Cybersecurity

Thought Piece

November 2022

Introduction

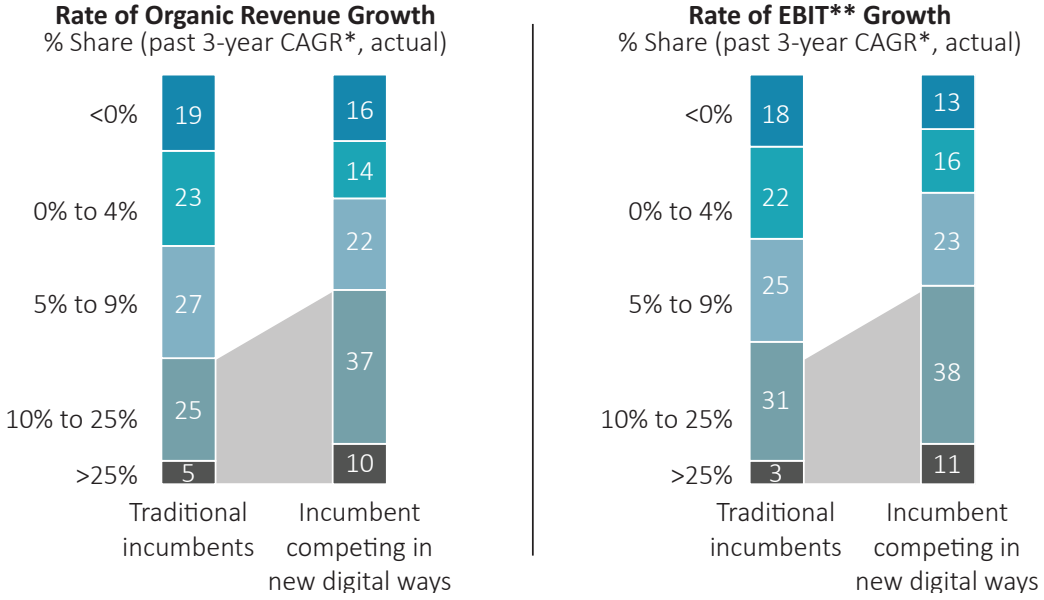
Over the past decade, as businesses have undertaken digital transformation initiatives to improve efficiencies and outcomes, cyberattacks have continued to increase in both frequency and complexity. These cyberattacks are increasingly committed by well-funded criminal and state-sanctioned groups seeking to exploit vulnerabilities and disrupt operations for financial gain or to steal intellectual property and other sensitive data for competitive gains or national intelligence purposes. Since the onset of the COVID-19 pandemic, businesses of all sizes have responded to new, unexpected customer and employee needs by accelerating their investments in digital technologies. These investments have not only driven positive business outcomes but have also created new areas of vulnerability for companies across their entire technology supply chain and infrastructure. The increase in the number of endpoints resulting from the exponential growth of mobile computing and Internet of Things (IoT) devices, as well as the larger technology infrastructure surface areas supporting cloud-computing needs, has provided cyber attackers with more areas to potentially exploit and gain unauthorized access. These cyberattacks contribute to a wide variety of adverse outcomes—lost revenue from network downtime, increased costs from ransom payments, fines and/or mitigation spending, lost data integrity, impact to the business from increased reputational risk and, in certain cases, national security risks. As businesses continue to invest in digital transformation to accelerate growth initiatives, the increased threat from cyber criminals will also require larger and more targeted investments in next-generation cybersecurity defense technology to protect digital assets and networks while minimizing the operational and financial costs of a cyberattack.

Digital Transformation & Network Vulnerabilities

The digital transformation era has brought about a major change in how businesses build and operate their networks as well as how they communicate and interact with their customers. Before the evolution brought on by digitization initiatives, the traditional office network consisted of on-premises data centers accessed by intranet capabilities and VPNs (Virtual Private Network), which were reserved for remote access to only the most critical applications. In addition, customer communication and marketing were primarily accomplished through email and telephone. However, as we have witnessed over the past decade, businesses have begun implementing digital strategies to enhance business productivity, accelerate revenue and pursue margin growth opportunities.[1]

As businesses implement these digital-first strategies, they are moving data center and workload infrastructure to the cloud, utilizing IaaS/PaaS tools provided by vendors such as Microsoft Azure, Amazon Web Services (AWS) and ServiceNow alongside SaaS applications such as Salesforce.com and Adobe. Businesses are making investments to support remote work and enhance productivity, resulting in more endpoint devices such as personal laptops and smart tablets being used to connect to the network outside of the

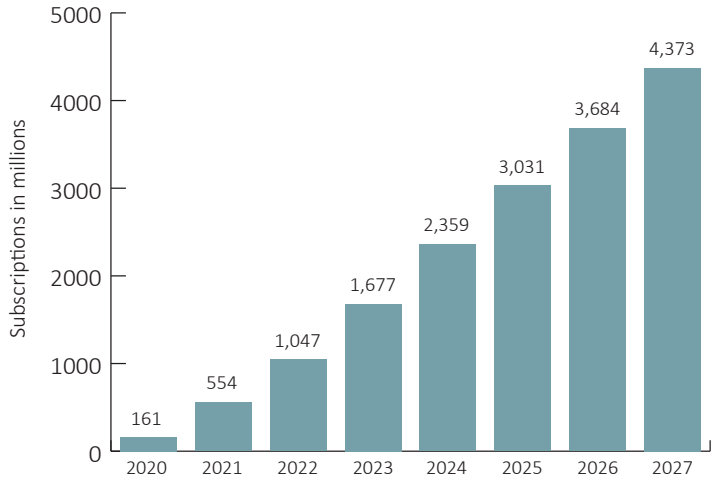
Bold, tightly integrated digital strategies are the most effective approach to digital transformations.



Note: Numbers may not add up due to rounding.
**Compound annual growth rate*
***Earnings before interest and taxes*
Source: 2017 Digital Strategy Survey

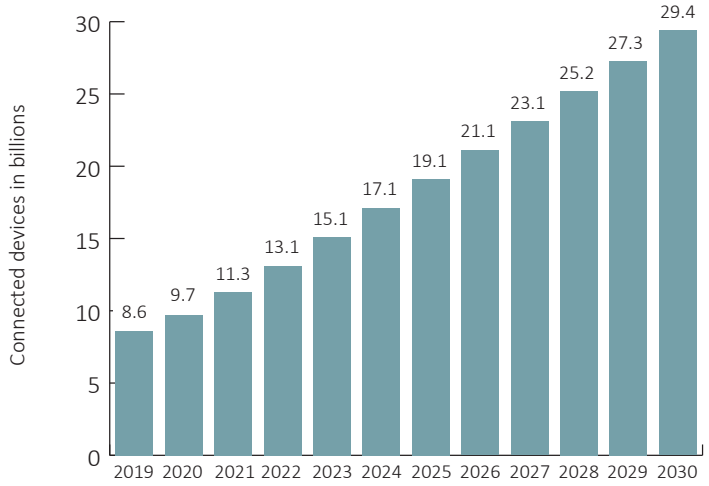
traditional corporate firewall. The approach to customer communication is also evolving with a multichannel strategy incorporating digital media platforms such as Facebook, TikTok, Instagram and Google. At the same time, investments in 5G technology and infrastructure have supported a rapid increase in 5G-enabled and IoT devices for both consumer and industrial end markets.[2,3]

Mobile 5G Subscriptions Worldwide Forecast 2020-2027



Source: Ericsson

Number of IoT Connected Devices Worldwide 2019-2030



Source: Transforma Insights

While digital transformation investments allow for more cost-effective network architectures that enhance productivity and efficiencies, they also ultimately result in larger attack surfaces with more potential vulnerabilities that can be leveraged for malicious intent. As an example of the increased threat surface due to the growth of IoT devices, a survey by the security firm Extreme Networks found that 84% of organizations have IT devices connected to their networks and more than 50% of them have not upgraded security protocols beyond the default password.[4] This type of vulnerability extends to many other network devices, highlighting the threat posed to networks resulting from the rapid growth of endpoints. While a business may have more robust security protocols implemented in other areas of the network infrastructure, a single unexpected point of vulnerability, such as an IoT device with weak security properties, can be used to compromise the integrity of the entire business's network.

Cyberattack Techniques

While businesses continue to invest in digital initiatives, cybercriminal groups themselves are benefiting from digital transformations. These cyber attackers use distributed computing technology and tools such as ransomware-as-a-service, malware-as-a-service, Artificial Intelligence and automated computing to accelerate the development of the attack protocol, ultimately resulting in an increase in the frequency of attempts and the number of successful breaches. In its 2021 report, the cybersecurity firm FireEye estimated that there are more than 1,900 distinct hacking groups comprised of state-sponsored groups, financially-motivated groups and a third uncharacterized group.[5] The techniques used by these groups to exploit vulnerabilities and infect systems with malicious software vary, but by far the most common approach remains phishing emails sent to business employees. Other areas of vulnerability include poor user practices, lack of training and weak password management. What this all has in common is that human error is the key weak point. In fact, it has been estimated in a study by Stanford University and Tessian that 88% of all data breaches are due to human error and employee mistakes.[6]

The unfortunate factor of human error being the weak link in cyber defenses has been demonstrated many times. In September 2022, Uber was the victim of a cyberattack after an external contractor failed to follow security protocols and accepted a two-factor authentication login that was initiated by the attacker. As a result, the cybercriminal group known as "Lapsus$" was able to gain access to Uber's privileged access credentials and breach the company's entire network infrastructure, which included gaining access to customer data. One of the largest breaches and thefts of customer data occurred during the 2016 attack on Yahoo, when cybercriminals, believed to be state-sponsored, sent a spear-fishing email to a Yahoo employee which, when opened, allowed the hackers to steal personal data from an estimated 3 billion accounts over a 3-year period. The May 2021 Colonial Pipeline ransomware attack by "DarkSide", a Russia-based cybercriminal group, was enabled through the manipulation of a former employee's password for a VPN that was not secured by multi-factor authentication technology and also had not been removed from the privileged access management list. As a result of this hack, the company's main pipeline that supplies 45% of the East Coast fuel supply was shut down for five days. Hacks such as these make it clear that cybercriminals are using technology to increase the frequency and complexity of attacks while also discovering vulnerabilities to gain unauthorized access.

Cybercrime & National Security

In recent years, with the increased sophistication of cyberattacks, it is believed that cybercriminal groups are operating in tandem with or on behalf of nation-states. These groups receive funding for operations and use advanced technology resources that include super-computing power and Artificial Intelligence (AI). This new dynamic can elevate the severity of the outcome of successful cyberattacks in the United States and around the world. In a recent report, the Office of the Director of National Intelligence (ODNI) highlights the national security threat and severe consequences of cyberattacks and cyber espionage perpetrated by China, Russia, North Korea and Iran. Specifically, the ODNI states, "North Korea's cyber program poses a sophisticated and agile espionage, cybercrime and attack threat,"[7] and "Iran's growing expertise and willingness to conduct aggressive cyber operations make it a major threat to the security of U.S. and allied networks and data."[8] Regarding the Chinese threat, the report states, "China presents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private sector networks. China's cyber pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology-driven authoritarianism globally."[9] China's strategic goal of using cybercrime as a weapon and espionage tool was demonstrated through the successful network breaches and data theft that occurred over a five-year period and affected the Office of Personnel Management (OPM), Marriott Hotels, Anthem Health and Equifax. Through these breaches, Chinese People's Liberation Army (PLA) military hackers gained sensitive employment information for all 21 million civilian government employees, health insurance records for 80 million people, personal information including 5 million passport numbers for 400 million Marriott accounts, and personal identifiable information (PII) for 147 million individuals. As Wired magazine explains, through the use of AI data analysis, the theft of this data is not just economic espionage, but also presents a tangible threat to national security: "This data and its layers work both to identify existing US intelligence officers through their personnel records and travel patterns as well as to identify potential weaknesses—through background checks, credit scores, and health records—of intelligence targets China may someday hope to recruit."[10]

Costs of Cyberattacks

The costs of cyberattacks can be financial, operational and reputational, all of which have a direct impact on the business. Besides the massive threat to privacy stemming from the 2017 Equifax breach, the total cost of the attack is estimated at over $2.5 billion. This includes at least $2 billion to remediate the breach and upgrade technology systems as well as a $425 million fine levied by the Federal Trade Commission (FTC). As a result of an earlier cyberattack in 2016 in which Uber paid $100,000 to the attackers to delete the stolen data, the company was eventually required to pay $148 million to settle a legal dispute alleging the company covered up the fact that the attack exposed sensitive data of over 57 million customers and drivers. In the case of the 2021 SolarWinds cyberbreach which affected 18,000 customers, including Fortune 500 corporations and U.S. government agencies, the total cost of mitigating the damage, which infiltrated software supply chains for at least 6 months, is estimated to be in the tens of billions of dollars.[11] With this increase in total attacks, businesses are also seeing an exponential increase in the number of ransomware attacks, as cybercriminals benefit from the ease and anonymity of payments afforded by the proliferation of cryptocurrencies. According to a recent SonicWall Threat Report, the number of ransomware attacks increased by almost 319 million between 2020 and 2021, representing a year-over-year rise of 105% and a 232% increase versus 2019.[12] Following a ransomware attack in 2020, Cognizant Technology Solutions announced the costs of the ransom to restore IT services as well as future remediation would be between $50 million and $70 million.

While these sizable payments are specific to ransomware attacks, the overall costs of any given cyberattack have also continued to increase. The costs of a data breach, which includes forensic and investigation activities, fines and compensation to affected parties, reached an average of $4.35 million in 2022, with the highest cost globally in the U.S. at $9.44 million.[13] The average cost rose 2.6% from 2021 and 12.7% from 2020, which was of $3.86 million. The impact of cybercrime on businesses and economies globally is sizable and growing. Cybersecurity Ventures, a leading publisher of global cybersecurity statistics, estimates the current overall cost of cybercrime to businesses globally is $6 trillion, up from $3 trillion in 2015 and expected to grow to an estimated $10.5 trillion in 2025.[14]

Cybersecurity Market Growth & Opportunities

The growth of cloud-based architectures to support digital transformation initiatives has led to an increase in the complexity of technology architecture. Concurrently, the risk of misconfiguration and potential network breach points has also increased. A 2021 AWS study revealed the biggest challenge facing IT departments is the complexity of securing the technology stack across multiple clouds and multiple software vendors—71% of the IT professionals surveyed agreed on this, up considerably from 2020 when only 49% viewed this as the biggest cloud security threat.[15] Historically, the cybersecurity industry has been quite fragmented with thousands of vendors focusing on specific parts of the security supply chain, as IT departments often buy multiple products from multiple vendors to secure their networks, and this has underpinned these complexities. In many cases, IT departments have been too siloed operationally. As a result,

IT security strategy has remained relatively static even as digital transformations focused on front-office and revenue-enhancing efficiencies in recent years. This dynamic is rapidly changing, as businesses are confronted with the increasing threats that have been described throughout this paper.

For many businesses, cybersecurity is now a key area of focus for the C-suite and Boards of Directors. As a result, investments in providers with next-generation network and cloud protection capabilities have accelerated. As businesses continue to spend on next-gen product offerings to support their digital transformation initiatives, we believe there will be four key areas of investment: Cloud Workload Security, Endpoint Security & Infrastructure Protection, Access Management and Application Security. Gartner estimates total spending on cybersecurity software will grow almost 15% per year from $79 billion in 2021 to over $100 billion in 2023, representing an annual growth rate that is three times that of total IT spending over the same period.[16,17] The four key areas identified above are expected to represent ~65% of total cybersecurity spending at almost $67 billion by 2023. Through the use of a cloud-based modular platform architecture that equates to a security-as-a-service approach, these next-gen security providers offer products that secure multiple areas of the IT supply chain while also utilizing Artificial Intelligence (AI) to efficiently analyze system configurations and detect network anomalies or increased threat vulnerabilities. We believe the monetary value of these next-gen components such as AI is readily apparent—the most recent IBM Global Threat study highlights that organizations with a fully-deployed AI and automation cybersecurity strategy saw the total costs of a breach at $3.15 million, a 65% reduction versus organizations that do not use AI for security or deploy automation software.[18]

Conclusion

As C-level executives seek to minimize the risk of disruptions from a misconfigured architecture and to improve the overall posture of their business's security profile, they are increasingly consolidating the number of vendors and investing in next-generation software solutions. A recent Gartner survey confirmed this trend, as 75% of surveyed businesses indicated they were consolidating the number of security vendors in 2022, a significant increase from the 29% who said the same in 2020.[19] We believe companies such as Crowdstrike, a leading provider of endpoint security & protection, will benefit from the trend toward vendor consolidation as they increase penetration with existing customers by cross-selling modular solutions developed both organically and through M&A. In its August 2022 investor presentation, Crowdstrike emphasized what it sees as significant growth opportunities due to consolidation and new product opportunities, estimating that its Total Addressable Market (TAM) will grow roughly 30% per year from 2022 to reach $126 billion in 2025.[20] We believe businesses will continue to invest in next-generation security software providers such as Crowdstrike as part of their digital transformation strategies. While a 100% success rate in defending against cyberattacks is impossible, we believe the duration and total costs of the breach can be significantly reduced through the use of next-generation cybersecurity products.

[1]McKinsey: "The Next Normal: The Recovery Will Be Digital" p.13
[2]Source: Ericcson, February 2022
[3]Source: Transforma Insights, December 2020
[4]Nearly 70 Percent of Organizations Globally Suffered IoT Attacks: Survey (cisomag.com)
[5]Fireye Mandiant Services Special Report: M-Trends, 2021
[6]Security Awareness is Everybody's Business, says Cybersecurity Expert (cisomag.com)
[7]Annual Threat Assessment of the US Intelligence Community, February 2022, p. 17
[8]Annual Threat Assessment of the US Intelligence Community, February 2022, p. 15
[9]Annual Threat Assessment of the US Intelligence Community, February 2022, p. 8
[10](https://www.wired.com/story/china-equifax-anthem-marriott-opm-hacks-data)
[11]SolarWinds Hack Recovery May Cost Upward of $100B (govtech.com)
[12](SonicWall Threat Intelligence Confirms Alarming Surge in Ransomware, Malicious Cyberattacks as Threats Double in 2021 - SonicWall)
[13]IBM Security: Cost of a Data Breach Report, 2022, p. 5-7
[14]Cybercrime To Cost The World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)
[15]AWS Cloud Security Report, 2021, p. 5
[16]Gartner Identifies Three Factors Influencing Growth in Security Spending
[17]Gartner Forecasts Worldwide IT Spending to Reach $4.4 Trillion in 2022
[18]IBM Security: Cost of a Data Breach Report, 2022, p. 3
[19]Gartner Survey Shows 75% of Organizations Are Pursuing Security Vendor Consolidation in 2022
[20]Crowdstrike Corporate Overview Investor Presentation, August 2022, p. 25