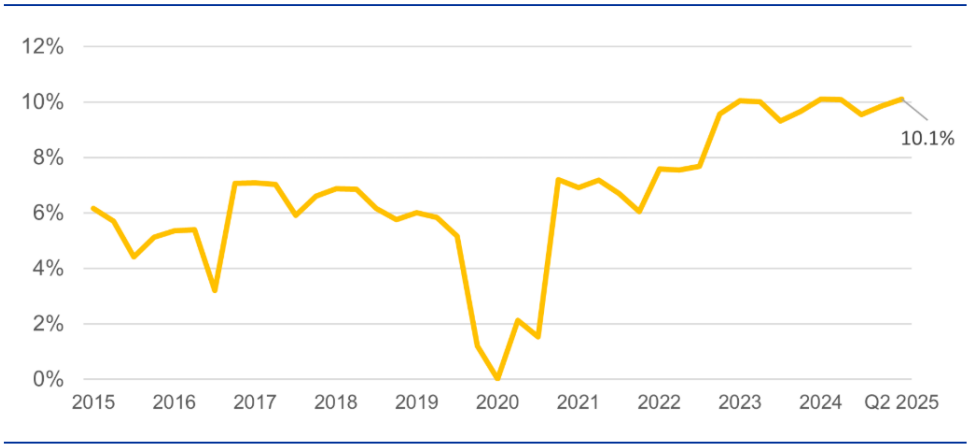
Asset quality



Source: ECB supervisory banking statistics.

Chart 3

Euro area banks' return on equity



Source: ECB supervisory banking statistics.

To learn more:
https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp251114~5895764cc6.en.html

Number 5

Global Economic and Trade Resilience and China's Contribution

Keynote Speech by PBOC Deputy Governor and SAFE Administrator Zhu Hexin at the Annual Conference of Financial Street Forum 2025, Beijing, China

Distinguished Vice Premier He Lifeng, Party Secretary Yin Li, Mayor Yin Yong, and dear guests,

Good afternoon! It's a great pleasure to join you at the Financial Street Forum. Just now, Vice Premier He Lifeng delivered an important speech, making arrangements for the financial system to implement the guidelines of the fourth plenary session of the 20th Communist Party of China (CPC) Central Committee. We will ensure its effective implementation. The fourth plenary session of the 20th CPC Central Committee has defined the guiding principles and main objectives for China's economic and social development during the 15th Five-Year Plan period. It has drawn a grand blueprint for the next five years, calling for greater high-standard opening-up to foster a new stage of win-win cooperation. The session emphasized that opening-up should serve as a driving force for reform and development, enabling China to share opportunities and pursue common progress with the rest of the world. To implement the guidelines of the session, I would like to share some thoughts on global economic and trade resilience and China's contribution from the perspective of advancing high-standard opening-up.

In recent years, despite multiple challenges such as the pandemic, geopolitical frictions, and the resurgence of unilateralism and protectionism, global economic and trade activities have demonstrated remarkable resilience. According to World Bank data, total global trade grew at an average annual rate of 5.4 percent between 2019 and 2024, 4.6 percentage points higher than that in the previous five years. Since the beginning of this year, global trade has continued to expand at a relatively fast pace despite a complex and volatile environment. According to the latest forecast by the United Nations, global trade will exceed USD33 trillion this year, reaching a new record high. Behind this resilience lie two key driving forces—technological innovation and open cooperation.

On the one hand, the new round of sci-tech revolution and industrial transformation has been further advanced, injecting fresh momentum into global economy and trade. Artificial intelligence is developing explosively, semiconductor trade is expanding rapidly, and the annual trade volume of integrated circuits has surpassed the USD1 trillion mark. Global green trade is rising swiftly. The annual trade volume of new energy products has grown from tens of billions of US dollars a decade ago to hundreds of billions in the past three

years, marking an order-of-magnitude increase. The digital economy is flourishing, giving rise to new forms of trade such as cross-border e-commerce and fueling the rapid expansion of trade in services. In 2024, global exports of digital services doubled from a decade ago.

On the other hand, opening-up and win-win cooperation serve as the endogenous driving forces behind the steady growth of global economic and trade activities. Practice has repeatedly proven that division of labor, cooperation and mutual benefit among nations are not only the sources of development, but also the foundation for risk resilience and an inherent feature of market economies. Although globalization has faced headwinds in recent years, multi-level economic and trade cooperation among countries and regions has become even closer. The entry into force of the Regional Comprehensive Economic Partnership (RCEP), the full completion of negotiations on the Version 3.0 China-ASEAN Free Trade Area (CAFTA), and the official launch of the African Continental Free Trade Area (AfCFTA) are among the new milestones that continue to emerge, helping to uphold a diverse and stable international economic landscape and trading system.

As the world's second-largest economy and the largest trader in goods, China has shared its development opportunities with the rest of the world and made important contributions to enhancing the resilience of global trade and upholding global economic and trade rules.

First, China has played an important role in maintaining the stability of global industrial and supply chains. With the most comprehensive range of industrial sectors and the most complete supporting system in the world, China has offered strong support to the smooth functioning of the global economic cycle by providing high-quality manufactured goods and reliable supplies as well as by strengthening international cooperation along industrial and supply chains.

Second, China has actively shared the opportunities presented by its super large market. By steadfastly deepening reform and expanding opening-up, China has provided not only stability on the supply side, but also vast demand on the consumption side. Over the past five years, China's annual imports of goods and services have averaged USD3 trillion, making the country one of the world's most important consumer markets.

Third, China has continued to cultivate new growth drivers for international cooperation in emerging sectors. By accelerating the development of new quality productive forces and advancing industrial transformation, China has been deepening international cooperation in areas such as the digital economy, artificial intelligence, and new energy. In 2024, the value added of China's core digital economy industries accounted for about 10 percent of GDP, while imports and exports of digitally deliverable services exceeded USD400 billion, underscoring China's vital role in supporting global digital trade.

Fourth, China has actively participated in global governance and promoted multilateral cooperation. China has put forward the Global Governance Initiative, firmly upheld the multilateral trading system with the World Trade Organization at its core, and advocated inclusive economic globalization. Through high-quality

Belt and Road cooperation, China has provided strong support for developing countries to better integrate into global value chains and the international trading system.

At the same time, China has advanced deep-seated reforms and high-level opening-up in the foreign exchange sector, facilitated cross-border trade, investment and financing, and deepened the development of the foreign exchange market. These efforts have created favorable conditions for various market entities to efficiently allocate foreign exchange resources, manage exchange rate risks, and better participate in global economic and trade cooperation. In 2024, the trading volume in China's foreign exchange market increased by 37 percent compared with 2020, while the scale of external receipts and payments rose by 64 percent over 2020. In the first three quarters of this year, China's external receipts and payments totaled USD11.6 trillion, reaching a record high for the same period. High-standard opening-up has become a strong driving force for China's economic development.

Ladies and gentlemen,

General Secretary Xi Jinping has profoundly pointed out that economic globalization is an irreversible historical trend. The more challenging the times, the more we should stay true to our original aspiration for peaceful coexistence and strengthen our confidence in win–win cooperation. We will fully implement the arrangements made at the fourth plenary session of the 20th CPC Central Committee, coordinate development and security, continue to deepen reform and opening-up in the foreign exchange sector, and defend the bottom line whereby no systemic risks will occur. Our goal is to build a sound foreign exchange management system featuring "greater convenience, expanded opening-up, enhanced security, and upgraded intelligence".

First, we will improve the foreign exchange policy system that rewards greater integrity with greater convenience. We will enhance the quality and coverage of banks' foreign exchange operations reforms as well as reforms regarding trade and investment facilitation. The number of enterprises now able to handle transactions directly based on instructions has increased more than fivefold compared with the end of 2020. Focusing on trade facilitation, we will soon introduce nine new policy measures, which mainly aim to expand the scope of high-level opening-up pilot programs for cross-border trade and the range of netting settlement transactions, optimize foreign exchange fund settlement for entities in new forms of trade, and ease management of reimbursable expenses in trade in services—all designed to further promote innovation and high-quality development in trade.

Second, we will promote high-standard institutional opening-up in the foreign exchange sector. We will strengthen the overall planning of reforms, promote RMB internationalization and the high-quality opening-up of the capital account in a coordinated manner, and deepen the reform of foreign exchange management in key areas such as direct investment, cross-border financing, and securities investment. In September, we introduced a package of policy measures on cross-border investment and financing. In the near future, we will also roll out

policies on integrated RMB and foreign currency cash pooling for multinational companies and on the management of funds raised from overseas listings by domestic enterprises. Meanwhile, we will implement integrated reform and innovation in foreign exchange management within pilot free trade zones to help open up new horizons for China's self-initiated opening-up.

Third, we will enhance our capacity for foreign exchange regulation and risk management in an open economy. We will strengthen the integrated regulation of the foreign exchange market from the perspectives of macro prudential management and micro regulation, leverage artificial intelligence, big data, and other digital tools to empower smart regulation, and reinforce monitoring and early warning of cross-border capital flows. We will also improve our effectiveness in combating illegal and irregular activities, effectively guard against external shocks, and provide greater stability and certainty to support open cooperation and strengthen the resilience of global economic and trade activities.

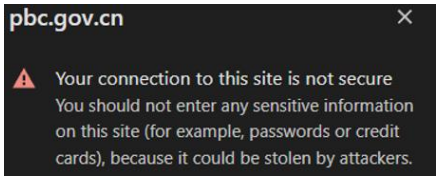
Ladies and gentlemen,

As the capital of China, Beijing serves as the nation's center for politics, culture, international exchanges, and sci-tech innovation. Over the past three years, Beijing's total goods trade has consistently exceeded RMB3.6 trillion, while its trade in services has grown at an average annual rate of nearly 10 percent. The State Administration of Foreign Exchange will continue to support Beijing in taking the lead in piloting more pioneering foreign exchange policies, further enhancing the quality and effectiveness of policies such as pilot programs of high-level opening-up of cross-border trade and investment, as well as the Research Funding Facilitation Policy. We will intensify our support for the development of Beijing as "Four Centers" and "Two Zones", and help the city play an even more important role in promoting stable and sustainable global economic and trade development.

Last but not least, I'd like to wish this year's Financial Street Forum a complete success. Thank you!

To learn more:
http://www.pbc.gov.cn/en/3688110/3688175/5892101/index.html

Note: This is a http, not https web site.

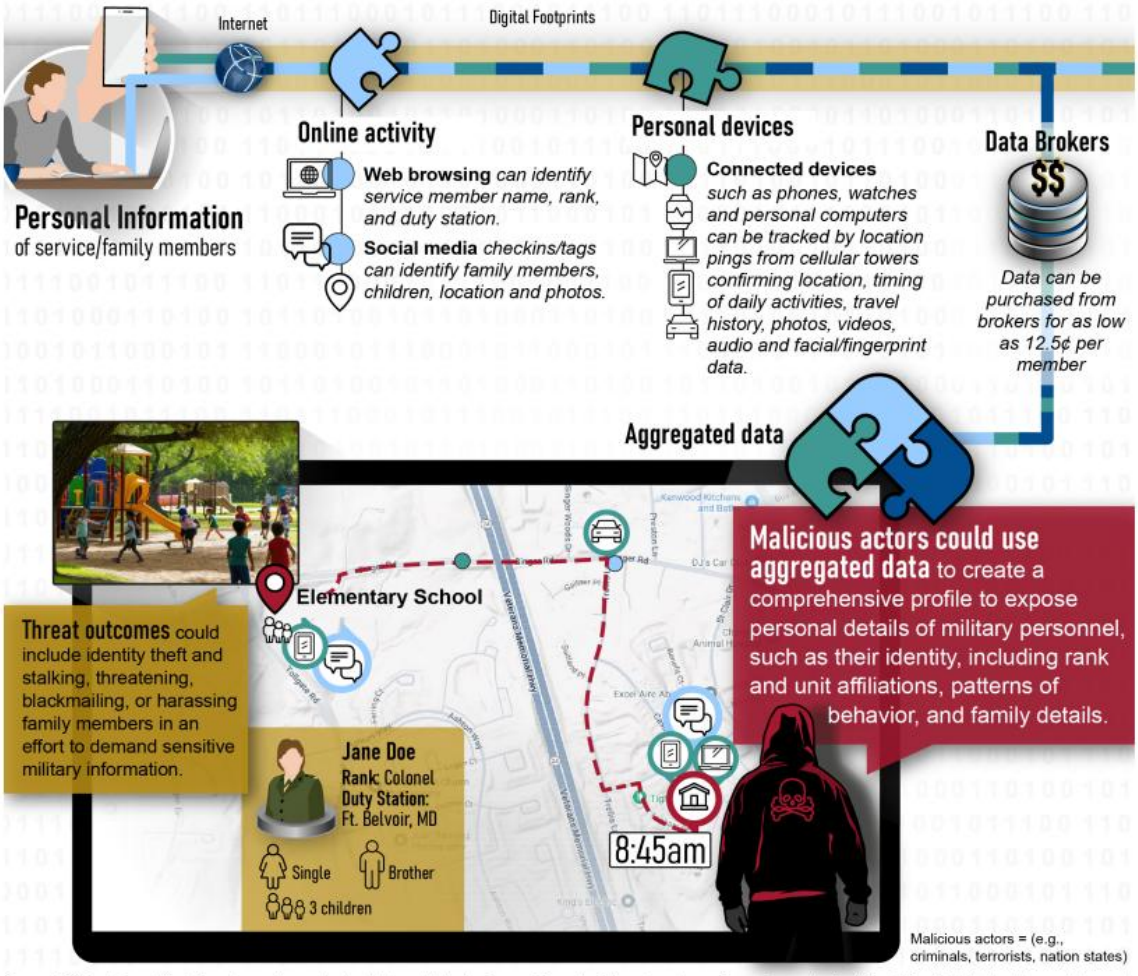


Number 6

United States Government Accountability Office
INFORMATION ENVIRONMENT
DOD Faces Risks with Publicly Accessible Information
Testimony Before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate, Statement of Joseph W. Kirschbaum, PhD
Director, Defense Capabilities and Management

GAO

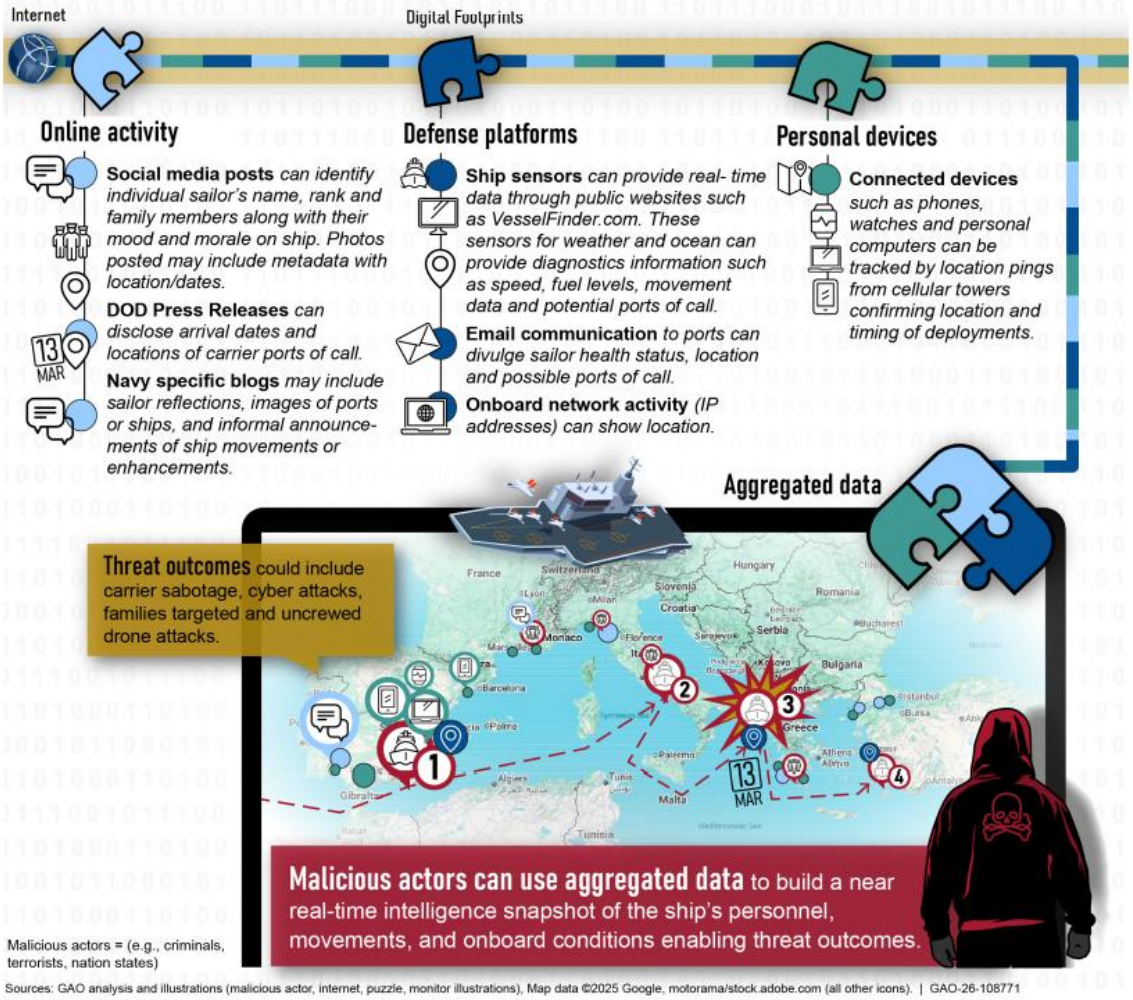
Figure 1: Scenario of Threat Outcomes from Exposure of DOD Personnel Information



Sources: GAO analysis and illustrations (person at computer, hand/phone, data broker icon, malicious actor, internet, puzzle, monitor, service member illustrations), SaroStock/stock.adobe.com (playground photo), Map data ©2025 Google, motorama/stock.adobe.com (all other icons). | GAO-26-108771

Chairwoman Ernst, Ranking Member Slotkin, and Members of the Subcommittee: I am pleased to be here today to discuss the risks of the growing use of electronic devices and online activities by the Department of Defense's (DOD) personnel and their operations.

Figure 2: Scenario of Threat Outcomes from Disclosure of Naval Operations

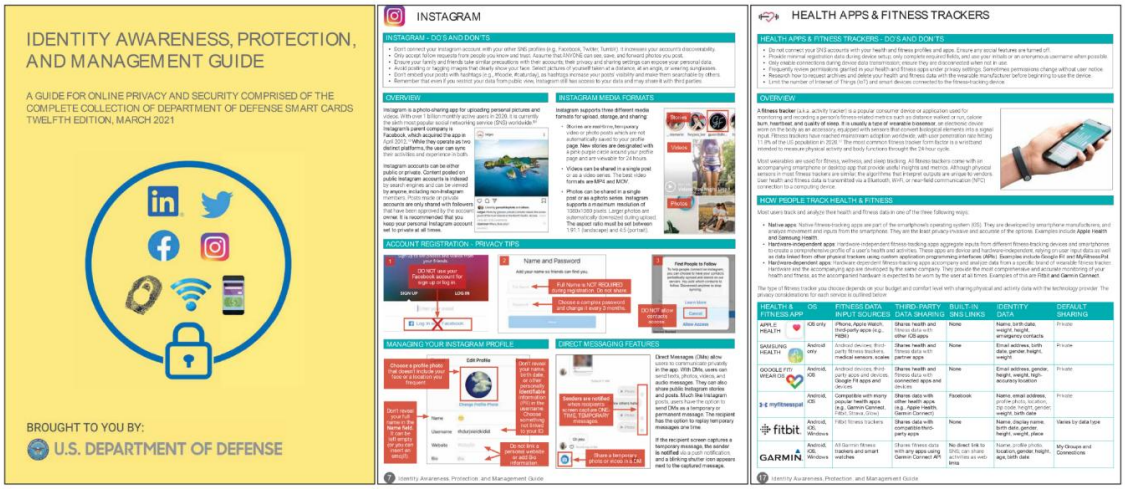


Throughout the day, people— including DOD service members, employees, contractors, and family members— leave behind massive amounts of traceable data that can be collected and aggregated by the public, data brokers, and malicious actors. These data, in the aggregate, can undermine national security and pose significant security, privacy, and safety risks.

All of this digital activity generates volumes of traceable information—also known as a digital footprint. Over time, multiple footprints can create a digital profile that can reveal potentially sensitive or classified information. We have previously issued reports highlighting how this escalation in volume, the interconnectedness of data, and the evolving DOD information environment have changed the landscape of information and national security.

My testimony summarizes our pending report entitled Information Environment: DOD Needs to Address Security Risks of Publicly Accessible Information. This statement focuses on (1) risks of publicly available data about DOD personnel and operations, and (2) DOD's approach to address security-related risks.

Figure 4: Example of Department of Defense's Smartcards on Securing Digital Profiles



Source: DOD Identity Awareness, Protection, and Management Guide. | GAO-26-108771

In conducting our work, we developed and examined threat scenarios that depict potential consequences from the exploitation of publicly accessible digital data. We developed these scenarios based on analyses of literature research, interviews, and our own investigation.

We also collected and reviewed information from officials from the Office of the Secretary of Defense and a non-generalizable sample of 10 DOD components. Our work was performed in accordance with generally accepted government auditing standards. We conducted our related investigative work in accordance with investigation standards prescribed by the Council of the Inspectors General on Integrity and Efficiency. More detailed information on the scope and methodology of our work can be found in our report.

To learn more: https://www.gao.gov/assets/gao-26-108771.pdf

United States Government Accountability Office

Testimony

Before the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. ET
Tuesday, October 7, 2025

INFORMATION ENVIRONMENT

DOD Faces Risks with Publicly Accessible Information

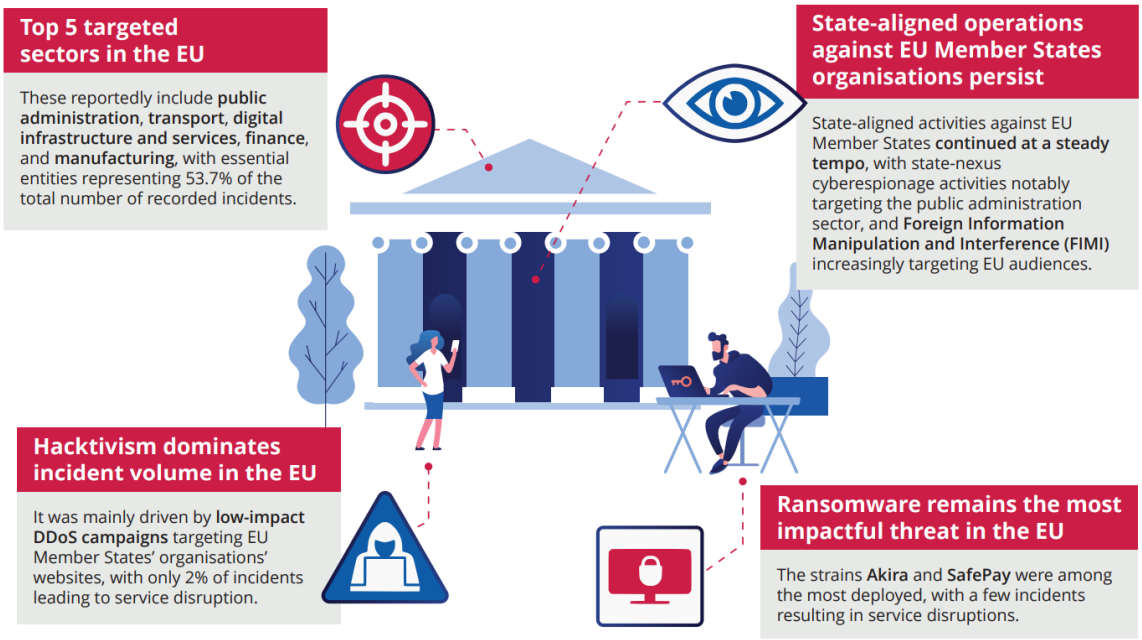
Statement of Joseph W. Kirschbaum, PhD
Director, Defense Capabilities and Management

Number 7

ENISA Threat Landscape 2025

This year's ENISA Threat Landscape (ETL) introduces a revised and concise format designed to deliver insights through a threat-centric approach and enhanced contextualisation.

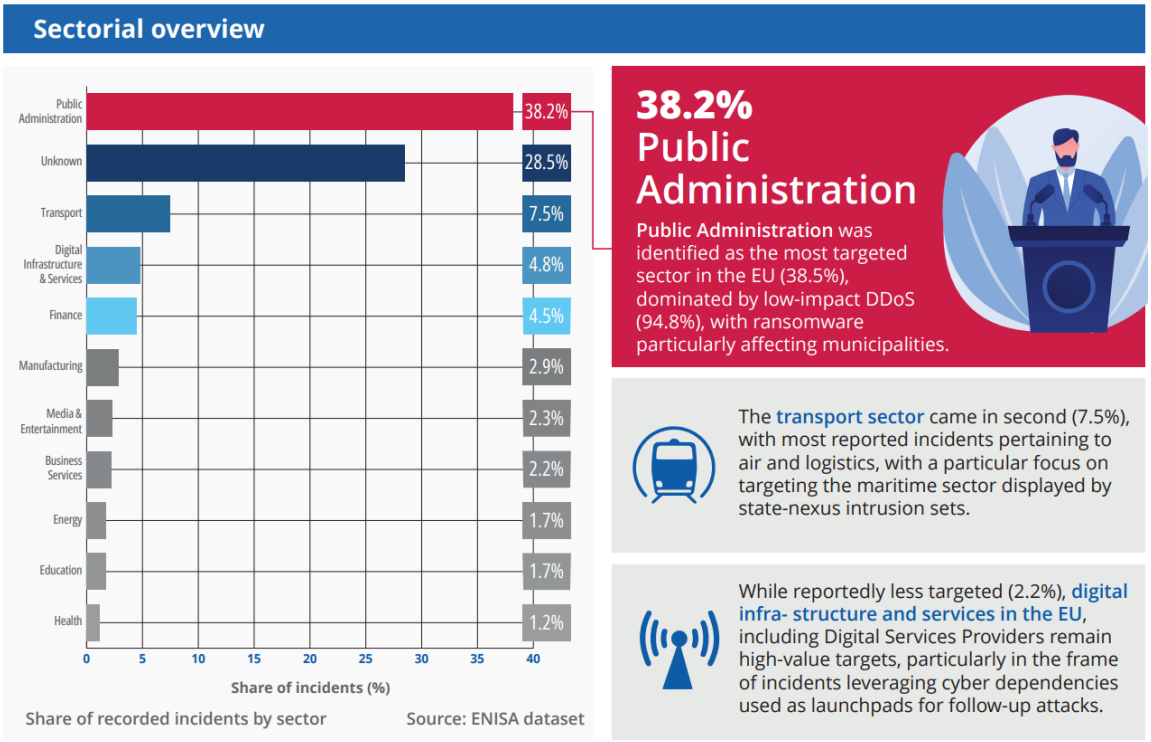
This edition integrates additional analysis of adversary behaviours, vulnerabilities and geopolitical drivers, aimed at both strategic and operational audiences, offering an actionable perspective on trends shaping the EU's cyber threat environment.



The ETL 2025 provides an overview of the European cyber threat ecosystem from July 2024 to June 2025, drawing on nearly 4 900 selected and curated incidents.

The reporting period highlights a maturing threat environment characterised by rapid exploitation of vulnerabilities and growing complexity in tracking adversaries.

Intrusion activity remains significant, with ransomware at its core. Cybercriminal operators notably responded to the actions of law enforcement by decentralising operations, adopting aggressive extortion tactics and capitalising on regulatory compliance fears.



The continuous proliferation of ransomware-as-aservice models, builder leaks and the services of access brokers has further lowered barriers to entry and diversified ransomware families, fuelling a professionalised and resilient criminal ecosystem.

In parallel, state-aligned threat groups intensified their long-term cyberespionage campaigns against the telecommunications, logistics networks and manufacturing sectors in the EU, demonstrating advanced tradecraft such as supply chain compromise, stealthy malware frameworks and abuse of signed drivers.

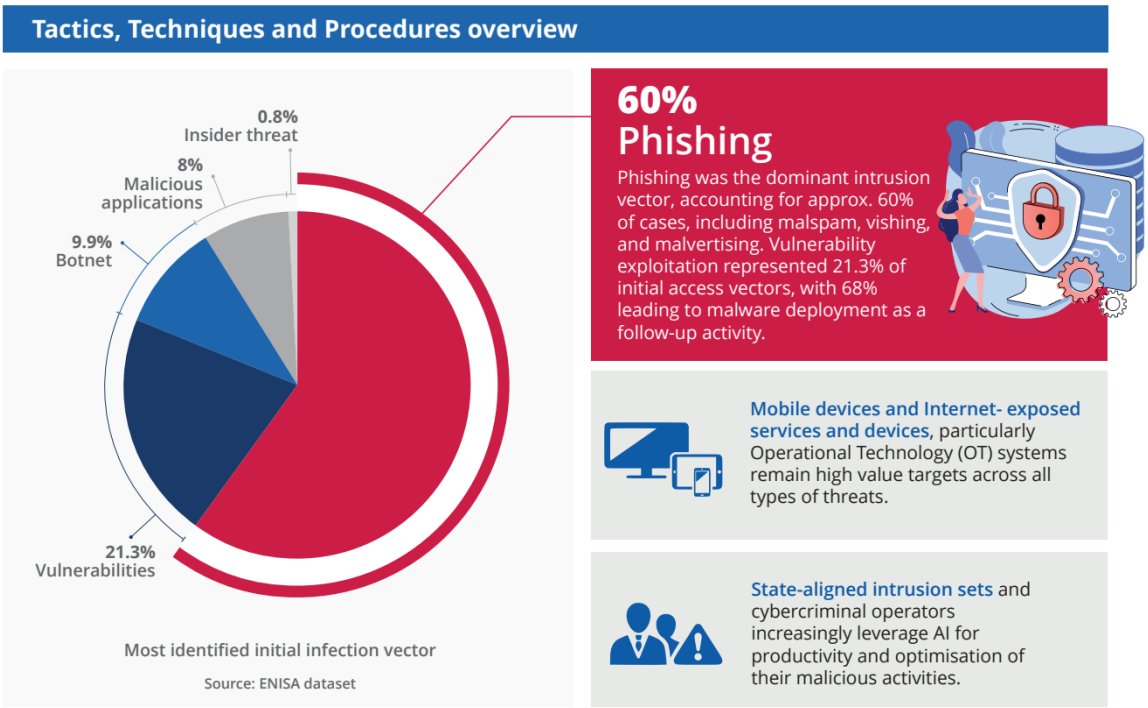
Hacktivist activity continues to dominate reporting, representing almost 80% of recorded incidents and driven primarily by low-level distributed denial-of-service operations.

While overall resulting in very low impact, these campaigns demonstrate how low-cost tools are scaled for ideology-driven operations.

Sectoral targeting patterns reinforce the EU' systemic exposure.

Public administration networks remain the primary focus (38%), notably for hacktivists and state-nexus intrusion sets, while transport emerged as a high-value sector, particularly maritime and logistics.

Aviation and freight operations have faced ransomware disruptions, while digital infrastructure and services remain strategic targets for both cyberespionage and ransomware operators. Phishing remains the dominant intrusion vector (60%) and is evolving through techniques used in largescale campaigns.



The availability of phishing-as-a-service platforms demonstrates the industrialisation of phishing operations, enabling adversaries of all skill levels to launch complex campaigns.

Abuse of cyber dependencies have also intensified, as shown by compromises in open-source repositories, malicious browser extensions and breaches of service providers, amplifying risk throughout interconnected digital ecosystems.

Across all campaigns, adversaries continue to rely on a consistent set of tactics, techniques and procedures.

Vulnerability exploitation remains a cornerstone of initial access (21.3%), with widespread campaigns rapidly weaponising them within days of their disclosure—underscoring the need to ensure patch availability and to implement and enforce basic measures for cyber hygiene.

Artificial intelligence has become a defining element of the threat landscape.

By early 2025, AIsupported phishing campaigns reportedly represented more than 80 percent of observed social engineering activity worldwide, with adversaries leveraging jailbroken models, synthetic media and model poisoning techniques to enhance their operational effectiveness.

The threat landscape depicted in this edition reflects how the cyber threat landscape is shifting toward mixed, possibly convergent pressure, with fewer single high impact incidents, and more continuous, diversified and convergent campaigns that collectively erode resilience.

To learn more:
https://enisa.europa.eu/publications/enisa-threat-landscape-2025

Number 8

Disrupting the first reported AI-orchestrated cyber espionage campaign

ANTHROP\C

Executive summary

We have developed sophisticated safety and security measures to prevent the misuse of our AI models. While these measures are generally effective, cybercriminals and other malicious actors continually attempt to find ways around them. This report details a recent threat campaign we identified and disrupted, along with the steps we've taken to detect and counter this type of abuse. This represents the work of Threat Intelligence: a dedicated team at Anthropic that investigates real world cases of misuse and works within our Safeguards organization to improve our defenses against such cases.

In mid-September 2025, we detected a highly sophisticated cyber espionage operation. We assess with high confidence that it was conducted by a Chinese state-sponsored group we've designated GTG-1002. It represents a fundamental shift in how advanced threat actors use AI. Our investigation revealed a well-resourced, professionally coordinated operation involving multiple simultaneous targeted intrusions. The operation targeted roughly 30 entities and our investigation validated a handful of successful intrusions.

To learn more:
https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf

Number 9

Google vs. “Lighthouse.”

Plaintiff Google LLC (“Google”), by and through its attorneys, brings this Complaint against Does 1–25 (the “Defendants”) for injunctive relief and damages. Google alleges as follows:

INTRODUCTION

1. The scam begins with a text message. It may alert you to a problem with the delivery of a package and invite you to click a link to correct your address and pay a small delivery fee. Or it may warn you of an unpaid toll or ticket, directing you to a toll collection website that appears legitimate to pay the outstanding charges.

2. Or perhaps you see an online advertisement promising, for example, a low price for a popular, name-brand water bottle and directing you to an e-commerce website where you can pay by credit card or Google Pay.

3. Millions of Americans have received these text messages and seen these ads, clicked on links to fraudulent websites, entered payment and other personal information, and thereby have become victims of the criminal scheme at the heart of this Complaint.1 Google is seeking an injunction to disrupt the criminal enterprise behind this scheme and stop its spread.

4. Defendants are a group of foreign cybercriminals who have engaged in relentless phishing attacks against millions of innocent victims, including Google customers, to steal personal and financial information. These attacks have collectively swindled innocent victims out of millions of dollars and harmed Google through the unauthorized use of its trademarks and services.

5. The key to Defendants’ phishing attacks is a powerful phishing software kit called “Lighthouse.” Defendants created Lighthouse to serve as a “phishing for dummies” kit for cybercriminals who could not otherwise execute a large-scale phishing campaign.

For a monthly licensing fee, criminals can select either an SMS or e-commerce version of the software, which includes hundreds of templates for fake websites, domain set-up tools for those fake websites, and other features designed to dupe victims into believing they are entering sensitive information on a legitimate website (the “Lighthouse Schemes” or “Schemes”).

The templates are designed to mimic trusted institutions—like government entities, financial institutions, and postal services— to leverage the public’s confidence in such institutions.

6. The scale of Lighthouse phishing attacks is staggering. In a 20-day period, approximately 200,000 fraudulent websites created using Lighthouse were used to attract "well over 1,000,000 potential victims" in at least 121 countries.

Lighthouse was used to launch 32,094 distinct United States Postal Service ("USPS") phishing websites from July 2023 through October 2024; between 12.7 million and 115 million credit cards may have been compromised in the United States alone.

Lighthouse-supported phishing websites have received an average of 50,000 page visits per day.

7. Although the software simplifies the creation of phishing websites, executing largescale phishing attacks still requires coordination and cooperation among multiple actors.

Some specialize in collecting contact information of potential targets, others focus on the logistics of sending SMS messages in bulk, and still others help to sell victims' stolen information.

The members of these groups, along with the developers of Lighthouse and those who license the software to carry out attacks, are referred to herein as the "Lighthouse Enterprise" or the "Enterprise."

The Enterprise created and maintains an online community of discussion forums that are used to plan and execute Lighthouse phishing attacks and recruit new members.

There, Enterprise members market and sell Lighthouse, train members to use the software, and improve the operation's efficiency.

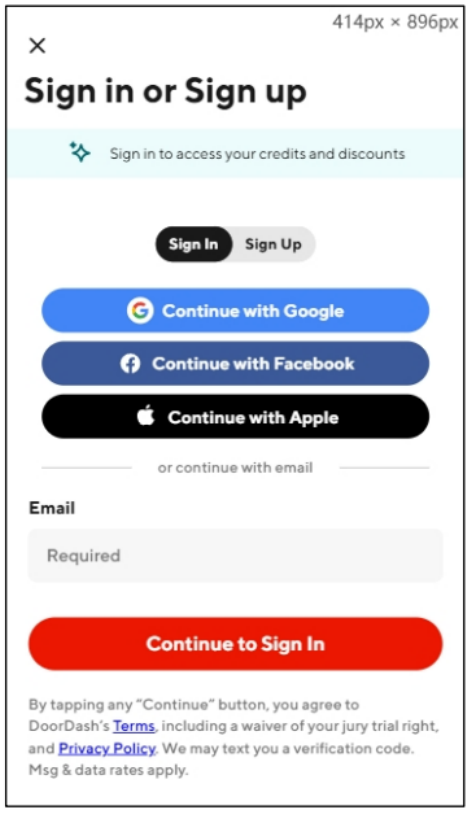
8. In facilitating and executing these phishing campaigns, the Lighthouse Enterprise preys on the public trust in Google, a leader in the technology space, by misappropriating Google branding, including by using Google logos on fraudulent websites.

The Lighthouse Enterprise also causes financial harm to Google, interferes with Google's relationships with its users (and potential users), harms Google's reputation, impairs the value of Google's products and services, and forces Google to devote substantial resources to investigate and combat the Lighthouse Enterprise's criminal activity.

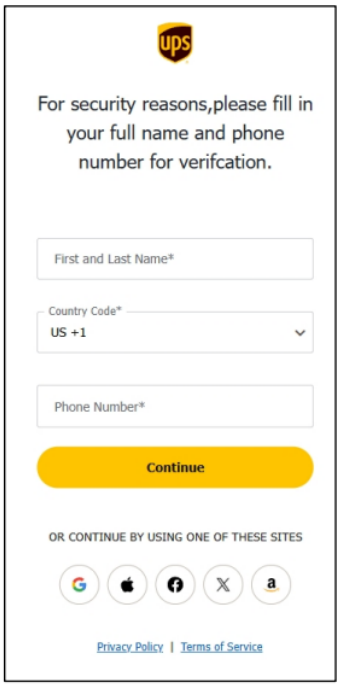
9. Disrupting the Lighthouse Enterprise will require persistence because the Enterprise can execute new phishing schemes with little effort, thanks to the Lighthouse software and coordination on Lighthouse discussion forums.

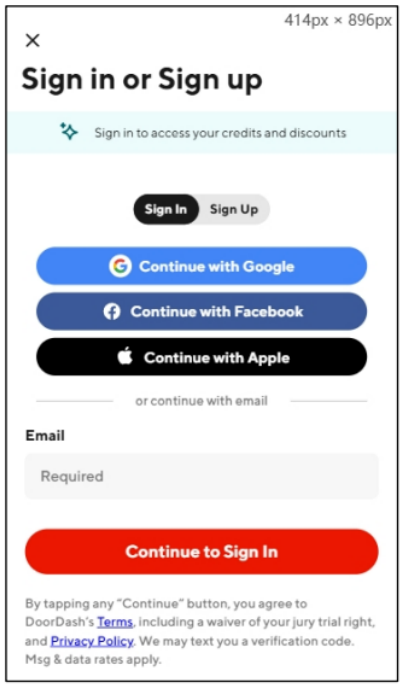
As the Enterprise detects threats to its infrastructure, it adapts its tactics and can shift its servers and domains within a matter of hours.

website, and update time. At least 116 templates feature a Google logo (YouTube, Gmail, Google, or Google Play) on the sign-in screen.

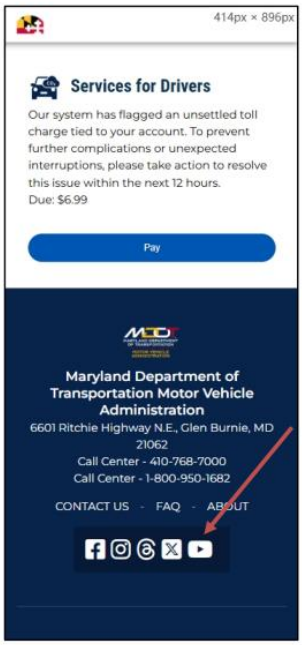


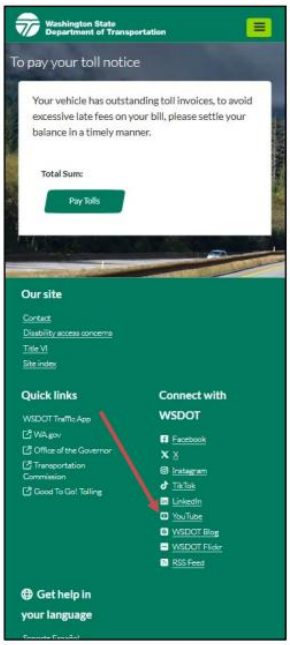
112. Some spoofed websites feature the Gmail logo, inviting targets to log in using their Gmail credentials.

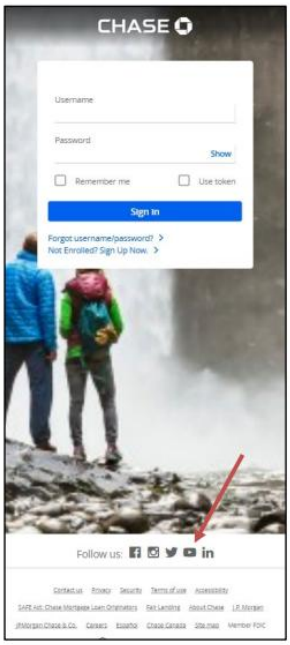




114. Other spoofed websites include the YouTube logo along with other prominent social media sites.







Case 1:25-cv-09421-LAK Document 1 Filed 11/12/25 Page 1 of 50

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

GOOGLE LLC,
Plaintiff,
v.
DOES 1–25,
Defendants.

Civil Action No.:

COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF

To learn more:
https://storage.courtlistener.com/recap/gov.uscourts.nysd.652891/gov.uscourts.nysd.652891.1.0_1.pdf

Number 10

Defending the cloud: Azure neutralized a record-breaking 15 Tbps DDoS attack

Microsoft

On October 24, 2025, Azure DDOS Protection automatically detected and mitigated a multi-vector DDoS attack measuring 15.72 Tbps and nearly 3.64 billion packets per second (pps). This was the largest DDoS attack ever observed in the cloud and it targeted a single endpoint in Australia.

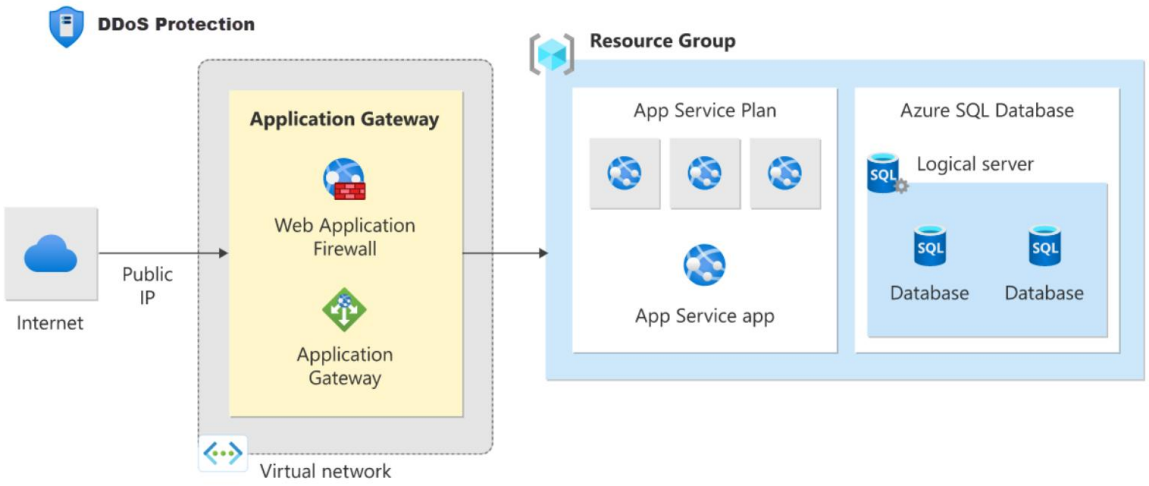
By utilizing Azure's globally distributed DDoS Protection infrastructure and continuous detection capabilities, mitigation measures were initiated. Malicious traffic was effectively filtered and redirected, maintaining uninterrupted service availability for customer workloads.

The attack originated from Aisuru botnet. Aisuru is a Turbo Mirai-class IoT botnet that frequently causes record-breaking DDoS attacks by exploiting compromised home routers and cameras, mainly in residential ISPs in the United States and other countries.

The attack involved extremely high-rate UDP floods targeting a specific public IP address, launched from over 500,000 source IPs across various regions. These sudden UDP bursts had minimal source spoofing and used random source ports, which helped simplify traceback and facilitated provider enforcement.

Attackers are scaling with the internet itself. As fiber-to-the-home speeds rise and IoT devices get more powerful, the baseline for attack size keeps climbing.

As we approach the upcoming holiday season, it is essential to confirm that all internet-facing applications and workloads are adequately protected against DDOS attacks. Additionally, do not wait for an actual attack to assess your defensive capabilities or operational readiness—conduct regular simulations to identify and address potential issues proactively.



What is Azure DDoS Protection?

Distributed denial of service (DDoS) attacks are some of the largest availability and security concerns facing customers that are moving their applications to the cloud. A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet.

Azure DDoS Protection, combined with application design best practices, provides enhanced DDoS mitigation features to defend against DDoS attacks. It's automatically tuned to help protect your specific Azure resources in a virtual network. Protection is simple to enable on any new or existing virtual network, and it requires no application or resource changes.

To learn more:
https://techcommunity.microsoft.com/blog/azureinfrastructureblog/defending-the-cloud-azure-neutralized-a-record-breaking-15-tbps-ddos-attack/4470422

Disclaimer

Despite the great care taken to prepare this newsletter, we cannot guarantee that all information is current or accurate. If errors are brought to our attention, we will try to correct them, and we will publish the correct information to the LinkedIn pages of the Association.

Readers will make their own determination of how suitable the information is for their usage and intent. The Association expressly disclaims all warranties, either expressed or implied, including any implied warranty of fitness for a particular purpose, and neither assumes nor authorizes any other person to assume for it any liability in connection with the information or training programs provided.

The Association and its employees will not be liable for any loss or damages of any nature, either direct or indirect, arising from use of the information provided on this newsletter, or our web sites.

We are not responsible for opinions and information posted by others. The inclusion of links to other web sites does not necessarily imply a recommendation or endorsement of the views expressed within them. Links to other web sites are presented as a convenience to users. The Association does not accept any responsibility for the content, accuracy, reliability, or currency found on external web sites.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the association has no control and for which the association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of interpretative;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts. It is our goal to minimize disruption caused by technical errors. However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

Readers that are interested in a specific topic covered in the newsletter, must download the official papers, must find more information, and must ask for legal and technical advice, before making any business decisions.

General Terms and Conditions for all visitors:
https://www.risk-compliance-association.com/Privacy.htm

The International Association of Risk and Compliance Professionals (IARCP) is a global community of experts working in risk and compliance management that explore career avenues and acquire lifelong skills. The IARCP is a business unit of Compliance LLC, a company incorporated in Wilmington, NC, and offices in Washington, DC, a provider of risk and compliance training and certification in fifty-seven countries.

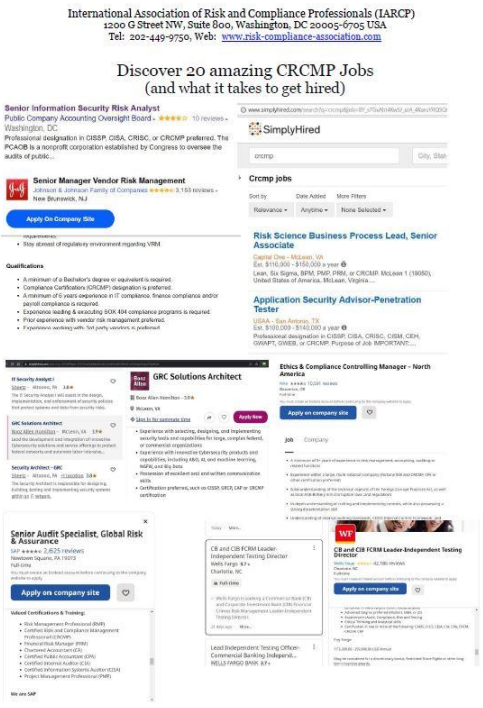
To learn more: https://www.risk-compliance-association.com/Privacy.htm

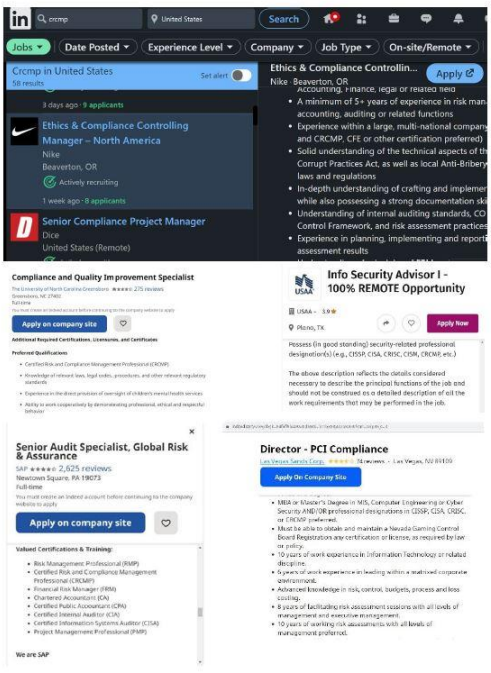
Our training and certification programs:

1. Certified Risk and Compliance Management Professional (CRCMP), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in fifty-seven countries. Companies and organizations around the world consider the CRCMP a preferred certificate.

You can find more about the demand for CRCMPs at: https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf





2. Advanced Specialization, Certified Risk and Compliance Management Professional in Hybrid Risk and Resilience Management - CRCMP(HR²M), online training and certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_HR2M.htm

The CRCMP(HR²M) program is designed to extend the capabilities of CRCMPs into the advanced domains of hybrid risk and resilience. This advanced specialization:

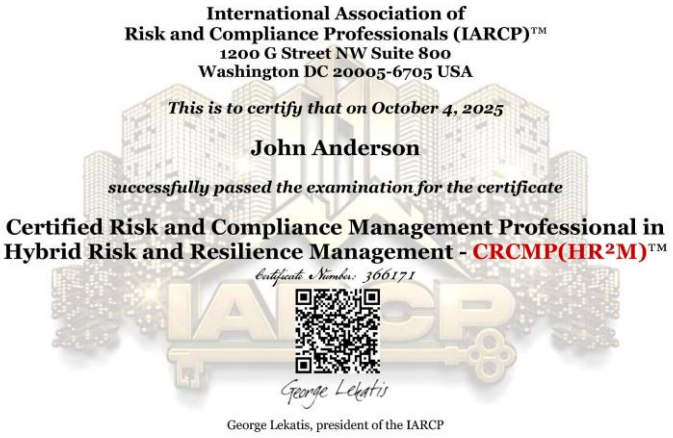
1. Moves from traditional risk and compliance frameworks into the management of multi-vector, cross-domain, and asymmetric threats that transcend conventional boundaries.

2. Develops expertise in hybrid risk governance.

3. Equips with the skills to design cross-sector resilience strategies, integrate governance across silos, and align risk frameworks with organizational, regulatory, and geopolitical realities.

4. Provides practical methodologies for hybrid stress testing, assisting organizations to withstand hybrid risks.

5. Advances the careers of CRCMPs by adding specialized expertise in hybrid risk and resilience, and offering strategic, cross-sector perspectives that are highly valued by organizations and boards.



Enrollment in the CRCMP(HR²M) program is restricted to professionals who have already passed the Certified Risk and Compliance Management Professional (CRCMP) exam.

To preserve the credibility and value of this credential, the association does not allow substitutions, equivalency credits, or waivers of any kind. The curriculum assumes mastery of the CRCMP body of knowledge.

3. Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program.

You may visit:
https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm

Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program

Overview

One of the most common (and costly) mistakes organizations make in the areas of risk management, compliance, IT, information security, and privacy, is relying solely on expert opinions that are **not grounded** in relevant laws and regulations. While professional expertise and technical insight are essential, they must be aligned with the legal and regulatory frameworks that govern these domains.

Without this alignment, organizations risk exposure to significant legal, financial, and reputational damage. For example, implementing information security controls based only on best practices, without accounting for legal requirements, can leave critical compliance gaps. Using risk management frameworks without tailoring them to specific regulatory requirements leaves organizations exposed to risk and compliance challenges.

4. Certified Cyber (Governance Risk and Compliance) Professional CC(GRC)P, distance learning and online certification program. You may visit:
https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm

Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program

Overview

There are still companies and organisations that consider cyber risk a technical risk. But even the most advanced organizations must adapt and build their risk management framework on the foundation that we now operate in a fundamentally different world, one where cyber risk is a core component of hybrid risk. The old mindset is dangerously outdated. Today, cyber operations are embedded in economic warfare, political conflict, supply chain disruption, and military strategy. Cyber risk today is not just about protecting networks, it's about protecting societies from hybrid threats.

A hybrid risk management framework should identify primary cyber threats, map their cascading effects on financial, legal, and business operations, and develop cross-functional response strategies.

5. Certified Risk and Compliance Management Professional in Insurance and Reinsurance CRCMP(Re)I, distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/CRCMP_Re_I.htm

Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I, distance learning and online certification program

Overview

In the aftermath of the global financial crisis of 2007–2009, and more recently the COVID-19 pandemic and the macroeconomic shocks triggered by inflation, geopolitical tensions, and climate-related events, the insurance and reinsurance sectors have faced escalating pressure to adapt to increasingly complex, interconnected, and systemic risks that challenge traditional risk models. These crises revealed not only the extraordinary complexity of risk exposures in the industry, but also the gaps in risk comprehension, governance, and compliance preparedness.

Mispriced risk, regulatory blind spots, and insufficient oversight contributed significantly to systemic instability. For insurers and reinsurers, the stakes remain immense. These firms serve as financial shock absorbers across society, and when their risk frameworks falter, the consequences ripple across markets, governments, and policyholders alike.

6. Travel Security Trained Professional (TSecTPro), distance learning and online certification program. You may visit: https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm

Travel Security Trained Professional (TSecTPro), distance learning and online certification program

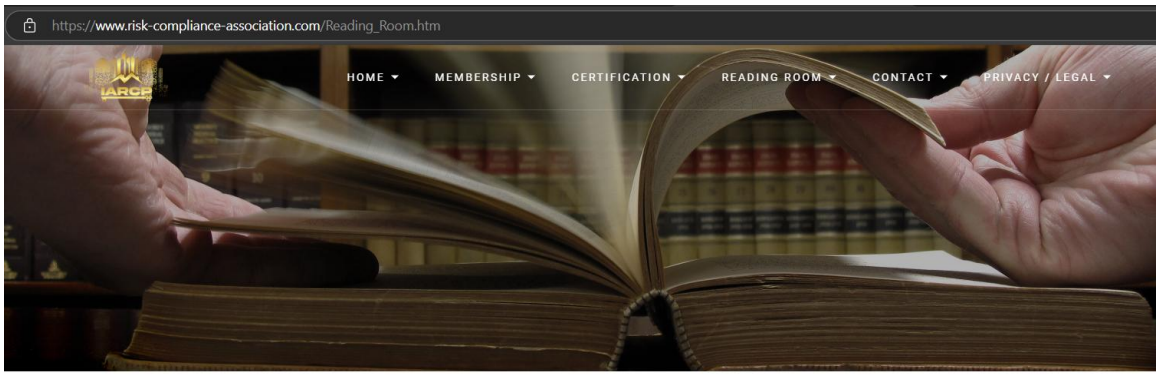
Overview

Professionals love international travel. For so many board members, senior executives, managers and employees, business travel taken for work purposes is also an opportunity for pleasure and satisfaction. It is about visiting new places, meeting new people, eating delicious food, having fun. For many, emotional or physical intimate relationships play a central role in the overall travel experience.

Intimacy refers to the closeness and connection – from intellectual intimacy (sharing thoughts, ideas, and professional experience) to emotional and sexual intimacy.

Travelers hate to think that travel also means increased risk, health challenges, legal uncertainty, and new unique threats. They often do not understand (or prefer to ignore) what it means to become subjects to the laws and the legal system of the countries they are visiting.

Our reading room: https://www.risk-compliance-association.com/Reading_Room.htm



Reading Room, International Association of Risk and Compliance Professionals (IARCP)

Welcome to the Top 10 risk and compliance management news stories and world events that, for better or worse, defined this week's agenda — and a look ahead at what's coming next. This is the newsletter from the International Association of Risk and Compliance Professionals (IARCP).

You may contact:

Lyn Spooner
Email: lyn@risk-compliance-association.com

George Lekatis
President of the IARCP
1200 G Street NW, Suite 800
Washington, DC 20005, USA
Tel: (202) 449-9750
Email: lekatis@risk-compliance-association.com
Web: www.risk-compliance-association.com
HQ: 1220 N. Market Street Suite 804,
Wilmington, DE 19801, USA
Tel: (302) 342-8828