A Unified Response to Cyberattacks, Fraud and Financial Crime

These days, virtually all aspects of public life are visible online. With this trend comes abundant risk. Organizations are negatively affected more frequently by cyber-related issues, including cybersecurity intrusions, fraud and financial crimes (e.g., money laundering, bribery, tax evasion). Financial institutions may suffer greater impact from this trend, but other industries feel similar pain and may find lessons to learn.

Criminals are creative, inventive, and discover quickly what works and what does not. If customers are affected by nefarious activity, they do not care how the organization solves the problem as long as it is resolved promptly and effectively. Organizations must be prepared to rally their full resources; however, they often unintentionally dilute their efforts by handling cybersecurity, fraud and financial crimes in separate silos. A new approach is needed.

Illustrating the Problem

According to the Verizon *2021 Data Breach Investigations Report*,[1] financial gain continues to be the most common motivation for cyberattacks (**figure 1**).

Although an enterprise's outlay on cybersecurity is increasing at a staggering pace, the related crime numbers have not slowed and are instead surging.

Expenditures on cybersecurity products and services worldwide are expected to exceed US$1.75 trillion cumulatively from 2021 through 2025.[2] According to the US Department of the Treasury's Financial Crimes Enforcement Network, as of September 2020, enterprises across the United States lose a total of US$1 billion each month due to cybercrime.[3] Such numbers are disconcerting by themselves, but they are even more so in cases of fraud, where additional losses from associated costs may exceed US$3 for every dollar stolen.[4]

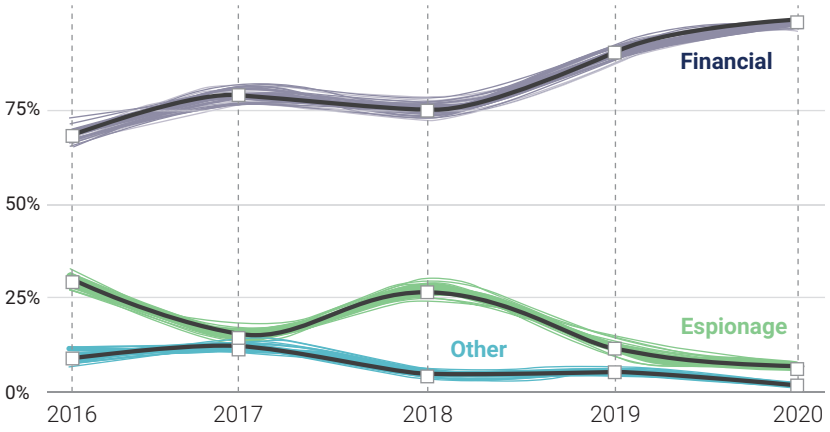
Though numerous examples of cybercrime exist, one famous event is worth highlighting. In 2016, hackers attempted to steal US$1 billion from the Bangladesh Bank by focusing on SWIFT, the system through which banks transfer funds internationally.[5] The hackers used custom-designed keylogger software to steal official bank credentials and a custom malware kit to cover their tracks. They monitored the bank's activity and timed the transfers perfectly so that they would appear genuine. Only through a stroke of luck and a typographical error were the hacks discovered and partially stopped, with losses limited to US$101 million.[6]

VISHAL CHAWLA

Is a cybersecurity and privacy professional. Over the last 25 years, Chawla has advised a number of global Fortune 500 clients on cybersecurity, privacy and operational risk management, spending significant time with boards of directors, C-suite and risk committee members to help them develop an approach to providing oversight to cybersecurity across their enterprise. Chawla is a senior partner at PricewaterhouseCoopers (PWC), focusing on the cybersecurity, risk and regulatory practice. Previously, he was the US leader of Grant Thornton risk advisory practice and a leader of Deloitte's advisory practice in India. Chawla has written for publications such as *Consulting Magazine, Compliance Week* and *The Wall Street Journal*, and is a frequent speaker on cybersecurity, privacy, strategic risk and operational risk.

FIGURE 1

Motivation for Cyberattacks



Source: Verizon, *2021 Data Breach Investigations Report*, USA, 2021, *https://www.verizon.com/business/resources/reports/dbir.* Reprinted with permission.

Hackers have become familiar with cybersecurity vulnerabilities and banking processes, controls and possible attack points. They hold enterprises hostage through ransomware attacks. They steal confidential information, spoof identities and practice social engineering to gain access to and interruption of business operations. Their attempts are boundless.

Typical Approach to Managing Risk

Protecting against risk in organizations requires a delicate balance. Consider the general customer journey in a bank (**figure 2**). Consumers have learned to trust the digital environment and engage in a purely online customer experience, forgoing human interaction with bank staff. The customer can open an account online by submitting vital information such as their name, address, phone number and Social Security number. Funds are deposited, managed and transferred (including payment of bills to third parties) via online processes. But each step leads to risk exposure.

Banks that can meet customer expectations of rapid, cohesive and safe customer experiences will benefit from increased revenue; in contrast, those that cannot will suffer from decreased value and lost business. To compete today, banks must find equilibrium between careful risk management and approving customer transactions in split seconds.

To keep user data and assets safe and secure, banks usually apply three types of countermeasures (**figure 3**):

1. Identifying and authenticating customers
2. Monitoring and detecting suspicious transactions and behaviors
3. Mitigating risk and issues

There is little distinction between the countermeasures in that they are applied regardless of the type of risk, whether it is for a cybersecurity breach, fraud or other financial crimes. Even so, these three types of risk are often managed by different

FIGURE 2

Bank Customer Journey

	Opening a Bank Account	Making Changes to the Account	Transferring Funds	Making a Deposit	Paying Bills
	Customer opens a new account online	Customer makes changes such as address or phone number updates	Customer transfers funds through an online transaction	Customer makes a deposit	Customer pays bills electronically to third parties and vendors
Cyberthreats	Credential stuffing, malware	Malware account takeover	Phishing emails to transfer funds to a criminal's account	Phishing emails, malware, untrusted websites	Malware (eskimming), fake invoices, phishing emails
Fraud	Identity theft	Addition of false beneficiary	Wire transfer to fraudsters' accounts	Fake deposit scams, fake check scams	Person to person (P2P) Automated Cleaning House (ACH) credit, bill pay fraud

FIGURE 3
Typical Countermeasures

Integrated Fraud and Cybercustomer View
Both functions leverage similar data and processes.

	User Screening and Validation	Surveillance and Monitoring	Analysis, Investigation and Reporting
Forensics and Fraud Team	• Validation and verification of user identity	• Automated alerts identify suspicious transactions • Analytics on mobile and other devices to monitor transactions	• Conducting root cause analysis and developing recommendations
Cybersecurity and Privacy Team	• Digital identity • Credential proofing • Credential management	• Defining common use cases to build surveillance models across the ecosystem to leverage data analytics to operationalize through security information event management (SIEM)/ security operation center (SOC)/ artificial intelligence engines	• Cyberfusion center, updating SIEM/SOC, investigation and remediation teams

departments in silos, each with its own tasks, responsibilities and accountabilities.

Criminals do not restrict themselves in this way. They attack at the most vulnerable access points, regardless of department. When banks make their weak spots more secure, cybercriminals move to the next weakest point within the bank's technological structure.

The increasing success of cyberattacks demonstrates the failure of the use of silos in protecting organizations. There is an urgent need for a simple but fundamental change.

Integrated Approach to Risk Management

To more effectively and proactively protect their customers and assets, financial institutions should look at the three types of risk as a unified threat to the enterprise. They must take an outside-in approach that integrates coverage of cybersecurity, fraud and financial crimes. If separate departments are maintained (as opposed to merging all into one), enterprise management must foster collaboration by holding the individual departments equally accountable and tying rewards and penalties to unified outcomes. All departments should work jointly to reduce the risk to the organization while also helping drive better customer experiences. The more closely these departments can work (with the option of merging to a single entity), the more advantageous the results. Integration can save money, reduce gridlock among controls and enable innovation. It has also been shown to reduce the risk associated with cybercrime.[7]

Enterprises that have achieved a more complete integration are seeing benefits. One international bank chose to fully merge all crime-related operations and, as a result, has decreased its operating costs by approximately US$100 million while gaining a better understanding of beginning-to-end customer risk.[8]

To embark on this holistic journey, organizations must establish an integrated risk framework (**figure 4**) and assessment process by preparing a fundamental risk rating structure for the three risk types combined and then designing controls by leveraging a common

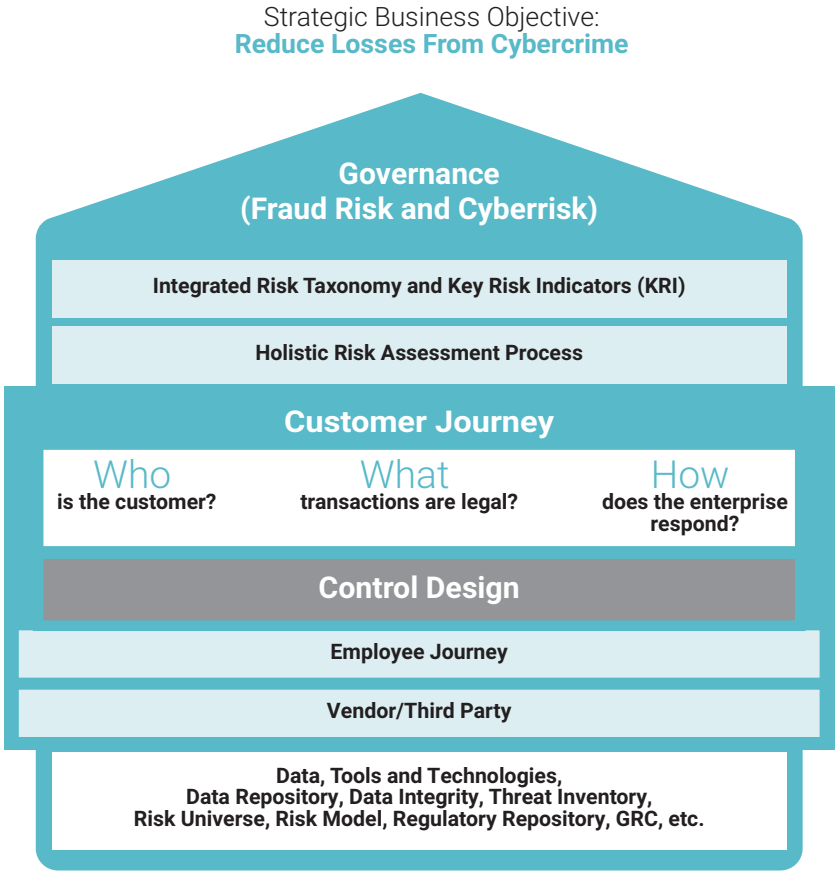
LOOKING FOR MORE?

- Read *Auditing Cybersecurity. www.isaca.org/auditing-cyber-security*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> "To more effectively and proactively protect their customers and assets, financial institutions should look at the three types of risk as a unified threat to the enterprise."

FIGURE 4

Integrated Fraud and Cybersecurity Framework



set of data elements. The intention is to mitigate risk in alignment with the enterprise's risk appetite and business strategy.

The risk assessment process should be defined across user journeys (e.g., customer or employee). Within each journey, end-to-end business processes should be identified across which the integrated risk assessment will be conducted.

For example, consider the customer journey and business process of opening a bank account. First, the user's identity must be validated to develop a secure self-registration process, and the fraud department should evaluate whether someone is creating fraudulent accounts. A holistic risk assessment approach encompasses both.

Threat countermeasures must be supported by solid analytics, providing insights for early detection and, in some cases, the prevention of cybercrime. Artificial intelligence can enhance the analysis and combination of cyberthreat data (e.g., indications of compromise) and fraud/financial crime surveillance data.

Conclusion

A complete, holistic approach can be a more inclusive and effective way of reducing customer risk, lowering operating costs and improving the odds against cyberattacks, all leading to significant gains in customer trust.

Author's Note

The opinions in this article are based on the author's research and personal experience. They have no association or any links to PwC LLP.

Endnotes

1 Verizon, *2021 Data Breach Investigations Report,* USA, 2021, *https://www.verizon.com/business/resources/reports/dbir/*

2 Braue, D.; "Global Cybersecurity Spending to Exceed $1.75 Trillion From 2021-2025," *Cybercrime Magazine,* 10 September 2021, *https://cybersecurityventures.com/cybersecurity-spending-2021-2025/*

3 Magrath, M.; "Fraud Spurs Wave of New Financial Regulations—What Security Leaders Need to Know," *Security Magazine,* 30 March 2021, *https://www.securitymagazine.com/articles/94637-fraud-spurs-wave-of-new-financial-regulations-what-security-leaders-need-to-know*

4 LexisNexis Risk Solutions, *LexisNexis Risk Solutions 2018 True Cost of Fraud Study,* USA, August 2018, *https://risk.lexisnexis.com/-/media/files/financial%20services/research/2018-true-cost-of-fraud-overall-rep%20pdf.pdf?la=en-us*

5 Zetter, K.; "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired,* 17 May 2016, *https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/*

6 *Ibid.*

7 Bull, M.; "Cybercrime and the Risks to the Financial System," *International Security Journal,* 17 September 2020, *https://internationalsecurityjournal.com/cybercrime-and-the-financial-system/*

8 *Ibid.*