ESG Implications of Cybersecurity Threats and 5 Actions to Take

By Mark Peters, *Managing Director* and Jude Erondu, *Analyst*

The word 'cybersecurity' often triggers fear and anxiety. The concerns vary in nature. For individuals, cybersecurity can mean ensuring personal information and payment cards are secure when shopping. For small businesses, the focus may be on the secure transmission of revenues from the point of sale to business accounts. For defense industry giants such as Boeing or General Dynamics, cybersecurity may be about protecting airplanes and defense equipment from malware that could trigger disasters. And for government officials such as the president's national security adviser, it is about protecting the country's national interests from foreign and domestic threats.

While cybersecurity might have different connotations, cybersecurity threats are a national security issue and a danger to critical U.S. infrastructure. According to Accenture's 2021 Cyber Threat Intelligence Report, "The global ransomware crisis has entered a new phase, as threat actors adopt stronger pressure tactics and new targets – in particular, manufacturing and critical infrastructure. Ransom impact is more widespread, with attacks often highlighting weaknesses in a company's security posture." The World Economic Forum's 2021 Global Risks Report cites cyberattacks among the top 10 global risks with a high probability of occurring. [1]

A simple cyber incident can have significant environmental, social, and governance (ESG) implications. It could damage a business's reputation and trigger substantial financial losses. Companies big and small increasingly recognize cybersecurity as a significant business risk that needs to be mitigated, often at a high cost.

This note examines the ESG implications of 'cyber-*in*security' and offers basic steps businesses and individuals can take to address cyber threats.

Environmental Costs and Implications of Cybersecurity

Companies in the energy sector have continued to experience the higher threat posed by the dangers of cyberattacks unleashed by foreign and domestic bad actors. A single cyber intrusion and attack can pose a significant pollution liability to businesses of all sizes, especially in the energy and utility sectors that are critical parts of our infrastructure. For instance, a successful cyberattack can cause a company to lose control of its warning systems. Equipment that is critical in controlling toxic material or toxic emissions could be unknowingly released, resulting in the potentially catastrophic environmental pollution in the form of spills or other emissions.
Attacks that compromise equipment controls could also lead to fires and explosions, with significant damage to capital equipment and personal injury, as well as environmental cleanup costs and liability claims from the injured. [2] The energy sector systems are mostly built on Supervisory Control and Data Acquisition (SCADA) systems, a prime target for cyberattacks.

For example, in 2017, a Saudi Arabian Petrochemical plant suffered a cyberattack from Russian government-backed hackers that nearly resulted in an explosion. [3] The explosion was prevented due to an error in the attacker's computer code. If the attack had been successful, it would most likely have had adverse environmental consequences.

Social Cost and Implications of Cybersecurity

As our society continues to adopt digital technology to power our social and financial interactions, and with this adoption accelerated by the COVID-19 requirements for social distancing, **cybercrime has quickly become the fastest-growing form of criminal activity.** The social cost of cyberattacks goes beyond dollar values. Daily activities such as travel can be disrupted, the hacking of critical life-saving healthcare systems by foreign and local bad actors can lead to death, and cyberattacks on the food supply chain could cause food shortages.

The Colonial Pipeline remains an interesting case that offers insights into the vulnerability of the United States' critical infrastructure. The attack on the Colonial Pipeline had such a large impact because the pipeline is a vital component of the nation's essential infrastructure system. [4] The system's decommissioning shut off gas supplies throughout the whole east coast of the United States, generating confusion and fear. Many households went into panic buying gas as the fear of gas price hikes

rose. [5] Air travel was also impacted by the Colonial Pipeline ransomware attack due to a shortage of aviation fuel. American Airlines, for example, temporarily changed their flight schedule to adjust to a growing fear of fuel shortages. [6]

Governance Cost and Implications of Cybersecurity.

As cyberattacks become more frequent and severe, cybersecurity is emerging as one of the top governance concerns within environmental, social, and governance factors. Companies big and small can view cybersecurity through the lens of preventing reputation risk, maintaining revenues, and avoiding extraordinary expenses. Reputation risk tied to cyberattacks has continued to be a significant issue since the acceleration of remote working during the global lockdown. [7] In recent years, organizations such as the Internal Revenue Services ('IRS"), Equifax, and Target are among companies and organizations that have experienced some form of cyberattack from foreign and domestic bad actors.

The Internal Revenue Services ("IRS"), one of the United States government agencies in charge of collecting taxes, suffered one of its worst cyberattacks in 2015. Cyber-hackers gained access to personal data of more than 700,000 taxpayers accounts. The hack was a nightmare for the IRS, one that raises questions as to how safe taxpayers' information is in the hands of "Uncle Sam."

In 2017, Equifax, one of the largest consumer credit reporting agencies, suffered a massive blow from cyberattacks orchestrated by a group of Chinese hackers. [8] This data breach accessed the private records of 147 million Americans. [9] The data breach was a hit to Equifax's reputation and resulted in a $700 million monetary settlement to customers affected. [10]

Target and T-Mobile have also had significant data breaches. In 2013, the data for more than 60 million Target customers were stolen by a hacker, resulting in an $18.5 million multistate settlement. [11] In 2021, T-Mobile, one of the nation's largest telecommunications companies, experienced its worst data breach ever, exposing the personal information of 47 million Americans. [12]

What can businesses and individuals do to protect against cyberattacks?

Businesses and individuals can protect themselves from cyberattacks by following steps such as

1. Think before you click: Although a simple concept, businesses and individuals find it challenging to follow through and "think before you click" to avoid sophisticated phishing attacks from foreign and domestic hackers. Simple questions should be asked, such as: How accurate is the email or text? Do I know this person? Does the email, text, or phone call sound funny? Should I report this email, text, or phone call to the computer team for verification? How urgent is this email, text, or phone call, and is this a false urgency? Does the email or text contain some typos, errors, or false names?

Individuals and businesses can effectively avoid phishing emails by simply pausing, verifying, and thinking through the content and context of the email, text, or phone call before opening or responding to any email, text, or phone call that might be considered phishing. Remember, most organizations never call to demand immediate payment, and most will not call about taxes or payments that are owed without first having mailed you a bill. [13]

2. Secure Hardware: Businesses should protect themselves with secure password-protected and physically protected hardware infrastructure installed and maintained with guidance from industry experts.

3. Increase cybersecurity budget: Businesses would be better armed against cyberattacks when their cybersecurity budget is substantial enough to purchase and install appropriate cybersecurity protections. Businesses will not be able to defeat suffocated hackers with ill-equipped cyber protective tools. Cybersecurity remains an art of war that can only be dominated with the best technology, which requires money.

4. Invest in Cybersecurity Insurance: Cybersecurity insurance may be helpful as a part of the toolkit used by businesses and individuals to protect themselves from the fallout of data breaches, which may result in litigation and settlements.

5. Strengthen Existing Cybersecurity Policy: Businesses should periodically and proactively review existing cybersecurity policies to determine they are adequate and robust enough to withstand new and ever-evolving cyberattacks.

[1] World Economic Forum. "The Global Risks Report 2021, 16th Edition." The World Economic Forum. January 19, 2021. Accessed September 28, 2021. http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[2]
[3] Kate O'Flaherty. "How The Russian Government Created The Most Advanced Industrial Malware Ever Seen." Forbes. October 23, 2018. Accessed September 28, 2021. https://www.forbes.com/sites/kateoflahertyuk/2018/10/23/how-the-russian-government-created-the-most-advanced-industrial-malware-ever-seen/?sh=11a8fff02dfa
[4] Jason Bordoff. "The Colonial Pipeline Crisis Is a Taste of Things to Come." Foreign Policy. May 17, 2021. Accessed September 28, 2021. https://foreignpolicy.com/2021/05/17/colonial-pipeline-crisis-cyberattack-ransomware-cybersecurity-energy-electicity-power-grid-russia-hackers/
[5] H.J. Mal. "An Extended Pipeline Shutdown Could Affect Gas Prices In Southeast U.S."
[6] Leslie Josephs. "Pipeline outage forces American Airlines to add stops to some long-haul flights, Southwest flies in fuel." CNBC. May 11, 2021. Accessed September 28, 2021. https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html
[7] Skadden, Arps, Slate, Meagher & Flom LLP. "ESG in 2021 So Far: An Update." JdSupra. September 3, 2021. Accessed September 29, 2021. https://www.jdsupra.com/legalnews/esg-in-2021-so-far-an-update-6642887/
[8] Benner, Katie "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking." New York Times. February 10, 2020. Accessed September 29, 2021. https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html
[9] Federal Trade Commission. "Equifax Data Breach Settlement." Federal Trade Commission. January 2020. Accessed September 29, 2021. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
[10] Jazmin Goodwin and Kelly Tyko. "Equifax breach settlement: Wednesday is last day to file a claim for free credit monitoring or money." USA Today. January 17, 2020. Accessed September 29, 2021. https://www.usatoday.com/story/money/2020/01/17/equifax-data-breach-settlement-2019-deadline-claim-free-credit-monitoring/4490366002/
[11] Kevin McCoy. "Target to pay $18.5M for 2013 data breach that affected 41 million consumers." USA Today. May 23, 2017. Accessed September 29, 2021. https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/
[12] Richard Lawler. "T-Mobile data breach exposed the personal info of more than 47 million people." The Verge. August 18, 2021. Accessed September 29, 2021. https://www.theverge.com/2021/8/18/22630446/t-mobile-47-million-data-breach-ssn-pin-pii
[13] Daniel Howley. "7 tax scams to watch out for this year." Yahoo. April 7, 2019. Accessed September 29, 2021. https://www.yahoo.com/now/tax-scams-to-avoid-154428486.html

Disclosure

This communication 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.

Any tax advice contained herein, including attachments, is not intended or written to be used, and cannot be used, by a taxpayer for the purpose of (i) avoiding tax penalties that may be imposed on the taxpayer or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.