Deloitte.
Insights

The connected defense: Elevating the fight against financial crime

Using 4IR technologies to prevent and detect the growing ecosystem of financial crime

The pressure to tackle financial crime has never been greater. Deloitte is at the forefront of the fight against financial crime and has assisted many of the world's leading financial institutions in developing, implementing and remediating all aspects of Financial Crime Risk Management programs, as well as investigating financial crimes. Our solutions include anti–money laundering or sanctions, anti-bribery and corruption, financial crime investigations, and financial crime analytics.

Contents

Introduction

AT THE HEIGHT of the Roman Empire, 250,000 miles of road connected two million square miles of land. The connectivity spurred innovation to levels never witnessed before in history. The network of roads made it possible for engineers to be deployed across the empire to transform rural landscapes into new cities and towns; it also made it possible to recruit and deploy more than 450,000 soldiers across the empire.[1]

However, over the centuries, the same innovation and technology that led to the rise of the Roman Empire contributed to its downfall. Increased trade turned relatively low-threat barbarian tribes into wealthier existential threats to Rome, as they were now equipped with modern weaponry and improved agricultural tools. Simultaneously, the sheer size of the empire gave way to the formation of dozens of smaller provinces. By 476 C.E., the now-sophisticated tribes completely outmatched the disparate and less-coordinated provinces—leading to the sacking of Rome and the toppling of one of the greatest empires in history.

Today, akin to the early road design and construction of Rome, Fourth Industrial Revolution (4IR) technologies like the Internet of Things (IoT) and cloud computing connect us in ways we had never imagined. This has led to an unprecedented level of business innovation and advanced technical solutions while also creating a converging landscape of cyber, financial crime, and money laundering risks.[2] These blurred lines have, in turn, given birth to new and more innovative forms of financial crime—forms that are sophisticated in their approach and agnostic to industry and geography.

Traditionally, these threats manifested in the financial sphere, but they're now surfacing in other industries as well. From our homes to our workplaces to our cars and airports, our collective connectivity increases the digital attack surface for cyber, with potential threats cutting across smart factories, health care institutions, and even home appliances.[3] Further, a new digital underground society of cybercriminals has emerged, seeking to exploit any vulnerability they can find in our digital platforms and the myriad connection points generated by the proliferation of IoT technologies, making it easier to monetize system attacks and steal data on an industrial scale. These new-age fraudsters can operationalize global campaigns to misappropriate funds and their fellow launderers can adopt modern digital technologies—like blockchain—to anonymously operate across borders (see sidebar, "The changing face of financial crime").

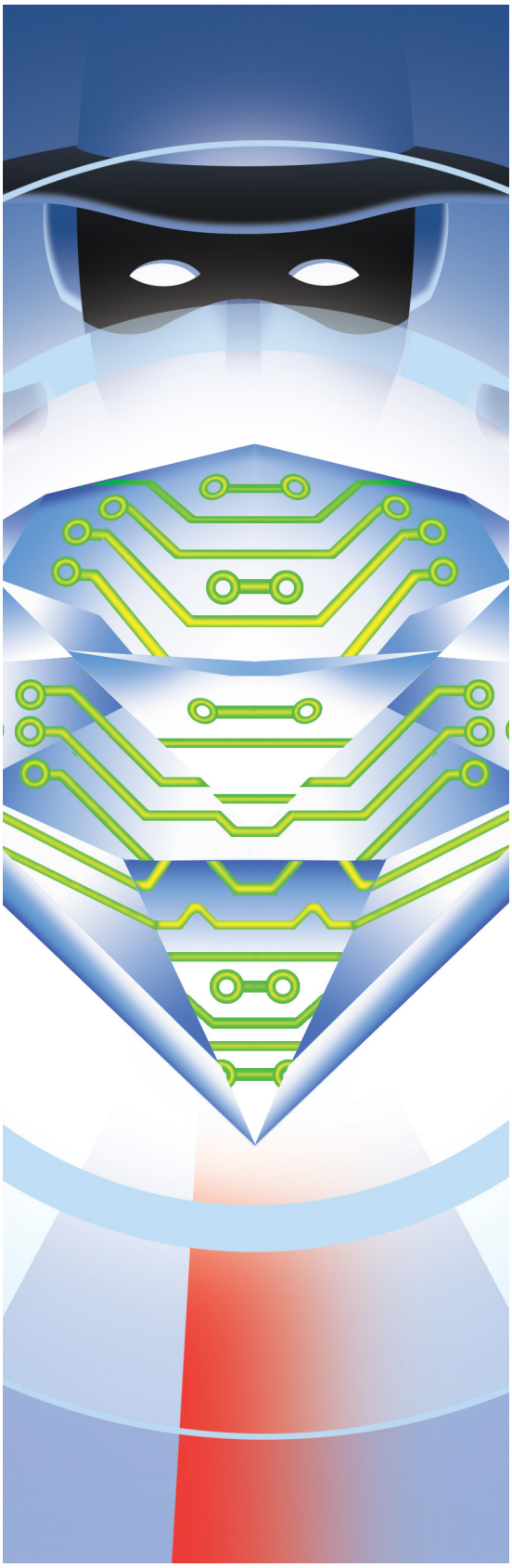
Both at home and at work, our collective connectivity increases the digital attack surface for cyber, with potential threats to smart factories, health care institutions, and home appliances.

But there is good news: The same technologies that are responsible for creating the present-day digital criminal ecosystem can be harnessed to detect and, in many cases, prevent these crimes before they occur. In this article, we explore how companies can elevate and intensify the fight against financial crime beyond the level of battling criminals by taking the following steps:

- **Developing cross-organization goals:** Financial crime has become too big an issue for any one organizational team to solve. It's also difficult to get a sense of where to start. Organizations should have a coordinated strategy to share information, data, and technologies in unison. This often requires integrating—and interrogating—data sets across cyber, fraud, and anti–money laundering (AML) teams. Without this, organizational resources can become locked into a repetitive tactical fight where each problem is battled in isolation, in the absence of a complete picture of the overall damage incurred.

- **Creating global partnerships:** Financial crime is occurring on a global scale. A hospital's patient data can be compromised in one country and sold on the dark Web to criminal gangs in another country for identity theft and fraud. As such, it is important for organizations to cultivate visibility across the globe through internal and external collaboration and information-sharing partnerships. Concurrently, they must navigate each jurisdiction's local regulations related to financial crime and data privacy.

- **Elevating the solution set:** This, perhaps, is the first and last mile of combating financial crime. Companies can leverage the power of threat intelligence, data science–driven advanced analytics, and machine learning techniques to detect and prevent criminal activities in a more precise and timely manner.



THE CHANGING FACE OF FINANCIAL CRIME

The connectivity between cyber, financial crime, and money laundering changes the way we identify and fight myriad economic criminal activities—terrorist financing, human trafficking, tax evasion, fraud, handling the proceeds of a crime, and bribery, to name a few. Below, we list some of the most prevalent techniques employed to carry out these crimes, along with the costs incurred by the global economy.

Modern techniques of financial crime:

- **AI-powered phishing schemes:** On the lines of targeted marketing campaigns, criminals are creating complex online profiles to more effectively reach and message individuals and deceive them into providing personally identifiable information (PII) or clicking corrupted links.[4]
- **Advanced financial crime:** Criminals are increasingly relying on sophisticated computing and artificial intelligence (AI) techniques to commit financial crime. In one case, fraudsters used AI to mimic the voice of a company's CEO to successfully request a US$243,000 fund transfer to an overseas supplier.[5]
- **Enhanced malware:** As cyber defenses become better at identifying and defending malware, criminals are increasingly relying on AI to assess hardware configurations and determine if a person or a machine is operating the device. [6]
- **Blockchain-based criminal activities:** Traditionally, companies and authorities attempt to thwart criminal activity by identifying the IP address of the user and alerting authorities to censor all traffic from that address. However, blockchain is both decentralized and anonymized, meaning that no individual internet service provider owns the system—making it incredibly difficult to identify the end user. In this environment, it's easier for criminals to carry out illegal activities like money laundering on blockchain. Also, with blockchain smart contracts, criminals can sell and procure items like malicious codes in a safer environment.[7]

The global impact of financial crime:

- **The cost of fraud:** One study estimates global annual fraud costs to be upward of US$3.7 trillion, of which only an estimated 14 percent is recovered. [8]
- **The cost to defend:** Across the private and public sector, an estimated US$1.28 trillion is spent annually to combat financial crime.[9]
- **The cost of fines and sanctions:** Over the last decade, companies have incurred US$26 billion in fines and sanctions for their noncompliant anti–money laundering and know your customer (KYC) practices—the United States incurred 91 percent of this amount.[10]
- **Other potential costs:** Less quantifiable but still highly relevant costs are incurred to organizations through reputational damage, competitive disadvantages, and productivity losses.

Connected technology: All roads lead to Rome

FINANCIAL CRIME AIDED by technology is a multifaceted and far-reaching problem impacting nearly every organization. Paradoxically, in the face of greater worldwide connectivity, organizational structures can't always keep pace with the speed of technological change. While criminals are indifferent to corporate structures, many organizations still have dedicated, standalone teams to combat and detect cyberattacks and financial crime. These teams often operate in silos, similar to the Roman provinces fighting off each new threat in isolation. But, unlike the fall of the Roman Empire, which spanned centuries, threats to even the largest multinational business can be manifest in seconds.

As a result, companies in most industries, as well as their risk management teams and systems intended to combat financial crime, are facing unprecedented strain. The cost of fraud and cyberattacks is estimated to exceed US$3 trillion across the globe annually.[11] Yet, most risk monitoring systems yield unproductive and inefficient investigatory work to ensure that compliance regimes are met at the base level, rather than effectively identifying suspicious activity with high levels of confidence.

Navigate the Web of crime: Define specific goals

Thankfully, organizations today have access to a wealth of data, tools, and modeling techniques they can use to combat even the most sophisticated crimes. However, the options and approaches to tackling these crimes can be overwhelming, and the regulatory climate doesn't always keep up with the capabilities deployed by bad actors. Most organizations are just trying to keep pace with compliance requirements rather than matching criminal adversaries in their approach. This often leads to rigid and more easily circumvented rule sets to detect financial crime—for example, rules relating to exceeding predetermined spending limits. Further, insider threats can relay even the most complex rule sets to those looking to maneuver around them.

Unlike the fall of the Roman Empire, which spanned centuries, threats to even the largest multinational business can be manifest in seconds.

In an era of 4IR technologies and AI, the natural response is to replace monitoring rule sets with more advanced analytical techniques, such as using machine learning to more accurately detect cases of fraud. While these techniques may be more effective, it's no small feat to overhaul years, even decades, of old infrastructure and corporate practices with new risk management structures and methodologies. There are two primary reasons for this:

- First, it requires companies to move out of their comfort zones. This entails high-level leadership coordination and a willingness to

procure or share data with others, both of which can necessitate navigating corporate politics and long-standing corporate policies.

- Second, the overwhelming number of tools, modeling techniques, and data sources available cultivate a rather complex environment to both choose from and implement. Therefore, determining the *right* approach for your organization is not always a straightforward endeavor.

The best way to make these formidable issues more manageable could be to articulate more specific goals while combating financial crime. By going deeper than a "stop all cases of fraud" goal, organizations can get a better sense of the data required, people with whom to coordinate, and the most effective analytical approaches to address the issue. There are four areas in which organizations can define more manageable goals with a view to protect themselves from various forms of financial crime. They are:

- **Fidelity—reducing false positives:** Rule-based solutions often lead to false positives (that is, *incorrectly* alerting teams to possible improper behavior). These false positives can lead to investigators unnecessarily spending significant hours researching cases that more sophisticated approaches would have never identified in the first place. So, reducing false positives would save a lot of time that can be directed toward fighting and detecting real frauds and money laundering.

- **Efficiency—rapidly identifying illegitimate activity:** When a malicious person or bot gains access to customer credentials, the behavior pattern would inevitably change to produce anomalies. For example, machine learning techniques can use granular data (such as typing speed) to quickly alert monitoring teams of improper logins to bank accounts.

- **Coverage—expanding the scope of protection:** The connected nature of technology has increased the threat landscape. As such, it's important for organizations to inventory all potential areas exposed to possible attacks. This means understanding business value chains, the supporting systems, processes, and resources, and then assessing how critical each threat is to the overall health of the business.[12]

- **Prediction—telegraphing the criminal element:** Proactive attack prevention is made possible through predictive analytics techniques. For instance, threat modeling and scenario analysis provide a line of sight into an organization's attack surface, which in turn can help teams preemptively address high-risk areas for financial crime.

The best way to make formidable crime management issues more manageable is to articulate more specific goals while combating financial crime.

Starting with the board and top management teams, these key action areas should be agreed upon, communicated, and prioritized across the organization. Specific goals can become a rallying cry for gaining internal and external support, providing direction on how to improve processes (regardless of organizational silos), and determining the best tools and analytical techniques to address the issue. As an example, if the goal is to rapidly identify anomalies, the cyber,

fraud, and AML departments can work together to build a single database across the organization that identifies bad actors, rather than have each group figure this out in isolation—and after several attacks on the company.

Sharply defined goals help companies to react in a more agile manner. In a recent panel discussion for *Risk.net*, executives discussed the need to simplify the objectives to defend against financial crime in a more agile manner. Specifically, it requires ensuring that cybersecurity, application security, fraud, and data scientists are working collaboratively to consolidate data sources in order to gain an enterprise-wide view of vulnerabilities and opportunities to share knowledge in the fight against financial crime.[13]

Starting with the board and top management teams, these key action areas should be agreed upon, communicated, and prioritized across the organization.

Get by with some help from friends: Forge partnerships

As financial criminals function in ecosystems, so too should the institutions tasked with defending against them. Businesses and law enforcement can work in tandem to thwart these criminal ecosystems through fast and effective sharing of information on bad actors, knowledge related to new criminal schemes, and intelligence on best practices for prevention and detection of financial crime. To do so effectively, organizations should consider a two-fold approach: Elevate the importance of procuring third-party data and participate in public-private partnerships (PPP) to share information and best practices.

CREATE THIRD-PARTY DATA PARTNERSHIPS

Sharing data outside the organization is not a new concept—retailers and suppliers have been doing it for decades. However, the level of granularity, sensitivity of information, and sheer volume of data required to combat financial crime is compelling many organizations to look outside their own four walls. When multiple institutions artfully combine their data, they can piece together a mosaic of criminal activity that none can discern in isolation, thus creating actionable insights in aggregate.

Banks are some of the earliest adopters of third-party data-sharing and have been safely and appropriately exchanging data with external parties for decades. Many banks understand that one of the best ways of defending against financial crime is by proactively building "herd immunity." This entails sharing intel to collectively learn from one another and preemptively put measures in place to prevent or minimize future crimes.

This is manifesting in the financial services industry through third-party platforms, which provide cloud-based communities for standardizing and sharing information across vendors.[14] Perhaps more promisingly, recent innovations like homomorphic encryption and multiparty computation enable organizations to compare data sets and perform complex analytical routines against an aggregated data set.[15] By doing so, they can collectively extricate insights from patterns of malicious behavior that indicate criminal activity—with a higher rate of fidelity than previously possible.

For example, consider IP addresses with a troubled history. Companies can contribute and upload "bad" device data on a shared database and use it as

a data modeling attribute. These data sources can help companies uncover IPs that either have a direct malicious history (sending spam emails, account takeovers, and malware data) or are in a nexus with IPs that do.[16]

ENTER INTO AND PARTICIPATE IN PPPS

Many government agencies around the world are working to combat various types of financial crime but they can be significantly more effective if they collaborate more with the private sector—and vice versa. These PPPs can provide law enforcement with quick access to intelligence related to relevant case work and inform organizations of the most current status of the threat landscape.[17] Further, they can create a safe environment for both groups to share information and data.

Public-private partnerships can provide law enforcement with quick access to intelligence on cases and inform organizations of the current threat landscape.

Such partnerships seem to be growing across the world. One notable example is the United Kingdom's Joint Money Laundering Intelligence Taskforce (JMLIT). This group consists of more than 20 large banks, the National Crime Agency (NCA), the Home Office, and the Financial Conduct Authority (apart from a number of other agencies). Together, they can tackle cases of financial crime, such as human trafficking, and share information and data to better understand patterns of criminal behavior and the identities of potential bad actors. By working directly with banks, government agencies can share "red flag" activities that indicate trafficking behavior, such as payments made to cover multiple individuals' travel expenses from a country the financer has never personally visited.

Such PPPs don't have to be limited to financial institutions. Retailers, for instance, are frequent targets of criminals looking to steal consumers' bank details. Retailers can provide insights on suspicious transactions and use of online resources to authorities and financial institutions. Similarly, automotive dealers or high-end consumer credit brokers can share consumer spend information to help alert the authorities and banks of potential money laundering.

Where we're going, we don't need roads

THE SAME SOPHISTICATED tools, technologies, and techniques that make financial criminals formidable adversaries for organizations can be repositioned to fight crime. But companies first need to ensure that the basics are in place—that is, they have defined specific and concise goals, are working collaboratively across silos, and sharing relevant data and information *safely* with external parties. These foundational practices can put organizations in prime position to explore the full potential of 4IR technologies in combating financial crime.

The same sophisticated tools, technologies, and techniques that make financial criminals formidable adversaries for organizations can be repositioned to fight crime.

With 4IR technologies, data can be organized, shared, and analyzed in the cloud more easily. Specifically, organizations can fuse data across cyber, fraud, and anti–money laundering functions into a single data set—and interrogate the information through more sophisticated means than traditional rule sets. By combining this data with AI and predictive analytics, organizations can safeguard highly targeted information and alert teams to high-risk scenarios through the following data capture and analysis methods:

- **Digital entity fingerprinting:** Organizations can conduct validation tests to detect suspicious activity. This includes assessing if the device is foreign to the expected user, determining if the access location strays from routine behavior, or alerting the business that the IP address has a bad actor reputation. For example, if a transaction to transfer corporate funds to a new and suspicious account originates from an unfamiliar broadband router—and the physical location originates from an unexpected region—then it's most likely a suspicious user.

- **Session monitoring:** Session logs are rich in user behavior. Analyzing a user's behavior and journey during an authenticated session in application logs can help determine whether a human is in control or if there's bot activity going on.

- **Behavioral biometrics analytics:** This utilizes passive biometrics such as typing speed, cursor movement, and reaction times to authenticate the user.

Each of the methods mentioned above employs a structured modeling technique to identify criminal behavior. That is, a human informs the model what good-versus-bad behavior looks like. Other techniques such as machine learning can elevate these approaches to a new level of sophistication—and analyze the digital entity's fingerprinting, session monitoring, and behavioral biometrics data in concert. Machine learning is an iterative process that employs a variety of complex algorithms to analyze data patterns; further, it typically adjusts

its predictions based on new data and information that enters into the system.

With unsupervised modeling (that is, modeling techniques that draw conclusions without human intervention), machine learning can identify unique groups of behavior that may indicate some form of financial crime. These same groups can then be entered into more structured machine learning approaches to score and assess the likelihood of improper behavior. For instance, various platforms are coming to market that employ machine learning to analyze transactions from a consortium of thousands of e-commerce websites to defend against online fraud and abuse.[18] Each time a potential fraudster initiates an activity on one of their partnering websites, a fraud score is updated and shared across the consortium.

Encouragingly, these techniques are growing in popularity. One study suggests that by 2021, 72 percent of organizations will employ automated monitoring and anomaly detection, and 50 percent will rely on predictive analytics and advanced modeling techniques to combat financial crime.[19] As more and more organizations adopt advanced technologies to combat crime, the pressure is expected to mount on those still relying on outdated crime monitoring systems to change as they will likely become relatively easier targets for cybercriminals.

Defending your empire

WHETHER YOU OPERATE in the financial industry or not, increased digital connectivity is making combating financial crime a universal problem. To forge your own organizational path to defend against bad actors, your leadership team should consider implementing the following advice:

Rome wasn't built in a day. An organization has a considerable number of moving parts across governance, culture, people, process, technology, and data. However, it isn't necessary to accomplish everything in a single seismic shift. Starting with specific goals, consider seeking opportunities for internal fusion at a smaller scale. Within your organization, that could mean looking to areas where skill sets, core processes, enabling technologies, and mutual data synergies exist. Increasingly, cyber offers opportunities to connect with physical security and fraud departments. Bringing these teams together, even just through closer collaboration, can help improve their respective effectiveness and operational efficiencies.

Know thyself. It is a strategic imperative to build a comprehensive, current, and accurate knowledge base of your business value chains and the critical assets that enable a business to function. This represents your organization's attack surface and, therefore, the potential opportunities for an adversary to steal, manipulate, or disrupt your key systems, people, data, and workflows. This attack surface also extends through to your larger business ecosystem (including your customers, supply chain, and industry peers).

Know thy enemy. Seek out credible intelligence on adversaries and triangulate this information across multiple sources. Strategic advisory groups, external data-sharing platforms, and a consortium of peers can help your organization build a better understanding of who, how, and why a criminal group might attack your business.

Plan for the worst, hope for the best. Analytically based intelligence and empirical data makes it possible to prioritize preventative countermeasures—and measure their efficacy. By building a comprehensive map of scenarios mapped to controls, it becomes easier to identify commonalities and redundancies, and therefore, improve consistency of coverage and realize operational efficiencies.

Seek out credible intelligence on adversaries and triangulate this information across multiple sources.

Drill your defense strategies. Rehearsing predicted scenarios and plans to prevent, detect, and respond to attacks can create opportunities to challenge old assumptions and refine solutions. By socializing these learnings, businesses can raise awareness on new threats and cultivate a culture that supports core goals and objectives.

By taking the above steps, organizations can proactively build an ecosystem of security to match—and possibly eventually exceed—the criminal elements they are charged with thwarting.

Endnotes

1. Richard A. Gabriel, "Why Rome fell," *HistoryNet*, accessed September 24, 2019.
2. Deloitte, *Forensics and the Fourth Industrial Revolution: The value of an analytics-driven approach*, accessed September 24, 2019.
3. Nick Galletto, Ed Powers, and Timothy Murphy, "Cyber, cyber everywhere: Is your cyber strategy everywhere too?," *Deloitte Review* 25, July 29, 2019.
4. Stephen Helm, "Artificial intelligence part 2: Cyber criminals get smart with AI," Secplicity, August 27, 2018.
5. Catherine Stupp, "Fraudster used AI to mimic CEO's voice in unusual cybercrime case," *Wall Street Journal*, August 30, 2019.
6. Helm, "Artificial intelligence part 2."
7. Alastair Paterson, "How cybercriminals are using blockchain to their advantage," Security Week, August 30, 2018.
8. Fcase, "The actual cost of fraud," October 18, 2018.
9. Che Sidanius, "Financial crime report: Costs & fighting back," Refinitiv, May 30, 2018.
10. Mara Lemos Stein, "Regulators raked in $26 billion in global penalties since 2008," *Wall Street Journal*, September 26, 2018.
11. Fcase, "The actual cost of fraud."
12. Galletto, Powers, and Murphy, "Cyber, cyber everywhere."
13. Risk.net, "Deploying agile analytics in the fight against fraud," September 23, 2019.
14. Dan Kinsella et al., "*Resetting the front line of defense: Managing risk across the extended enterprise,"* Deloitte Insights, September 20, 2018.
15. Casey Crane, "What is homomorphic encryption," Hashed Out, June 20, 2019.
16. Talos, "IP and Domain Reputation Center," accessed September 25, 2019.
17. The Institute of International Finance and Deloitte, *The global framework for fighting financial crime: Enhancing effectiveness & improving outcomes*, accessed October 31, 2019.
18. Frank McKenna, "11 companies that teach machines to detect fraud," Frank on Fraud, February 21, 2017.
19. Tanmay Tiwary, "Fraud detection using artificial intelligence to triple by 2021: Study," TechCircle, June 26, 2019.

Acknowledgments

The authors would like to thank **Timothy I. Murphy** of Deloitte Services LP and **Chris Bostock** of Deloitte LLP for their contributions to this article.

About the authors

Don Fancher | dfancher@deloitte.com

Don Fancher has 30 years of experience assisting clients on matters including forensic investigations, dispute consulting, intellectual property services, and reorganization services. He has testified as an expert witness in federal, state, and bankruptcy courts. He has also provided assistance in licensing negotiations, enterprise and technology valuation, market and industry assessments, and intellectual property portfolio management. Connect with him on LinkedIn at https://www.linkedin.com/in/jdfancher/ and on Twitter @jdfancher.

Tim Erridge | terridge@deloitte.co.uk

Tim Erridge has a demonstrated history of cybersecurity advisory experience, both in industry and in a consulting capacity. His expertise ranges from governance and risk strategy, ISO 27001 and security policy, through to the full breadth of modern cybersecurity operations including threat intelligence, preventative architecture and solutions design, vulnerability management, as well as devising advanced detection and response strategies. Connect with him on LinkedIn at https://www.linkedin.com/in/tim-erridge-453617/.

Michael Shepard | mshepard@deloitte.com

Michael Shepard oversees a wide variety of anti–money laundering, sanctions, and financial crime–related projects and investigations primarily at global and US financial institutions. Prior to Deloitte, he was head of financial crime compliance and deputy general counsel at a leading full-service US retail national bank, partner in the white-collar crime practice of a major law firm, and US Department of Justice prosecutor. Connect with him on LinkedIn at https://www.linkedin.com/in/michaeldshepard/.

Rob Wainwright | rwainwright@deloitte.nl

Rob Wainwright is a renowned global security executive and keynote speaker. He was formerly executive director of Europol, driving its transformation into a world-class security institution. He pioneered the use of data and technology to drive a better response across Europe to cybercrime, terrorism, and other major threats. In 2018, he was appointed Knight Commander of the Most Distinguished Order of Saint Michael and Saint George (KCMG) by Her Majesty Queen Elizabeth II. Connect with him on LinkedIn at https://www.linkedin.com/in/sir-rob-wainwright-68429838/ and on Twitter @rwainwright67.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Don Fancher
US and Global leader, Deloitte Forensic | Partner, Financial Advisory | Deloitte FAS LLP
+1 404 220 1204 | dfancher@deloitte.com

Don Fancher specializes in assisting clients on matters including forensic investigations, dispute consulting, intellectual property services, and reorganization services. He is based in Atlanta.

Tim Erridge
Director, Risk Advisory | Deloitte LLP
+44 20 7303 3872 | terridge@deloitte.co.uk

Tim Erridge is a cybersecurity director focused on financial services and insurance, specifically leading transformation programs in advanced security operations, leveraging hands-on practitioner experience. He is based in London, United Kingdom.

Michael Shepard
Global Financial Crime Practice leader |Principal, Risk and Financial Advisory |Deloitte Transactions and Business Analytics LLP
+1 215 299 5260 | mshepard@deloitte.com

Michael Shepard's practice focuses on anti–money laundering, sanctions, and financial crime–related projects and investigations primarily at global and US financial institutions. He is based in Philadelphia.

Rob Wainwright
Partner, Risk Advisory | Deloitte Risk Advisory BV
+31 882880032 | rwainwright@deloitte.nl

Rob Wainwright is a leading partner in North and South Europe's cyber and financial crime practices and was formerly the executive director of Europol, the EU's law enforcement agency coordinating global operations against cyber, criminal and terrorist networks. He is based in Amsterdam, Netherlands.

Tim Murphy
Senior manager| The Deloitte Center for Integrated Research| Deloitte Services LP
+1 414 977 2252 | timurphy@deloitte.com

Timothy Murphy is a researcher and analytical scientist at Deloitte Services LP, developing thought leadership for Deloitte's Center for Integrated Research. His research focuses on managerial implications of behavioral sciences within workforce and marketplace.

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Prakriti Singhania, Nairita Gangopadhyay, Preetha Devan, Aparna Prusty, and Anya George Tharakan

Creative: Adamya Manshiva

Promotion: Alexandra Kawecki

Cover artwork: Charlie Largent

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.