GLOBAL X ETFs RESEARCH

Rising Cybersecurity Threats Expected to Continue in 2022

Authored by:

Pedro Palandrani and Alec Lucas

Date: Jan 28, 2022
Topic: Thematic

Related ETFs

Please click below for fund holdings and important performance information.

BUG – Global X Cybersecurity ETF

We expect the cat-and-mouse game between organizations, consumers and the cybercriminals who covet their data to intensify this year. The latest concern is a vulnerability in internet software known as Log4j that could jeopardize hundreds of millions of systems globally. This threat follows multiple high-profile breaches in 2021, including the ransomware attack that compromised Colonial Pipeline's fuel distribution across the eastern U.S. Cyber events like these continue to grow more frequent and costly, especially attacks on critical infrastructure and supply chains. And this threat is likely to only grow more acute as the global economy continues to digitalize and put sensitive data at risk. As a result, we expect heightened awareness of and expenditure on cybersecurity solutions to create long-term tailwinds for the cybersecurity investment theme.

Key Takeaways:

- Cyberattacks were prevalent and costly in 2021, a trend likely to continue into 2022. The average data breach cost increased from $3.86 million in 2020 to $4.24 million in 2021, the highest total cost in the 17 years IBM has published its Cost of a Data Breach Report 2021.[1]
- Corporations, governments, and consumers are increasing their cybersecurity commitments and enhancing measures to protect themselves. Corporations, for example, are expected to spend $172 billion in 2022.[2]
- Identity, network, and endpoint security continue to be points of emphasis for cybersecurity efforts with network security expected to grow the fastest at 24% between 2021 and 2026.[3]

The Digital World Reveals Its Vulnerabilities in 2021

The world now creates an estimated 2.5 quintillion bytes of data every day—that's 2.5 followed by 18 zeros.[4] As a result, hackers have more access to sensitive data than ever, and they will have many more opportunities as the world continues to digitize and data volumes increase. In particular, the Internet of Things (IoT) devices will be a major contributor to the data pool. At the end of 2021, there were 14.6 billion connected devices.[5] That number could grow nearly 18% in 2022, and then more than double by 2027.[6]

The economy's shift to hybrid and remote work also creates significant opportunities for cybercriminals. Pandemic-induced lockdowns eased in the U.S. in 2021, but as many as 45% of full-time employees continued to work from home at least part-time.[7] Whether due to new variants or employee preference, work-from-home initiatives are likely to remain intact, resulting in data vulnerabilities for the foreseeable future. According to an IBM report, remote work was a factor in 17.5% of reported data breaches in 2021.[8] The average cost of these breaches was also 16.6% higher than breaches where remote work was not a factor.[9]

In 2021, several high-profile companies were victims of costly cyberattacks. The ransomware attack on Colonial Pipeline resulted in a $4.4 million payout to their attackers.[10] CNA Financial paid ransomware hackers $40 million to decrypt parts of their digital infrastructure from which they locked the company out of.[11] And JBS, the largest meat producer in the world, shut down several of its plants due to a cyberattack.[12] These examples are just a few of the major attacks that victimized companies last year, at times resulting in multi-million dollar losses.

BIGGEST CYBER AND RANSOMWARE ATTACKS OF 2021

Source: CRN, "The 10 Biggest Cyber And Ransomware Attacks Of 2021," December 23, 2021., Microsoft, "Microsoft Exchange Server Remote Code Execution Vulnerability," March 2, 2021.

Major Cyberattacks 2021	Industry	Date	Millions of $ Paid or Requested
Microsoft Exchange	Technology	01/5/21	Undisclosed
Kia Motors	Automotive	02/13/21	$20.00*
Bombardier	Manufacturing (Aviation)	02/23/21	Undisclosed
CNA Financial	Financial Services	03/21/21	$40.00
Harris Federation	Education	03/29/21	$8.00*
Colonial Pipeline	Energy	05/7/21	$4.40
Brenntag	Chemicals	05/11/21	$4.40
JBS	Food	05/30/21	$11.00
Kaseya	Information Technology	07/2/21	$70.00*
Accenture	Technology	08/12/21	$50.00*
Acer	Technology	10/5/21	$50.00*

*Requested but not paid in full.

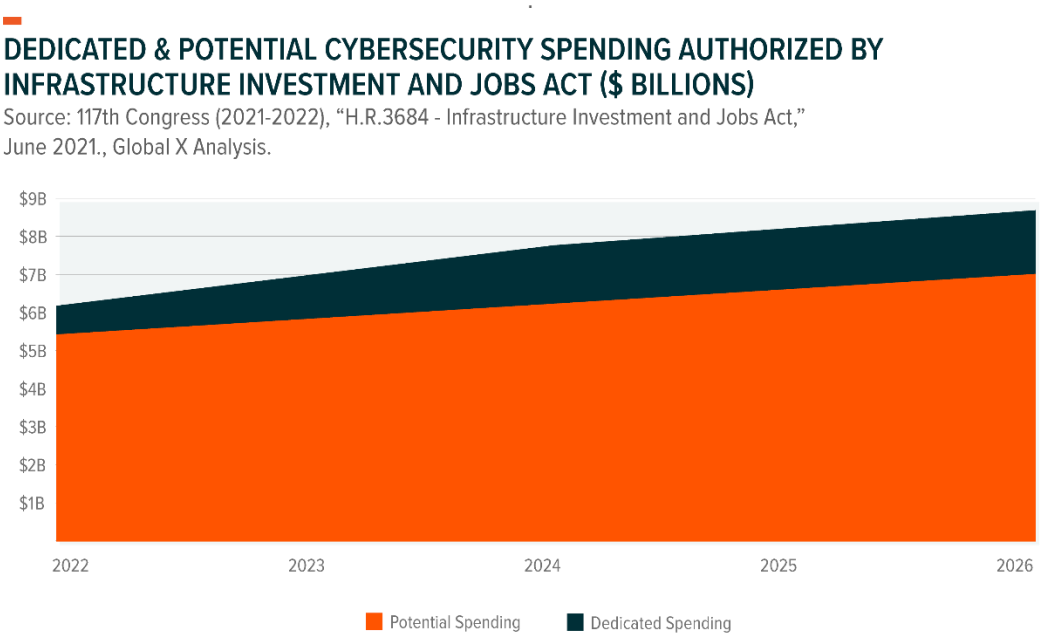
Recent Attacks Encourage Cybersecurity Spending

Even the most sophisticated solutions may not be able to eliminate all vulnerabilities, but they can stymy many threats and help protect against the worst outcomes. In 2021, companies, the U.S. government and consumers demonstrated a growing awareness of cyber threats and commitment to preventative measures.

- **Corporations:** Victims of ransomware attacks, their suppliers, customers and their competitors understand the disruption security breaches can cause. The cost of damages often exceeds the cost of investment in proper solutions. Large enterprises typically spend $2–5 million on cybersecurity annually, while a single ransomware breach costs companies $4.62 million on average.[13,14] That cost is one reason why in a recent survey of more than 3,000 executives, 69% of respondents anticipated more cybersecurity spending in 2022.[15] By one estimate, spending on data protection and risk management could increase 11% from 2021 to $172 billion in 2022.[16]

- **Governments:** In May 2021, President Biden signed an executive order that aims to modernize federal cybersecurity capabilities, standardize response strategies to cyberattacks, and increase information sharing requirements for government contractors. Then in July, Biden signed a national security memorandum that aims to prevent cyberattacks on critical infrastructure, especially power, water, and transportation. These measures translated into real dollars in the Infrastructure Investment and Jobs Act, which directs $1.7 billion in dedicated spending and about $7 billion in potential spending toward improving the country's cybersecurity.[17]

  Also last year, the Senate unanimously confirmed the White House's first national cyber director. Congress created the position as part of the 2021 National Defense Authorization Act, signaling an increased emphasis on cybersecurity in administrations to come.



- **Consumers:** A small but growing share of cybersecurity spending comes from consumers. About 53% of consumers are victims of at least one cybercrime, prompting many to take precautions such as personal VPNs, two-factor authentication, and identity theft protection services.[18] The pandemic exacerbated threats to individuals, as emboldened scammers capitalized on the inflated time consumers spent online. Americans lost $586 million to COVID-related scams as of October 2021.[19] However, consumers are conscious of the heightened threat. Last year, almost 40% of adults took steps to safeguard their online activity as a direct result of the pandemic.[20] Digital protection habits learned during the pandemic could accelerate consumer adoption of cybersecurity services.

Key Cybersecurity Areas to Watch

- **Identity Security:** With the explosion of remote work, securing who's accessing critical data, resources, and apps is a must for organizations. Within this vertical, cybersecurity sub-segments include Identity and Access Management (IAM), Privileged Account Management (PAM), and Identity Governance & Administration (IGA). These sub-segments are forecasted to grow by an average compound annual growth rate (CAGR) of 19% between 2021 and 2026.[21]

- **Network Security:** Companies in this vertical are responsible of protecting a network's integrity, confidentiality, and accessibility from misuse or breaches. Overly permissive networks can cause cyberattacks to move horizontally (i.e. from user to user) once an individual has been compromised. Zero Trust Networks, for example, provide users with access to internal apps, without the need to connect to a company's network or expose those users to the internet. Within this vertical, cybersecurity sub-segments include Zero Trust Network Access (ZTNA), Software-Defined Networking (SDWAN), Network Detection and Response (NDR), Firewall / NGFW / Unified Threat Management (UTM), and Secure Access Secure Edge (SASE). These sub-segments are forecasted to grow by an average CAGR of 24% between 2021 and 2026.[22]

- **Endpoint Security:** The multitude of internet-connected devices presents new entry points for hackers, adding challenges and complexity to effectively manage security for firms and individuals. Successful IoT deployments will require multi-layered, end-to-end security that ranges from up front

baked-in security requirements to the ongoing management and protection of sensitive machine-generated data. Within this vertical, cybersecurity sub-segments include Endpoint Protection Platform (EPP), Endpoint Detection and Response (EDR), and Data Loss Prevention (DLP). Overall the Endpoint Security vertical is forecasted to grow by an 8% CAGR between 2021 and 2026.[23]

Beyond these fast-growing areas, cybersecurity companies are increasingly looking at consolidation. Typically, cybersecurity providers specialize in specific verticals, forcing customers to secure their data using a patchwork of different providers. This dynamic can lead to costly delays and other potentially damaging inefficiencies; indeed, the average data breach took 287 days to identify and contain in 2021.[24] In an effort to improve protection capabilities end to end, several prominent cybersecurity providers engaged in mergers and acquisitions in 2021. Noteworthy activity included CrowdStrike Holdings' $352 million acquisition of Humio, and Rapid7's $335 million acquisition of IntSights, allowing the companies involved to field more integrated product offerings.[25, 26] This surge in consolidation activity is likely to continue in 2022, with antivirus and VPN service providers Norton and Avast set to merge in a deal valued over $8 billion.[27]

Conclusion

2021 featured some of the most impactful cyber intrusions in recent memory, and the world's ongoing digital transformation only increases the likelihood of comparable attacks in the future. However, we believe that digital protection lessons learned during this period could further accelerate the adoption of cybersecurity services. In our view, recent financial commitments to thwart cybercriminals can form tailwinds for cybersecurity companies in 2022 and strengthen the long-term investment case for the cybersecurity theme overall.

[1] IBM, ""Cost of a Data Breach Report 2021," July 2021.
[2] Soffid, "Cybersecurity Trends for 2022, December 29," 2021.
[3] Metric derived from average CAGRs featured in the following sources: Markets and Markets, ""Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026," Feburary 2021., Research and Markets, "SD-WAN - Global Market Trajectory & Analytics," April 2021., Market Growth Reports, "Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026," July 2021., Expert Market Research, "Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed

UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments," 2021., Markets and Markets, "Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026," August 2021., Global X Analysis.
[4] CloudTweaks, “Infographic: How Much Data is Produced Every Day?,” accessed on Nov 15, 2021.
[5] Ericsson Mobility Visualizer, “Connected Devices,” accessed on Nov 15, 2021.
[6] Ibid.
[7] Gallup, “Remote Work Persisting and Trending Permanent,” October 13, 2021.
[8] IBM, (n1).
[9] IBM, (n1).
[10] CNBC, “Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate,” June 8, 2021.
[11] Bloomberg, “CNA Financial Paid $40 Million in Ransom After March Cyberattack,” May 20, 2021.
[12] CNBC, “Meat supplier JBS paid ransomware hackers $11 million,” June 9, 2021.
[13] PCH Technologies, “Cost of Cyber Attacks vs. Cost of Cyber Security in 2021,” July 7, 2021.
[14] IBM, “Cost of a Data Breach Report 2021,” July 2021.
[15] PwC, “Global Digital Trust Insights 2022,” October 2021.
[16] Gartner, “Gartner IT Symposium/Xpo Americas,” October 2021.
[17] Infrastructure Investment and Jobs Act, H.R. 3684, 117th Cong. 2021.
[18] Norton, “2021 Norton Cyber Safety Insights Report Global Results,” May 2021.
[19] CNBC, “Covid-related scams have bilked Americans out of $586 million,” October 18, 2021.
[20] Norton, “2021 Norton Cyber Safety Insights Report Global Results,” May 2021.
[21] Metric derived from average CAGRs featured in the following sources: Technavio, "Privileged Access Management Solutions Market by Deployment and Geography - Forecast and Analysis 2022-2026," January 2022., Mordor Intelligence, "Identity Governance And Administration Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)," January 2022., Technavio, "Consumer Identity and Access Management (IAM) Market by Deployment and Geography - Forecast and Analysis 2022-2026," December 2021.
[22] Metric derived from average CAGRs featured in the following sources: Markets and Markets, ""Zero Trust Security Market by Solution Type (Data Security, Endpoint Security, API Security, Security Analytics, Security Policy Management), Deployment Type, Authentication Type, Organization Size, Vertical, and Region - Global Forecast to 2026," Feburary 2021., Research and Markets, "SD-WAN - Global Market Trajectory & Analytics," April 2021., Market Growth Reports, "Global Network Detection and Response (NDR) Market Growth (Status and Outlook) 2021-2026," July 2021., Expert Market Research, "Global Unified Threat Management Market: By Component: Hardware, Software, Virtual; By Service: Consulting, Support & Maintenance, Managed UTM; By Deployment Mode; By Company Size; Regional Analysis; Historical Market and Forecast (2017-2027); Market Dynamics; Competitive Landscape; Industry Events and Developments," 2021., Markets and Markets, "Secure Access Service Edge (SASE) Market with COVID-19 Impact Analysis, by Offering (Network as a Service and Security as a Service), Organization Size (SMEs and Large Enterprises), Vertical, and Region - Global Forecast to 2026," August 2021., Global X Analysis.
[23] Mordor Intelligence, "Endpoint Security Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027)," January 2022.
[24] IBM, (n1)
[25] Crowdstrike, “CrowdStrike Completes Acquisition of Humio,” March 5, 2021.
[26] VentureBeat, “Rapid7 acquires threat intelligence platform IntSights for $335M,” July 19, 2021.
[27] Norton, “NortonLifeLock and Avast to Merge to Lead the Transformation of Consumer Cyber Safety,” August 10, 2021.