Deloitte.

Forensics and the Fourth Industrial Revolution

The value of an analytics-driven approach

Beginning about 250 years ago, humankind began to experience a series of industrial revolutions; from the first industrial revolution of steam power in the 1700s, to the second which saw the advent of electricity and internal combustion about a century later, and next to the third which benefited from digital technology at the close of the millennium.

Then within just a decade, we saw the beginning of the Fourth Industrial Revolution to—which represents the technology breakthroughs of the past two decades that are transforming how people live, work, and interact. Whether it be smartphones and social media, algorithms that prioritize our buying patterns, or the promise of autonomous vehicles and connected devices—all represent the "fusion of technologies that is blurring the lines between the physical, digital, and biological spheres."[1]

These advances bring benefits but also challenges, and one of the most significant and darker challenges is new and more technologically sophisticated fraud and financial crime. From accounting scandals such as Enron to the Bernie Madoff Ponzi scheme and, more recently, to the rapid increase in cybercrime, industrial/technological advances have enabled bad actors to commit increasingly more sophisticated acts of malfeasance against individuals, corporations, and society at large.

The problem is as simple as it is pervasive. Corporations must contend with a constant stream of technologies and increasingly large data sets, all of which create the tools and opportunity for criminal activity. How can corporations keep up with and address the constant stream of technological threats to protect themselves, their customers, and stakeholders?

The answer is that they cannot.

Technology has weaponized financial crime by equipping the less sophisticated with tools to run scams with unsettling ease, while offering more-seasoned criminals a wealth of creative tactics for more harmful incursions. Corporations that try to react to each incident will likely become overwhelmed.

A potentially more effective path for corporations is to adopt a proactive, integrated, analytics-driven investigations and fraud risk management infrastructure that embraces a holistic approach to legal, risk, and compliance operations.

The challenge of growing threats

Protecting data, intellectual property (IP), and finances is a growing priority in business board rooms and the highest offices of governments, as criminals proliferate and adapt to more sophisticated controls and monitoring. As data volumes continue to increase, so does the potential for data to be stolen and misused. An estimated 1.7 megabytes[2] of data will be created every second in 2020, for every person on earth[3] By 2025, data creation is predicted to reach 163 zettabytes or 163 trillion gigabytes.[4]

Effective antifraud programs, systems, and controls have been shown to significantly reduce fraud losses, but even organizations that have them can encounter investigation hurdles. One impediment is overreliance on rules-based testing. Such tests typically assess and monitor fraud risks across a single data set, giving only a yes or no answer. Investigators scan data for potential fraud triggers, such as threshold-exceeding payments or round-dollar transactions. One risk of this approach is the potential for numerous false positives. Also, sophisticated schemes underway in lower tiers of the financial structure can be overlooked, discoverable only through advanced analysis of factors such as profit margins or location data.

Information silos further impede analytics-aided investigative efforts. Organizations often struggle to balance the need for locally-tailored processes with the potential benefits of integrated data sharing. In the process, they can unintentionally create barriers to investigative exploration. For example, a company looking into possible employee fraud might analyze time and expense reports but overlook clues in travel agent data or public social media. Analysis of travel agent data can help determine if the employee took trips for which no expenses were submitted, a hint that off-the-books funds were used. In addition, social media analysis can uncover activities on the trip that shed light on certain transactions.

The huge, growing volumes of unstructured data present another challenge. Videos, images, voice, emails, and text files are potentially invaluable in an investigation. However, they are difficult to crack with traditional investigative approaches and tools.

Finally, legal, internal audit, and compliance organizations are often overmatched in the fraud wars, relying on manual processes and ad-hoc data analysis at significant dollar and time expense. While most organizations are susceptible to criminal ingenuity, those that lack robust antifraud capabilities are predictably worse off, suffering twice the median fraud losses of those that have controls in place.[5]

---

1 The Fourth Industrial Revolution: what it means, how to respond," Klaus Schwab, World Economic Forum, Jan. 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

2 For reference, a high-quality picture is usually 2-3 megabytes

3 Data Never Sleeps 6.0," Domo infographic, https://www.domo.com/learn/data-never-sleeps-6.

4 The value of data: forecast to grow 10-fold by 2025," Information Age, April 2018, https://www.information-age.com/data-forecast-grow-10-fold-2025-123465538/

5 "The Staggering Cost of Fraud," 2018 Report to the Nations, Association of Certified Fraud Examiners, https://www.acfe.com/rttn2016/costs.aspx

Elements of an integrated approach

Encouragingly, technology advancements in the Fourth Industrial Revolution are enabling businesses to better identify and investigate attacks and head off future strikes. An integrated, analytics-driven investigation approach is an important component of exploiting these advancements. For example, technology that improves efficiency, risk awareness, and contract management in a legal organization can free attorneys to focus on more productive, strategic priorities. Also, legal and the business can assess risk and implement tools and procedures to manage exposures more effectively.

Core elements of an integrated, analytics-driven approach include:

Data integration—A fundamental capability of an advanced analytics approach is the integration of structured and unstructured data from internal and external sources into risk models. Structured data alone often provides a severely limited view of patterns that might point to fraudulent activity. Likewise, when data is only available in organizational silos, the links between potential patterns may be hidden. Development of integrated data marts (also known as a subject oriented database) can bring together structured and unstructured data from across the enterprise. Combining this data with data from external sources such as watch lists and social media offers a broader picture of activities and transactions. Applying advanced analytics to this data, experienced forensic investigators can often piece together a scheme with fewer false positives.

Predictive tools—Predictive tools can help investigators discover the root cause of problems faster and more effectively. Artificial intelligence, machine learning, and statistical concepts of cognitive analytics, in combination with skilled forensic investigation, can unlock secrets to fraudster motives and methods. Along with more rapid issue resolution, this approach can improve the sensing capabilities of investigators, helping them reduce the reoccurrence of problems.

Refined risk scoring—Transactions don't commit fraud—employees, vendors, customers, and other external actors do. Advanced, data-driven models incorporating text analytics and network analysis enable organizations to rank risks at the individual or entity levels, rather than the transaction level. Employing statistical concepts rather than arbitrary risk ranking presents a broader picture of an entity than test-by-test analysis.

Attention to organizational requirements

The longer fraud perpetrators go undetected, the greater financial harm they may cause. Meanwhile, recovery becomes more difficult with time.

Organizational factors that can impede fraud detection and avoidance include overwhelming data volumes, scarce forensic analytical skills, and the expense of needed technology and training. Also, an organization that hires data scientists to conduct fraud analysis may discover such individuals can crunch numbers but lack critical domain knowledge.

How effectively an organization uses analytics tools to ward off attacks is, in part, a function of its maturity as a crime-fighting operation. The ability to conduct an analytics-driven investigation begins with determining where an organization resides within a maturity model that captures the people, process, and tool dimensions of fraud analytics and forensics. Factors that contribute to analytics maturity include how often the organization conducts analysis, the types of tools it uses, and whether analysis is conducted in silos or in an integrated, enterprise-wide manner.

An important consideration in evaluation of analytics capabilities is the commitment of different business units across the enterprise. Functions such as marketing, customer experience management, and supply chain typically have strong analytics operations. Those operations could be good potential sources of help in ramping up investigative capabilities.

Keys to analytics-driven efficiency

Across industries today, artificial intelligence and robotic process automation are freeing up resources for critical initiatives, to rapidly streamline processes, and to develop other competitive advantages. Those capabilities can also be used to support risk and compliance efforts. For example, analytics can be applied to a company's whistleblower hotline to assess the risk impact of each identified issue and provide insights about the various issues raised over time.

An ongoing monitoring system that uses artificial intelligence to analyze mountains of data can assess specific areas of risk to the enterprise faster and more accurately than previously possible. Natural language processing and data abstraction can support development of a true contract lifecycle management system that helps create, negotiate, and execute contracts, all while analyzing both the process efficiency as well as the ongoing risks and compliance associated with those agreements over time.

These and many other transformational capabilities are being developed now with Fourth Industrial Revolution technologies. Legal, risk, and compliance functions that adopt these capabilities are likely to have

a distinct advantage over those that do not, enjoying many potential benefits, from the speed at which they adapt to new opportunities and threats, to the way they analyze and model various risks, to the ability to sense risks and opportunities far more in advance than they ever could before.

Transformational technologies

The duration of typical fraud schemes amplifies the need for new types of technologies—and new uses of technology—to uncover, deter, and respond to threats. Research has found more than half of frauds continue at least 18 months before detection, and nearly one-third go undiscovered for two years or more.[6]

Predictive analytics and continuous monitoring are among the most transformational technologies. Predictive analytics tools include advanced analytics techniques, such as machine learning and cognitive computing. Continuous monitoring refers to an automated process designed to flag suspicious transactions or entities. The process may be rule-driven, for example producing an alert anytime a transaction exceeds a threshold amount or is processed outside of normal business hours.

Continuous, however, is a relative term in this context. Real-time, 24/7 monitoring may not be necessary, especially to detect complex fraud schemes. Frauds typically evolve over time, and a single transaction may mean little. In contrast, monitoring the transaction trend on a monthly, weekly, or other basis could speak volumes.

Proactive monitoring that leverages predictive analytics can help identify trends, as well as new schemes not based on known fraud instances. Rather than relying on rules, analytics produce new insights driven by what the data is showing.

Attention to several considerations can help organizations increase the value of analytics and monitoring activities:

Embrace the deterrent effect. People are incentivized to fall in line when they are being watched, whether by humans or machines. The mere existence of monitoring, properly communicated, can help nurture compliance with protocols, policies, and guidelines.

Consider in-house monitoring. Conducting monitoring in-house instead of turning to an outside party offers several advantages. One is better data security and privacy. Also, data can be analyzed more easily on a continuous basis. Plus, in-house personnel can learn both how the solution works and how to maintain it. If the solution needs to be expanded in the future, the work can be done within the organizational infrastructure and not require additional data exporting.

Tailor solutions. Disparate organizations, industries, and locations can present different exposures and threats. In addition, the formats, complexity, and availability of data can vary widely. Understanding trends and working with business units to adapt fraud solutions to specific situations can help capture greater value from monitoring activities.

Leverage existing resources. Some of the tools needed to conduct monitoring may already exist within the organization. Resources in areas such as finance and supply chain may be adaptable to risk management needs. Along with avoiding duplication, such collaboration can enhance communication among different parts of the business, strengthening fraud awareness.

Explore tool options. Different risks can require different analytical tools and approaches. *Unsupervised modeling* creates statistical profiles of normal transactions or entities and then identifies outliers from these profiles. *Supervised modeling* uses documented fraud cases and output from unsupervised modeling to learn fraud characteristics, classify new observations as fraudulent, and detect what human observation cannot. *Network analysis* may be required if an apparent scheme involves collusion. And, *natural language* processing may be a valuable approach if important clues appear to lie in unstructured text.

Involve stakeholders. Risk management is no longer just the responsibility of internal audit and compliance. Business units and other functions have roles to play in identifying, understanding, and addressing fraud risks.

Conduct a proof of concept. Monitoring solutions are complex and touch disparate parts of the business. The investment and time required to implement them can seem overwhelming. Instead of casting a wide net, a highly-focused approach to monitoring can pay dividends. A specific proof of concept can aid understanding of how a solution works and the value it could potentially provide.

---

[6] 2018 Report to the Nations, Association of Certified Fraud Examiners, https://www.acfe.com/rttn2016/about/executive-summary.aspx

A technology/analytic enabled culture drives future challenges

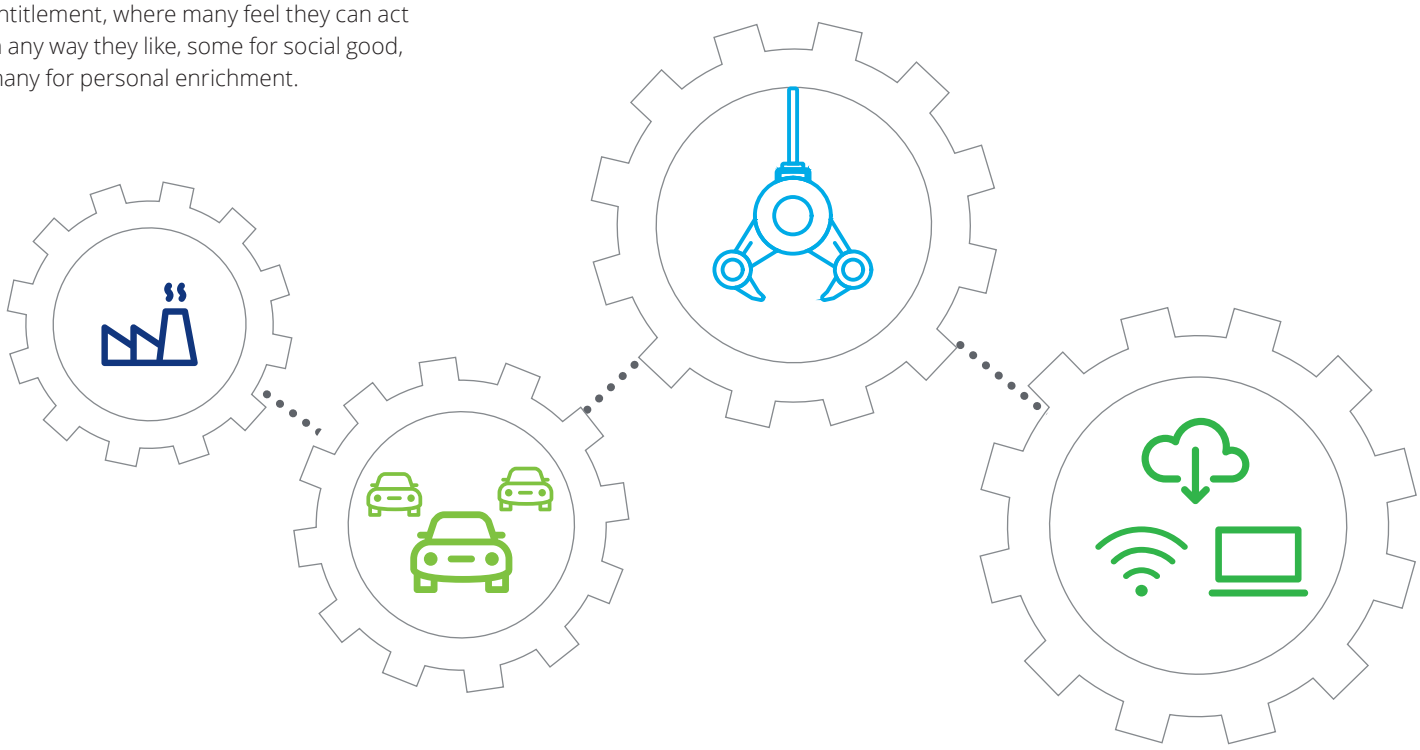
It is ironic that present day analytic/technology advances have transformed our culture in a way that has brought us full circle back to the start of the Industrial Revolution in the 1700's. The original impact of the Industrial Revolution was to centralize means of production from individual households into centralized facilities like factories. Culture consolidated around cities and towns and away from individualized, agrarian lifestyles.

Today, 21st century technology has enabled people to once again disengage from a centralized culture, allowing them to work at home or offsite, connected only by the networks they choose or that their current employer promulgates. They are armed with powerful tools that still allow them to impact the economy and the corporations that drive them as individuals as well as collectively through networks. This in turn has fostered a culture of data analytics entitlement, where many feel they can act in any way they like, some for social good, many for personal enrichment.

It is this culture that now underscores and drives many of the bad actors victimizing companies, governments and organizations, putting legal, risk, and compliance functions on the frontlines of this ongoing struggle for the foreseeable future. It is critical the companies adopt an integrated, analytics-driven approach to risk mitigation and incident response if they are going to be prepared for the inevitable incursions to come. With the right level of tone from the top, empowered governance and investment, I believe aspects of a technology-enabled culture will always provide more benefits to corporations and the world's economy than to those intent on exploiting us all!

Let's talk about the impact of analytics on your organization:

Don Fancher
Principal | Deloitte Risk and Financial Advisory
US & Global Leader | Deloitte Forensic
Deloitte Financial Advisory Services LLP
+1 404 220 1204 | dfancher@deloitte.com



Deloitte.