Looking to the Horizon: The Future of Risk in Banking

Banking faces a multitude of risks that seem to evolve daily. But your institution doesn’t have to be a victim. Find out how you can be more proactive about identifying and managing these risks—and how technology can help keep you a step ahead of potential threats.
A Changing Risk Landscape

Financial organizations across the world face new risks, such as cyber and physical threats, including ATM skimming, identity theft, data breaches, scams, and phishing. Worse yet, hackers often target financial institutions to steal corporate information and transactional data or funds.

Additionally, regulations, such as the General Data Protection Regulation (GDPR) are in play, and banks are required to comply with these growing legalities. Large multinational institutions, in particular, must be able to respond to various regulations wherever they operate.
Evolving Risks

Each day brings new threats, cyber risks or physical attacks, all designed to grasp hold of bank deposits and potentially affect brand reputation.

- **Attempted fraud** against bank deposit accounts reached $19.1 billion in 2016, up from $12.9 billion in 2014.
- **Check fraud** (35 percent of fraud losses) has increased, particularly at larger banks.
- **Criminal networks** are increasingly becoming more sophisticated.
- The introduction of **chip card technology** has propelled an increase in fraud in other areas.

The bottom line is that fraud is always increasing, and it is a constant battle for banks to manage.

**Hear How Delta Credit Union Addresses Risk**

Corporate Security Manager, Kim Hodgkin, shares how his credit union addresses fraud and achieves their business goals.

---

**5 Risks You Should Worry About**

- Cyber Schemes
- Bank Deposit Fraud
- Physical Security Breaches
- Check and Credit Card Fraud
- Criminal Networks
Regulations

With the growing complexity and intensity of cyber threats, it's no surprise that more and more regulations are being developed to protect personal data. The increasing use of the IoT and smart devices has made the transfer and sharing of data easier than ever before, but how can consumers be assured that their most sensitive information is kept secure? Government and industry have answered with regulatory initiatives designed to achieve stronger data protection.
The Impact on You

GDPR applies to all companies processing and holding personal data of data subjects residing in the European Union, regardless of the company’s location. The California Consumer Privacy Act (CCPA) signed into law in mid-2018 also incorporates the same concept as the GDPR, “focusing on transparency, control and accountability.”

Legislation such as the GDPR and CCPA will only become more common as we move toward a universal understanding of data protection and privacy. These regulations greatly affect numerous aspects of an enterprise organization, with one being its security systems and devices. Officials must ensure that they keep a balance between privacy and efficient monitoring and investigative efforts.

“Banks are a repository for the private information covered in the GDPR. Many banks are multi-national and do quite a bit of their business in Europe. They have to pay attention to it.”
Herb Kelsey, Managing Director, Cognitive Strategies

What Changes Are Impacting You?

- GDPR/Regulations
- Advanced threats like imposter schemes and identify theft
- Cyber security
- Bank deposit fraud
- Market competition

READ MORE ON VERINT’S BLOG
SEE RESULTS
Leveraging Big Data

Our world runs on data. And most likely, your business runs on data. Information can be a valuable tool in fraud mitigation and prevention. Learn how to best manage valuable information to boost your fraud reduction efforts.
The Data Problem
Today's security and IT applications generate massive amounts of data and the hunger for more and more data grows daily. The significant interest in data expands as users realize that important information can be derived from multiple sources. In today's age, it is video that is driving the use of data for a multitude of purposes including operational efficiency, situational awareness, marketing and fraud reduction.

The Role of Technology
Big data plays a key role in fraud reduction, helping financial institutions identify security threats and vulnerabilities in real time. With the right information, security leaders and fraud investigators can better mitigate risk, ensure operational compliance, and improve fraud investigations.

A Predictive Model
Over the past year, banks have demonstrated that they are willing to invest in projects and technologies that help improve speed to resolution as well as long-term costs. Access to data is driving an overall trend of moving from simply reacting to situations to proactively identifying the potential areas where fraud can occur and address the exposure before it becomes a problem.

Worldwide revenues for Big Data and business analytics reached $150.8 billion in 2017 and were expected to maintain a compound annual growth rate of 11.9 percent through 2020 when revenues will be more than $210 billion.

Hear from Verint’s Matt Tengwall, Vice President & General Manager of Surveillance and Fraud Investigation Solutions, as he discusses the market today.
Leveraging Data Points

Banks need to develop a predictive model for addressing fraud, risk and compliance. To reach this goal, institutions require tools and data management methods that can help sort through what is important and what is not.
Reduce Risk
The ability to leverage information from multiple sources, systems and sensors is extremely valuable. The data collected from these sources can be used not only to reduce risk but protect a brand, increase operational efficiency, enhance customer engagement, and modernize and automate functions.

Increase Operational Efficiency
The fusion of technology creates a surplus of information, and users seek to gain more insights from this combined data to enhance security and business operations alike. There are significant benefits to leveraging video and security data to optimize operations. For example, leaders can evaluate video to see how to best manage staffing and traffic flow throughout a branch. And this is only the tip of the iceberg: New use cases are being rolled out on a daily basis as users find innovative ways to leverage the intelligence gleaned from captured data.

Integrated applications, which include advanced video analytics, facial recognition, and advanced identification via deep learning, can automatically pinpoint potential breaches and significant events, and send alerts to the appropriate personnel and agencies. This approach can be influential in fusing together critical information that can be valuable to close investigations. Overall, these types of intelligent platforms can deliver a simplified and modernized operating environment.

Enhance Customer Engagement
With further evolution of data-capture technologies, banks will find sources that will enable them to better manage, support and reduce fraud mitigation efforts. Additionally, leaders will find new ways to leverage data that can help improve the customer experience.

Manage Brand Protection
In today’s environment, banks, credit unions, and financial organizations of all types are primary targets for hackers. But it’s not just the monetary loss that these businesses need to be concerned about – there is also a threat to the brand, customer trust, and employee safety. Ensure that you have a plan to address brand protection – that is a topic senior leadership is very interested in.
Selecting the Right Technology

Modern technology solutions can help banks identify security threats and vulnerabilities in real time, mitigate risk, ensure operational compliance, and improve fraud investigations. Intelligent solutions, video surveillance, and centralized investigation management platforms can provide stronger protection from fraud, safeguard assets, and enhance the customer experience.
Advanced Fraud Prevention and Security Solutions

Increased risks from ATM skimming, identity theft, data breaches, scams, and phishing are driving the adoption of new solutions. It's imperative to explore and adopt new tools and technology to address this risk.

Advanced fraud prevention and security solutions help your organization:

- Reduce investigation time.
- Improve investigator effectiveness by allowing them to leverage multiple data sources to enhance the quality of investigations and close more cases quickly.
- Develop automated reports that flag transactions that need to be investigated.
- Create automated alerts that automatically notify investigators when a potential security event occurs.

Banks can gain significant benefits from deploying technologies that aid stakeholders in reaching new levels of intelligence and situational awareness. Let's take a closer look at these technologies.

**Video Surveillance**
Video surveillance is a valuable tool to help understand alarms, incidents and accidents. It adds additional "eyes" to your fraud efforts and can ease collaboration with other banks and law enforcement. Video is an important tool in the investigation process.

**Video and Transaction Data**
Correlating data from video surveillance with transaction systems can enable investigators to find potential anomalies quicker, modernizing a once time-consuming process.

**Video Analytics**
Video analytics automates the video identification process by automatically notifying your team of potential issues. Analytics can also simplify video search and help solve the problem of "too much data" while enabling you to identify the information that means the most to your institution.

**Video Management**
Video management is essentially the core of your video surveillance system. These software-based platforms unify various systems and devices into a single-pane-of-glass view of your video operations. You can view and manage video from other bank locations, manage video and set-up alerts within the video management system to get the best use out of your investment in video surveillance.

**Cybersecurity**
Ensuring the cybersecurity of networked platforms and devices is critical, especially in today's risk-filled environment. Vendors are focusing on hardening their IP-based technologies, but banks also need to address the cybersecurity of their devices internally. Partnering with internal IT teams is critical, especially as cyber criminals and schemes become more sophisticated.
Collaborating for Greater Security

Fraud reduction cannot happen in a vacuum. Collaboration is critical and therefore, IT, security and fraud teams must build partnerships--both internal and external--to best protect the brand.
Collaboration is Critical

As we continue to move toward a world of more interconnected devices, partnerships and collaboration will become more critical to overall success. By working together, whether internally, externally or as an industry, financial organizations can improve overall cyber protection, reduce the opportunity for fraud and ensure the highest levels of safety.

Internal Collaboration
One of the benefits of an increased focus on cyber protection is greater collaboration between physical security and cybersecurity teams. This approach can further propel stronger security measures across an institution’s infrastructure.

True Partnerships
Selecting a service partner is an important component of any fraud reduction program. It is critical that your vendors share the same cultural and business goals as your organization. They should take time to ensure they understand your business and they understand what you are trying to achieve. Ask the questions that are most important for you and your business.

“Fraud reduction cannot happen in a vacuum.
- Herb Kelsey, Managing Director, Cognitive Strategies

Part of the Team
Technology and service partners are valuable additions to your fraud mitigation efforts. Look for those that specialize in your specific market space and understand the challenges of the banking environment. Those partners can help you build a program that incorporates best practices and technology - bringing together the best of both worlds.

Work Backwards
Technology and service providers should understand your business challenges and offer solutions to address them. Look for organizations that will factor your bank’s unique requirements into the solutions they propose.
Future Trends

As the market evolves, so does the bank of the future. It will be more mobile, have more interactive branches, and offer more services and products. Learn about the future of banking.
The Bank of the Future

The bank of tomorrow will look very different from the bank of today. Here are some trends we see occurring in the near future:

- Reduce investigation time
- Improve investigator effectiveness by allowing them to leverage multiple data sources to enhance the quality of investigations and close more cases quickly
- Develop automated reports that flag transactions that need to be investigated
- Create automated alerts that automatically notify investigators when a potential security event occurs

Advanced Services and Products

There is a growing adoption of software-based solutions that allow data to be correlated from multiple systems to deliver increased situational awareness and more proactive fraud reduction efforts. Both large financial services organizations and small-to-medium-sized credit unions are interested in improving security by fusing data from a wide range of devices, including video, audio, social media, access control, building management, license plate recognition software, and intrusion-detection systems. By aggregating data from multiple sensors, banks can enable efficient data analysis, gaining the ability to share information easily within and across branches to facilitate timely response and investigation.

“Our fraud department says that Verint has helped them achieve a time savings in their investigations of up to 85% over previous manual methods. And as we all know, time is money.”

Kevin Owens, Vice President of Security and Safety, VyStar Credit Union

There are many financial leaders focusing on fraud today. Hear how these thought-leaders are paving the way.