Mitigating the Next "Super Spreader:"

Fraud Prevention and Risk Management in the Remote Work Environment

By Nicholas Ciabattone

This article is an excerpt from the Spring 2021 RMAI Insights magazine (pages 17, 21 and 27), originally published April, 2021.

While social distancing and shifting to a virtual work environment are believed by many to help curb the spread of COVID-19, it is actually being labelled by some as a "super spreader" event. Though certainly a minority viewpoint around the world, this view is prominent among professionals in the fraud and financial crimes industry who feel COVID-19 has led to a wildfire-like spread of fraud as more and more of the economy moves online and an influx of employees/individuals interact virtually

For all the negative impacts associated with the coronavirus, of which there are many,COVID-19 is among the most accomplished "lobbyist" for digital transformation in decades, helping to accelerate change in regulations and business processes within a matter of months in a battle that has been plaguing stakeholders for many years. Select items that have historically required a physical presence are now permitted to be done virtually. Examples include ARM businesses now permitted to operate virtually (varies by state) or a consumer opening a bank account and not being physically required go to a branch. Even court hearings are now being conducted via Zoom.

In a survey published by Gartner[1], a market research firm, over 74% of CFOs expect at least some of their employees will continue to work from home (WFH) after the pandemic ends. The economic advantages are clear and very well published (decreased commute time, improved employee morale, etc.), but a deeper look into a potential downside of the growing trend is startling. While rushing to virtually connect remote workers to the workplace, employers and personnel may have overlooked the importance of security as they work to balance flexibility and cost – and cybercriminals have already begun to take advantage. Securing remote work models will likely save organizations time and money and give them a long-term competitive advantage, particularly in identity and access management, in the cloud, and in modernizing their network architectures. Remote work vulnerabilities are top of mind for any CTO, and organizations may need to reassess their approach and controls related to addressing workforce management, people culture, and performance management skills.

Risks associated with internal fraud have heightened due to an abrupt change in work practices. Enterprise-wide controls to prevent and detect fraud and network breaches may not be designed to operate in near-100% virtual environments. Anti-fraud, compliance, and cybersecurity concerns may have also been deprioritized in favor of maintaining business-as-usual services. While management's attention may be diverted to focus on business operational metrics or client focus, employees are now under less scrutiny and oversight than ever before, stressing the importance of compliant solutions to prevent fraudulent or risky behavior.

According to Verizon's 2020 Data Breach Investigations Report[2], 30% of recorded data breaches involved internal actors. Credential theft, social attacks (i.e., phishing and business email compromise), and errors caused a majority of the data breaches. Employees working from home could be particularly vulnerable to these types of attacks, and as such, prevention efforts by organizations should be focused here. Having a concise internal policy response on suspicious links or email content, continuous vulnerability management, secure configurations, email/web browser protections, account monitoring, implementation of security awareness/education/training, and data governance will help mitigate risk.

An additional risk factor to consider for organizations navigating the WFH environment is time theft. Time theft occurs when employees take advantage of reduced oversight and inaccurately log work hours, work inefficiently, or do not work at all while logged in. If time theft runs rampant in your organization, it can ultimately impact productivity metrics and profitability. This risk can be mitigated by enforcing a productivity assurance agreement across your employees, scheduling regular check-ins by managers, or using time-tracking or keystroke monitoring software. While most business owners don't consider this a huge problem and trust their staff, time theft could lead to bigger issues down the road if left unchecked.

Consumers/debtors are dealing with similar issues of identity theft, fraudulent transactions, and rising security concerns. In February 2021, the Federal Trade Commission (FTC) reported that cases of identity theft doubled[3] in the U.S. from 2019 to 2020. Disputes around fraudulent payments are increasing as more and more payments are made via credit card and via online and virtual channels.

The uptick in fraud and financial crimes is not going unnoticed. Investors are flocking to the space given to the growing market opportunity created in part by the pandemic. In September 2020, BioCatch, an industry leader in behavioral biometrics, raised $20 million in additional Series C funding from Barclays, Citi, HSBC, and National Australian Bank[4] (bringing total funding above $200 million). In January 2021, Equifax entered into a definitive agreement to acquire Kount[5], an artificial intelligence fraud prevention and digital identity solution business, for $640 million. In February 2021, there was even a $300 million Special Purpose Acquisition Company (SPAC)[6] announced by Dave DeWalt, ex-CEO of FireEye and McAfee, with the goal of merging with a cybersecurity business after going public.

The statistics and data outlined above paint a dim outlook, but not to fret, there are several ways to help "curb the spread" of fraud and financial crimes. Understanding the severity is the first step. Reassessing your approach and controls related to addressing the concern is the next order of business.

Often overlooked is maintaining an updated data security policy for your organization to adhere to. If you haven't already updated this to reflect the impact of COVID, it should be a priority. A good reference guide[7] is the RMAI "Data Security Policy" certification standard for certified businesses/vendors. Certification Standard A7 requires that an annual risk assessment be performed on how the company protects consumer data from "reasonably foreseeable internal and external risks" (i.e., storage of consumer data, antivirus software, PII protection, encryption, disposal, etc.). There are major financial and legal implications if your business is responsible for a data breach.

Transitioning to a remote work environment in an expedited manner (as many businesses were forced to do) creates risk. This risk can be mitigated by various factors such as requiring the use of secure networks; implementing firewalls or virus scanners on all authorized devices being used by employees; issuing company-owned devices to control components, as opposed to use of personal devices by employees; ensuring that only IT administrators have credentialed access to monitor software updates; developing protocol for acceptable use policies for electronic devices and company data; providing annual security training to all employees; incentivizing the use of multi-factor authentication for email or other critical systems; and frequently evaluating virtual private network (VPN), virtual desktop infrastructure (VDI), firewalls, anti-malware, and intrusion-prevention software(s). These may seem like exorbitant costs or measures to go through, but the cost of a data breach may far exceed the initial spend. In a 2020 report published by IBM[8] regarding data breach, they estimated the average total cost incurred by an organization to be $3.86M. This varies across industries, with healthcare or financial services often being even more costly (i.e., in 2019, a medical debt collector filed for bankruptcy protection[9] in the aftermath of a data breach).

Given the rapidly evolving nature of the industry, your IT team should be engaging in regular dialogue with technology vendors that specialize in protecting your systems from data breaches and fraud. Home grown (or proprietary) systems are good but need to be regularly updated to stay abreast of changes. Luckily for you, the RMAI Annual Conference[10] takes place April 12-15 (in person and virtual) and will feature numerous vendors/sponsors that specialize in this market. Getting intelligence on your current vendors, capabilities, and policies and procedures will lead to more meaningful conversations.

The digital and virtual environment, the "new normal" as some might say, is here to stay. Do your part to help "curb the spread" of fraud and stay diligent to its impacts, especially in the remote work environment. It is not an easy feat and, as such, it will require prioritization among your management team. Consider updating policies and procedures and leveraging technology vendors to limit exposure for you and your client. Don't become a "super spreader!"

Notes

[1] Joseph F. Kovar, *Some May Work From Home Permanently After COVID-19: Gartner*, April 13, 2020, CRN.com, found at https://www.crn.com/news/running-your-business/some-may-work-from-home-permanently-after-covid-19-gartner?itc=refresh

[2] 2020 *Data Breach Investigations Report*, Verizon.com, found at https://enterprise.verizon.com/resources/reports/dbir/

[3] *Identity Theft Awareness Week starts today,* February 1, 2021, FTC.com, found at https://www.consumer.ftc.gov/blog/2021/02/identity-theft-awareness-week-starts-today

[4] *Major Global Banks Invest $20 Million in BioCatch and Join American Express Ventures on New Client Innovation Board*, September 30, 2020, BioCatch.com, found at https://www.biocatch.com/press-release/major-global-banks-invest-20-million-in-biocatch-and-join-american-express-ventures-on-new-client-innovation-board

[5] *Equifax Announces Definitive Agreement to Acquire Kount*, January 8, 2021, Kount.com, found at https://kount.com/announcements/equifax-announces-definitive-agreement-to-acquire-kount

[6] United States Securities and Exchange Commission, Form S-1 Registration Statement, February 9, 2021, SEC.gov, found at https://www.sec.gov/Archives/edgar/data/1837067/000119312521034596/d61319ds1.htm

[7] RMAI Certification Resources, RMAINTL.org, found at https://rmaintl.org/certification/certified-receivables-business/certification-resources/

[8] *2020 Cost of a Data Breach Report,* IBM.com, found at https://www.ibm.com/security/data-breach

[9] Charlie Osborne, *Data breach forces medical debt collector AMCA to file for bankruptcy protection*, June 19, 2019, ZDNET.com, found at https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/

[10] RMAI 2021 Annual Conference, RMAINTL.org, found at https://rmaintl.org/events/2021-annual-conference/

Nick Ciabattone
Vice President
Corporate Advisory Solutions

Nick Ciabattone is a Vice President at Corporate Advisory Solutions (CAS) providing transaction and advisory support to clients in the tech-enabled Outsourced Business Services industry. Nick serves as lead deal support on M&A transactions and is responsible for closing numerous sell-side and buy-side transactions as well as completing various portfolio/company valuations, strategic consulting and compliance/audit assignments. Nick is also a member of the Receivables Management Association International (RMAI) Public Relations and Marketing Committee and served on the committee since 2016.