Safety in the digital era
Approaching fraud and security with big data analytics
Intelligence Quarterly is published quarterly by SAS Institute Inc. Copyright © 2015 SAS Institute Inc., Cary, NC, USA. All rights reserved. Limited copies may be made for internal staff use only. Credit must be given to the publisher. Otherwise, no part of this publication may be reproduced without prior written permission of the publisher.

SAS and all other SAS Institute Inc. product or service names are registered trademarks or trademarks of SAS Institute Inc. in the USA and other countries. ® indicates USA registration. Other brand and product names are trademarks of their respective companies.

SAS is the leader in business analytics software and services, and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS helps customers at more than 75,000 sites improve performance and deliver value by making better decisions faster. Since 1976 SAS has been giving customers around the world THE POWER TO KNOW.
Stem the tide of security risks and financial crime
Prevent fraud, achieve compliance and preserve safety with analytics

Cyberattacks. Terrorism. Fraud and abuse. The threats are diverse, but the response is the same: Stop cybercriminals, fraudsters and other perpetrators from destroying profits, eroding customers’ trust and compromising citizens’ safety.

But stopping them is difficult if you can’t see the possible entry points or blind spots. They’re always changing tactics and looking for opportunities you might have missed. So you have to view your organization or agency in the same way intruders do. With analytics, you can look three or four moves ahead to find the doors and windows before they do.

In this issue of Intelligence Quarterly, we look at the different ways big data analytics is used to improve the many facets of safety and security. For example:

• **Preventing cyberattacks.** Companies harness analytics to understand who the bad players are, quickly detect malicious behavior and take early, effective action (Pages 3 and 6).

• **Combating financial crime.** Institutions use big data and analytics to examine past patterns of fraud, predict current and future fraudulent activity, and determine relationships between conspirators (Pages 16 and 26).

• **Thwarting terror threats.** Analytics empowers organizations to counter terrorist activities, limit their potential risks and consequences, and prevent harm to citizens (Page 28).

In short, analytics plays a vital role in countering the changing nature of threats to safety and security that the world will face in the years to come. Continue reading to learn how you can be better prepared.
Analytics

Billions in losses every year can be prevented.

The quicker criminals adapt, the higher the cost to financial institutions. But using the right technologies to fight fraud, abuse and improper payments is changing all that. With our predictive analytics, you can detect suspicious activities sooner, move beyond ‘pay and chase’ benefits claims, identify security threats before they occur and even improve the efficiency of programs.

Read the paper sas.com/StateOfFraud
Five steps companies must take to beef up cybersecurity
Advice from a former government intelligence director

It used to take an army to invade a country. Today, an Internet connection and some programming skills create what Ray Boisvert calls “asymmetrical threat factors” that are likely behind some of the most headline-grabbing data breaches of the past two years.

But it isn’t just credit card numbers that are at risk. Municipal water supplies, the power grid, and critical research and innovation are all potential targets of cybersecurity attacks. “Small, previously insignificant actors who would normally have very little capability now have disproportionate power,” explained Boisvert, CEO and founder of I-Sec Integrated Strategies (ISECIS), and the former Assistant Director of Intelligence for the Canadian Security Intelligence Service (CSIS).

After laying out the grim realities, Boisvert spoke to the problems corporations are having in acting quickly on the issue. With the exception of financial institutions, the C-suite can be distracted by other pressing matters – from acquisitions to supply chain problems, Boisvert said.

“They’re disinterested in managing what many see as the nuts and bolts of business activities and are prone to sending the issue of cyberattack down the chain of command. Small and midsize companies don’t think anyone would bother attacking them, and thus don’t take necessary precautions. Municipalities don’t have it on their radars, and universities are horribly unguarded. It’s not in their DNA,” said Boisvert. But universities are increasingly connected to the business world,
The solution lies in harnessing data and methodologies in ways that help organizations understand who the bad players are and quickly detect malicious behavior so they can take early, effective action.
Weapon of choice: Cyberanalytics

Cyberanalytics can help organizations meet two of their biggest challenges: coordinating cybersecurity efforts and producing practical metrics to quantify the effectiveness of those security efforts. Cyberanalytics can also:

- Provide near-real-time analysis that automatically generates attack alerts while simultaneously dramatically reducing the number of false positives.
- Aggregate, correlate and merge data from all relevant network devices and other sources to provide enhanced network domain and situational awareness.
- Detect and score the severity of possible attacks before they happen to support prevention and timely interventions.
- Provide early recognition of anomalies in network traffic and uncover otherwise hidden relationships and behavior patterns that might indicate low and slow attacks.

Analytics contributes to a holistic view of the entire chessboard — where the pieces are located, both white and black. This holistic view can help organizations better understand, use and protect their data, regardless of volume, condition, state or location.

noted, "will leave you unprotected and potentially stranded after an attack occurs — and it very likely will." Most critically, companies need people who understand the behavioral side of cybercriminals and hackers, and not just the technical part of the solution.

“Many of us have lived in a world where the rule of law and honesty are the basis for business dealings," Boisvert said. "Many in the rest of the world don’t get that, and don’t follow it.”

Rather than pouring millions of dollars into bigger and better firewalls and more anti-virus software, Boisvert sees cybersecurity as a task for analytics that can help organizations tease out the proverbial signal from the massive Internet noise around serious threats. The challenge is to identify the right threat vector related to the most valued elements an organization holds dear. The organization will only be successful if it has technology to quickly digest huge streams of data in real time so that it may begin to see patterns that can thwart further fraud.

What’s the future of cyberrisk in banking? Find out in this report: sas.com/iq-bankingcyberrisk
Data-driven cyberthreat detection

A cybersecurity case study

Web attacks. Electronic espionage. Network or point-of-sale intrusions. Payment card skimmers. Denial of service attacks and even insider misuse. Cybersecurity threats run deep and affect all industries, exploiting vulnerabilities, destroying profits and eroding customers’ trust.

The vast amounts of sensitive data collected and stored today are attractive targets. Disrupting the operations of mission-critical systems might be the work of school-age boys down the street or highly trained employees of unfriendly nations. Motivations may differ, but it’s clear that cyberattacks are growing in sophistication and intensity.

Compromised by cybercrime

A few years ago, the high-security network computing system of a large US information services provider was hacked by some enterprising teenagers. The incident was a major blow to the company’s IT security establishment, as it had invested heavily in bolstering the security infrastructure following an earlier breach. As it turns out, the company was learning the hard way what many in IT security now have come to accept: Your network is only as secure as its weakest link—the user.

The company housed a large database of personal data, including sensitive, private information such as Social Security numbers, as well as individuals’ public record data. The database was primarily accessed through the web by the company’s myriad customers, ranging from law enforcement agencies to private debt collectors.

The forensic investigation revealed that the security breach and the subsequent exfiltration of personal data were
Insider threats: A growing problem

Cyberthreats are not just external. Some of the worst damage has been done by insiders. Every organization that entrusts its employees, partners or contractors with access to sensitive data and resources faces the risk of insider threats. Despite in-depth background checks and the hiring of well-intentioned individuals, there’s a real possibility that anyone at any time could abuse this access and trust. People face difficult financial situations, changing ideologies, fluctuating stress levels and more—all variables that can trigger unexpected behavior. And before you know it, your organization is compromised.

But not all threats are intentional. Users may unknowingly download spyware via email or accidentally violate a policy that leaves their organization vulnerable. Couple these threats with ongoing cyberthreats and the ease with which bad actors can gain access to internal networks via legitimate (and stolen) credentials, and it’s easy to see why the insider threat problem is a complex challenge.

Who are the perpetrators of unintentional breaches? Most of the threat comes from outsiders, but breaches can also come from state-affiliated actors, committed insiders, business partners and involved multiple parties.

executed through a legitimate account and credentials of a state law enforcement officer. The officer’s endpoint machine was compromised by the hackers, who lured the officer into downloading a keylogger—a keystroke recorder that captures the user’s activity—via a phishing scam.

Blocking future intruders
Smarting from the costly litigations and the massive public relations backlash that followed, the company sought a better, data-driven and analytically derived intrusion detection system—one that would augment and complement its existing security.

Under guidance from the SAS Advanced Analytics Lab, the customer initiated a project to demonstrate the value of analytics and data mining in detecting malicious user activity within the customer’s network. Project data included:

- Web and system logs of user activity, such as login and logout, search and browser transaction history.
- User metadata, such as name, organization and other organizational details.
- Call center and service logs, such as requests for changes.
- A variety of other data, such as blacklists of users and IPs.

The company used behavior-based analytics to detect unusual and extreme user behavior. This included the use of historical activity or usage patterns to establish “normal” behaviors that can be used to monitor future activity.

The detection engine uses a variety of analytical methods, including simple business rules that tracked known suspicious user behavior; univariate and multivariate anomaly detection that utilized peer group comparisons; and link analytics that identified potential collusive activity. Alerts generated by the detection engine are displayed in a security dashboard used by the analysts in the company’s security operations center.

Security analysts agree that the detection engine provides a new perspective they never had with their existing security tools. Of particular value are the aggregated views of not only the user, but the IPs, businesses and groups of linked users, as well as intuitive threat risk scoring. Initial results validate many of the known threats that the security team was already tracking, and the system will generate alerts on a near-real-time basis.

Drive detection with analytics
As this company learned, being able to detect and prevent potential data breaches is crucial. Analytics provides the ability to process and get insight from the volumes of disparate data and stay ahead of cybercrime.
Intelligence for action
How three countries use analytics to deter threats, combat crime and protect the public

As greater volumes of data become available to governments throughout the world, they each face the same dilemma. Namely, how to manage and exploit the increasing sources and volumes of data to prevent and deter crime, terrorism and other threats.

Successful operations are able to make use of this vast and varied information to maintain an understanding of the broader intelligence picture. By collecting, managing and analyzing information, intelligence organizations are better able to keep citizens safe and secure. The real-world stories that follow illustrate how public security groups in three countries are doing just that.

Intelligent sharing
In a country experiencing sectarian and insurgent-fueled violence, the government as a whole managed security-related intelligence data in a piecemeal, ad hoc manner. Security and intelligence agencies couldn’t access potentially valuable information gathered and held by other groups, leading to an incomplete understanding of threats and limited ability to protect the population.

To change things, international advisers worked with local police and intelligence agencies to develop a standard intelligence format. Such an approach would allow the agencies to share relevant data with each other as well as reserve items deemed too sensitive for dissemination.

Working with SAS, the advisers helped secure a military aid package that provided for a complete, countrywide intelligence data sharing network. With the network in place, the country’s agencies and police forces will be able to better anticipate threats and target individuals and networks that represent a threat to its citizens and general stability.

Intelligent security
As part of a major transformation program, a security organization in the Middle East will use SAS® for Intelligence Management to oversee its complete intelligence life cycle for up to 5,000 concurrent users. The intelligence platform will also include SAS® Enterprise Case Management to create a standard environment and process across the organization for core records, tasking, search and investigation — all critical business processes that have been fully presented in Arabic to ensure maximum usage.

In addition, considerable data integration efforts will ensure the organization has all the relevant data it needs through a single interface. The complete solution,
Comprehensive intelligence management

SAS for Intelligence Management helps turn data into information, information into intelligence and, where required, intelligence into evidence. With SAS, public security agencies can rapidly and securely collect, evaluate, grade and manage intelligence gathered from big data sources. Specifically, you can:

- **Proactively manage the growth of data volume, velocity and variety.** Access, integrate, cleanse and standardize data. Integrate data from virtually any source and interactively exchange data between different platforms.

- **Derive essential meaning from big data to build the complete intelligence picture.** Analyze unstructured data and perform entity extraction and ontology management. Reveal unknown and abnormal patterns of behavior, and apply link analysis to reveal relationships between entities.

- **Ensure effective management of your intelligence.** SAS supports all the key stages of the intelligence life cycle – planning, collection, processing, analysis and dissemination – making it easier for agencies to direct, track and audit information as it moves through the system.

- **Reduce the time you spend managing your data.** Effectively manage data and use real-time alerts and notifications to ensure the correct users are able to act upon new intelligence.

- **Secure your intelligence.** Information access control is based on individual roles and responsibilities through our role-based security model.

Intelligent policing

One of the UK’s largest police forces deployed a SAS intelligence platform across the entire enterprise. The mission-critical system:

- Contains 12 million documents and 9 million structured records.

- Is used by more than 40,000 officers and police personnel daily.

- Can be accessed securely by other government agencies.

- Provides real-time intelligence 24 hours a day, seven days a week, 52 weeks a year.

The platform provides integration with confidential, highly specialized and highly secure protected units. With the intelligence management system in place, information can be acted upon in real time to protect the public around the clock.

online

How to manage the intelligence life cycle: sas.com/iq-intelligencepaper

Learn more about SAS for Intelligence Management: sas.com/iq-intelligencemanagement
Project Odyssey is a European Union-funded research and development project to develop a ballistics data-sharing system for criminal investigations. The project chose SAS software to integrate and intelligently mine large sets of ballistics and crime data, helping investigators quickly and efficiently find answers to queries about firearm crime from a central database.

Project Odyssey, partially funded under the EU’s Seventh Framework Programme and coordinated by Sheffield Hallam University (SHU), was set up to explore the challenges of establishing a pan-European ballistics and crime information network and to propose solutions, including a demonstrator prototype system.

The project partners include Atos Origin, Forensic Pathways Ltd., Europol, XLAB, SESA, Politecnico di Milano, National Ballistics Intelligence Service, Royal Military Academy, North Yorkshire Police, An Garda Síochána, and Direzione Centrale Anticrimine - Servizio Polizia Scientifica. The project had a range of key technical goals, several of which involved the use of industry-leading data mining and data integration software from SAS.

The main objective was to develop a database through which gun crime data could be shared with relevant stakeholders across Europe. The system needed to be able to look across all of the appropriate databases. At the same time, the tools and techniques used for uploading, downloading and sharing data had to be secure – and sensitive data kept invisible to certain groups.

The second important technical goal was to allow individual police officers, forensic scientists and other stakeholders...
to enter new data and check for connections to any existing data across Europe, using SAS to find relevant matches.

These queries, typically relating to firearm crime, can then be left indefinitely in the system, which checks at regular intervals to see if new data coming into the system—e.g., the discovery of a weapons cache in Germany—has changed the answers to those queries.

The third level was to look for patterns regarding the kinds of firearms that are being used in crimes in Europe. This would allow cross-region views of gun crime patterns and answer queries such as: Are gun crime patterns in Eastern Europe being replicated in Ireland, or are there connections between criminal gangs in the two regions? Again, the SAS data mining software had a key role to play in discovering relevant patterns and helping analyze peaks and troughs in the level of gun crime in different countries. This information could then be made available to national police forces or regionwide organizations such as Europol.

How it worked
SAS was used throughout the project as part of the back-end project platform to allow SHU, in particular, to carry out intelligent research of the large data sets that were generated.

The project platform supported answering queries to the system. Typically, these were at three different levels. An initial query would draw basic parallels between specific crimes; a second would query features of those crimes; and a third, more general, query would draw parallels between types of crimes and types of weapons, people or places.

This information helps police to follow a range of specific lines of inquiry, address patterns of behavior they need to understand, and draw up strategies, such as preventing guns from being manufactured in one country and subsequently being used for gun crime in another. SAS helped here by enabling investigators to find this kind of information quickly and efficiently.

“One of the key advantages of using SAS software was that it was backed by one of the world’s leading and most highly respected software companies.”

Professor Simeon Yates
Director of the Culture, Communication and Computing Research Institute, Sheffield Hallam University
To ensure the system was made secure, SHU first defined the types of data that police forces typically use in the gun crime domain. It then developed a domain-specific language called the Odyssey Semantic Language (OSL). All queries and data entries that went into the system had to be encoded using OSL, and only validated OSL statements would be processed. All results were also translated into OSL to be processed by the Odyssey user interface. Data mining queries presented in OSL would be processed and sent to SAS, allowing users to securely explore connections between individuals, firearms and specific crimes.

Key benefits
A key feature in the fight against gun crime is to identify large-scale patterns and undertake data mining to highlight key issues. The ability to pinpoint the use of a particular type of weapon or ammunition in crime across Europe can help reveal the source of the arms and ultimately help cut off its supply through police, border security, or international political and economic action.

The SAS platform has been instrumental in helping the project team to achieve this. In particular, it has had a key role to play throughout the project in helping extract and identify meaningful data that the team could use to determine the distribution of gun crime. Ballistics data that appears to map to similar incidents can be called up instantly to show connections between crimes, allowing agencies to share and cross-reference information based on more accurate evidence. Similarly, agents in other locations are automatically alerted to matches on gun and bullet signatures so they can build a profile of crime networks that may affect their area.

“The benefits of working with SAS extend beyond the functionality of the solutions,” says Professor Simeon Yates, Director of the Cultural, Communication and Computing Research Institute at SHU. “For Project Odyssey in general and for us in particular, one of the key advantages of using SAS software was that it was backed by one of the world’s leading and most highly respected software companies.”
Are m-payments a money-laundering dream for criminals?  
Or can you tackle this potential problem with analytics?

In the fall of 2013, US prosecutors took down the global currency exchange Liberty Reserve and charged it with being the largest online money-laundering operation in history, the “bank of choice for the criminal underworld.” More than a million customers used the Costa Rica-based company to wash more than $6 billion, according to an indictment. Besides drug traffickers, it alleged, Liberty Reserve’s illicit users included a wide array of gangsters and thugs, and criminal organizations engaged in credit card and investment fraud, identity theft, computer hacking and child pornography.

But while Liberty Reserve and similar currency exchanges are getting a lot of attention these days from regulators and enforcement agencies, another global money-laundering frontier is not: mobile payments. Millions of people now use their mobile phones to do their banking, especially in developing parts of the world, and their numbers are growing daily. And hidden among them are criminals who some experts believe are engaged in just as wide a range of criminal activity as those using Liberty Reserve, albeit on a smaller scale—for now.

“M-payments will be one of the next big laundering methodologies that we have to confront,” says John Cassara, who spent 26 years as a covert CIA case officer and US Treasury agent investigating financial crimes. “It’s difficult for law enforcement around the
world to get a handle on this problem because there is a lack of understanding and reporting about it. But sooner rather than later, we are going to be confronted with this issue.”

John Cassara
Former CIA case officer and US Treasury agent

“M-payments will be one of the next big laundering methodologies that we have to confront. It’s difficult … to get a handle on this problem because there is a lack of understanding and reporting about it. But sooner rather than later, we are going to be confronted with this issue.”

“People using their phones to do their banking will put a serious dent in credit cards and ATMs, and it will have a major impact on how money is hidden and laundered.” The trouble, he says, is that “nobody is really looking at this in terms of how are criminals taking advantage of this.”

Here’s the problem: Landline-based telecoms and banking networks are expensive to build, which is one reason why only one in five of the world’s 7 billion people have direct access to banks and financial services. But there are 5 billion cellphones out there that could be used as virtual wallets, or personal ATMs. By 2020, some experts predict, there will be 50 billion connected devices, and m-payments will most likely be the most popular form of banking in much of Africa, Asia and Latin America.

Here’s how it works: The best example of m-payments is Kenya, where Safaricom launched one of the first mobile payment programs, called M-Pesa, in 2007 (pesa means “money” in Swahili). M-Pesa now has 15 million users, who transfer more than $1 billion a month in East Africa. Its model is being imitated in more than 50 other countries, including much of Africa, Brazil, Afghanistan and India.

However, the places where m-payments are skyrocketing also happen to be where corrupt governments, transnational crime syndicates and traffickers of all stripes flourish. “This is going to be huge,” says Cassara, who has written two books on terror finance, wrote a State Department report on m-payments in 2008, and now advises governments and multinationals on the subject. Thousands of street-corner shops in Kenya sell mobile-phone airtime, usually in the form of scratch cards. More than 60,000 of them have also registered as M-Pesa agents, far outnumbering Kenya’s 840 bank branches. Annual transactions on M-Pesa are equivalent to more than 20 percent of the country’s...
Customers exchange cash for virtual value that goes into their phone, which becomes an electronic wallet or stored value card. They can then pay bills, buy things, transfer money and, importantly, receive credit on the card. Besides being easy to use, it's usually cheaper than traditional money-transfer services. Foreign workers can be paid by phone, and then transmit the money to their family back home in seconds. Travelers can deposit lots of cash and then simply withdraw it in another country. Many big banks are now rushing to incorporate m-payments, and so are multinationals like McDonalds, Starbucks and Western Union.

Here's where the system breaks down: M-payments are most popular in countries with weak laws and enforcement against financial fraud and money laundering. Customers often need little in the way of identification. The whole process often bypasses a country's financial reporting system. That makes it almost impossible for authorities to monitor m-payments, even if they had the expertise -- which, Cassara and others say, they don't.

And because transactions are made via mobile phones and text messages, there's usually no way to trace them, let alone secure evidence for prosecutions. As Cassara testified before Congress in May 2012, criminals always gravitate toward the weak link in the financial system, and they've now glommed onto m-payments. In Kenya, M-Pesa has been used to launder fake currencies, to bribe corrupt officials, and to facilitate kidnapping and extortion and a range of other crimes. In response, Safaricom started requiring more customer information last year, especially for those using prepaid cards for their phone service.

But such stories aside, there isn't much evidence of m-payments facilitating crime. Cassara says that's only because no one is monitoring the transactions for criminal activity. Financial authorities in Africa, Asia, Europe and the United States would seem to agree, and have been raising concerns in recent reports, official testimony and public speeches. They're especially worried about the rise of m-payments in countries where the informal money-transfer system known as hawala has stymied their efforts to track terrorist financing. In Pakistan, for instance, where 90 percent of adults don't use banks, a firm called Easypaisa has more than 100 million subscribers.

When Cassara travels overseas and finishes one of his presentations, “They're all concerned,” he says. “They all nod their head, they all know [this] is going to be a problem but nobody does anything.”

This article was originally published by Quartz (qz.com) and is republished here with permission.

Learn how analytics can address fraud and m-payments:
sas.com/iq-mpayments

SAS provides identity management capabilities and advanced analytics for risk scoring using rules, predictive models, anomaly detection, network link analytics and association analysis. The result is a hybrid analytical approach that has been proven in the financial and telecom industries to detect fraud early, prioritize threats, and enable companies to immediately act to prevent losses. Plus, SAS’ approach is designed to adapt to the evolving m-payment infrastructure as technology changes.

Learn more:
sas.com/iq-fraudframework
Finding the patterns in financial crime
Laurentian Bank pulls together data to combat fraud and money laundering

Financial crime costs Canadian financial institutions more than $1 billion a year. And while banks’ analytic systems are often very effective at detecting and shutting down suspicious transactions through a single channel, patterns of criminal activity are often very sophisticated and involve more than one channel, account or identity. With a myriad of touch points, including transactional accounts, credit card accounts, mortgages and other financial instruments, along with falsified addresses, phone numbers and other identification information, making connections between the players and their games is very complex.

Laurentian Bank of Canada, which manages more than $33 billion in balance sheet assets and has 3,800 employees across Canada, is redefining the standards for managing suspicious banking activity by integrating three critical components of SAS® Enterprise Financial Crimes for Banking, which allows the bank to pull together the “big picture” of fraudulent transaction networks and their associated identities. It is the first bank to bring together three financial crime solutions—SAS Anti-Money Laundering, SAS Fraud Network Analysis and SAS Enterprise Case Management—to identify potential fraud and money laundering quickly and effectively.

Achieving a comprehensive view of fraud
Combining SAS Fraud Network Analysis into the mix provided the bank with the ability to uncover unknown relationships among its customers, accounts and businesses through the use of link analysis technology upon bank data. This solution enabled the visualization of the relationships identified between entities, uncovering unknown relationships while helping to identify the use of synthetic IDs that may use a common piece of identifying information—a popular tool for analyzing the card application process to better understand and confirm the identity and creditworthiness of the applicant.

“SAS Fraud Network Analysis allowed us to move from a transaction and product view of fraud risk to a complete view of fraud risk at the customer level,” affirmed Isabel Rainville, Senior Manager of Fraud Prevention for Laurentian Bank.

Before the bank combined the power of all three crime-fighting solutions, it used a case management system developed in-house, referred to as GDI. While this system was effective in its own way, it had limitations, particularly with respect to associating identities and cases. For
The benefits of integrating fraud and AML programs

SAS provides end-to-end technology for detecting, preventing and managing financial crimes across business lines. The benefits of this approach are compelling:

• **Avoid duplication of resources and processes.** Consolidating AML and fraud-related technical and procurement support may limit deployment of redundant or incompatible technology, prevent technology silos, and rationalize existing applications and software.

• **Gain a more accurate view of financial crime activity.** With a more holistic view across channels, products and business entities, the organization gains a new vantage point from which to assess risk and detect suspicious activity, as well as understand how well fraud programs are working at an enterprise level.

• **Improve investigator efficiency.** A converged system delivers more accurate alerts, objectively automates the scoring of events and offers a shared platform to view all relevant data to speed decision making. Investigators can find more criminal activity faster, with less cost and effort.

• **Enhance the organization’s reputation with all stakeholders.** By integrating its financial crime management efforts and gaining an enterprisewide view, the organization affirms its commitment to compliance and strong risk management, earning the trust of regulators, shareholders and customers.

The efficiencies have bred more productivity for Laurentian Bank’s financial crimes crew. Because of the bank’s increased effectiveness at spotting irregular transactions, “The numbers are not staying still. They’re going up,” Quevillon says. More staff members must be assigned to handle the increased volume of cases.

The unprecedented marriage of the three solutions was challenging. SAS and Laurentian Bank worked hand in hand to bring the components together, creating a blueprint for other companies in the financial services sector.

By unifying that data under SAS Enterprise Case Management, analysts can view in a single window the relationships between subjects and cases. But the example, if a subject’s identity had multiple phone numbers, addresses or other identifying information, separate subjects had to be created for each instance. And subjects could only be associated with a single case; new subjects had to be manually created, with all that duplicate information, for each case the subject was associated with.

A year into the project, measuring the return on investment is easier on the fraud side of the house than when dealing with money laundering crimes. Fraudulent traffic can be detected in near-real time; but by its very nature, money laundering can only be detected after the fact. “We’re not real time,” says Celine Demers, Manager of Anti-Money Laundering Solutions at Laurentian Bank.

But by getting suspicious transaction reports and unusual transaction reports – whether they’re automatically generated or flagged by bank staff – into SAS Enterprise Case Management faster, analysts can make the call on whether an account should be shut down faster. Such decisions took six to eight days using the previous system. Now they’re made in about two hours, limiting the bank’s exposure.

Using SAS Enterprise Case Management, a single unique subject can have multiple addresses, phone numbers, spellings of names and so on, folded into a single identity. And that identity can be associated, in a variety of roles—subject, victim or witness—across the various cases or incidents that are relevant. “Cross-referencing across several cases and identities tells you you’re dealing with a criminal network,” says Robert Quevillon, Assistant Vice President of Corporate Security for Laurentian Bank.

By unifying that data under SAS Enterprise Case Management, analysts can view in a single window the relationships between subjects and cases. But the
To many criminals, insurance companies make easy and attractive targets for fraud—from single individuals misrepresenting the extent of their losses to large networks perpetrating elaborate schemes. The FBI estimates that fraud costs insurers as much as $40 billion each year.

For CNA, the eighth-largest commercial lines carrier in the US, with annual revenues of more than $9 billion, fighting fraud is critical. According to Tim Wolfe, Assistant Vice President of CNA’s Special Investigations Unit, elements of fraud may be found in as many as 10 percent of the claims that CNA processes.

“We train our adjusters to identify the red flags,” he says, “but we reached a point where we understood that we had an opportunity to do a better job in both identifying likely fraud and avoiding the wasted expense of investigating false positives.”

Within two years of implementing SAS® Fraud Framework for Insurance, CNA had opened 101 new provider investigations with an exposure of $18 million. At the same time, savings generated from the implementation of four predictive models reached over $6.4 million.

Improving fraud detection
CNA operates in four key segments that are most attractive to fraudsters: commercial property, commercial auto, general liability and workers’ compensation.

At one end, workers’ comp cases include disability and medical claims for fabricated or exaggerated workplace injuries. At the other, networks of affiliated providers submit claims for improper, excessive or nonexistent services to rack up thousands of dollars in unearned reimbursements.

“There are new and highly sophisticated schemes emerging all the time, so we were constantly vulnerable to new threats,” says Wolfe. “Our Executive Vice President of Claim, George Fay, who has a strong background in military intelligence, challenged us to find state-of-the-art ways to improve our fraud detection results.”

20 percent hit rate
The company chose the SAS Fraud Framework for Insurance. With SAS, CNA built predictive models and now runs weekly analyses against its structured claims data, as well as text notes from adjusters.

“We have an excellent working relationship with SAS,” says Wolfe. “They took the time to learn from us and truly understand the nuances of claims fraud at CNA so that we could build...
Are you equipped to successfully combat fraud?

In a recent survey of 72 European insurance companies across several lines of business, findings revealed significantly higher levels of fraud detection among insurers using advanced analytics solutions. In fact, results showed that among such insurers, 57 percent had seen the amount of fraud they detected year over year increase by more than 4 percent. In contrast, only 16 percent of those with no solution, or using only a business rules-based approach, saw a similar increase. Other key findings include:

• The majority of respondents already have either a dedicated investigation unit (33 percent) or a team that operates across the insurer’s different departments (35 percent).

• Just over half (54 percent) are actively detecting claims fraud, and 39 percent were detecting fraud at a new business or underwriting stage.

• 81 percent of insurers were using some form of automated detection technologies, with 49 percent using business analytics.

• 21 percent of insurers monitor their fraud levels in real time, while 64 percent monitor their fraud levels on a monthly or quarterly basis.

Read the full research report:  sas.com/iq-insurancefraud

Are you equipped to successfully combat fraud?

In a recent survey of 72 European insurance companies across several lines of business, findings revealed significantly higher levels of fraud detection among insurers using advanced analytics solutions. In fact, results showed that among such insurers, 57 percent had seen the amount of fraud they detected year over year increase by more than 4 percent. In contrast, only 16 percent of those with no solution, or using only a business rules-based approach, saw a similar increase. Other key findings include:

• The majority of respondents already have either a dedicated investigation unit (33 percent) or a team that operates across the insurer’s different departments (35 percent).

• Just over half (54 percent) are actively detecting claims fraud, and 39 percent were detecting fraud at a new business or underwriting stage.

• 81 percent of insurers were using some form of automated detection technologies, with 49 percent using business analytics.

• 21 percent of insurers monitor their fraud levels in real time, while 64 percent monitor their fraud levels on a monthly or quarterly basis.

Read the full research report:  sas.com/iq-insurancefraud

effective predictive models for each line of our business.

“Each Monday morning, after a weekend data run, SAS provides our staff with a percentage of claim alerts that score high for fraud potential. Right now, we’re reviewing about 100 alerts a week, and we’re finding that we are averaging a 20 percent hit rate — about one in five alerts that we review is a good case for investigation.”

One quarter, 15 new cases

Next, CNA uses SAS Social Network Analysis to find broader patterns and connections among providers indicative of fraud conspiracies.

“We have a separate team investigating the provider networks, and SAS is having an important impact there,” says Wolfe. “Not many providers can deliver that visual representation and the links to the individual entities that are potentially perpetrating these larger-scale frauds.

“These investigations can sometimes take months or years to reach fruition. But in just the first quarter, we initiated 15 different investigations. It is expected that finding these fraud rings will prevent up to $20 million in fraudulent claims. SAS found more viable cases than we’d anticipated.”

$6 million savings right away

“Industry research indicates 10 percent of all claims contain an element of fraud,” says Wolfe, and as of the end of 2010, CNA was seeing just 3.7 percent of its claims referred as potential fraud. “That’s considerably below the industry average, and we wanted to find out how much we were missing that wasn’t identified by our adjustors.”

Within two years of full implementation of the models, CNA had seen the share of cases flagged for potential fraud rise to 8.1 percent, resulting in recovered or prevented fraudulent claims totaling over $6.4 million, directly attributable to SAS.

And investigations now operate more efficiently because CNA can focus on high-likelihood cases instead of false positives.

“The implementation of such ground-breaking technology and its impact inspires confidence and gratitude among our customers,” Wolfe says.

“Our employer customers are as eager as we are to root out the fraud,” he adds. “One or two bad claims can put a small company out of business. So they really appreciate that we have this program in place on their behalf and ours.”

1 FBI, Insurance Fraud report:  http://www.fbi.gov/stats-services/publications/insurance-fraud

online

How to stop claims fraud before it starts:  sas.com/iq-stopfraud
Boasting the highest per capita GDP of any of the former Soviet republics, Estonia achieved rapid economic success after asserting autonomy and turning to the open market. The tiny Baltic country’s new way of doing business provided new opportunities for fraudsters looking to bilk the government. Thanks to its prowess in fraud detection, the Estonian Tax and Customs Board makes it hard for the tax cheats to win.

A favorable business climate requires effective government—and the Estonian Tax and Customs Board plays a leading role in making sure it stays that way. The board is charged with ensuring the receipt of budget revenue from state taxes and customs duties, fostering legal economic activities, carrying out national tax and customs policies, ensuring tax compliance, and enforcing customs regulations.

Cost-effective efforts

Among fraudsters, activity primarily involves claiming unearned VAT rebates and circumventing income taxes through illegal underground salaries. According to Ivar Laur, Head of the Analysis Division, and Anneli Nappus, Head Analyst of the board’s Intelligence Department, the organization needed a cost-effective way to pursue suspicious activity while avoiding audits of law-abiding taxpayers.

“We knew that we were losing significant revenue,” Laur says, “but the tools we were using—primarily Microsoft Access and Microsoft Excel—were not adequate for the analyses we needed.

“They were inflexible, slow and error-prone,” he adds. “The cheaters would find loopholes, and it would take us a while to fix those gaps. We needed to be able to change our risk models and features fast enough to keep pace with the cheaters. That’s when we began to use SAS.”

More creative models

Every month, the board receives nearly 25,000 tax filings that require immediate evaluation using a dynamic set of criteria.

“Without SAS, we would have had to manage a constant cycle of software adaptation, which would have been expensive and time-consuming,” says Nappus. “With SAS, we can access live data from multiple Oracle databases. We don’t need to make data requests. We can explore the information and learn more about the data to develop more creative approaches and models to identify fraudulent patterns.”
“We’re correctly analyzing the data to target fraud or mistakes in 80-90 percent of the filings that we audit. That makes our team much more productive.”

Egon Veermäe
Deputy Director General of Core Processes, Estonian Tax and Customs Board

Faster, more accurate decisions
Nappus and Laur report that by using SAS to build and evaluate fraud-detection models, Estonia is improving its ability to pinpoint fraudulent filings.

“Our decisions are much faster and much better because they are based on data, not hunches,” says Laur.

Before SAS, the team had to rely on hunches and intuition. With SAS, they now take decisive action quickly and confidently. “We’re identifying investigation targets and detecting risks as soon as they happen and initiating audits to get to the truth,” Nappus says. “Previously, we could only look for basic irregularities on a smaller set of filings. Now, we can ask more sophisticated questions and analyze a much broader range of filings, so we have greater and more thorough coverage – and it’s faster, too.”

Precise audit selection
Previously, the audit team selected its investigation targets. Today, however, the analysis team is charged with finding fraud candidates. If the wrong cases are chosen – and the audited filings are legitimate – law-abiding taxpayers are needlessly bothered, the audit team is unproductive, and the fraudsters continue to elude authorities.

“If our team only has time to audit, say, 100 taxpayers, you want there to be a very high likelihood of fraud so that there’s revenue recovery and a criminal is apprehended,” Nappus says.

Greater revenue recovery
“SAS is our tool for determining our risks,” says Egon Veermäe, Deputy Director General of Core Processes. “Before we implemented this system, we were spending too many resources on taxpayers who hadn’t made mistakes. As many as 70-80 percent of our audits yielded no problems or recoveries. Today with SAS, among other tools, we’re correctly analyzing the data to target fraud or mistakes in 80-90 percent of the filings that we audit. That makes our team much more productive and allows us to focus on more important things.”

“When we compare what we did before versus what we do now, we’ve noted significant time savings,” Laur says. “Our team is able to review and analyze more data than ever – about five times as much as we did five years ago – more risks, more fields, more ability to discover more possibilities.

“This is much more advanced than what other European countries are using,” Laur adds. “When a new risk type emerges, we have immediate access to the data and can instantly modify our models. We can see how big our risk exposure is and react accordingly. The universality and flexibility of SAS help us adapt in a fast-changing environment. Our declaration forms change every year, and it would be hard to keep up using other tools or systems.”

How agencies can proactively identify fraud schemes:
sas.com/iq-hybridapproach
A recent Accenture citizen pulse survey on policing found that citizens believe police forces still rely a lot on traditional media sources—TV news, newspapers, and radio. Of the citizens polled, though, 72 percent believe social media can aid in investigations and prosecution, 53 percent believe it can improve police services and 47 percent see it as a tool for preventing crime.

And citizens aren’t the only ones who believe social media is a valuable tool for law enforcement. In the European Commission’s Composite Project report, police officers said that they often find information on social media that would have been difficult and time consuming to find elsewhere. Sometimes the information may not even be available anywhere else.

The report is based on “in-depth analyses, interviews and group discussions with IT experts and officers representing the police forces of thirteen European countries.” In the report, you’ll find three best practices for using social media in law enforcement:

1. Move beyond the special-teams approach and educate all officers in simple social media investigative methods.

2. Take your social strategy to the next level—talk to citizens and give them a venue to talk back.

3. Apply analytics to identify suspicious activity and incriminating information.
Build a social investigation machine
The commission’s research found that many police forces are already using social media—reactively. For instance, most forces routinely examine a suspect’s public social media activity for information that can be used in criminal investigations. This public information helps round out a subject’s profile and fill holes in the investigation. For access to private information—like messages, emails or IP addresses—police can often contact the social media provider. (When the provider is based in another country, access may take more time.)

Become a community partner
Establishing a social presence can deliver significant benefits at low cost. For instance, it’s especially useful for pushing information during periods of crisis (when traditional IT systems often become overloaded). It’s also a good way to engage the public in investigations. And the IACP Center for Social Media, a US organization established to support forces in their adoption of social media, says it’s a great way to show citizens that police officers are people who love and support their communities.

Find the hidden nuggets
There’s a downside to monitoring social media, though: The vast majority of social media traffic is just noise. What forces need is a way to sift through the noise to uncover criminal activity and spot concerns in the community before they become problems. This is where advanced analytics comes in:

- **Social media analytics** highlights key topics and uncovers relationships between people, objects and locations of interest.
- **Social network analysis** identifies the people involved, their human networks and the ring leaders.
- **Ontology management** highlights commonalities and relationships between different words and terms, identifying common references from multiple sources.
- **Sentiment analysis** uncovers changing attitudes, highlighting positive, negative, and neutral opinions that may indicate a move from words to action.

It’s the powerful combination of these analytic technologies that lets intelligence professionals effectively use social media to get answers to key questions: Who said what? About what? Who are they influencing? And what might happen next?

In the end, a combination of these three best practices can help improve police efficiency, increase mutual trust and facilitate increased communication and a closer connection with the public—despite shrinking budgets.


**online**
Fighting crime through social media and social network analysis:
sas.com/iq-socialcrimefighting

---

**Social network analysis**
Social network analysis explores the relationships between connected groups and individuals. It can help law enforcement detect and prevent crime by going beyond individual views to analyze all related activities and relationships at a network dimension. With SAS® Fraud Network Analysis, you can:

- Visualize social networks and see previously hidden connections and relationships in a highly intuitive manner.
- Achieve unrivaled detection rates using advanced data network building and analytic techniques.
- Maintain extremely low false-positive rates with true, large-scale network analytics that delivers more alerts that you can act on.
- Evolve from parameter-driven, rules-based systems to neural network and modeling approaches.
- Perform supervised and unsupervised scoring, using predictive analytics to spot anomalies in the data.
- Gain a true enterprise view by aggregating alerts from multiple systems into a single environment.
- Take full advantage of external data sources and customize the solution as needed.

Learn more:
sas.com/iq-fna
Crack down on financial crime with data visualization

Seeing the big picture of data is key in driving prevention and intervention

Across the world, law enforcement agencies are making more intensive use of data visualization technologies. Consider police forces using systems that provide real-time views of locations, layered with crime, traffic, geospatial, weather and other data. As a result, decisions can be based on solid, robust data and resources allocated to guide intervention and crime prevention. Data visualization can make this possible for you, too.

The data your agency holds is the key to seeing this big picture and overcoming the challenge of detecting and preventing crime in an increasingly complex criminal environment. But too much data can have an adverse effect. Data is already proliferating, and much of it is unstructured (text-based) and therefore hard to manage and exploit.

Visualizing the way forward

Without the ability to visualize the big picture, critical information can go unseen, leading to incorrect decisions or no action at all. This, in turn, can put public safety at risk. Data visualization addresses this by providing a single environment to access, visualize, search and analyze the data.

This approach allows you to quickly find answers to key questions within your big data. It also helps you spot trends and interpret visual patterns in data; regularly develop multiformat tactical and strategic reports; and allocate resources effectively to guide...
prevention and intervention. Visual analytics complements the approach, enabling police to dig deeper into the data, uncover hidden opportunities, identify key relationships and make faster, more accurate decisions.

With visual analytics, tactical and strategic reports can be rapidly created for executive briefings using data taken from a wide variety of sources and delivered in multiple formats, including web and mobile-based platforms.

In addition to the straightforward view of the data police have traditionally relied on for investigations, visual analytics helps them see the more complex relationships in the data. For example, it can help your agency understand if there is a correlation between an increase in drug offenses and the way you are deploying officers.

Visual analytics can also be deployed to help police achieve wider benefits for society. For example, motor vehicle crashes cost society an estimated $300 billion each year, and in human terms, the cost is much greater. Police can use visual analytics to uncover crash causes or identify accident black spots so that potentially lifesaving changes can be made.

It’s critical that visual analytics also drives self-service. IT departments may be feeling the squeeze, but visual analytics is intuitive and supports a self-service approach, enabling police to create their own visual reports without help from IT.

Momentum building
Data visualization technology can bring benefits to almost everyone within the police force—and benefits extend into the wider community. The more police are able to see the big picture, the higher the likelihood of crime getting solved quickly. Momentum is now building behind the concept.

As a Principal Technical Consultant with SAS’ global public security team, Pete Snelling works closely with domain experts and clients around the world to develop a clear understanding of the challenges faced by public security organizations and the role business analytics can play in areas including policing, border management and intelligence.
Why big data analytics holds the key to tackling the changing terror threat
Finding the answers without knowing the who, what or when to look for

There are fewer large-scale terrorist attacks today, and what we learned from the big ones has helped us discover several planned attacks before they could be carried out. There’s a shift in the kind of attacks we’re seeing. So what about the lone wolves, like Anders Behring Breiviks and the Tsarnaev brothers? How do we find a trail that leads to those unknowns?

Donald Rumsfeld’s famous comment in a US Department of Defense news briefing in 2002 comes to mind. “As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don’t know we don’t know ... it is the latter category that tend to be the difficult ones.”

While widely mocked, Rumsfeld’s speech perfectly captured the challenge of the time and even more accurately describes the changing threat landscape we face today. Back in the ’90s—before the threat from al-Qaeda was fully understood—the world was one of organized plots involving known groups and financing routes. Then, intelligence services were typically working with “known knowns.”

Known unknowns
Post-9/11, agencies started focusing on “known unknowns.” They concentrated on filling knowledge gaps associated with the new threat from extremism and gathering intelligence to counter that threat.
Getting that information means there must be a starting point—a known organization or set of individuals that can act as a gateway to more intelligence. With organized threats, agencies can ask targeted questions about the organization and its inner workings.

Success is about asking the right questions to build up intelligence and identify the known unknowns. But today, you’re more often dealing with “unknown unknowns.”

According to Rand Corp., few terrorist groups have ever achieved victory. But there are a couple keys to success for terrorists—places law enforcement can concentrate efforts:

1. Religious terrorist groups take longer to eliminate than other groups and rarely achieve their objectives.
2. The largest groups achieve their goals more often and last longer than the smallest ones do.
3. Groups from upper-income countries are more likely to be left-wing or nationalist and less likely to have religion as their motivation.

The authors conclude that policing and intelligence, rather than military force, should be the backbone of any efforts to stop terrorism.

Unknown unknowns
These groups may be operating independently with little or no organization, but they still pose a very real threat. They’re elusive and low profile, so agencies often don’t see them as high risk. So, how do you find the trail left behind by these potential attackers from all of the data you have? The real challenge of the unknown-unknown scenario is that you simply don’t know what questions to ask—or who or what to look for.

Use a big data stick
That’s where big data analytics comes in. Everyone leaves a data footprint behind—bank accounts, travel patterns, phone records and online activity. This kind of data can be your best source of intelligence. And analytics can be your most effective weapon against the unknown unknowns.

The advantage of advanced analytics is that you don’t need to know what you’re looking for. The technology can spot behavior in the right kind of area. It can be particularly helpful when you’re looking for the lone wolf.

Advanced analytics lets you flag individuals who have disturbing behavior profiles—not just the ones who are connected to networks or groups that are already under suspicion.

Analytics gives you a place to start, which is likely to be crucial in countering the changing nature of the threats the world faces. Ultimately, it lets you unveil these unknown unknowns, “the difficult ones” identified by Donald Rumsfeld more than a decade ago.


Learn more:
sas.com/iq-modelfactory
Can analytics help prevent child abuse and fatalities?
Florida uses trend analysis to protect the state’s most vulnerable children

In 2012, an estimated 1,640 children died from abuse and neglect in the US, according to the US Department of Health and Human Services. In Florida, this staggering number caught the attention of the governor’s office, where child advocates wondered, what if data and analytics could be used to help keep children safe and secure?

To answer that question, Florida’s Department of Children and Families (DCF) teamed up with SAS and consulting firm North Highland to analyze nearly six years of data on children that had some contact with DCF. Using de-identified data on more than 1 million children, the SAS analysis considered factors such as prior removals due to sexual abuse, prior removal due to drug abuse, and physical or mental disabilities.

The resulting five-year Child Fatality Trend Analysis is helping investigators better predict the needs of families in crisis.

Some of the key findings include:

- Overall, child deaths within the agency are trending downward.
- Children who received prior service from the agency saw their odds of dying reduced by 90 percent.
- Children who experienced prior removal due to physical abuse had increased odds of death by a multiple of 14.
- Children who experienced prior removal due to parental drug or alcohol abuse had increased odds of death by a multiple of 15.
Albert Blackmon, who works in the SAS Advanced Analytics Lab, recently presented the findings at the Federal Commission to Eliminate Child Abuse and Neglect Fatalities. The commission is a diverse group of experts from child welfare, law enforcement, public health and technology that is dedicated to reducing the number of child fatalities caused by abuse and neglect.

“I was eager to present to the commission on our success in using data to inform the practice of child welfare and protect Florida’s most vulnerable,” Interim DCF Secretary Mike Carroll said. “This recent study has helped us determine which children are at a greater risk and offers an additional tool for DCF and partners to better assess and provide for the safety of children.”

Blackmon believes the analysis can help shift the approach to child welfare from mitigating tragedy to improving outcomes.

“Our research showed the tremendous positive effect of a visit from a caseworker,” said Blackmon. “But child protective services agencies across the country are overburdened. Analytics can help caseworkers identify the most at-risk kids, as well as pinpoint the services that can lead to the most positive outcomes.”

Data from the report was so convincing that Florida enacted a pilot project that deploys two child protective investigators on cases involving the state’s most vulnerable children: those under 3 years old in families with key risk factors. What’s more, Florida is also using the data and analysis to enact policy reforms for child welfare programs.

Going forward, the state plans to include more data sources in future analyses. Additional sources will paint a more holistic view of risks and therefore enable social workers to provide the most effective support programs that yield optimal outcomes.

In a similar program focused on child safety, Virginia’s Office of Comprehensive Services (OCS) uses analytics to ensure that high-risk youth receive the right assistance at the appropriate time – and with the proper cost oversight.

Tasked with providing programs, activities and resources for at-risk children and families, OCS needed a single platform to examine the impact of expenditures and services on outcomes of programs targeting these groups. With a data integration and analysis solution designed by SAS’ Advanced Analytics Lab, the agency is able to:

• Integrate siloed data from multiple sources, including state agencies, local governments and funding streams.
• Produce outcome analysis of services provided for each child in the program. This supports program evaluation and enhancement.
• More efficiently rank and score cases of potential fraud, waste and abuse, mitigating misuse of limited state resources.

Linking program spending with each child and service provider yields a greater understanding of state resources used for children’s services purchased across Virginia. As a result, agency leaders can examine and improve the impact of funding and services for at-risk youth and families.

online
SAS Solutions OnDemand:
\text{sas.com/iq-ondemand}