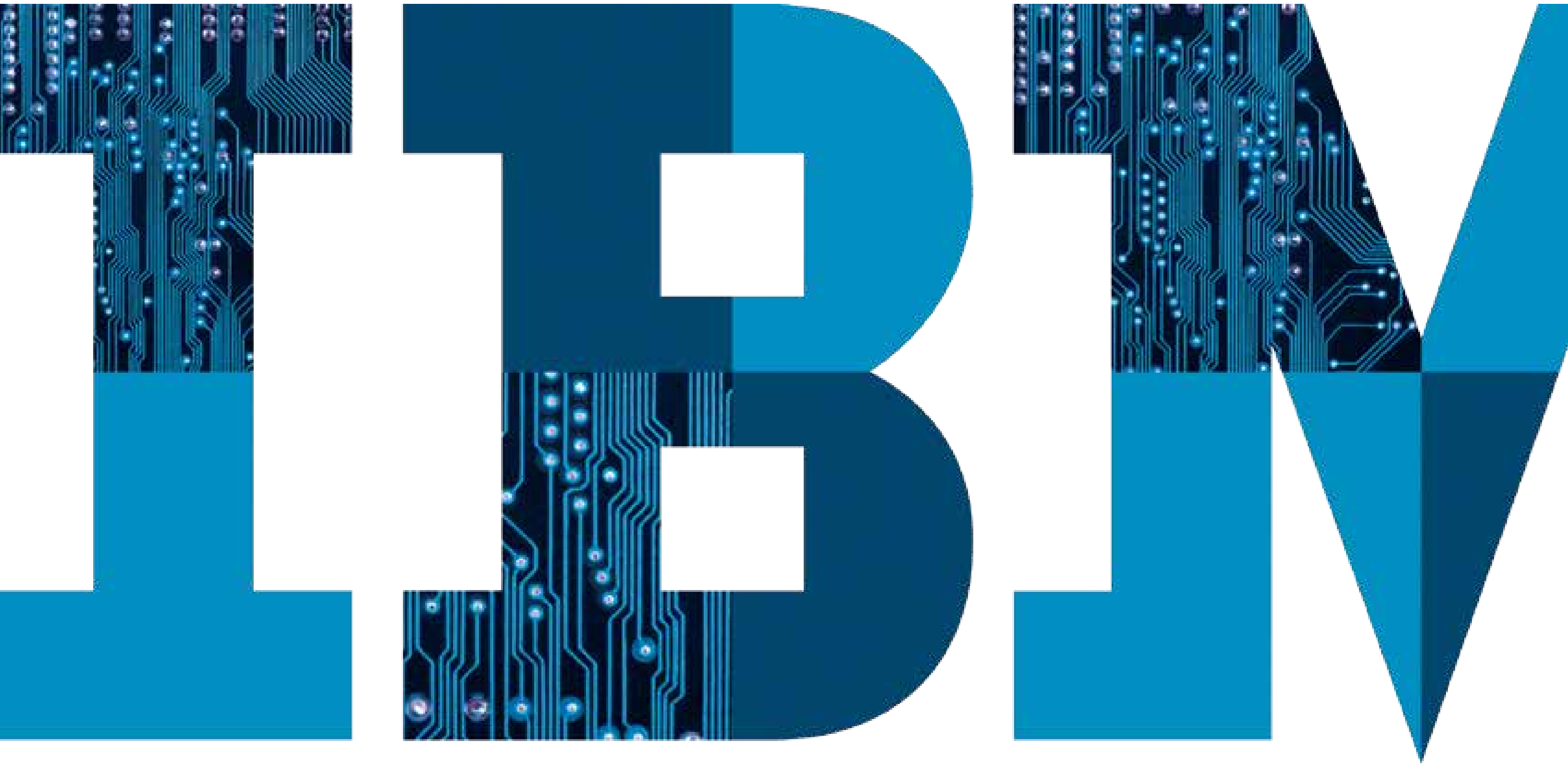
Predictive Threat and Fraud Analytics: Meeting the Challenges of a Smarter Planet



Contents

Introduction

A smarter planet creates new possibilities, as well as new complexities and risks. Thanks to recent technological advancements, including mobile devices, cloud computing and social media, we have created an interconnected, instrumented and intelligent world in which there is virtually infinite access to information. While this has opened the door to new and exciting possibilities, it also provides an opening for new threats and vulnerabilities. From external factors such as national security and the economy—to internal factors such as insider fraud, credit risk and information management—organizations face a multitude of threats every day. These threats are increasing in number and severity, and can cost organizations millions, even billions, in losses.

For example:

- According to a recent study by the Association of Certified Fraud Examiners, the typical organization loses 5 percent of its revenue to fraud every year. Globally, it's estimated that annual fraud losses exceed $3.5 trillion.[1]
- Nearly half of organizations that are victimized by fraud are unable to recover their losses.[2]
- Estimates from National Heath Care Anti-Fraud Association put health care frauds costs in the US at $68 billion annually. Other estimates range as high $230 billion.[3]
- The total cost of insurance fraud (non-health insurance) is estimated at more than $40 billion annually, costing the average US family up to $700 in increased premiums, according to the FBI.[4]
- Globally, the total cost of credit card fraud is estimated to be $5.5 billion. In the US alone, ten percent of citizens have been victims of credit card fraud.[5]

It is therefore not surprising that threat and fraud mitigation has become a top priority for business. In addition to the monetary losses mentioned above, there can also be a significant cost to the reputation and value of an organization that is unprepared for threats and fraud. According to a recent IBM global study of senior executives, 75 percent say that data theft and cyber attacks impact customer satisfaction and brand reputation. And 61 percent say they are they are the greatest threats to their company's reputation.[6]

The best defense against threat and fraud is a systematic approach to reducing exposure and minimizing negative impact. But where do you begin? In an ever-changing world, you must be diligent about managing the threats you are aware of, as well as those yet to be identified. For example, you need to be able to anticipate how an insider might infiltrate your secure IT systems, look for signs of potential terrorist activities, predict the likely impact of future economic events or identify new patterns of fraud—all with a high degree of accuracy.

In this paper we will discuss how to build a proactive threat management strategy based on business analytics technology, and then deploy that information to the individuals responsible for impacting unwanted behavior. You'll see examples of how organizations worldwide are applying business analytics solutions to minimize the negative impact of risk and maximize positive results. You will also learn the practical steps you can take to combat threat and fraud in your organization.

What is business analytics?

The term "business analytics" refers to a comprehensive, data-driven approach that combines the science of predictive analytics with advanced business intelligence capabilities. Predictive analytics uses advanced analytical algorithms to process historical data and create models that can make predictions about future outcomes. Business intelligence capabilities then deliver these predictive insights to key personnel and departments across the organization to help them achieve their goals and objectives.

Each of these technologies is powerful in and of themselves. When combined as business analytics, they provide superior capabilities for improving business performance across a wide range of functional areas. According to analyst firm IDC, organizations that utilize predictive analytics in addition to business intelligence achieve an average return on investment of 250 percent.[7]

Modern business analytics software is easy to use and can be operated by users with different skill levels, from front-line business users to experienced analysts. Businesses across many industries use business analytics to understand their customers, increase profitability and improve operational efficiency and effectiveness. When applied to threat and fraud prevention, this technology provides similar benefits by providing the ability to connect data to effective action by drawing reliable conclusions about current conditions and future events.

Reduce exposure and minimize impact

Mounting regulatory demands, the growth of online transactions and communication, the increased use of mobile devices and the constant shadow of an uncertain economy underscore the importance of proactively managing threats in all their forms—whether related to business, data or events. That means not only understanding what has happened in the past, but being able to look forward to anticipate what might happen in the future, and how your business will respond to these situations. Organizations that do this well can significantly maximize efficiency and reduce the impact of threats, as well as differentiate their business model from those who have not adopted a culture of analytics.

Business analytics is the key to reducing exposure and minimizing the negative impact of the thousands of threats your organization faces every day. It provides you with access to fact-driven predictive insights in real-time, driven by your organization's specific needs.

Today's dynamic environment requires a systematic approach to managing threats. By using business analytics throughout your decision-making lifecycle, you can continuously refine the decisions you make and the strategies you use as an organization to take control and take actions that are based on insight. As illustrated in Figure 1, when you apply business analytics, you become empowered to:

- Define adaptive, forward-looking policy definitions and parameters based on past actions, new challenges and internal or external changes, which can include anything from the weather to evolving regulatory requirements.
- Monitor your environment continuously using a broad range of data from multiple sources; adding new data as needed and learning from your data to develop insights so that you can identify triggers and alerts.
- Detect suspicious behavior such as threats, information breaches, crime and fraud, using business analytics to identify anomalies and determine the likelihood that an action poses a potential risk.
- Prevent or allow a potential threat based on its anticipated impact on your organization, and either eliminate or manage the risk to ensure a controlled, output-driven approach that reduces exposure or loss and maximizes the positive impact of any action taken. For example, a bank can analyze a credit card applicant's information, including credit score, marital status, longevity at current employer and current salary, to determine how these factors into the relative risk of default. The bank may determine that while the likelihood of default isn't high enough to prevent it from securing the credit card, they cannot afford to issue the card at a low interest rate, thereby mitigating some of the risk it is assuming.

As you can see, this cycle is continuous: as you acquire new data, you analyze it and learn from it. The insights you gain then help you improve policies and parameters so that your organization is constantly shielded from negative risk at each stage.

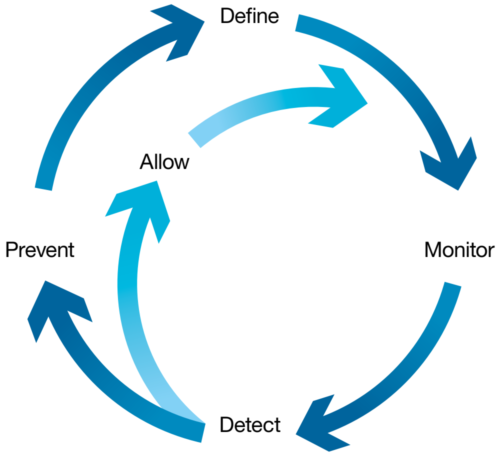


Figure 1: Today's dynamic environment requires a systematic approach to managing threat and risk.

Mastering business analytics is a journey that starts with using the information you have to find insights, and continues through determining the next best action for a particular individual, scenario or decision maker. By applying business analytics techniques organizations are able to identify key threats, accommodate regulations, or refine and monitor policies based on what they know about past events as well as data obtained in real-time.

That can mean, for example:

- Determining that an auto insurance or medical claim is fraudulent as it is processed.
- Sending police into areas most likely to have high crime activity on a particular day based on key predictors such as the weather, previous days' behavior, day of the week and other factors.
- Identifying the person in your enterprise who suddenly seems to be engaged in irregular network and data activity.
- Providing current, customized threat intelligence reporting to specific employees across the organization so they can anticipate and address risks within their areas of responsibility.

Having the answers ahead of time gives you the ability to control what action you take and when so that you can plan, forecast, implement and prevent. Without analytics, you can react only when a threat is identified, which puts your organization into "fight or flight" mode, instead of enabling you to respond in a controlled and formulated way that will ensure the best outcome. This can be very costly to your organization—costly in terms of lost revenue or opportunity; reduced credibility in the eyes of employees, partners and investors; negative environmental impact; or even lives lost.

With a business analytics-based risk management strategy in place you become able to:

- **Access threat information across the organization in real time to determine the best time to accept the risk or stop it altogether.**
- **Make decisions faster and spend less time "putting out fires."**
- **Gain more confidence and trust in decisions that are made.**
- **Reduce costs and make better use of resources.**
- **Build a stronger organization that is resilient to change and ready to exploit new opportunities.**
- **Support business innovation while reducing or maintaining an acceptable level of operational risk.**
- **Avoid negative publicity.**

Identify organizational threats with business analytics

Patterns that point to threats or suspicious behavior are often hidden in huge amounts of data. This is why a proactive approach to threat management starts with analyzing the masses of data your company collects and stores such as transactional data, email, network reports, survey data, constituent information, tax records and call center notes. It's equally important to monitor and analyze the massive amount of information flowing through social media sources such as networking sites, blogs and comment sections of websites.

Business analytics solutions feature sophisticated techniques that enable your organization to analyze both the “structured” data found in tables and databases as well as “unstructured” text, including content found in email chains, chat forums, social networks or survey data. In contrast to rules-based analysis and detection methods alone, business analytics can identify relatively unusual behaviors, even those with subtle differences that other methods often miss. And because new schemes continually emerge and change over time, this process also helps identify new threats.

This allows organizations to combine a diverse range of data types, including data that is specific to your industry in terms of benchmarks or external data. Business analytics gives you the ability to combine a wide variety of data dimensions, types and sources on an ongoing basis. This makes it possible to quickly and reliably detect inadvertent signatures from hackers, criminals or terrorists generating new cyber chatter or trying new tactics to gain access to sensitive information, or to determine the risk of granting an individual a credit line. Different techniques can be used to help you decide which next best action you should take.

Once you have an understanding of your data, including what constitutes normal and unusual behavior, you can develop key predictors, or indicators of potential threats, that can be used alongside your key performance indicators to highlight areas of concern for your business or organization. You can then begin to base strategic and operational decisions on predictive intelligence that not only shows future outcomes and behavior, but also details the factors that influence those events. This increases your ability to proactively stop threats before they occur.

Business analytics also enables organizations deliver the models and business rules that support consistent, automated decisions at the “point of impact.” This could mean deploying analytic results directly to key people through business intelligence reports, dashboards or other meaningful visualizations such as graphs or maps. Employees receive customized reports that address their particular area of concern, and are able to drill down into the data to find root causes and gain deeper insights for predicting and preventing the negative consequences of threats.

These insights can be also embedded within operational systems such as websites and call centers to drive smarter decisions and actions that are aligned an organization’s overall strategy and goals. This capability provides a critical layer of optimized decisions where a company’s staff or automated systems interact with customers, prospects, suppliers or partners. Information about results is then used to refine predictive models and future recommended actions.

Let’s look at some areas in which business analytics-based risk and threat control strategies are particularly effective.

Eliminate insider threats

For most organizations, data has become an invaluable asset— the lifeblood of their operations. Access to this data is available to an expanding user base, including employees, business partners, suppliers and customers. IT infrastructures are more extensive, more complex, more distributed—and more accessible. This interconnectedness affords many benefits for businesses, government agencies and consumers alike—but it also introduces a great deal of potential risk. Companies and government agencies must answer to stringent regulatory requirements and protect intellectual capital from competitors or subversive political entities. And consumers are typically most concerned with the potential for identity theft and other privacy violations.

The WikiLeaks scandal involving the US State Department is an ideal example of one of the primary challenges to data security: the authorized insider threat. In this instance, massive amounts of secret documents— including thousands of embassy cables and hundreds of thousands of documents relating to the war in Afghanistan and Iraq—were copied by authorized users to CDs and DVDs and sent to WikiLeaks.

Intrusion analysts at a national government agency are often flooded with several million events per day—many of which are mapping requests or information gathering, rather than actual threats. This large number of events makes detecting real attacks or potential problems difficult. Using IBM Business Analytics software, analysts can focus on the alarms most likely to be cause for concern, in one instance reducing the number of events requiring manual review by 97 percent in a single 30-day period.

Authorized insider threats are not unique to the government or the military. Virtually any organization that possesses sensitive business information such as earnings releases, merger and acquisition plans, marketing plans, research and development data, personally identifiable information, or sensitive internal emails are at risk.

One of the greatest areas of concern regarding the breach of sensitive data is within the healthcare industry. There have been a number of high profile cases recently in which personal health information was stolen due to insufficient safeguards. For example, the Utah Department of Health reports that social security numbers, addresses, diagnoses, dates of birth and other confidential information for 780,000 patients was compromised during a hacker attack in 2012. This is not an isolated incident. Government figures show that hundreds of thousands of patient records have been stolen from a variety of healthcare organizations.[8]

Both the WikiLeaks and healthcare breaches demonstrate the value of implementing business analytics technology for the prevention of data theft.

Reduce credit card risk

In today's turbulent financial market, credit card issuers need to know as much about their customers as possible. They need to understand the factors and behaviors that indicate whether a potential customer is a good credit risk, as well as patterns or trends that point to the probability a customer or applicant will miss payments or default. In addition, they need to devise more sophisticated strategies to keep the good customers and limit the risks associated with unprofitable ones. IBM Business Analytics software allows organizations to build credit models that are based upon a more refined segmentation strategy that takes into account customers' unique and individual data, ensuring that credit policies are aligned with customers' level of risk to ensure the most profitable outcome.

A private and independent banking institution in Switzerland improved the performance of its credit risk management system by implementing a new credit risk scoring system based on IBM Business Analytics software. This solution enabled the bank to improve the management of credit risk and the overall collection procedure, and has reduced unpaid debts by 15 percent.

Detect and prevent fraud

Fraud is an expensive problem that costs industries and countries billions of dollars. The range of fraud, and the resourcefulness of fraudsters, poses a daunting problem for those charged with its detection and prevention. Yet these criminal activities have one thing in common: each of them leaves a trail of behavioral and transactional data — insurance claims, mortgage or benefit applications, healthcare submissions, tax returns and so on — which are filed alongside information from legitimate interactions. Conventional analytics can be used to detect fraud after it has happened. IBM Business Analytics software can forecast what is likely to happen in the future, as well as detect events as they happen. Consistent fraud intelligence is provided to the people on the front lines of the business to catch fraud in the act, or even prevent it before it takes place.

- The anti-fraud agency of a southern European country implemented IBM Business Analytics technologies to significantly improve the speed, effectiveness and ease of fraud detection thanks to accurate, automated identification of high-risk taxpayers.
- Leading healthcare organizations around the world use IBM Business Analytics solutions to minimize the impact of fraudulent claims by ensuring early detection of likely instances before payment occurs.
- Claims and warranty departments can reduce costs and improve supplier relationships by redirecting fraudulent warranty claims and presenting this information via reporting methods inside of claims systems.

Minimize inventory loss

Business analytics helps identify products, store conditions, personnel or customers who may be linked to stock shrinkage. Shrinkage solutions from IBM provide retailers with insights into product and store performance around stock control and fraudulent activities, and can help increase the profitability of store operations.

Assess network outages

Business analytics can help telecommunications companies or large retailers improve network asset management outcomes by predicting which network will fail next, and the impact this will have on operations and customer experience. IBM Business Analytics solutions ensure that organizations can take quick action to repair at-risk, high-traffic networks, enabling them to avoid the risk of downtime, as well as customer dissatisfaction and lost revenue.

Prevent energy fraud

Energy fraud can be difficult to detect and cause major financial losses for energy agencies and higher prices for consumers. IBM Business Analytics solutions help prevent energy fraud and theft by detecting suspicious activity based on distribution, consumption, pricing and smart meters and then determining appropriate intervention strategies. They also help agencies better allocate their investigative resources, predict high-risk areas for fraud and theft, anticipate recurrence risks and increase customer satisfaction decreasing the costs associated with energy theft.

Protect national borders

Protection against threats often begins at border crossings, airports and in harbors. IBM Business Analytics solutions help agencies identify which containers entering a port could contain unwanted/dangerous materials, which passengers on an airline should be investigated more thoroughly, or predict the risk level associated with vehicles at land crossings. Predictive analytics enables agencies to make optimal use of inspection staff, increase detection rates and ensure better protection of the country and its citizens.

Border crossing analytics

One large country with approximately 300 border crossing points uses cameras to record the registration plate of every vehicle that attempts to cross. Once the plate is read, screens in the crossing control booth advise supervisors to either let the vehicle pass or direct it to the secondary inspection area. If a vehicle is selected for secondary inspection, information is sent to the mobile device of the inspector showing the likelihood of each risk type (drugs, weapons, contraband, illegal immigrants, etc.), providing the inspector with guidance on what to look for. Vehicle selections, risk assessments and inspection outcomes are recorded to enable ongoing reporting on inspection rates by risk type, hit rates, false positive rates and the amount and value of seizures. This strategy makes optimal use of inspection staff, has increased detection rates, better protects the country and its citizens, and improves the experience of low-risk travelers by expediting their crossing.

Keep communities safer

Police departments and other public safety agencies can use business analytics to combine data from disparate sources and help agencies make the best use of the people and information at hand to monitor, measure and predict crime and crime trends. Business analytics provides insight that lets officers track criminal activities, predict the likelihood of incidents and effectively deploy resources, helping to reduce crime and increase citizen safety and satisfaction. For instance, public safety agencies are now using these solutions to identify sources of crime, conduct robbery investigations, manage repeat offenders and increase the safety of police officers.

The Memphis Police Department deployed IBM Business Analytics technology to provide unparalleled insight into criminal activity and crime trends as they occurred. Now, the department can change tactics and redirect patrol resources as needed to prevent crimes and catch more criminals in the act. The program has reduced serious crime by 30 percent, cut violent crime by 15 percent, increased conviction rates fourfold—and realized an 863 percent ROI, based on an assessment conducted by independent analyst firm Nucleus Research.[9]

The same technology can also be used by educational institutions to make their campuses safer. For instance, IBM Business Analytics solutions can help create what-if scenarios to determine the most effective constraints, policies and intervention strategies to maximize the safety of students and school personnel. Campus security departments can use analytic insights to anticipate the most effective ways to allocate resources to minimize crime. Predictive crime insights can be delivered via email alerts, interactive dashboards and scorecards for consistent intelligence that can be put to good use by officers, supervisors, administrators, researchers, professors in the criminology department and others across the institution’s ecosystem.

As you can see, business analytics solutions enable organizations in every industry to efficiently and reliably analyze the variables related to internal and external threats. Using a comprehensive but flexible set of techniques, including risk scoring and anomaly detection, you can spot suspicious conditions and react quickly to stop fraud or mitigate the consequences. You can also focus your investigative resources on the transactions or events that are most likely to be fraudulent, resulting in increased success rates and reduced costs. And because the models can be updated easily, organizations can continue to detect unusual situations or behavior even when tactics or conditions change.

Manage financial risk

IBM Business Analytics can supplement IBM's established risk management portfolio and help executives make risk-aware decisions and meet regulatory requirements with smarter programs and methodologies. The broad range of capabilities in this area includes solutions for liquidity risk, market risk, operational risk, actuarial modeling, governance, policy and compliance management. Combined with predictive threat and fraud solutions, they provide a comprehensive strategy for streamlining risk processes and ensuring an increased return on capital in a rapidly evolving marketplace.

Identify the next-best action

Business analytics is quickly becoming a pervasive technology in organizations of all types. While usage and adoption may vary from the enterprise level to the departmental level, those moving toward a consistent, controlled approach to managing risks are experiencing significant ROI and benefits.

Some organizations are more advanced in their adoption and use of business analytics than others, but there are generally two types of approaches. Providing insight for decision makers is the top priority for many businesses, and in such cases advanced analytic techniques help to paint a clear picture of what is happening and why—regulatory reporting and making strategic decisions based on key threat indicators, are examples of this type of approach. Other organizations seek to move beyond insight to actually identify the next best action in a mission critical process—such as determining where a police officer should be stationed on a given day, whether a car should be checked at a border crossing or whether an insurance claim is potentially fraudulent and requires further investigation while it is being processed.

Our experience shows that organizations grow in analytics maturity step by step. Many have some type of reporting or analytical technologies in place but then find that these technologies don't adequately address critical business challenges or give the organization full control of the decisions they can or should make. This realization moves the organization to take steps toward becoming more analytically mature through the use of business analytics, which enhances decision-making abilities. Organizations that make this leap are able to differentiate themselves by improving processes and proactively managing their understanding of and responses to threats. We can describe these organizations as "masters"—that is, they are using business analytics in sophisticated, innovative ways to protect themselves from potential harm and using the data they have to their best advantage in their decision making.

> *"On short notice, we're able to shift officers to a particular ward, on a particular day, right down to the shift level. It's a bit like a chess match and the IBM solution is enabling us to make arrests we never could have before."*
>
> — Larry Godwin, Former Director of Police Services, Memphis PD

The most advanced organizations are practicing information-based decision-making to help them manage threats across the enterprise in real time. What is the next best action, based on the information I have? How should I allocate my resources? And how can I ensure that threats are identified at the point of interaction, instead of after the act has occurred? What is the risk that this borrower will default on a potential loan?

Organizations at this level are using their knowledge of what has happened in the past to predict what is likely to occur in the future, and applying that insight to build strategies which enable them to respond appropriately at the point of impact.

- Infinity Property & Casualty Corporation of Birmingham, Alabama, makes business decisions more accurately, more consistently and in less time with business analytics. Since implementing IBM Business Analytics solutions, Infinity has doubled the accuracy of fraudulent claim identification, added $1 million to its bottom line by eliminating about $70,000 per month in third-party collection fees and achieved a 403 percent return on investment from a reduction in claims payments and enhanced subrogation.[10]
- MedeAnalytics, which helps hospitals to optimize the payment collections process, incorporated IBM Business Analytics into its solution so that clients can prioritize which self-pay patients are likely to pay their bills, and focus their collections efforts on this high-yield segment of the population.[11]

Adoption of business analytics for threat and fraud detection can also help your organization succeed with other critical strategies that are often related, such as customer intimacy and operational excellence. For example, when Infinity Property & Casualty deployed business analytics to identify potentially fraudulent claims faster and with greater accuracy, it also experienced significant increases in customer satisfaction. Because the entire claims process was more efficient, legitimate claims submitted by low-risk policy holders could be processed and settled quickly, while suspect claims were flagged for special handling and given the time and attention required to determine whether or not fraud was a factor.

Although you may be at a different stage of adoption, achieving "master" status is an achievable target if you approach it with a solid understanding of how you are currently using data to control threats, and the steps you need to take to reach your ideal level.

> *"With business analytics, we were basically able to close a hole in our pocket where money was leaking out steadily."*
>
> — Bill Dibble, SVP of Claims Operations, Infinity Property & Casualty

Five steps to a proactive threat management strategy

In order for organizations to manage threats in today's intelligent, instrumented and interconnected world, they need to look at how to apply business analytics at the point of interaction, where real-time, pattern-based strategies merge with situational context. This level of transformation requires a series of changes in how an enterprise manages information and then applies that information to achieve its goals.

IBM can work with you to create a road map that includes a series of incremental steps designed to move you towards your threat management goals. We recommend that before you make any decisions concerning specific technologies or solutions, you should be able to answer some critical questions about your organization's current strategy and use of enterprise data:

1. Determine your organization's current threat management strategy: Identify your approach to threats, both as an enterprise and in key operational areas such as finance or customer service, and the types of actions you are currently taking to control threats. Would you describe yourself as reactive, proactive or somewhere in between, depending on the situation or opportunity? How advanced would you like to be in your use of business analytics? How are you using analytics to define the parameters of your policies? Is this process dynamic, enabling you to modify policies as conditions change?

2. Examine how you are using business analytics today. Where are you using it, and how? What types of results have you experienced? Are you accurately recognizing threats and opportunities, and taking preventive measures to cope efficiently with risks? How are you proactively monitoring the activity that is taking place today?

3. Integrate threat management into business as usual and ensure the positive commitment of all stakeholders. Are you able to fulfill your regulatory obligations? Can you leverage data further so that it becomes an asset, and not just a deliverable—that is, something that can be used to drive the organization going forward and to minimize costs?

4. Assess your enterprise and external data. What data are you including in your threat analysis, and what other data should you be including? What types of data are available? Are departments operating in silos? Are you taking advantage of the wealth of information that can be found in unstructured data such as social forums, blogs or internal sources such as emails and call center notes?

5. Identify opportunities for automation and control. Are you proactively determining which types of threats you will allow versus those that you would like to prevent? Are you controlling the outcome when it comes to threats or is it more of a corrective process? Do you have processes or decisions that can be easily automated? Can any decisions be made in real time?

Your responses to these questions will help you begin to identify the areas in which you can start achieving real results that will benefit your organization.

> *"We want to maximize the productivity of collectors by giving them a list of patients who are more likely to pay the hospital back and put the people who are unlikely to pay down at the bottom of the list."*
>
> — David Mould, Ph.D., Predictive Analytics Scientist, MedeAnalytics

Drive insights with IBM Business Analytics solutions

IBM Business Analytics solutions can help organizations achieve all the capabilities described above. IBM solutions are easy to use, do not require advanced technical skills and integrate easily with existing systems and technologies. Leading organizations rely on IBM Business Analytics solutions to help detect and prevent threats and fraud, and keep their personnel across their organization fully informed with the latest intelligence reporting.

With more than 40 years of analytic expertise, IBM SPSS® predictive analytics can help organizations predict with confidence what will happen next so that they can make smarter decisions and improve outcomes. With the full range of statistical analysis, data and text mining, predictive modeling, social media analysis and decision optimization capabilities, SPSS predictive analytics solutions can help your organization anticipate change and gain actionable insights from your data.

IBM Cognos® business intelligence and performance management software provides organizations with the integrated dashboards, scorecards, reporting, analysis, and planning and budgeting capabilities they need to gain and act on fact-based insights. Business users are able to create detailed, customized reports without the need for IT assistance, and can drill down into data to gain more meaningful insights to help them minimize the negative impact of the risks they face.

As fully integrated solutions, IBM SPSS predictive analytics and IBM Cognos business intelligence technologies provide organizations with the powerful capabilities and benefits of business analytics. They can help these organizations achieve actionable business insights and superior performance, ultimately enabling them to successfully execute their strategies and achieve their goals.

Conclusion

Our world is becoming more instrumented, interconnected and intelligent. While these factors create many opportunities for both commercial and public sector organizations, they also present challenges—such as increased exposure to threats.

The most forward-thinking organizations are turning to business analytics as a proactive approach to managing threats because it empowers them to:

- Monitor their environments by including a wide variety of data across multiple sources.
- Detect suspicious behavior to help them identify threats, information breaches, crime and fraud.
- Control outcomes so that they can deliver the best response to reduce exposure or loss and maximize the impact of any action taken.

Through business analytics, your organization can find a way to gain a deeper understanding of your data, and use that understanding to develop proactive resolutions to the multitude of threats and challenges you face every day.

About IBM Business Analytics

IBM Business Analytics software delivers data-driven insights that help organizations work smarter and outperform their peers. This comprehensive portfolio includes solutions for business intelligence, predictive analytics and decision management, performance management, and risk management. Business Analytics solutions enable companies to identify and visualize trends and patterns in areas, such as customer analytics, that can have a profound effect on business performance. They can compare scenarios, anticipate potential threats and opportunities, better plan, budget and forecast resources, balance risks against expected returns and work to meet regulatory requirements. By making analytics widely available, organizations can align tactical and strategic decision-making to achieve business goals.

For further information please visit **ibm.com**/business-analytics.

Request a call

To request a call or to ask a question, go to **ibm.com**/business-analytics/contactus.

An IBM representative will respond to your inquiry within two business days.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
May 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

[1] Association of Certified Fraud Examiners, "2012 Global Fraud Study" (http://www.acfe.com/rttn-highlights.aspx)

[2] Ibid.

[3] http://www.bcbsm.com/content/microsites/health-care-fraud/en/fraud-statistics.html

[4] Insurance Fraud, Federal Bureau of Investigation. (http://www.fbi.gov/stats-services/publications/insurance-fraud)

[5] Credit Card Fraud Statistics, (http://www.statisticbrain.com/credit-card-fraud-statistics/)

[6] 2012 IBM Global Reputational Risk and IT Study, (**ibm.com**/services/us/gbs/bus/html/risk_study.html).

[7] IDC: The business value of predictive analytics, June 2011, (http://forms.cognos.com/?elqPURLPage=4206&offid=wp_spssrc_business_value_of_predictive_analytics_ytw03183)

[8] Infographic: Biggest healthcare data breaches of 2012, Healthcare IT News. (http://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012)

[9] "ROI Case Study: IBM SPSS—Memphis Police Department." Nucleus Research. June 2010.

[10] "Infinity Property & Casualty: Driving the auto insurance industry forward." IBM Corporation, 2011.

[11] "Helping hospitals capture more revenue: MedeAnalytics employs IBM SPSS Modeler to help prioritize providers' collection efforts." IBM Corporation, 2010.