Accessible version

BANK OF AMERICA
INSTITUTE

BANK OF AMERICA

Transformation

Cybersecurity: Landscape, impact and what comes next

24 May 2023

Key takeaways

- With more than 1,800 data breaches across the US in 2022, 63% more than a pre-pandemic year (source: Identity Theft Resource Center report), cybersecurity controls and cybersecurity companies are under increasing pressure to do more.
- But BofA Global Research believes that factors such as an uncertain economic outlook, challenges with the Zero Trust framework, artificial intelligence risks and an ever-changing landscape of data solutions, could only reinforce the critical importance in maintaining a robust cybersecurity stack as the increasing velocity of cyberattacks may intensify.
- Recently, BofA Global Research analysts spoke with Chief Information Security Officers (CISOs) and distributors across a broad range of industries about cybersecurity budgets, spending patterns and trends for 2023.

Cybersecurity landscape

Cyberattacks are becoming more frequent and expensive as trends such as digitalization, hybrid work, and the transition to the public cloud increase the potential for a cyberattack across organizations' networks. In 2022, widespread corporate adoption of a post-pandemic hybrid working model meant that cybersecurity controls were sometimes bypassed, contributing to an increase in cyber threats. That same year, there were more than 1,800 data breaches in the US, 63% more than a pre-pandemic year (source: Identity Theft Resource Center report) and the average cost per incident in the US was $4.2 million, the highest in 17 years (2021 data, Cost of a Data Breach Report 2022, IBM).

With an uncertain economic outlook for 2023, including some anticipation of a recession, cybersecurity companies are under increasing pressure to do more, potentially with less. But as we learned in the 2008 recession, which saw a 47% increase in the number of data breaches (source: Identity Theft Resource Center report), lax security will likely incentivize cybercriminals to create new types of threats. There are a few reasons why: 1) budgets could contract for information security products and solutions, 2) the industry may see a skills shortage, meaning that the hiring of expertise could slow significantly and 3) innovation could suffer if security vendors lose budget for research and development. So, while budgets currently remain intact, the question of a slowdown in cyber spending remains to be seen.

Budgets intact, price increases, scrutiny on procurement slowing cyber spend

At a recent cybersecurity conference, BofA Global Research analysts spoke with Chief Information Security Officers (CISOs) and distributors across a broad range of industries including tech, media, retail, and financial services about cybersecurity budgets, spending patterns and trends for 2023. Across the board, they found that 2023 budgets remain intact, and the large majority of CISOs even noted a slight uptick in budget (~10% on average) given that the increasing velocity of cyberattacks reinforces the criticality of maintaining a robust cybersecurity technology stack, driving resiliency in spend across enterprises.

However, despite relative spend durability, budget allocation has shifted to having a greater focus on price increases from existing vendors in addition to procuring new solutions to address critical needs. The observed price increases ranged from 10-30%, with some vendors asking for a 50% increase at the time of contract renewal. As a result, CISOs are taking longer to renew contracts as they evaluate contract scopes and competitor offerings, which could account for some of the recent sales elongation seen in cybersecurity earnings.

In our view. enhanced scrutiny from procurement teams is the main headwind to cyber spend, despite the budget runway. As enterprises look to tighten spend, firmwide updates to procurement processes have been introduced, adding additional friction to the buying process. Many of the CISOs that BofA Global Research spoke to are now required to develop return-on-investment analyses, show proof that technology is not duplicative, and justify the business need. They also underscored that the complexity of cybersecurity technology has made it challenging to gain support from necessary business partners such as Chief Financial Officers and Chief Operating Officers.

Is the cyber skillset gap widening?

While cybersecurity spend is mission critical for enterprises, BofA Global Research expects the longer procurement processes to persist beyond macro challenges as companies pull back from spend at all cost mentalities that have persisted over the last few years. And with recent CY23 budget allocation skewing towards tools versus compensation, a shortage of specialized skills in cyber is likely to continue. In fact, the global cybersecurity workforce gap - the shortfall between supply and demand for cybersecurity professionals - was estimated at 2.7 million in 2021 (source: WEF).

Cyber insurance: A promising concept, but a challenging reality

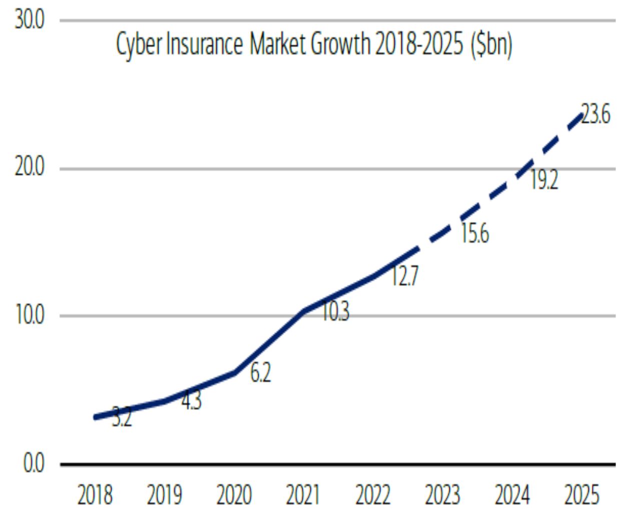
Enterprises are increasingly leveraging cyber insurance as a cost-hedging strategy, yet the cost of insurance, and the level of protection insurance companies are willing to provide have worsened over time. The cyber insurance market grew ~25% in 2021, to $10.3 billion, representing ~1% of total commercial insurance spend. And according to BofA Global Research, the market is poised to grow at a 25% CAGR through 2025, reaching a total market size of $23.6 billion, versus the 9.7% CAGR of the broader commercial insurance market.

Strong growth in the market is driven by multiple trends including the accelerating frequency and scale of cyberattacks, the growing cost of data breaches and ransomware remediation and premium increases. Privacy laws that enforce strict protections on consumer data, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA), are now being adopted across various other states, and continue to drive growth for the cyber insurance market. However, privacy laws are still in their early innings as they have yet to be widely adopted across the US, and their impact on cyber insurance growth has been limited to mostly large global organizations.

While the cyber insurance market is forecasted to grow faster than the broader insurance market, there are a few possible restraints on growth: 1) declining appetite for full policies as premiums rise and coverage is reduced, 2) organizations band together to form group policies, which would negatively impact growth and margins for cyber insurers and 3) reinsurers lower the amount of cyber risk they are willing to take on, which will impact the number and scope of policies insurers are able to underwrite.

Exhibit 1: Cyber insurance market growth through 2025 ($bn)

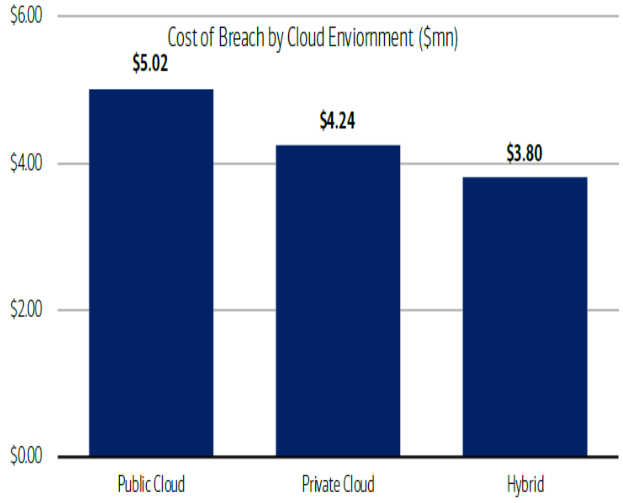
The cyber insurance market is growing at 25% CAGR through 2025



Source: MarketsandMarkets, BofA Global Research

Exhibit 2: Cost of breach by cloud environment ($mn)

Public cloud breaches are more costly than private cloud and hybrid cloud breaches



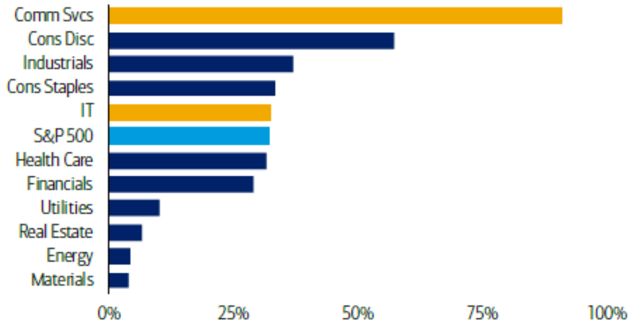
Source: IBM, BofA Global Research

Cybersecurity and ESG

Major ESG-related controversies, including data breaches, have wiped out $600 billion+ of S&P 500 market cap since 2013. The stock bottoming process lasted for more than one year on average, and it took an average of two years for employees' perception of their company's culture to improve following ESG scandals. And ESG "darlings" tended to fall harder on negative headlines, as ESG funds were quick to reduce exposure. In fact, 65% of ESG funds liquidated or cut their stock position within three months of an ESG controversy breaking. In addition, 90% of S&P Communication Services companies suffered recent data privacy or security-related controversies vs. 30% of the overall S&P 500 (Exhibit 3).

Exhibit 3: Percentage of companies with data privacy and security controversies, by sector as of 2/14/23

91% of Comm Svcs. and 32% of Tech companies have had recent controversies in data privacy and security



Source: Sustainalytics, BofA Global Research

Are companies responsible for their own cyberattacks, or are they victims?

One hotly contested issue is: who is accountable in a cyberattack? Should a company whose systems have been compromised be held responsible for breaches, or is the company a victim of cybercrime? Some suggest that burden should fall on the company provided it has established that it did not perform adequate due diligence around information technology (IT) asset security. But firms that hold their executives accountable for their own data breaches are the exception not the rule, perhaps due to the shortage of cyber expertise on boards and management teams. The proportion of Fortune 100 companies with executive compensation tied to cybersecurity/privacy issues dropped to just 7% vs. 11% in 2021 (source: Harvard Law). And IT and Communication Services lag most in aligning CEO compensation with ESG goals in the US.

CISOs more muted on Zero Trust, citing implementation difficulties

A Zero Trust security framework requires all users, whether in or outside of an organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. This framework has been gaining steam over the last few years after President Biden signed an Executive Order requiring federal agencies to adopt Zero Trust architecture. Shortly after, the National Institute of Standards and Technology (NIST) published official guidelines for implementing Zero Trust, and the Cloud Security Alliance, an organization dedicated to defining the best cloud computing practices, invested in a Zero Trust advancement center providing training to industry professionals. While CISOs and distributors agreed on the importance of the Zero Trust framework, implementation difficulties and architectural complications have made adoption challenging.

Micro-segmentation, a key component of the framework, was cited as the main difficulty when implementing and maintaining Zero Trust. Micro-segmentation involves dividing the network into smaller segments, typically at the application layer, and then implementing granular security policies for each segment. The purpose of micro-segmentation is to reduce the attack surface by restricting lateral movement within the network.

In practice, micro-segmentation can be challenging to implement given the complexity of defining the segments and the necessary security controls for each segment. Additionally, each new application that is introduced into the network needs to be mapped to the appropriate segmentation and subsequent policies. As a result, the Zero Trust architecture can become very complex in a short amount of time, with each change to the network adding to the complexity. While CISOs are in favor of the theoretical benefits of Zero Trust, current products in the market have difficulties easing the implementation, creating a barrier of implementation for many.

AI creates more risks than opportunities, specifically around data security

We would be remiss not to mention artificial intelligence (AI). Cybersecurity is not immune from the reaches and growth of AI, and in fact, as mentioned in our recent publication, Me, Myself & AI, AI may create more risks than opportunities for the industry. Starting with the opportunities: Microsoft recently announced the launch of Security Copilot, which will provide real-time security information to IT teams while helping to remediate security risks. The tool is expected to reduce manual burdens on already overstaffed security teams and a plethora of new companies are expected to integrate AI into threat detection, security policy creation and identity moving forward.

However, many CISOs expressed concerns about AI's impact on the threat landscape, particularly in regard to data security, governance and privacy. Data risks stemming from AI usage include sensitive data leakage, compliance to data privacy laws and IP ownership of data created by AI. To mitigate risks, CISOs are prioritizing investments in data security and governance solutions. Examples of these solutions include: 1) tools that contextualize and filter out sensitive data such as credit card information or proprietary customer data, 2) tools that ensure AI requests do not send customer data to the wrong customers and 3) policies around AI management and the data stores it is able to pull from.

CISOs also noted how simple it is for hackers to generate new threats as generative AI models can write and copy specific lines of code that previously took sophisticated engineers hours to write. For example, a cybercriminal with no coding or technical knowledge can easily ask AI for the details of a specific vulnerability in a historical breach and the response will include the exact code targeting the vulnerability, which can then be used to attack multiple sites simultaneously. CISOs unanimously agreed that the most effective way to handle the risks of AI are to embrace it so that employees do not use backdoor methods for access, which would create an even broader vulnerability surface as there would be no monitoring or safeguards in place. However, there are still many security challenges around AI yet to be solved.

The next frontier for cybersecurity?

Secure Enterprise Browsers pose a serious threat to Secure Web Gateway

Secure Enterprise Browsers (SEB) are gaining traction and CISOs are evaluating the technology as a potential replacement to Secure Web Gateway (SWG) solutions. What's the difference? Both technologies address internet traffic security but do so in different ways.

SWG is deployed at the network level and acts at the gateway between internet traffic and the network. On the other hand, SEB is a web-based browser that is deployed on endpoints and configured to prevent attacks on web applications. While SWG has been the preferred technology over the last few years, SEB is proving to be a competitive alternative for cloud native companies and companies that rely on virtual private networks (VPN) for their workforce. Because SEB is deployed at the endpoint level, it prevents malicious code from spreading across the network unlike SWGs that run at the network level and therefore do not provide the same level of isolation.

Similarly, SEB is able to isolate an individual user's browser sessions and prevent malicious code from running, while it is difficult for SWG to protect users at such a granular level. As a result, SEB solutions may be better suited than SWG for companies with disperse workforces. SEB granular control over data and application access and usage, as well as ease of deployment, is an advantage compared to SWG, which becomes more difficult to configure and manage as network complexity grows. The rise of SEB could put pressure on SWG vendors especially in verticals that are heavily skewed towards cloud native or remote workforce companies, however once deployed, SWG solutions tend to be sticky given their complexity.

API security has become a top budget priority for CISOs in 2023

Application Programming Interface (API) security remains relatively new, yet CISOs and industry experts that BofA Global Research analysts have recently spoken with view APIs as a key focus in 2023 and believe API security will likely become integral to protecting the network.

In general, APIs serve as the building blocks for application and infrastructure design by creating connections between databases, apps, networks, and devices. Many APIs are publicly available, which allows developers to integrate services and features in a "plug and play" format and brings some much-needed simplicity to the development lifecycle.

APIs are used for both internal- and external-facing applications to reduce complexity and time to production for developers to push new features to end users. The use of APIs has exploded with the adoption of cloud computing and has created another key attack vector, or way for attackers to enter a network or a system, for bad actors.

Like cloud resources, many security teams are unable to manage and even identify the number of APIs in their digital ecosystems. Additionally, since developers are often not security-focused, there is room for oversight from a lack of awareness and communication between security and DevOps teams from an API stance. This can lead to vulnerabilities within the network should a cybercriminal compromise an API, as they could have access to sensitive data, account credentials and other critical digital network assets. As a result, API security is becoming one of the most talked about security fronts among cybersecurity professionals.

Context is king with data security solutions

Data security technology has been an important part of the cybersecurity stack for many years. Tools such as data loss prevention (DLP), data security posture management (DSPM), and data backup and restoration command a material amount of cybersecurity budgets. Data scanning and relationship mapping is another innovation that can help protect against attacks as it correlates data to applications and users while uncovering duplicative and shadow data that could pose risks to the enterprise.

However, most data solutions lack a critical function - context. As networks modernize and identity becomes the new network perimeter, context becomes crucial for data protection.

Context allows for more granular protections necessary for modern networks, and emerging vendors are adding context to standard data security solutions in a multitude of ways. Some vendors are adding behavioral AI/ML (artificial intelligence and machine learning) elements to solutions that notify security teams when a user's network movements look suspicious compared to typical patterns. Others are introducing different protocols depending on initial identity verification.

Take for example an incoming request to make changes to sensitive customer data. Current solutions grant the request as long as the identity and endpoint have been verified, regardless of identity type (machine, workload or user) or the source of the request (API, container or endpoint). Because of this, even if credentials or devices are stolen, hackers are still able to move around the network without being identified.

Embedding context into data security solutions is necessary to maintain the security and compliance that data requires.

Disclaimer

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness, or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to, warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Contributors

Vanessa Cook

Content Strategist, Bank of America Institute

Sources

Tal Liani

Research Analyst, BofA Global Research

Madeline Brooks

Research Analyst, BofA Global Research

Savita Subramanian

Equity & Quant Strategist, BofA Global Research

Dimple Gosai

US ESG Strategist, BofA Global Research

Haim Israel

Equity Strategist, BofA Global Research

Martyn Briggs

Equity Strategist, BofA Global Research

Felix Tran

Equity Strategist, BofA Global Research

Disclosures

These materials have been prepared by Bank of America Institute and are provided to you for general information purposes only. To the extent these materials reference Bank of America data, such materials are not intended to be reflective or indicative of, and should not be relied upon as, the results of operations, financial conditions or performance of Bank of America. Bank of America Institute is a think tank dedicated to uncovering powerful insights that move business and society forward. Drawing on data and resources from across the bank and the world, the Institute delivers important, original perspectives on the economy, Environmental, Social and Governance (ESG) and global transformation. Unless otherwise specifically stated, any views or opinions expressed herein are solely those of Bank of America Institute and any individual authors listed, and are not the product of the BofA Global Research department or any other department of Bank of America Corporation or its affiliates and/or subsidiaries (collectively Bank of America). The views in these materials may differ from the views and opinions expressed by the BofA Global Research department or other departments or divisions of Bank of America. Information has been obtained from sources believed to be reliable, but Bank of America does not warrant its completeness or accuracy. Views and estimates constitute our judgment as of the date of these materials and are subject to change without notice. The views expressed herein should not be construed as individual investment advice for any particular client and are not intended as recommendations of particular securities, financial instruments, strategies or banking services for a particular client. This material does not constitute an offer or an invitation by or on behalf of Bank of America to any person to buy or sell any security or financial instrument or engage in any banking service. Nothing in these materials constitutes investment, legal, accounting or tax advice.