protiviti®
Global Business Consulting

COMPLIANCE INSIGHTS

Collaboration: The key to better management of cybercrime and financial crime

By Carol Beaumier and Bernadine Reese

Sharing information and lessons learned has become increasingly critical for the effective management of cybercrime and related financial crime. This need requires financial institutions to rethink how they have historically managed these risks.

We are in the Fourth Industrial Revolution.[1] Extraordinary technological advances have changed, and will continue to change, the way we live and work. These advances provide not only enormous benefits but also the potential for destructive behaviour.

We see this destructive behaviour manifested in the proliferation of cybercrime, which, as recent reports published in Europe and the United States indicate, is mostly motivated by the desire for financial gain.[2,3] Among other illegal acts, the proceeds of cybercrime have been linked to terrorist financing. In 2020, the U.S. Department of Justice announced the dismantling of three terrorist financing cyber-enabled campaigns involving the al-Qassam Brigades, Hamas's military wing; al-Qaeda; and the Islamic State of Iraq and the Levant (ISIS).[4] These realities suggest the need for — and the potential advantages of — stronger collaboration between cyber risk management and financial crime teams.

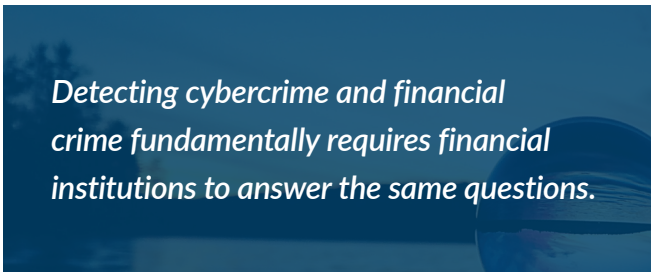
1 Fourth Industrial Revolution, World Economic Forum, www.weforum.org/focus/fourth-industrial-revolution.

2 2022 Data Breach Investigations Report, Verizon, www.verizon.com/business/resources/reports/dbir/.

3 "Cybersecurity: Main and Emerging Threats," Euroreporter, February 7, 2023, www.eureporter.co/defence/cybercrime-2/2023/02/07/cybersecurity-main-and-emerging-threats/.

4 Global Disruption of Three Terror Finance Cyber-Enabled Campaigns, Internal Revenue Service, August 13, 2020, content.govdelivery.com/accounts/USIRS/bulletins/29a1ec3#:~:text=WASHINGTON%20%E2%80%93%20The%20Justice%20Department%20today%20announced%20the,Islamic%20State%20of%20Iraq%20and%20the%20Levant%20%28ISIS%29.

Despite the explicit recognition by some jurisdictions of cybercrime as a predicate offence to money laundering and a national anti-money laundering/counterterrorist financing (AML/CFT) priority,[5,6] the day-to-day management of financial crime and cyber risk has traditionally been carried out separately in financial institutions. Yet, detecting cybercrime and financial crime fundamentally requires financial institutions to answer the same questions: With whom are we engaging, and how do we know what they are doing is legitimate? It seems intuitive, therefore, that stronger collaboration between cybercrime and financial crime risk management can lead to improvements in managing both risks.



The rising tide of cybercrime

Cybercrime is simply defined as any criminal activity carried out by means of a computer or the internet. There is some debate about when exactly cybercrime started, but most experts agree that it caught on in the late 1980s, when email became a commonly used technology.[7] While lone-wolf hackers were the early perpetrators of cybercrime, and still exist, cybercriminals today include well-established threat actors ranging from governments to organised crime.

Cybercrime has continually escalated over the last three decades but flourished even more during the COVID-19 pandemic, when more employees worked remotely, data that may traditionally have been centralised was shared more freely and more often, and employees were introduced to new tools and technologies with which they had no prior experience — circumstances that continue to some degree in the current hybrid work environment. In 2022 the global cost of cybercrime was estimated at USD 8.4 trillion. By 2026, annual cybercrime costs worldwide could exceed USD 20 trillion, an increase of almost 150%.[8]

Cybercrime carried out for financial gain involves accessing and/or misusing data. For financial institutions, their own data and their customers' data are at risk. The methods used by the cybercriminal are many, including those illustrated below.

[5] Anti-Money Laundering and Countering the Financing of Terrorism National Priorities, Financial Crimes Enforcement Network, June 30, 2021, www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[6] Directives, Official Journal of the European Union, European Union, November 12, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN.

[7] "Cybercrime's Evolution Since the 80's: Historical Facts and Figures," by Andrew Douthwaite, Virtual Armour, October 26, 2022, https://virtualarmour.com/cybercrimes-evolution-since-the-80s/#:~:text=Experts%20agree%20that%20%E2%80%9Ccybercrime%E2%80%9D%20as,today%20originated%20in%20the%201980s.&text=Cybercrime%20has%20increased%20300%25%20since,roughly%201.5%20million%20in%202010.

[8] Estimated Cost of Cybercrime Worldwide From 2016 to 2027," Statista, www.statista.com/statistics/1280009/cost-cybercrime-worldwide/#:~:text=The%20global%20cost%20of%20cybercrime,U.S.%20dollar%20mark%20in%202023.

Methods Used by Cybercriminals to Commit Financial Crime

Financial data breaches accounted for 153.3 million leaked records from January 2018 to June 2022 in the United States alone.[9] How do cybercriminals make money from these exploits? In some instances, the connection is direct (e.g., ransomware). In other cases, the original crime is only the beginning (e.g., stolen data is sold on the illegal market or used to obtain loans or access other financial institution accounts). So valuable is personal data to cybercriminals that it has been estimated that 11% of cybersecurity breaches are directly aimed at stealing data.[10]

Cybercriminals have also targeted the financial system directly. The 2016 Bangladesh Bank heist, which some believe was perpetrated by the North Korea–based Lazarus Group, resulted in the theft of USD 81 million from Bangladesh's central bank through the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. In this instance, hackers used official bank credentials, which were stolen by using malware, to transfer funds to the Federal Reserve Bank of New York with instructions to send the funds to accounts opened by the hackers in a bank in the Philippines, where it was quickly withdrawn.

The damage, in fact, could have been much worse, since the total value of the SWIFT instructions issued by the hackers was close to USD 1 billion, but the Federal Reserve Bank of New York blocked

[9] Financial Data Breaches Accounted for 153.3 Million Leaked Records From January 2018 to June 2022," by Paul Bischoff, Comparitech, July 27, 2022, www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.

[10] "The Chance of Data Being Stolen in a Ransomware Attack Is Greater Than One in Ten," Emisoft, July 13, 2020, www.emsisoft.com/en/blog/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

30 transactions because of suspicions raised by misspelled instructions. Misspellings, as we have all learned in our company security training, are a common tip-off signalling fraudulent transactions.

However, at USD 81 million, the Bangladesh Bank robbery does not come close to the largest heist of a financial services company. The 2018 hacking of Coincheck, a Japanese crypto exchange, enriched the criminals, who were also believed to be North Korean, by USD 534 million. In fact, four of the top five hacks in recent history have targeted cryptocurrencies firms; all four were successful and netted those involved USD 1.43 billion.[11]

While artificial intelligence (AI) is seen by many financial institutions as an advanced way of detecting and evaluating many financial crimes, AI technology is itself vulnerable to cyber hacks. In 2020, facial recognition software startup Clearview AI reported that it had been subject to a hack[12] that allowed criminals to gain access to its client list. Having access to change AI modelling or its use could have severe consequences for AI use, adoption and public confidence.

How collaboration can improve management of both risks

Would it help the financial crimes investigation team to know that the cyber team has noticed increased attempts to access the company's website from a jurisdiction known to be a high risk for cybercrime or a jurisdiction thought to be aiding Russia in evading sanctions? Would it help the cyber risk management team to know that the financial crime team has conducted an extensive investigation into a recent string of identity thefts and has identified some patterns of activity? The answer to these questions is yes. Sharing this information will make both teams smarter. While some financial institutions are already sharing information, the process in many institutions is unstructured and ad hoc.

While both cyber risk and financial crime risk generally fall under the purview of the risk committee of the board of directors, the day-to-day management of these risks is often bifurcated. Financial crime is often managed by a compliance team headed by a money laundering reporting officer (MLRO), who reports to the chief risk officer or the chief compliance officer, and cybersecurity is often managed by an information technology (IT) security team headed by the chief information security officer (CISO), who typically reports to the chief technology officer or the chief information officer.

This segregated approach impacts the way the risks are assessed and managed within financial institutions. While the financial crime and the cyber risk management teams may be facing off against the same bad actors using increasingly sophisticated means to perpetrate crimes, the technical compliance requirements for financial crime and cyber risk management differ, and in

[11] "Here Are the Biggest Digital Heists of the Last Decade," by Chris Stokel-Walker, Cybernews, June 29, 2022, https://cybernews.com/editorial/here-are-the-biggest-digital-heists-of-the-last-decade/.

[12] "Clearview AI: Face-Collecting Company Database Hacked," BBC, February 27, 2020, www.bbc.com/news/technology-51658111.

many cases, the compliance and IT security teams speak different languages. But a siloed approach means that institutions may not be sharing data that could help prevent, or at least more effectively detect, criminal activity.

Taking a broader view of risk

As financial institutions look to protect their customers and assets more effectively, they should be considering the increasingly significant overlaps between cybercrime and financial crime. This effort might take the form of greater collaboration between the two disciplines and regular touchpoints and information sharing between the MLRO and the CISO so that there is a collective understanding of criminal threats facing the organisation.

There are useful lessons to be learned from the recent collaboration between AML and sanctions teams that has occurred because of the Russian sanctions. These two teams, although both dedicated to financial crime compliance, have historically operated in their own silos, touching base primarily when a true sanction hit was handed over to the AML investigation team to determine whether it also warranted filing a suspicious activity report. What these teams learned over the last year is that regular touchpoints between the teams to share what they were seeing provided better context to both teams. This lesson would likely hold true for financial crime and cybercrime teams as well.

Financial institutions may also want to consider greater alignment of the teams' risk frameworks, including risk appetite statements, risk identification, assessment, monitoring, metrics and reporting. This linked view of risk will also be helpful for senior management oversight of the wider risk horizon.

Following are six steps financial institutions can take to integrate and improve cybercrime and financial crime risk management.

1. **Employee training and awareness: Ensure that cybercrime risks are incorporated in internal training and awareness programs.** It is a regulatory requirement for employees to understand the financial crime controls within their organisation, and inclusion of cybersecurity risks and controls is a valuable addition, particularly within the consideration of the wider financial crime environment. Senior managers and boards will need to understand the holistic risk assessment and be able to provide informed challenges of the financial crime risk framework.

2. **Risk assessment: Consider whether cyber risk is sufficiently embedded in the institution's enterprise AML/CFT risk assessment.** The financial crime team should understand the institution's cyber-threat assessment and use this information to help inform risks related

to geographies, products or services offered, customer groups, and payment methods. This understanding will assist the financial crime team with conducting investigations and developing reports of suspicious transactions.

Questions for financial institutions:

- How are risks and information relating to financial crime and cybercrimes shared across the organisation?
- Which products, services or locations are most vulnerable to use by cybercriminals?
- Where cyber incidents have occurred in the market, are all vulnerabilities assessed from both a cybercrime and a financial crime perspective?
- How can financial crime preventive and detective controls be enhanced through understanding cybercrime vulnerabilities?

3. **Client acceptance: Include red flags for cybercrime in account opening due diligence.** Those responsible for onboarding new clients and periodic updating of customer information should be knowledgeable about how cybercriminals may use stolen data to establish accounts at financial institutions. The Financial Crime Enforcement Network (FinCEN) in the U.S., among other national government agencies, has identified a number of red flags[13] related to the use of stolen documentation. They include the following:

   - The spelling of the name provided by the customer does not match the spelling of the government-issued identity documentation.
   - Pictures in identity documents are blurry or low-resolution or show signs of possible manipulation.
   - The customer does not physically match descriptive information on identity documentation.
   - The customer refuses to, or is hesitant to, provide supplemental documentation.

   Suspicions of identity theft should be shared with the cyber risk team, particularly when they involve current or past clients of the financial institution. These instances raise the possibility that the financial institution may have been hacked.

4. **Monitoring and detection: Establish formal information sharing between the financial crime team and the cyber risk management team on the typologies used by cybercriminals to conduct financial crime.** Financial crime and cybercrime prevention and detection rely

[13] Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic, FinCEN Advisory, July 30, 2020, www.fincen.gov/sites/default/files/advisory/2020-07-30/FinCEN%20Advisory%20Covid%20Cybercrime%20508%20FINAL.pdf.

on monitoring and detecting events designed to obfuscate who is behind the activity and its real purpose. The use of transaction monitoring and surveillance software as a financial crime control is well established. Risk information regarding certain transaction types or customer profiles, which may be linked to cybercrime, will enrich the ability of systems to detect potentially suspicious activity that might indicate cybercrime.

The laundering of the proceeds of cybercrime follows several familiar routes, and financial institutions should ensure that monitoring and surveillance systems are calibrated to detect this activity. Among the most prevalent are recruiting and using money mules to avoid detection of smaller amounts, using front companies to hide the identity of the criminals, and using cash businesses or financial representatives in certain higher-risk countries.[14] Cryptocurrencies are also increasingly used for laundering the proceeds of hacking and ransomware attacks, and financial institutions should apply greater scrutiny of such sources.

They should also prioritise scrutiny of online transactions with parties from high-risk countries and high numbers of payments made with prepaid cards, both of which have been identified as cybercrime red flags. Heightened monitoring procedures should be deployed following a known cyber incident that has the potential to affect a broad section of the customer base. These may range from enhanced procedures to verify requested changes in account details to lowering the thresholds and transaction values used to trigger alerts for the section of the customer base at risk.

5. **Combined incident responses: Information related to a security breach should be shared with the financial crime team as soon as possible.** Combined incident responses, including assessments of how data obtained through a cyberattack could be used to perpetrate financial crime against the financial institution or its customers, may enhance an institution's ability to prevent or identify additional crimes. Financial institutions that have a documented response plan will react more effectively, and consideration of the impacts on other aspects of financial crime will assist with identifying all areas of vulnerability should an event occur.

6. **Customer communication and education: The financial crime and cyber risk management teams should collaborate to optimise customer training and awareness.** For financial crime and cybercrime, customer communication and awareness are especially important, particularly as threats change over time or new methods are adopted by criminals to perpetrate cybercrime or fraud. Many customers are becoming more aware of the various methods used, but the needs of certain groups of customers, such as vulnerable customers, should be specifically addressed in the company's customer education efforts.

[14] Follow the Money: Understanding the Money Laundering Techniques That Support Large-Scale Cyber-Heists, BAE Systems and The Society for Worldwide Interbank Financial Telecommunication, 2020, www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf.

Conclusion

The technology advances that offer so much promise to how we work and live come also with risks such as increasingly sophisticated and widespread cybercrime. While financial crime has traditionally been managed separately from cybercrime, a more holistic approach by financial institutions will improve its prevention and detection. There are strides cybersecurity and financial crime compliance can make to improve information sharing, analysis, and assessment of risks from criminals and enhanced monitoring and detection. As technology develops further and criminal use of technology to perpetrate financial crime increases, strengthening cybersecurity and financial crime compliance will become an issue that requires proactive and extensive engagement at all levels.

About the authors

Carol Beaumier is a senior managing director in Protiviti's Risk and Compliance practice and leader of the firm's APAC Financial Services practice. Based in Metro D.C., she has more than 30 years of experience in a wide range of regulatory issues across multiple industries. Before joining Protiviti, Beaumier was a partner in Arthur Andersen's Regulatory Risk Services practice and a managing director and founding partner of The Secura Group, where she headed the Risk Management practice. Before consulting, Beaumier spent 11 years with the U.S. Office of the Comptroller of the Currency (OCC), where she was an examiner with a focus on multinational and international banks. She also served as executive assistant to the comptroller, as a member of the OCC's senior management team, and as liaison for the comptroller inside and outside of the agency. Beaumier is a frequent author and speaker on regulatory and other risk issues.

Bernadine Reese is a managing director in Protiviti's Risk and Compliance practice. Based in London, she has more than 30 years of experience working with financial services clients in risk and regulatory advisory. Reese has worked with a diverse range of financial institutions in responding to financial crime legislation, including anti-money laundering and sanctions compliance.

About Protiviti's Financial Crime and Cybersecurity practices

Protiviti's Financial Crime practice specialises in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of AML/CFT and sanctions risk assessment, control enhancements, and change capability to deliver effective operational risk and compliance frameworks. Our financial crime team assists organisations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct, and other financial business risk issues.

In applicable engagements, our financial crime specialists work in conjunction with Protiviti's Cybersecurity practice to help financial institutions understand and manage their evolving privacy risks, tailor their cybersecurity governance and communicate effectively with stakeholders. Our cyber team aims to preserve business value by identifying vulnerabilities to protect sensitive data while providing actionable remediation guidance.