ESG: The Importance of Effective Cybersecurity within the "G"

By: Jude Erondu, *Associate*

October 2020

Introduction

Businesses increasingly recognize that government and institutional investors are focused on cybersecurity as a top risk for companies. Cybersecurity is now viewed as one of the top environmental, social, and governance ("ESG") issues that will have a significant adverse impact on a company's market value within an investment portfolio if major problems arise.[1] Cybersecurity is seen as both a national security and a corporate governance issue.[2]

Eric Rosenbach, a former "Pentagon Cyber Czar" and co-director of the Belfer Center for Science and International Affairs at the Kennedy School at Harvard, explains cybersecurity in a simple term. According to Rosenbach, "cyber risk management is an essential part of governing. It is a fundamental component of operations. Understanding and mitigating risk has become an essential skill not only for security and technology specialists but also for leaders in government and business."[3]

As the frequency of cyber-attacks increases, institutional investors are at the forefront of the battle to understand their investments' exposure to cybersecurity risks.[4] Tragically, organizations are not immune to new cyber threats. The lockdown of 2020 linked to the novel coronavirus pandemic has further increased investors', businesses', and government agencies' exposure risk to cyber insecurity.[5] Cybercriminals have capitalized on the lockdown to increase their attacks as businesses, individuals, and governments embrace new practices such as working remotely and social distancing.[6] Due to a lack of preparedness, vulnerable businesses and government infrastructure are now more exposed to cyber-attacks.[7]

Unaddressed cybersecurity threats have a negative impact on the economy, businesses, and investors. However, government, businesses, and individual investors have a huge role in addressing cyber-attack risk.[8] A sustainable approach to addressing threats posed by growing cyber activity requires a shift to a proactive strategy instead of merely reacting as problems arise.

Cyber security as a governance issue that presents a risk to investors and businesses

Cybersecurity, if not managed effectively as part of a comprehensive plan of corporate governance (the "G" of ESG), will present a clear risk to the value of companies within an institutional investors' portfolio.[9] While many factors contribute to a need for increased cybersecurity, the lockdown of 2020 has dramatically changed how society interacts, does business, communicates, and travels, heightening risks for those who are not as effective at adapting to change.[10] Since the lockdown, business activities have increasingly shifted to digital platforms. Financial institutions are rethinking business strategies and increasing spending on information technology and cloud technology systems that enable employees to work remotely, in order to reduce the spread of the novel coronavirus (COVID-19).[11] As businesses strive to adapt to working remotely, businesses and investor risk exposure to cybersecurity has increased since the lockdown of 2020.[12]

A study by Deloitte Cyber Intelligence Centre concludes that "there has been a spike in phishing attacks, Malspams and ransomware attacks as attackers are using COVID-19 as bait to impersonate brands thereby misleading employees and customers."[13] Similarly, the Boston Consulting Group noted that, "financial services firms are 300 times as likely as other companies to be targeted by a cyberattack—and dealing with those attacks and their aftermath carries a

higher cost for banks and wealth managers than for any other sector."[14] Despite the growing need to strengthen information security and cyber resilience, many financial institutions are ill-equipped to respond effectively, thereby raising institutional and non-institutional investors' concerns.[15]

In June of 2020, the Security and Exchange Commission ("SEC") alerted the public about the rise of ransomware attacks on United States financial institutions.[16] According to SEC, its Office of Compliance Inspections and Examinations (OCIE) observed "an apparent increase in sophistication of ransomware attacks on SEC registrants, which include broker-dealers, investment advisers, and investment companies. The perpetrators behind these attacks typically demand compensation (ransom) to maintain the integrity and/or confidentiality of customer data or for the return of control over registrant systems."[17]

Furthermore, global institutional investors are also concerned about the growing implications cybersecurity risks pose to their investment portfolios.[18] A 2019 Responsible Investment Survey by RBC Global Asset Management stated that cybersecurity was the number one ESG risk of great concern to investors.[19] Similarly, in an Ernest and Young survey of more than 60 institutional investors with approximately $35 trillion in assets under management, respondents noted that cybersecurity would be the third highest threat to investment portfolios in the next three to five years.[20] Unaddressed or lack of preparedness for cybersecurity risk does poses a huge challenge to businesses and investors.[21]

For instance, in June 2020 Argenta, an Antwerp-based savings bank, experienced its first cyberattack resulting in a shutdown of approximately 143 cash machines. Argenta did not publicize the amount stolen, as it is standard practice for banks and financial institutions to keep the extent of such a crime confidential in order to not erode public confidence in their institution's security.[22] Similarly, in the early month of July 2020, the Twitter accounts of famous individuals, including Barack Obama, Elon Musk, and Bill Gates, were compromised as part of a bitcoin scam. At the time of the scam, Twitter's stock fell by 3% as the events exposed a huge security issue within the social media platform.[23]

Cybersecurity as a National Security Issue

Cybersecurity remains one of the significant national security issues affecting government organizations at every level, federal, state, and local. It is in the government's interest to strengthen its cybersecurity apparatus in order to prevent foreign and homegrown attacks against U.S businesses and infrastructure. The 2017 National Cyber Strategy ("NCS") captures a fifteen-year plan to defend the homeland by protecting networks, systems, functions, and data. Before and during the lockdown of 2020, the United States has continued to experience some form of cyber-attack from foreign adversaries, whether it is foreign interference with elections or attacks on state or local government. According to the Department of Homeland Security ("DHS") report on threat assessment, "Cybercriminals increasingly will target U.S. critical infrastructure to generate profit, whether through ransomware, e-mail impersonation fraud, social engineering, or malware. Underground marketplaces that trade in stolen information and cyber tools will continue to thrive and serve as a resource, even for sophisticated foreign adversaries."[24]

Lack of preparedness poses a huge challenge for the federal, state, and local government critical infrastructure. For instance, in 2019, the city of New Orleans incurred a $1 million cost linked to cyberattack ransomware.[25] In another example, Baltimore also incurred a loss of approximately 18 million dollars after experiencing a cyberattack.[26] School districts have also been hit hard by increasing cyber-attacks in the wake of the lockdown. A recent cyber-attack on the Miami-Dade County school district's virtual classes demonstrates how cyber-attacks can have a significant effect on both the government and the learning environment.[27]

What can Businesses and Government do to Address Risk posed by Cyber Insecurity?

Since a lack of preparedness and a lack of resources have been linked to the vulnerability of businesses and

government infrastructure to cyber-attacks, one must ask the question: What can business and government do to prevent and mitigate risk exposure to cyber-attack?

Addressing or mitigating the severe impact of cyber insecurity requires a sustainable strategy.[28] Business and government ought to see the cyberattack as invisible warfare that requires a proactive approach, combined with sophisticated due diligence.[29] Business and government can proactively mitigate cyber-attacks by securing hardware, by encrypting and backing-up data on a secured server; by investing in cybersecurity insurance, and by testing and strengthening their existing cybersecurity policy.

Secure Hardware

Several businesses were taken unaware by the novel coronavirus that shaped the way society interacts. However, businesses that invested in secure password-protected and physically protected hardware infrastructure were better off.

Invest in CyberSecurity Insurance

By investing in cybersecurity insurance, businesses and government agencies can deal with the significant financial costs related to a successful cyber-attack.

Encrypt and Backup Data in a Secured Server

A proactive cyberattack strategy consists of two features: preventing physical access to sensitive data and rendering the data useless if it falls into the wrong hands. Appropriate tools will include the ability to wipe devices remotely. In addition, to the extent that backup data captures an organization's digital livelihood throughout a day, an organization will be able to return to the period just prior to a data breach in order to avoid the pain of a debilitating ransomware attack.

Strengthen Existing Cyber Security Policy

Businesses and government agencies will benefit from continuously reviewing existing cybersecurity policies and actively updating the procedures for new attack methods. For instance, federal funding and guidance would help state and local governments invest in cybersecurity infrastructure in order to avoid the vicious cycle of ransomware attacks experienced by Baltimore and New Orleans.

About the Authors

Jude Erondu, *Associate*

Jude is an Associate on the Client Advisory team with a primary focus on Environmental, Social, Governance Investing ("ESG") and Impact solutions. Based out of our Boston office, Jude supports the Impact Committee with investment and impact research and analysis, client meetings and relevant deliverables. Jude is also responsible for assisting with thought leadership programs with relation to Impact and ESG, including helping craft white papers, Pathstone's quarterly Sustainable Investing Highlights, as well as the firm's Annual Impact Report.

Disclosure

This presentation and its content are for informational and educational purposes only and should not be used as the basis for any investment decision. The information contained herein is based on publicly available sources believed to be reliable but is not a representation, expressed or implied, as to its accuracy, completeness or correctness. No information available through this communication is intended or should be construed as any advice, recommendation or endorsement from us as to any legal, tax, investment or other matters, nor shall be considered a solicitation or offer to buy or sell any security, future, option or other financial instrument or to offer or provide any investment advice or service to any person in any jurisdiction. Nothing contained in this communication constitutes investment advice or offers any opinion with respect to the suitability of any security, and this communication has no regard to the specific investment objectives, financial situation and particular needs of any specific recipient. Past performance is no guarantee of future results. Additional information and disclosure on Pathstone is available via our Form ADV, Part 2A, which is available upon request or at www.adviserinfo.sec.gov.

Citations

[1] James Jorner. "A Business Leader's Beginner Guide to Cybersecurity." Entrepreneur. September 26, 2020. Accessed October 12, 2020. https://www.entrepreneur.com/article/355861
[2] Id.
[3] Barnet Sherman. "Municipal Cybersecurity: Governance Metrics For ESG Investors." Forbes. February 4, 2020. Accessed October 12, 2020. https://www.forbes.com/sites/investor/2020/02/04/municipal-cybersecurity--governance-metrics-for-esg-investors/#7570ecc5a603
[4] Id.
[5] Thaddeus Swanek. "The Evolution of Cybersecurity Threats During COVID-19 and What You Can Do About It." U.S Chamber of Commerce. September 30, 2020. Accessed October 12, 2020. https://www.uschamber.com/series/above-the-fold/the-evolution-of-cybersecurity-threats-during-covid-19-and-what-you-can-do
[6] Id.
[7] Id.
[8] Stephen A. Wilson, Dean Hamilton, and Scott Stallbaum. "The Unaddressed Gap in Cybersecurity: Human Performance." MIT Sloan Management Review. May 26, 2020. Accessed October 12, 2020. https://sloanreview.mit.edu/article/the-unaddressed-gap-in-cybersecurity-human-performance/
[9] Shannon Houde. "How ESG issues can become even more relevant in times of market crisis." GreenBiz. July 8, 2020. Accessed October 12, 2020. https://www.greenbiz.com/article/how-esg-issues-can-become-even-more-relevant-times-market-crisis
[10] Richard J. Shinder. "The Age of the 'Unknown Unknowns'." The Wall Street Journal. September 17, 2020. Accessed October 12, 2020. https://www.wsj.com/articles/the-age-of-the-unknown-unknowns-11600383351
[11] Dina Gerdeman. "How the Coronavirus Is Already Rewriting the Future of Business." Harvard Business School. March 16, 2020. Accessed October 12, 2020. https://hbswk.hbs.edu/item/how-the-coronavirus-is-already-rewriting-the-future-of-business
[12] Id.
[13] Tope Aladenusi. "COVID-19's Impact on Cybersecurity." Deloitte. March 2020. Accessed October 12, 2020. https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html
[14] Boston Consulting Group. "For Wealth Managers, Off Year Sparks Opportunity to Reignite Growth." Boston Consulting Group. June 20, 2019. Accessed October 12, 2020. https://www.bcg.com/press/20june2019-global-wealth-report
[15] Michael Coden, Karalee Close, Walter Bohmayr, Kris Winkler, and Brett Thorson. " Managing the Cyber Risks of Remote Work." Boston Consulting Group. March 20, 2020. Accessed October 12, 2020. https://www.bcg.com/en-us/publications/2020/covid-remote-work-cyber-security
[16] Melanie Waddell. "SEC Issues Ransomware Alert." Think Advisor. July 13, 2020. Accessed October 12, 2020. https://www.thinkadvisor.com/2020/07/13/sec-issues-ransomware-alert/
[17] Security and Exchange Commission. "Cybersecurity: Ransomware Alert." Security and Exchange Commission. June 10, 2020. https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf
[18] Julie Segal. "And the Top Alternative to Traditional M&A Deals Is... SPACs, of Course." Institutional Investors. October 6, 2020. Accessed October 12, 2020. https://www.institutionalinvestor.com/article/b1np6p1ljtwp50/And-the-Top-Alternative-to-Traditional-M-amp-A-Deals-Is-SPACs-of-Course
[19] RBC. "Cyber Security is the top ESG concern for institutional investors." RBC. 2019. Accessed October 12, 2020. https://global.rbcgam.com/sitefiles/live/documents/cgri/cyber-security-is-the-top-esg-concern-for-institutional-investors.PDF
[20] Stephen Klemash. "Emerging trends and developments in cybersecurity-related disclosures of Fortune 100 companies." Ernest and Young. August 10, 2020. Accessed October 12, 2020. https://www.ey.com/en_us/board-matters/what-companies-are-disclosing-about-cybersecurity-risk-and-oversight
[21] Id.

[22] Alan Hope. "Argenta shuts down 143 cash machines after new cyber-attack." The Brussels Times. July 13, 2020. Accessed October 12, 2020. https://www.brusselstimes.com/news/business/121291/argenta-shuts-down-143-cash-machines-after-new-cyber-attack/
[23] Max A. Cherney. "Twitter Stock Slides 3% After Hackers Target High-Profile Accounts." Barrons. July 15, 2020. Accessed October 12, 2020. https://www.barrons.com/articles/twitter-stock-slides-3-after-hackers-target-high-profile-accounts-51594864082
[24] Department of Homeland Security. " Homeland Threat Assessment." Department of Homeland Security. October 2020. Accessed October 12, 2020. https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf
[25] Charles Watson. " New Orleans cyberattack has already cost the city $1 million." New York Post. December 19, 2019. Accessed October 12, 2020. https://nypost.com/2019/12/19/cyberattack-in-new-orleans-has-already-cost-the-city-1-million/
[26] Id.
[27] Maggie Miller. "Teen arrested for alleged cyberattacks on Miami-Dade schools." The Hill. September 03, 2020. Accessed October 12, 2020. https://thehill.com/policy/cybersecurity/514998-teenager-arrested-for-alleged-cyberattacks-on-miami-dade-school-district
[28] Id.
[29] Jon Bateman. "War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions." Carnegie Endowment for International Peace. October 5, 2020. Accessed October 12, 2020. https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819