Re-organizing for Today's Cyber Threats:
Converging Fraud Risk Management with IT Security

High performance. Delivered.
Banks are facing an urgent need to bring the historic silos of fraud risk management and IT security more closely together to combat mounting data security and cyber threats from increasingly well organized criminal entities.
The past two decades have seen an accelerated rate of product development and technology adaptation within the financial services sector. From the introduction of the first online banking service in the US in 1994, the industry has developed and implemented increasingly innovative services. Customers today benefit from contactless card payments, mobile banking apps and person-to-person payments, to name just a few of these innovations.

The threat for banks however, is that, in tandem with the technological developments underpinning an ever increasing set of new service offerings, organized criminals have been developing multi-pronged strategies to exploit fresh weaknesses and vulnerabilities for fraudulent gain. If we were to think of financial institutions as homes, and organized criminals as potential burglars, then each time banks implement a new product or open up a new channel for customer interaction, this effectively adds a new window or door that could serve as an entry point for those criminals and therefore needs to be secured.

As the IT systems supporting banking services have become more advanced from mainframes in the 1960s, to today’s Web 2.0 and cloud technologies, criminals have become more sophisticated in their abilities to target and penetrate these systems. Today’s organized criminals are deploying a wide array of attack methods, such as screen capturing, man-in-the-middle attacks, trojans, falsifying mortgage applications, card cloning and embedding sleepers within the workforce, among many others.

For financial institutions, particularly in the areas of retail banking and payments, there are enormous opportunities to be gained from enhancing their digital offerings to customers. The overall experience is improved as customers gain greater flexibility in how they manage their finances, while at the same time banks are able to lower their operating costs, and also offer more personalized products and services to customers through better use of data and analytics capabilities.

The challenge for banks however, is to implement these new digital models at speed so they can maintain a competitive edge in the market, but without putting security at risk. To date, the speed at which many banks have evolved their technology and service offerings has been so rapid that their counter-fraud strategies have struggled to keep pace. And looking forward, the expectation is that the pace of change will only increase.

Convergence of Fraud Risk and IT Security

Source: 2015 Chartis RiskTech 100 report, December 2014
The Need for Convergence

Traditionally, banks have managed different categories of fraud within silos.

For example, there may be specific teams dedicated to check fraud, mortgage fraud, credit card fraud and so on. But often, these teams are not sharing data with one another, and they may be reporting into individual heads of fraud for each business line. Ultimately, the chief risk officer (CRO) would tend to be at the top of this umbrella.

Meanwhile, IT security issues, such as those concerned with systems access, tend to be managed solely by the IT function, often under the jurisdiction of the chief information officer (CIO).

As traditional risks converge with new risks such as cyber threats, banks are becoming exposed to security threats that can fall between the cracks of the various silos. Organized criminals are targeting several channels at the same time, aware that many banks are unable to connect the dots and spot wider patterns of behavior as a result of these historic structures and the lack of a holistic approach to risk and security.

Furthermore, legacy information security, event log management, and fraud and risk management software solutions, which still form the backbone of many risk and security architectures, lack the ability to provide deep insights into real-time user behaviors, transactions and data.

If security solutions remain siloed and banks continue to extend their offerings, then sophisticated criminals will simply run rings around them, bypassing existing controls and protections by abusing the business logic across multiple channels. To fight this organized crime, banks need a sophisticated, structured approach of their own. Developing such an approach however will require financial institutions to concentrate more of their budget on developing more advanced solutions to support the future shape of the industry, rather than focusing investments to respond to issues from past transgressions or remediation activities.
The threat of cyberattack is no longer something that can be addressed by individual organizations in isolation.

As the World Economic Forum notes in its Global Risks 2014 report, the increasing interconnectedness of every part of the world’s societies and economies, that rely on the same infrastructure, hardware and software standards raises the prospect of disruptions having systemic impact.

In the future, cyber governance must become a combined international effort. For instance, the growth of the “internet of things” means that more and more devices are now online, widening the reach of cyber connectivity into people’s lives across the world. This serves to create more points of entry for attackers and exacerbates the potential damage that could be caused. At the same time, the complexity of interaction between people and their “connected” devices across the globe is making those impacts harder to predict.

While banks and financial institutions are concentrating on boosting their own organizational defenses, what may be needed in the future is cooperation between nations, their governments and private organizations, to counter the common threats. Fresh thinking is required on how to preserve, protect and govern the common good of a trusted cyberspace.

Organizing an effective international response will not be easy however. Recent revelations surrounding the extent to which national security organizations have allegedly been using the internet for spying threatens repercussions that may make it more difficult to prevent widespread attacks, or contain them when they occur. If there is a breakdown of trust among nations, it could be disastrous for cybersecurity.

In the same way that piecemeal solutions within banks are unable to effectively combat multi-pronged attacks from organized criminals, solutions undertaken without cooperation between nations will fail to address the systemic threats that are emerging.
Integrating Fraud Risk and IT Security

In many countries, recently introduced banking regulations are driving firms to evaluate their risk management frameworks from a more integrated perspective than ever before.

At the same time, leading banks are responding quickly to the emerging threats posed by organized criminals by integrating their approach to fraud risk and cyberattack across the organization.

As they respond to these twin pressures, financial institutions will need to address challenges around people, processes and technology.

**People**

Banks must ensure that there is formalized knowledge sharing between those in the fraud risk function and the IT security function. In addition, they will need to align behaviors around risk management across the organization. Part of the solution will involve adjusting incentives and targets to ensure that both IT security and fraud risk personnel are measuring their performance and effectiveness in this area in ways that are aligned for the desired outcomes of the bank.

The differing cultures, experiences and backgrounds of the stakeholders will also need to be addressed, in order to establish a common level of understanding and use of terminology (for example, a unified taxonomy for risk and controls). The importance of an effective communications strategy in achieving this level of change cannot be over emphasized.

The wider business must also ensure that these two functions are in a position to be proactive, rather than reactive as has historically been the case. For instance, they need to be involved earlier in decision-making processes, especially around the future development of products and services – rather than being engaged at the end of a decision chain. Developing a product or service that cannot be supported does not benefit anyone.

**Process**

At present, many banks manage fraud cases through separate units, using different system tools to log activity. However, this approach does not reflect the way fraudsters are behaving, as they attack the bank from multiple angles in a coordinated manner. Banks must therefore shift to enterprise case management, enabling them to look at every fraud or risk case that arises within the organization as a single portfolio, to protect themselves more effectively.

Another key step is to ensure that there is common governance across risk and IT security. This will involve aligning risk and performance indicators. At the same time, policies must be realigned to ensure they reflect the new aggregation of responsibilities across the two functions. Underpinning this will be a need to re-engineer the management information processes and the key metrics being applied.

**Technology**

The foremost technology priority for banks is to ensure that organizational data is freed from siloes and shared across common platforms. This undertaking must help encompass both structured data, such as transactional and account data, as well as unstructured data, such as email, video, image and social media.

Ensuring that common data standards are enforced across functions will be another key aspect of this shift: at present, a lack of common oversight around data management means that different standards and taxonomies are often applied to the same data by individual business units. In addition, without consistency in reporting, it becomes almost impossible for the board to project organizational risk priorities accurately and respond appropriately. Therefore, a single data governance framework covering fraud and IT security is a critical success factor.

For many leading banks, the chief data officer (CDO) plays a key part in defining the appropriate policies and procedures for data governance.

Advanced analytics technologies provide the ability to gain a real-time understanding of behavior and spot anomalies that indicate threats. These analytics must also be appropriately intuitive and accessible: enterprise dashboards can deliver integrated fraud and security visualization capabilities depicting key risk and control metrics, for instance, with full drill-down capabilities into the source data.
Source: 2015 Chartis RiskTech 100 report, December 2014
The convergence we have discussed is a significant undertaking and clearly cannot be achieved overnight.

As with any business change of this scale, a phased approach will be required. And importantly, will need to be aligned to the strategy and desired positioning of the bank.

So while the sequence of the journey will be dependent upon each individual bank's current structure and culture, there are some common steps that all banks should consider.

Gap analysis and vulnerability assessments must be made to identify any weaknesses in controls and potential opportunities for malicious activity. The results of these assessments can then be used to design a target operating model that effectively protects against those highlighted risks. Once this has been identified, it is important initially to pursue the low-hanging fruit to build momentum and senior management support for the change process. For example, it may be that existing systems already hold some degree of shared data, so this would be an obvious starting point.

In addition, the scale and importance of the transformation may justify the appointment of someone with the appropriate skillset to oversee the change. Some large banks have begun to hire for roles entitled ‘Head of Operational Risk Change’, for instance. And in the same way that criminals today have grown in sophistication by working together in online networks, we expect to see increased sharing of insight across financial institutions, and some common platforms being established, along with laws and law enforcement evolving to enable banks to better collaborate and protect themselves.

While it is likely to take several years before the desired convergence is achieved, what is clear is that leading banks are already moving in this direction, and Accenture and Chartis expect this trend to extend across the industry. In some ways, financial institutions are involved in an arms race to improve their security defenses, but the good news is that there are multiple players involved. The banks that are leading the pack will naturally face fewer attacks, as criminals will always target those with the weakest defenses. And with financial institutions increasingly competing on their ability to act as custodians of customer data, the convergence of fraud risk and IT security will drive their competitive advantage in this area in future too.
Notes


About the Authors

Steve Culp is a senior managing director, Accenture Finance & Risk Services. Based in Chicago, Steve has more than 20 years of global experience working with clients to define strategy, and execute change programs across a broad spectrum of risk management and finance disciplines. Steve is responsible for leading the global group across all dimensions, from setting the strategic direction through to the enablement of local teams operating across diverse markets. In addition, he oversees Accenture’s efforts on large-scale transformation programs across Finance and Risk for some of our most important financial services clients.

Prior to his current role he was responsible for our Global Risk Management Practice, and prior to that he led Accenture’s Finance & Enterprise Performance consulting services for global banking, insurance and capital markets institutions. With his extensive experience in the financial services industries, combined with his knowledge of risk management and the finance function, he guides executives and client teams on the journey to becoming high-performance businesses.

Mark Daws is a managing director, Accenture Finance & Risk Services. Based in London, Mark has more than 25 years of financial services experience, specialized in large, complex, risk, regulation and compliance, and IT enabled business transformation client assignments and work. His deep experience across all sectors of the financial services space includes previous roles as a Technology Consultant leading large and complex Risk and Regulation IT implementations; a Solvency II Chief IT Architect leading the design and implementation of Solvency II solutions; a Forensic Technologist assisting clients in crisis-management situations including rogue trading and sanctions violations and; a Financial Services Regulator focusing on complex and high-profile investigations.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 319,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world’s most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

About Chartis

Chartis is the leading provider of research and analysis covering the global market for risk management technology. Our goal is to support enterprises seeking to optimize business performance through better risk management, corporate governance and compliance. We help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on the broad spectrum of risk and compliance technology offerings. Areas of expertise include:

- Credit risk
- Operational risk and governance, risk and compliance (GRC)
- Market risk
- Asset and liability management (ALM) and liquidity risk
- Energy and commodity trading risk
- Financial crime including trader surveillance, anti-fraud and anti-money laundering
- Insurance risk
- Regulatory requirements including Basel 2, Basel 3, Dodd-Frank, EMIR and Solvency II

Chartis is solely focused on risk and compliance technology giving it significant advantage over generic market analysts.

Chartis Research is authorized and regulated in the United Kingdom by the Financial Conduct Authority (FCA) to provide investment advice.

Visit www.chartis-research.com for more information.

Stay Connected

Accenture Finance & Risk Services:
http://www.accenture.com/microsites/financeandrisk/Pages/index.aspx

Connect With Us
https://www.linkedin.com/groups?gid=3753715

Join Us
https://www.facebook.com/accenturestrategy
http://www.facebook.com/accenture

Follow Us
http://twitter.com/accenture

Watch Us
www.youtube.com/accenture

Disclaimer: This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Rights to trademarks referenced herein, other than Accenture trademarks, belong to their respective owners. We disclaim proprietary interest in the marks and names of others.

RiskTech100® is a registered trade mark of Chartis Research Limited.

Unauthorized use of Chartis’s name and trademarks is strictly prohibited and subject to legal penalties.