A SERIES OF ARTICLES, WHITE PAPERS AND BEST PRACTICES

The Changing Face of Risk

A Closer Look into the Transformation of the Financial Market

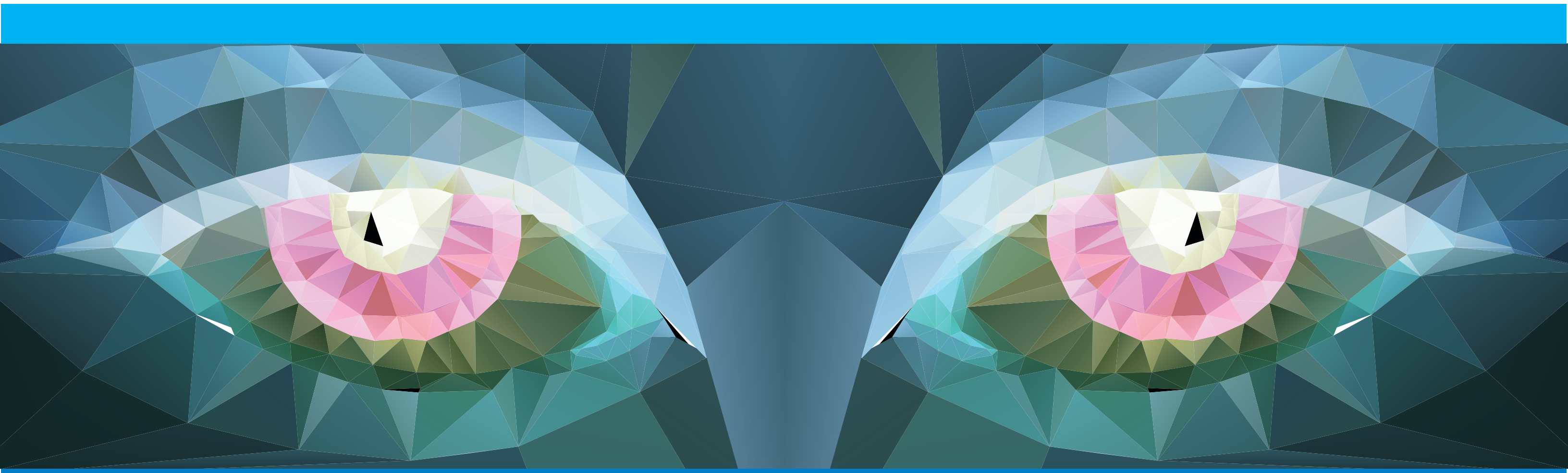


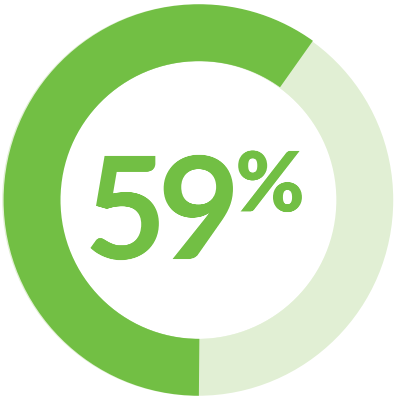
Table of Contents

The Evolution

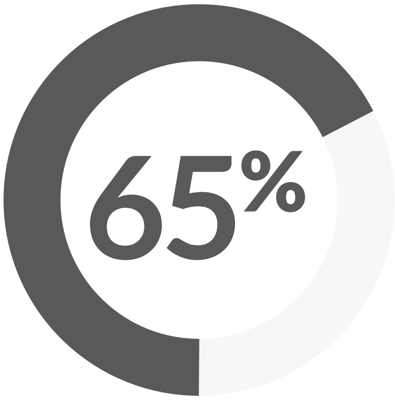
Financial institutions were developed hundreds of years ago to function under two fundamental concepts: to provide loans and accept deposits. Over time, the financial landscape has changed dramatically to meet customer demands by providing fast, friendly, flexible and convenient services. Today's financial institution customer conducts much of their business online and round-the-clock customer service is not only necessary, but is expected and has become a critical piece in the make up of financial institutions.

Security operations and risks have also evolved, forcing leaders to be more cognizant of the security posture of the entire organization. Securing a financial institution has moved from simply securing the perimeter of the bank, to physically protecting and securing ATMs, teller systems, dispersed branch locations, company networks and confidential customer information, from robbery, fraud and other potential threats. In addition, banking institutions must also consider business continuity, its brand and reputation as well as the customer experience when executing a security strategy.

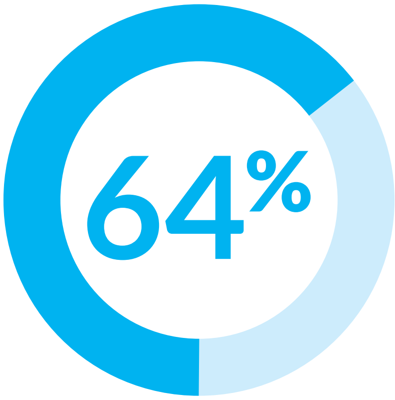
In the past, a security leader was given the responsibility of building a comprehensive technology infrastructure, which primarily consisted of video surveillance, access control and other systems, while fraud investigators were tasked with deterring and detecting risks, working with local law enforcement and other banks to mitigate criminal activity. But security and risk are much greater issues today than ever before, forcing many key players, such as IT, physical and cyber security, risk management and legal to work together to identify and manage risk. Over the years, it has become popular for organizations to employ a Chief Risk Officer who assumes all responsibility of managing risk, security and investigations. Other companies have created a department that oversees risk management, operating under security or IT.



59% of chief financial officers or equivalent in a senior executive position believe that the volume and complexity of risks have changed "extensively" or "mostly" in the last five years. This holds true for organizations of all sizes and types.[1]



65% of chief financial officers or equivalent in a senior executive position admits they were caught "somewhat" off guard by an operational surprise "extensively" in the last five years. This percentage was even higher for large organizations and public companies.[2]



According to the SANS Institute, **64% of financial institutions** cite reducing risk and improving overall risk posture as the key drivers for a robust IT security plan.[3]

[1] http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa_erm_research_study_2015.pdf

[2] http://www.aicpa.org/interestareas/businessindustryandgovernment/resources/erm/downloadabledocuments/aicpa_erm_research_study_2015.pdf

[3] http://www.sans.org/reading-room/whitepapers/analyst/risk-loss-security-spending-financial-sector-survey-34690

Risk and Security Drivers: The EvolMution of Risk and Security Within Markets, Organizations and the Global Climate

Globalization

Large financial institutions are expanding their geographic reach in order to compete in international markets. Remote and traveling employees are a reality in a global environment, which leads to a wider range of threats. Crime, severe weather, terrorist activity and travel delays are a way of life, and companies need to ensure business continuity by maintaining a high level of security to predict and respond to these threats.

Sophisticated networks

Criminals of today are better organized and more knowledgeable of high-tech schemes and tactics that place financial organizations at greater risk than ever before. Organizations are forced to implement cohesive solutions with input from various departments that help to minimize risk. Exposure to risk can impact an entire organization, which leaves executive leadership more concerned than ever before.

Collaboration

Today's data-driven environment requires that various stakeholders, departments, law enforcement and regulatory agencies share information, thereby improving the delivery of a wide variety of benefits. Information can be easily communicated across multiple locations, helping officials identify known criminals and detect patterns of fraud. This collaborative approach minimizes the risks that are inherent with siloed systems and locations.

Integrated solutions

Security officials and employees are empowered to make quick decisions that help improve safety by utilizing open systems that access real-time information from multiple sources. When incidents occur, it is imperative that operators are able to export video data, transaction records and other vital information, aiding in a faster, more effective investigation. Banks are able to maintain compliance through the exchange of ongoing information with regulatory agencies—which is critical to the institution.

Reputation and branding

Word travels fast in today's world, especially with the growth in social media and 24/7 news outlets. Sometimes all it takes is the wrong thing to happen at the wrong time to have an impact on an organization's reputation and brand. Incidents can occur that are extremely embarrassing to an organization driving leaders to extend the coverage of their risk efforts while increasing their technology investment by integrating new solutions to monitor employees and assets.

Technology Latency

Technology changes quickly. Financial institutions must strike a balance between the need to keep up technology innovation and managing costs associated with implementing constantly evolving technology solutions. In the instance of security technology we are seeing financial organizations look to proven best practices adopted by their own IT departments to apply to their security assets as well.

Big Data

Data that is gathered from a wide range of systems must be analyzed and prioritized by financial institutions and communicated to security departments who then implement solutions to mitigate potential risk. Organizations must be prepared to identify valuable data and separate it from non-essential information so that responders are better equipped to react when incidents that have the potential for risk occur.

These factors play a significant role in propelling the idea of "security" from situation management, to comprehensive risk intelligence and mitigation. Because the threat dynamics are changing, the proliferation of threat technology grows and creates new doors to be opened all across the organization. Risk is beginning to go down the same path security and safety are following, becoming just as dominant in influence. The rise of risk management is helping organizations realize new levels of security intelligence and therefore, enhanced situational awareness.

The Role of Situational Awareness

Financial organizations seek out solutions that can help assess intelligent ways to deter, detect and respond to potential risks. Improved information sharing and faster, more effective responses are enabled through the use of intelligent software platforms and solutions, designed to enhance levels of security and bring situational awareness to the forefront. One easy-to-manage solution combines multiple siloed systems into one interface, which enables security and business leaders to view data in a combined format, streamlining the identification of security, service and business trends to gain new levels of awareness across an organization.

Financial institutions competing in a global environment are implementing situational technology that ties disparate systems into one cohesive platform to achieve new levels of situational awareness and information sharing capabilities. Banks—whether a regional credit union or a global entity with locations spread all over the world—are better able to detect and respond to incidents in real-time by leveraging advanced surveillance, analytics, situational awareness platforms and investigation tools. As incidents occur, organizations can more effectively report to other business locations and branches, law enforcement and other agencies by using a centralized situational awareness platform.

$11
BILLION

According to American Bankers Association,
banks stopped $11 Billion in fraud attempts in 2014.[4]

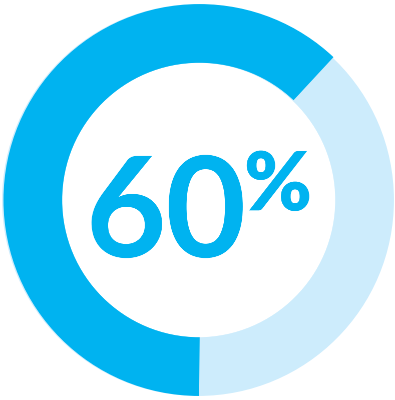
The risk of internal theft and fraud can be mitigated through improved situational awareness. In today's dynamic business environment, passwords for access to computers and individual employee badges for physical entry are required. Actionable intelligence on each user's activities can be obtained through the use of a situational awareness platform that fuses multiple data points together. For example, an alert in the system would be raised if an employee attempts to access financial information on the bank's network when the employee is not actually keyed into the building. Or, if the employee was found to repeatedly open new accounts for suspected fraudsters, officials could keep an eye out for potential criminal activity.

When correlated with other systems, potential fraud schemes can be identified pro-actively. For example, data from facial recognition can be monitored for connections that link to physical attributes from various sources (driver's license, credit card, license plate number, etc.) to validate that an individual is who they claim to be. By utilizing facial recognition technology, banks would receive an alert if an individual opened accounts using fake IDs at multiple branch locations. Additionally, access to certain areas of a building can be monitored and controlled through the use of facial recognition technology.

[4] http://www.aba.com/Press/Pages/012716DepositSurvey.aspx

1,042

According to the most recent Financial Institution Fraud and Failure Report, published by the U.S. Department of Justice, FBI, as of 2007, **the FBI was investigating 1,042 major Financial Institution Fraud (FIF) cases.5**



During the late 1980s and early 1990s, approximately 60% of the fraud reported by financial institutions related to bank insider abuse. Since then, external fraud schemes have replaced bank insider abuse as the dominant FIF problem confronting financial institutions. The pervasiveness of mortgage fraud, check fraud and counterfeit negotiable instrument schemes, technological advances, as well as the availability of personal information through information networks, has fueled the growth in external fraud. In many instances, the international aspects associated with many of these schemes have increased the complexity and severity in the fraud being committed.[6]

Situational awareness platforms help facilitate information sharing across multiple branches, as well as external authorities and agencies for a growing number of financial institutions. Security officials and law enforcement agencies are able to respond and investigate crime and fraud more efficiently and effectively in real-time. Banks must analyze the most critical data points, as big data continues to grow, and technological solutions to help increase security, reduce fraud and ensure longevity in their respective markets.

[5] https://www.fbi.gov/stats-services/publications/fiff_06-07

[6] https://www.fbi.gov/stats-services/publications/fiff_06-07

Mitigating Risk and Enhancing Bank Security: Real-World Impact

The National Commercial Bank Jamaica Limited (NCB) is in the midst of completing the final part of a multi-phased implementation of its security solutions. In 2013, the financial institution decided to further align its focus on mitigating fraud, enhancing investigations and applying advanced situational awareness across its countrywide locations. NCB of Jamaica, the island's largest financial services provider consists of 36 branches and 200 ATMs, uses innovative technology to drive operational efficiencies and enhanced services for its customers.

Using Verint video intelligence and situational awareness solutions to enhance the bank's security operations, NCB of Jamaica has improved security and fraud mitigation efforts at its remote ATM locations and bank branches. At the same time, it has achieved centralized security management across all of its sites. NCB deployed new video surveillance solutions at its ATM sites and branches to monitor all public areas, including entrances, exits and parking lots, as well as cash-handling areas. The bank also leverages IP cameras at its branch entrances and the head of its teller lines, using network video recorders and video encoders to capture high-quality video.

The new solution offers myriad benefits. Now, the fraud department and security personnel are able to view live and recorded video from their desktops to make real-time security decisions. A diagnostic and management application enables NCB of Jamaica to manage DVR properties, passwords and firmware to help deliver superior system uptime, enhanced management control and improved operational uniformity.

"Justification of the business case was simple. With Verint solutions, we have embraced the latest in IP surveillance technology, while still being able to leverage our existing analog infrastructure and easily scale to meet our future needs in a cost-effective way," says Glenroy Findlay, manager of safety, security and environment, NCB of Jamaica. "Further, we found that the solutions required minimal bandwidth to remotely view and download recorded video, enabling us to retrieve archived footage in good time."

In addition, Findlay saves valuable time managing the distributed surveillance system with enterprise-wide health monitoring, audit reporting, firmware management and permissions management. In particular, the automated system-wide health monitoring and diagnostics maximizes systems uptime and allows the security team to focus on investigations.

Today, the NCB of Jamaica is helping ensure its customers and employees are protected, and advancing its approach to fraud reduction, theft prevention and overall investigations while also streamlining operations, improving business efficiencies and reducing costs.

Verint Video and Situation Intelligence Solutions for the Financial Sector

More than 90 percent of the global Fortune 500 companies in the financial market rely on Verint's Actionable Intelligence and Situational Awareness solutions to identify and combat fraud, mitigate risk and ensure compliance. As consumers demand faster, flexible, and more personalized interactions, the financial industry must increase their level of service and convenience while being able to predict and respond in real-time to escalating threats. The Verint financial portfolio provides advanced, unified technology that includes predictive and analytical solutions, data protection, and 24/7 surveillance.

Achieve New Levels of Situational Awareness

The Verint Situational Awareness platform incorporates visualization and actionable intelligence capabilities to help security personnel achieve higher levels of security, compliance and risk reduction. Verint Situational Awareness is an open, unified software solution that helps enhance industry-standard workflows and supports operators in responding to both routine and emergency events. The system combines and analyses device relations, location data, integration, user management and data retention to drive functionality—unifying a wide range of sensors and systems into a centralized, intuitive security and situation intelligence solution.

Video Surveillance

Verint EdgeVMS Vid-Center software serves all video functions including DVR/NVR configuration, live and recorded video viewing, event search, system logs, and firmware and license feature updates. Verint EdgeVMS Vid-Center provides instant alerts, surveillance analytics, and is compatible with the entire line of Verint recorders, as well as mobile and legacy installations.

Enhanced Visibility and Operations

The Verint EdgeVMS network video recorder line is designed for large-scale, geographically distributed operations and boasts robust hybrid analog/IP capabilities and a range of analytic rules. Advanced capabilities include high-quality imagery, optimized bandwidth utilization, a secured embedded operating system and industry-leading interfaces.

Enhanced Surveillance Coverage

Verint IP cameras deliver high-definition video with ultra-efficient bandwidth management, enabling customized H.264, MPEG-4, or MJPEG compression formats with multi-streaming capabilities. Models come in a variety of forms—from fixed body and pan/tilt/zoom cameras to indoor and all-weather IP domes—to accommodate a wide variety of video surveillance application.

Robust Intelligence

Verint Video Surveillance Analytics helps security officials make sense of the vast amounts of video footage and data generated on a daily basis, creating Actionable Intelligence that enables more informed decision processes and faster, more effective responses. The application identifies and generates alerts for a variety of user-defined events relating to people, vehicles and static objects, including ATMs.

Improve Business Performance

Verint Video Business Analytics enables immediate response to customer activity and performance management. Applications include people counting, traffic analytics, customer behavior patterns such as dwell and wait times, and workforce optimization.

For more information on Verint's solutions for financial institutions, visit the company's website.