The Next Global Pandemic:
CYBERCRIME

Author

Glenn Cunningham
Analyst, Global Technology

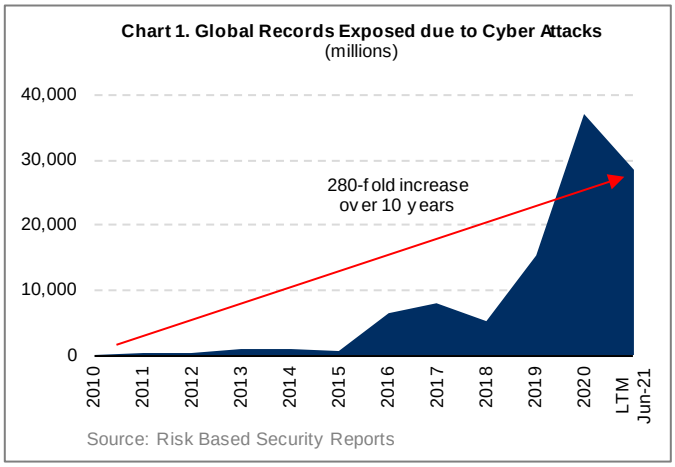
"WE NEED TO PROTECT OURSELVES AGAINST THE CYBER PANDEMIC THAT IS COMING. WE NEED TO PREVENT IT. WE KNOW IT IS COMING, WE KNOW IT WILL HAPPEN, AND WE MUST MAKE SURE IT DOESN'T CAUSE AS MUCH DAMAGE AS THE [COVID-19] PANDEMIC."

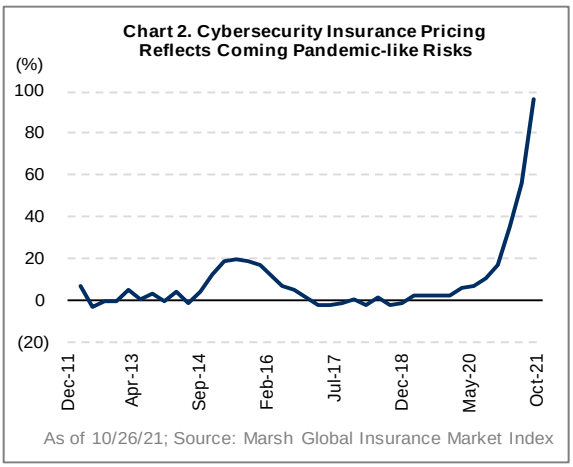
– GIL SHWED, CEO, CHECK POINT SOFTWARE

Data is growing exponentially and cybercrime is exploding.

2020 was a record year for data breaches, up 280-fold from a decade ago (**Chart 1**). Even with this backdrop, many companies around the globe and across all industries have significantly underinvested in protecting their data due to lack of talent, complexity of IT systems, and a focus on profitability.

Our contacts in industries ranging from insurance to cybersecurity to government defense are increasingly worried about a large-scale global cyber event and the potential for pandemic-like political and economic ramifications (**Chart 2**). Governments and regulators have started to engage with a more activist approach to safeguard individual and national interests, but sub-par data security is still one of the most significant and overlooked systemic ESG risks today.





TODAY'S HOTTEST COMMODITY: DATA

Data has become one of the world's most important commodities with the pipes through which it flows being among the world's most critical infrastructure. Elements of our daily lives that feel easier or more convenient are largely due to data mining and exploitation by the companies with which we interact. These companies are able to transform their targeting, customize their advertising, improve the delivery of their products and services, and attract loyal customers because our daily activities like grocery shopping, browsing the web, or streaming media content provide treasure troves of data.

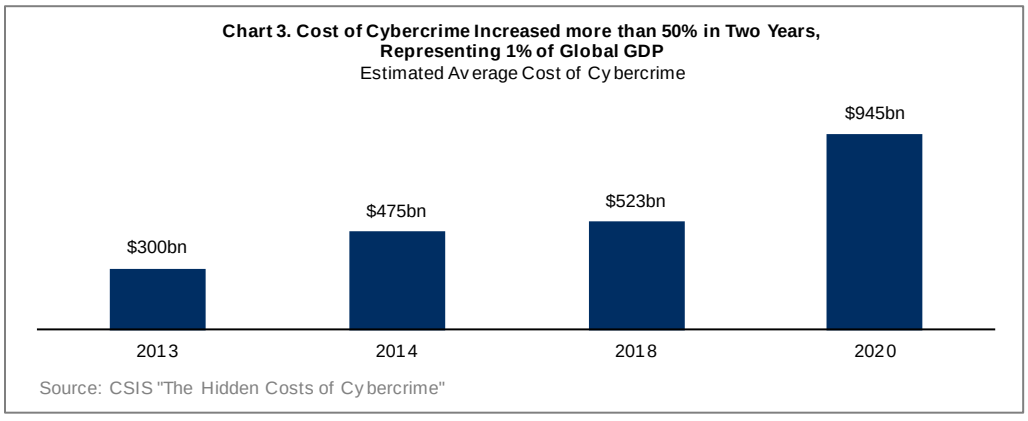
To an unassuming consumer, access to free content, free products, or free trials feels like a perk. But stated simply, if you are not paying for the product, you are the product. This begs the question, "Are the volumes of personal data about you – that are given away freely – adequately protected?"

UNDER ATTACK EVERY 11 SECONDS

The frequency (and associated cost) of global cybercrime has soared, as bad actors seek to gain access to increasingly valuable data. According to Embroker, a leading cyber insurance platform, a ransomware attack now occurs every 11 seconds, up from every 40 seconds in 2016.[1] These attacks are also becoming more audacious and impactful, as evidenced by the highly publicized Colonial Pipeline shutdown earlier this year.

A RANSOMWARE ATTACK NOW OCCURS **EVERY 11 SECONDS,** UP FROM EVERY 40 SECONDS IN 2016.

In its annual *Resilience Barometer Report*, FTI Consulting found that 78% of G20 companies have been victims of a cyberattack in the last year with 70% of respondents saying that data security and privacy concerns impacted M&A decisions.[2] In June 2021, the United States Securities and Exchange Commission issued its first-ever penalties against a public company for deficient cybersecurity risk controls. The potential for liabilities and reputational damage is rising at an unprecedented rate, as is the cost to try to control it. From 2018 to 2020, the estimated cost nearly doubled to $945 billion – representing 1% of global GDP (**Chart 3**).



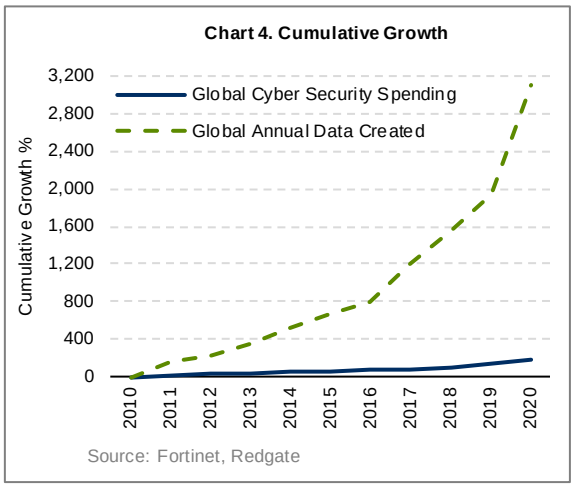
[1] *https://www.embroker.com/blog/cyber-attack-statistics/*

[2] The 2021 Resilience Barometer Report is based on a July 2021 survey of over 2,800 decision makers (C-suite and senior managers/executives) in large companies (over 250 employees or over US$50mm in annual global turnover or balance sheet over US$43mm) across all G20 countries.

Underinvestment in Cybersecurity is a Massive Risk

While data growth has exploded 3100% in the last decade, spending on cybersecurity has grown just one-tenth of that (**Chart 4**). Companies are spending a mere 3.6% of IT budgets[3] on this critical area despite the dramatically higher incidence of attacks. In fact, many companies still run on antiquated IT systems.

Compounding the issue is a shortage of skilled IT talent to assess risks, identify appropriate solutions, and manage upgrades or new system implementations. This complex problem is reflected in FTI Consulting's annual *Resilience Barometer Report*, where 69% of respondents noted that they were struggling to digitize.



In the geopolitical arena, the US government has underinvested to such an extent that President Biden signed an executive order in May 2021 directing the Federal government to accelerate its cybersecurity initiatives. Global underinvestment by countries and companies against threats to this most precious commodity is an enormous, unquantified risk, particularly in the face of increasingly aggressive, frequent, and sophisticated attacks.

Data is a Key Geopolitical Lever

Our contacts within the intelligence community have highlighted the growing prevalence of state actors in the cyber arena as one of the key near- and long-term geopolitical risks. For the last century, access to oil and cheap energy has been a critical factor in geopolitics. Now, data (both its use and misuse) is taking the place of oil as a primary geopolitical lever given its instrumental role in the functioning of the global economy. Examples include Russia's widely believed interference in the 2016 US Presidential election and involvement in the wide-ranging SolarWinds cyberattack in late 2020. The US and Israel famously used cyberattacks to cripple Iranian nuclear progress, while China and North Korea have invested heavily in offensive cyber capabilities.

Governments worldwide are increasingly intervening with more control of data sovereignty, security, and privacy. Due in part to data security issues, China is in the midst of an aggressive crackdown on its internet ecosystem, which has dramatically affected valuations of these companies. The EU released its GDPR regulations in 2016, which restricted companies' ability to remove data from the EU and added significant compliance costs to firms operating in the region. While the US has not yet enacted this kind of sweeping regulation, it is increasingly likely.

As the dangers associated with data become clearer, regulators become more active, and companies and governments are forced to make greater investments, underappreciated risks emerge for certain segments of the market. From our vantage point, these types of regulatory actions present particular challenges to global technology firms that have historically benefited from a combination of

2020 WAS A RECORD YEAR FOR DATA BREACHES, UP 280-FOLD FROM A DECADE AGO.

[3] Source: Gartner

significant growth, high profit margins, and minimal regulation. As it turns out, no companies are immune from the direct or indirect effects of the growing cybercrime issue.

Threat Prevention & Softening the Blow

Despite the challenges and pressures that global technology firms face due to new cybersecurity-related regulations, the themes of data security and privacy present significant opportunities for companies focused on addressing problems related to both. Continuous innovation in cybersecurity provides a steady stream of new, fast-growing companies entering the market. While we frequently admire these companies and the work they are doing to protect companies and consumers, they often trade at valuations that provide little margin of safety.

Particularly in fast-changing industries, it is critical to engage throughout the value chain to understand the dynamics shaping the future success – or failure – of companies in the ecosystem. We find that our relationships with venture capitalists are among the most valuable as we evaluate innovations, consider potential impacts, and assess fundamental drivers.

Currently, we are identifying compelling opportunities in two broad buckets:

- Companies that can help to **prevent** cybersecurity issues
- Companies that can help to **manage the impact** of issues

Companies and governments around the world must increase their investment in IT modernization and cybersecurity. This creates a lucrative opportunity for companies exposed to that spending. IT security companies like Check Point, Cisco, and NortonLifeLock directly supply security software and services. IT services providers like Cognizant act as trusted partners in helping companies digitize, thereby bridging the skills gap and skilled labor shortage. Finally, software and technology companies like SAP and Oracle are poised to benefit as companies upgrade their core, mission-critical systems, fundamentally improving cybersecurity.[4]

Additionally, there is a growing opportunity for P&C insurance companies, as brokers increasingly advise on cyber risk and insurers protect customers against cyberattacks and losses. The total addressable market is new, large, and fast growing; however, insurers are approaching it with considerable caution given the risks.

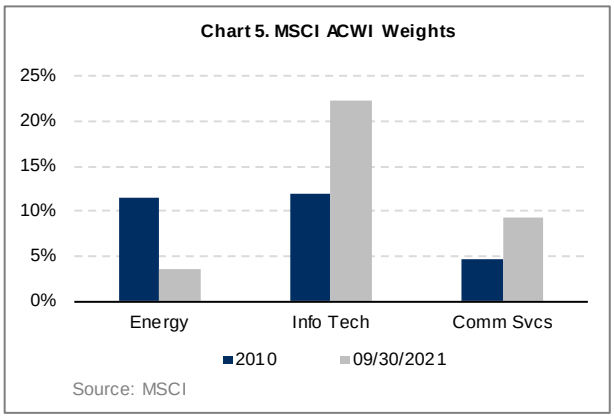
Sub-par data security is one of the most significant and overlooked systemic ESG risks today.

Data security and privacy are common discussion topics during our ESG engagements with companies across industries, as they are linked to both governance ('G') and social ('S') considerations. Our goal is to understand a management team's recognition of the risk and/or opportunity associated with cyberattacks and their commitment to protecting their company and their end constituents. The strength of their awareness and action plan has important ramifications on both long-term margin assumptions (i.e. will there be a need for additional spending?) and the potential impact of a high-consequence event (i.e. what are the ramifications of a large-scale cyberattack?). Through continued dialogue with company leaders and others in the ecosystem, we track progress and commitment to safeguarding company assets.

[4] The securities identified in this letter are not necessarily held by Altrinsic Global Advisors, LLC for all client portfolios, and should not be considered a recommendation or solicitation to purchase or sell these securities. It should not be assumed that any investment in these securities was, or will be, profitable. The outlook and opportunities noted in this letter are prospective and based upon the opinions of Altrinsic as of the date of this letter. There is no guarantee that we will be successful in our efforts to implement investment strategies that take advantage of such perceived opportunities. Please see Important Considerations and Assumptions at the end of this letter for important additional disclosures.

Conclusion

The world has changed and the only constant as we look ahead is the promise of more – and faster – change. The MSCI ACWI Index's composition is just one reflection of the increasing influence of data and its stature as one of the world's most valuable commodities. Over the last decade, the energy sector's representation within the index has dropped from about 11.5% to 3.5%. In contrast, data-intensive industries such as technology and communications services have risen dramatically (**Chart 5**).



After a decade of unimpeded growth, companies – particularly in the technology sector – are facing a new competitive environment shaped by increasing focus on data security, heightened awareness of privacy concerns, and more stringent regulations. This combination of factors has resulted in a higher cost of doing business. Simultaneously, all companies are at greater risk of highly consequential, de-stabilizing, and disruptive cyberattacks. As data becomes more valuable, the risk of cybercrime turning into the next pandemic increases. We believe that the associated political and economic risks are among the most underappreciated by the market.

With change and volatility comes opportunity. We are finding a growing number of compelling investment opportunities among companies that provide prevention and/or impact mitigation solutions to these data management and cybercrime related challenges. Insurers, consultants, and technology firms are the primary hunting ground for new investment ideas in this realm. We continue to leverage our deep domain expertise, broad industry networks, and global perspective to identify underappreciated investment opportunities amid the ongoing disruption.

About Altrinsic Global Advisors, LLC

Altrinsic Global Advisors, LLC, founded in 2000, is an employee-controlled and majority-owned investment management firm. Altrinsic manages approximately US$10.5 billion[5] in global and international equities, applying a long-term private equity approach to public equities. Altrinsic's clients include corporate and public pension plans, endowments, foundations, sovereign wealth and sub-advisory clients. For more information, please visit www.altrinsic.com or contact Sara Sikes at +1 (203) 661-0030.

[5] As of 09/30/21

Important Considerations & Assumptions

This document has been prepared solely for informational purposes and nothing in this material may be relied on in any manner as investment, legal, medical, accounting or tax advice, or a representation that any investment or strategy is suitable or appropriate to your individual circumstances, or otherwise constitutes a personal recommendation to you. All information is to be treated as confidential and may not be reproduced or redistributed in whole or in part in any manner without the prior written consent of Altrinsic Global Advisors, LLC ("Altrinsic"). The information contained herein shall not be relied upon as a primary basis for any investment decision, including, without limitation, the purchase of any Altrinsic products or engagement of Altrinsic investment management services; there is no and will be no agreement, arrangement, or understanding to the contrary. This material has been prepared by Altrinsic on the basis of publicly available information, internally developed data and other third party sources believed to be reliable. No assurances or representations are provided regarding the reliability, accuracy or completeness of such information and Altrinsic has not sought to independently verify information taken from public and third party sources. Altrinsic does not accept liability for any loss arising from the use hereof. Any projections, market outlooks, opportunities or estimates in this document are forward-looking statements and are based upon certain assumptions and are subject to change. Due to various risks and uncertainties, actual events or results, or the actual performance of any investment or strategy may differ materially from those reflected or contemplated in such forward-looking statements. Except where otherwise indicated, the information provided, including any investment views and market opinions/analyses expressed, constitute judgments as of the date of this document and not as of any future date. This information will not be updated or otherwise revised to reflect information that subsequently becomes available, or changes in circumstances or events occurring after the date hereof. This material, including any specific security or strategy references, does not constitute investment advice and should not be viewed as current or past recommendations or a solicitation of an offer to buy or sell any securities or to adopt any investment strategy. Readers should not assume that any investments in securities or strategies referenced were or will be profitable. Investing entails risks, including possible loss of principal. This document is not intended for public use or distribution.