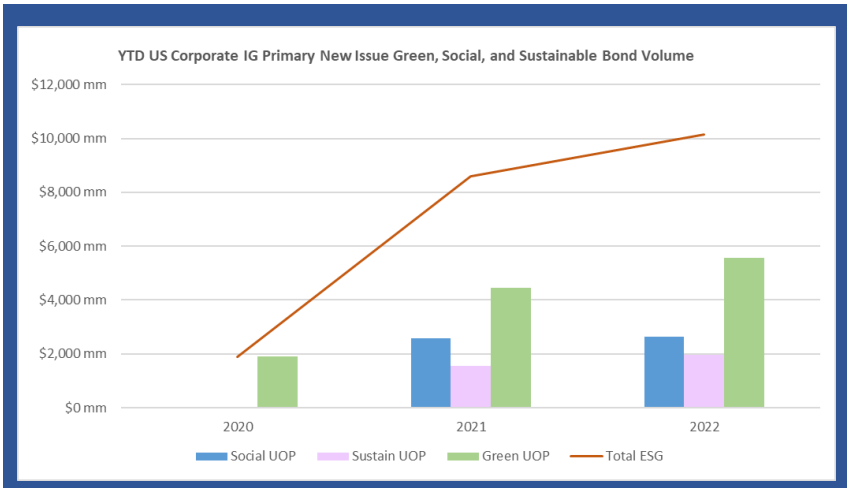
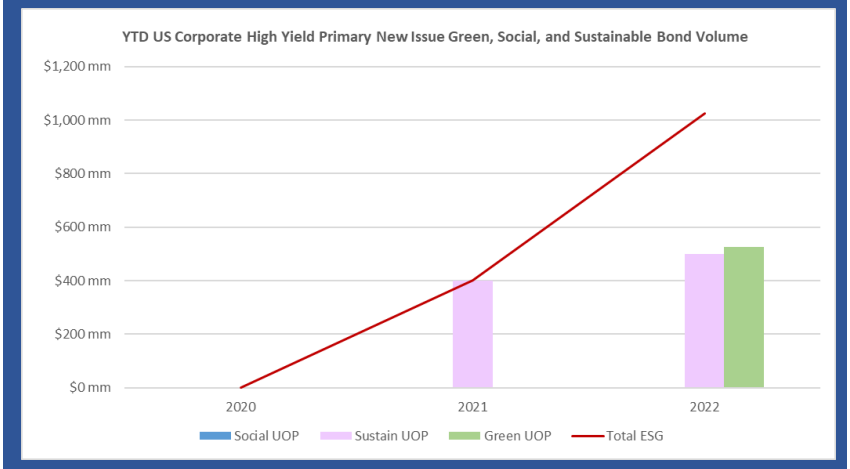
March 2022

With the increasing reliance on digital networks and data coupled with use of cyber-attacks by sanctioned and non-sanctioned threat actors, we continue our coverage on analyzing cybersecurity as a critical ESG issue. In this report we cover:

- Cyber-Threat Landscape
- 4-Ds of Cyber: Destroy, Disrupt, Discredit, Divert
- Economic Costs for Public and Private Sector
- Funding Cyber Resiliency



***Investment Grade**: 2022 ESG themed issuance remains strong compared to broader IG issuance. February saw seven issuers come to market with predominantly green use of proceeds bonds, including Amgen, Verizon, DTE, and Edison International. Archer-Daniel-Midland printed a $750mm inaugural Sustainability bond.*



***High Yield**: No ESG themed HY debt issuance to report for February 2022.*

The Data

This analysis comes from data provided by the Center for Strategic & International Studies' Significant Cyber Incidents tracker, which focuses on cyber-attacks directed towards government agencies, defense, and tech companies, and economic crimes with losses of more than one million dollars. Not all these reported instances are successful cyber-attacks, and some include reported thwarted attacks.

One key challenge to quantifying and tracking this information, in addition to the qualitative nature of cybersecurity reporting, is the time-space component and that many of these attacks are part of long-term campaigns (which can include thousands of attempts to breach). They are also hard to attribute, which is why we use the term "threat actor" and linked the action to the nation which CSIS reports. The term threat actor can also be confusing as it can be a multitude of roles, including hackers for hire or state sponsored terrorist organizations, governments, and criminal gangs.

Still, we tackle it and find that much of our previous geopolitical, ESG, and macro coverage is bolstered by this information and that the security of the networks which help propel our economy and critical infrastructure will remain an area of focus for investors and lawmakers alike for some time.

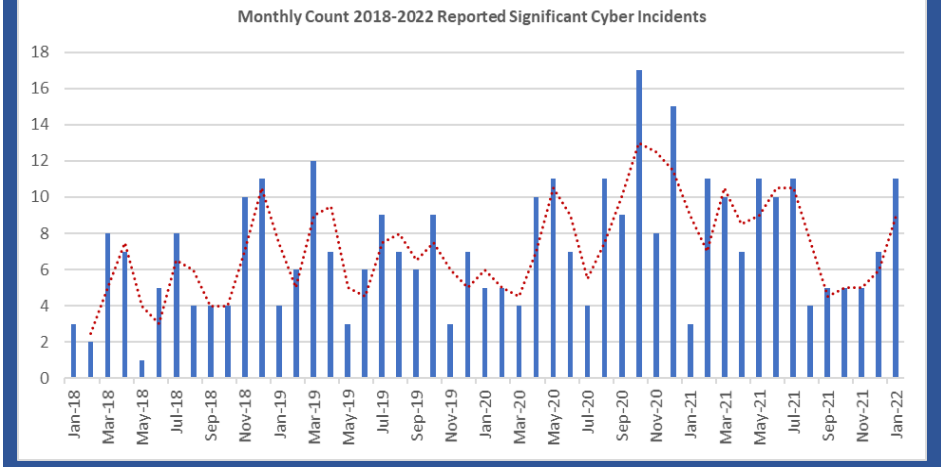
Summary, Critique, & Analysis:

A breakdown of the past ~3 years from the CSIS tracker reveals that global monthly significant cyber incidents continue to rise. In 2020, there was a large global uptick in campaigns, attacks, and breaches that persisted through much of the first half of 2021. While many of the threat actors' origins remain unknown or were unreported, those that have had attribution predominantly include China, Russia, Iran, and North Korea. These four nations account for almost 85% of reported significant cyber incidences in CSIS' tracker from 2018-2022 (mirroring the same comments from our

March 2022

Geopolitical Intelligence Group members!)

As for targets chosen by threat actors, the United States remains one of the top targets (only instances that included multiple nations topped the United States). Ukraine, Iran, Israel, and India followed. Despite China being the chief originator of cyber threat actions, from 2018-2022, China was only reported to be targeted five times (as opposed to the 72 times it was a reported originator).



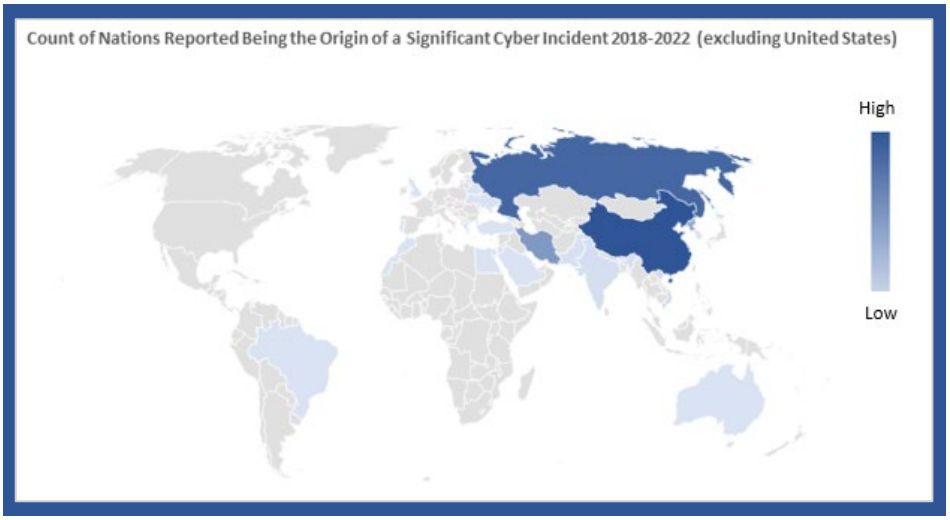
Sector	Russia	North Korea	Iran	China
Transportation Sector	-	-	-	Focus
Healthcare & Public Health Sector	-	Focus	-	Focus
Communications Sector	-	-	Focus	Focus
Government Facilties Sector	Focus	Focus	Focus	Focus
High Value Target/s	Focus	Focus	-	-
Defense Industrial Base Sector	-	Focus	-	-
Energy Sector	Focus	-	Focus	-
Military	Focus	-	-	-
Corporate	Focus	Focus	-	-
Information Technology Sector	Focus	-	Focus	Focus
Activists	-	Focus	Focus	-
Academia	-	-	Focus	-

The table above highlights the top areas/sectors of focus for breach attempts by threat actors from nations where cyber-attacks and threats are attributed. A hash mark does not indicate there has been no attempts, but rather that the sector listed is not a reported predominant focus.

Disrupt-Destroy-Discredit-Divert

If there were a way to synopsize the data, I would borrow from our recent webinar with Rear Admiral Danelle Barrett, where she discussed how threat actors primarily are either looking to ultimately disrupt or destroy. For example, more recently a Belarusian hacktivist group hacked railways to disrupt Russian supply movements. This is opposed to the Stuxnet worm, which was designed (and reportedly used) to destroy Iranian nuclear centrifuges.

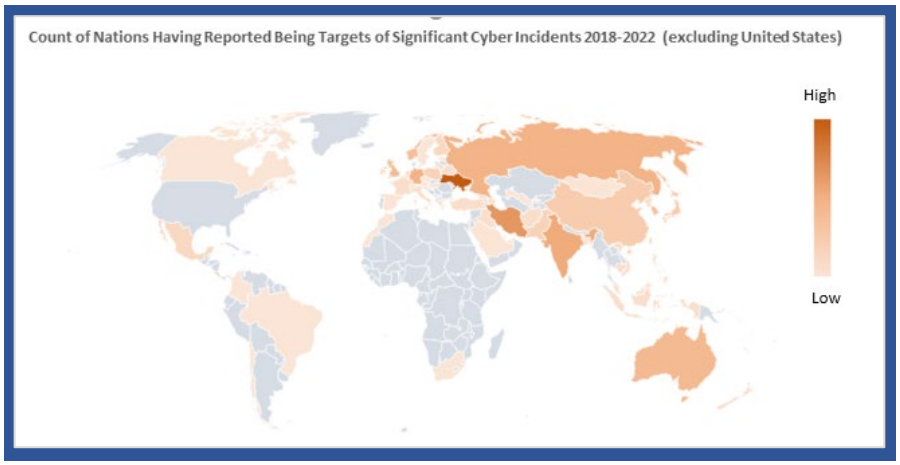
The disruption and destruction components were truly evident in the build up to the recent invasion of Ukraine. In the year leading up to the recent invasion, Russian threat actors launched several cyber-attacks and campaigns on Ukraine's foreign ministry, Secret Services, government officials, and file sharing networks.



In addition to Admiral Barrett's presentation, we would also add discredit and divert. There are several instances where government websites were hijacked to display messaging counter to the nation's prevailing agenda or fake website/social media accounts were established. Lastly, divert usually relates to money (bitcoin or currency) or information being sold. For instance, North Korean hackers in previous years have used SWIFT to divert millions of dollars from banks in Turkey, Mexico, and

India. Between 2015-2018, North Korea alone stole $670mm in currency and crypto.

2021 also saw numerous instances related to diverting or acquiring medical research related to COVID-19. Government health & research organizations, along with private companies, were chief targets. A majority of the 16 reported instances included targets in Europe, the United States, and Israel. China, Iran, and North Korea made up the majority of the nations identified as threat actors.



Cost

Economically, the cost of cybersecurity remains a challenge. Some reports anticipate global costs related to cyber-crimes will be $10.5 trillion annually by 2025. For example, in 2020, India reported that cyber-crimes cost the nation $17.9bn (.62% of its GDP).

CISA calculates the average related cost of cyber incidents per ratio of revenue for many companies at below 1%. Only three companies exceeded a 2% cost to budget ratio related to small and large cyber incidents—the largest was a corporate in 2015 which had a cyber incident resulting in an almost 12% cost-to-revenue ratio. For something like a data breach, the cost on average totaled over $7mm per breach, with investigations & forensics, along with legal defense making up almost 30% of costs. CISA also found that for most publicly traded companies, cyber incidents primarily impacted short-term stock performance.

In the United States more specifically, there were over $4.2bn in losses associated with cybercrime, of which those aged 50+ were the primary victims—with California, Texas, New York, and Florida making up the brunt of the victims' residencies. On average it is reported that the cost per cyber incident is $346mm, with a high-end of $1,866mm.

Bottom Line

Secure networks are already critical to global flows of information, capital, and energy, and will continue to be when considering the role that information plays in facilitating sustainable technology and processes. These networks, like we have mentioned previously, constitute a new "ecosystem" that we now operate in. Similar to how we think about funding "green" grids, we should also be considering how to fund "resilient networks," especially now that they are a chief (and cheap) battleground for interstate conflict. If you're a part of critical infrastructure, or if cyber security is in the top right section of your materiality matrix, then you should be including this in your sustainable financing framework.

- **Utilities and Distributed Energy, Port, Rail, and Logistics Infrastructure; Industrial Design (Ship, Auto, Air), Governments:**
  - Hardware, software, and training
  - Enhanced vendor audits
- **Banks and Financial Institutions:**
  - Internal improvements to systems, audits, and processes
  - Funding to CDFIs or small business to finance cybersecurity and data security improvements

March 2022

- **For Asset Managers/Investors:**
    - Security protocols and investment diligence across geographies
    - Who is on the board or team for investments to ensure:
        - Define high-value information assets?
        - Prioritize governance?
        - Defensive & ability to react?
        - Security conscious culture?
- Industrial design (Aircraft, Land & Sea Transport) & Medical Research are consistent targets

You should see more updates coming out soon as the FBI releases it IC3 report, and others release their yearly reporting on the subject.

Further Resources

McAfee Report: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

FBI Internet Crime Report: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

CSIS Cyber Incident Systemic Review: https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

CISA:https://www.cisa.gov/uscert/sites/default/files/publications/AA22-040A_2021_Trends_Show_Increased_Globalized_Threat_of_Ransomware_508.pdf

CSIS: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Citi Cyber & Human Risk: ***https://icg.citi.com/icghome/what-we-think/securities-services/insights/human-risk-in-cybersecurity***

Academy Cyber Webinar: ***https://www.youtube.com/watch?v=xQNIyO355ZU***