PRESCIENT

180 N Stetson Ave. • Ste. 2625 • Chicago, IL 60601
T: 312-667-0667 • **E:** info@prescient.com
W: www.prescient.com

Impact of Software Licensing Practices on Cybersecurity

Business practices and outsized vulnerabilities can lead to a “Cyber Tax” on small- and medium-sized businesses of up to 500%.

In collaboration with:

Coalition for Fair Software Licensing

November 2023

NOTE ON AUTHORSHIP

Prescient Comply LLC ("Prescient"), a cybersecurity and corporate investigations firm headquartered in Chicago, IL, was tasked with preparing a cybersecurity industry analysis of the impact, if any, of restrictive software licensing practices on behalf of the **Coalition for Fair Software Licensing** ("CFSL").

This report, prepared in October and November 2023, represents research-backed analysis and industry expertise gained from our digital forensics, incident response, and cybersecurity experience.

Sources included public records, news media, social media, and other publicly available information. Studies published by subject matter experts were screened for potential bias or other relevant ownership information whenever possible. Prescient experts often testify regarding the quality of products and software from security providers mentioned throughout this report.

SUMMARY OF FINDINGS

The severity of a cyberattack can be determined by examining the vulnerability under exploit and the breadth of the vulnerable software's deployment. History has shown that many severe cyberattacks - SolarWinds, the Microsoft Exchange Server hacks, and others - were especially damaging due to uniform information technology ("IT") architecture that spread vulnerable software across an entire business, industry, or government agency. This uniformity creates systemic risk in the form of a single attack surface and single point of failure in which attackers replicate the same attack within or across organizations.

Restrictive licensing is one of the most common ways technology vendors create uniform IT environments that span businesses, industries, and governments. They do so for good reason – it's great for their business, but not necessarily best for customers' overall security. Market-leading vendors like Microsoft may erect barriers to interoperability and / or implement other restrictions to limit choice.[1]

Our research and experience find that there is a connection between restrictive licensing and cybersecurity risk and cost. This "cyber tax" manifests itself in the form of incident costs, legal and regulatory expenses, additional security spend due to tiered pricing structures, added insurance costs, and security consultation, which come because of reliance on legacy software vendors, like Microsoft. According to a recent study by NetDiligence, when an incident occurs, small to medium-sized enterprises ("SMEs") spent on average an additional $103,000 on crisis services, $156,000 on legal and regulatory expenses, and $175,000 on incident costs.[2] For governments, the cyber tax also extracts an opportunity cost, as often limited resources are pulled away from public services.

We examined this "cyber tax" being levied on SMEs, which are the bedrock of the United States' economy and often rely on Microsoft Office 365 and other legacy software.[3] Our research found that SMEs who largely use Office 365 and Azure can end up paying a "tax" of up to $434,000 per incident - nearly 5x (498%) the cost of their annual spend on Office 365 and Azure ($87,120

[1] Dina Bass, Microsoft Customers Decry Cloud Contracts That Sideline Rivals, *Bloomberg*, available at: https://www.bloomberg.com/news/articles/2022-04-12/microsoft-customers-decry-cloud-contracts-that-sideline-rivals#xj4y7vzkg (Apr. 11, 2022).

[2] NetDiligence, *Cyber Claims Study: 2023 Report*, available at: https://netdiligence.com/cyber-claims-study-2023-report/.

[3] For the purposes of this report, we define SMEs as independent businesses with approximately 50-500 employees with less than $500 million in annual revenue.

annually on average).[4] [5] Combined with outsized vulnerabilities associated with Microsoft products and the restrictive licensing practices mentioned above, this "tax" is only likely to increase over time.

Ransomware and business email compromise ("BEC") were the two leading causes of cyberattacks, accounting for 46% of insurance claims and 72% of total incident cost during the five-year period between 2018 and 2022.[6] Research suggests that Microsoft "leads the pack" with most vulnerabilities associated with ransomware.[7] In fact, studies indicate that Office 365 users were more than twice as likely to experience a claim compared to Google Workspace users. Furthermore, on-premises Microsoft Exchange users were nearly three times more likely to experience a claim compared to businesses using Google Workspace.[8] Other studies underscore the disproportionately high vulnerability of Microsoft products, even when adjusted against their relatively smaller competitors: one study identified Microsoft as the vendor with the largest number of zero-day vulnerabilities,[9] while another concluded that nearly 30% of the known exploited vulnerabilities are attributable to Microsoft—more than the next five providers combined.[10]

These findings closely mirror our own experience. Prescient's team has conducted numerous ransomware, business email compromise, and other topically relevant cybersecurity investigations for clients, large, small, and in between. We provide digital forensics and incident response services, virtual Chief Information Security Office (CISO) consultation, cybersecurity audits and risk assessments, and other related services.

Prescient has observed that most of the cybersecurity incidents we encounter involve Microsoft-related technologies.

[4] Average annual Office 365 and related product spend calculated after extensive consultation with one of the United States' largely and fastest-growing IT managed service providers.

[5] For the purposes of this study, we focused on SMEs, though it is certainly possible that a similar "tax" exists for larger enterprises and government agencies with wider attack surfaces and who hold more sensitive data.

[6] NetDiligence, *Cyber Claims Study: 2023 Report*, available at: https://netdiligence.com/cyber-claims-study-2023-report/.

[7] Invanti, *Ransomware Research Reveals 12 Vulnerabilities Have Become Newly Associated with Ransomware in Q1 2023*, available at: https://www.ivanti.com/company/press-releases/2023/ransomware-research-reveals-12-vulnerabilities-have-become-newly-associated-with-ransomware-in-q1-2023 (May 18, 2023).

[8] Coalition, *2023 Cyber Claims Report: Mid-Year Update*, available at: https://info.coalitioninc.com/rs/566-KWJ-784/images/Coalition_2023-Claims-Mid-Year-Update.pdf.

[9] ZeroDay.CZ Tracking Project, Zero Day Vulnerability Statistics, available at: https://www.zero-day.cz/research/.

[10] Cybersecurity & Infrastructure Security Agency, *Known Vulnerabilities Catalog*, available at: https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

Contents

Our research is structured as follows**:**

Part I provides a glimpse into the changing cybersecurity landscape, why these changes increase risk from breaches and other cybersecurity incidents, and why the current cybersecurity market dynamic leads to increased costs for customers.

Part II details our experience with one common element of cyber tax: tiered pricing of cybersecurity products, its risks and ultimate costs imposed on customers.

Part III discusses additional restrictive licensing practices and provides examples of their costs to customers.

PART I
A CHANGING CYBERSECURITY LANDSCAPE

While international terrorism dominated the rankings of national threats for a full decade after 9/11, by 2013, cybersecurity firmly took the number one spot among a ranking of global threats and has been the focus among non-nation-state-specific threats ever since.

From the moment cybersecurity became a buzzword, the only constant in this wide-ranging field has been its ever-changing nature. Some of the trends and challenges of recent years were predictable, such as the increased use and dependence on technologies. Some new challenges perhaps less so, such as business practices that would evolve around those technologies. Nevertheless, the rate of change is rapidly accelerating, putting pressure on the leaders in both the public and private sectors to scrutinize their current software, infrastructure, and cybersecurity assets and procedures.[11]

The increased cybersecurity challenges are the price for the economic benefits and convenience of being online. Unfortunately, the real costs of falling behind these rapid changes are also increasing. Multiple reports suggest that damages from ransomware, the fastest growing type of cybercrime, are increasing every year.[12] [13] In addition to ransomware payments, victims suffer losses because of downtime, reputational damage, legal costs, and further investments in new security solutions.[14] Moreover, the increasing dependency on interconnected networks leads to additional, hidden costs that reach far beyond the primary victim of the attack.

Cyber Incidents on the Rise

The ongoing and measurable consequence of the rapidly changing cybersecurity landscape is the increase of breaches and other cybersecurity incidents.

Although specific figures tend to vary due to measurement methods and the impossibility of comprehensive coverage, outlets tend to agree on one fact: throughout the last two decades, the

[11] Jim Boehm, Charlie Lewis, Kathleen Li, Daniel Wallance, and Dennis Dias, *Cybersecurity Trends: Looking Over the Horizon*, McKinsey & Company, available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon (Mar. 10, 2022).
[12] Steve Morgan, *Global Ransomware Damage Costs Predicted to Exceed $256 Billion by 2031*, Cybercrime Magazine, available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (Jul. 7, 2023).
[13] Blackfog, *Beyond the Ransom: The True Cost of Ransomware Attacks,* available at: https://www.blackfog.com/the-true-cost-of-ransomware-attacks/.
[14] *Id*.

number of data breaches has regularly increased exponentially.[15] Statista reports a 500% increase in the decade leading to 2014,[16] while Forbes observed that the same decade had seen over 300 data breaches involving the theft of 100,000 or more records.[17] Even so, multiple sources report nine of the ten biggest breaches in history occurring after 2014.[18] [19]

In the simplest of senses, a global increase in data breaches can be correlated with an increase in the amount of data organizations and consumers store, generally. One figure estimates that global data production in 2020 was 44 times greater than it was in 2009.[20]

More recently, studies point to an increasing complexity and sophistication of ransomware attacks specifically. Cybersecurity firm Sophos conducts an annual, vendor-agnostic survey of thousands of IT professionals in mid-sized organizations. Their 2022 report revealed "an ever more challenging attack environment," finding that the complexity and sophistication of ransomware attacks had increased, and that the proportion of organizations directly impacted by ransomware had nearly doubled over the prior twelve months.[21] The firm's 2023 report found that ransomware had affected the same proportion of respondents, 66%, but noted that adversaries were more able to "consistently execute attacks at scale."[22] In early 2022, the U.S. Cybersecurity & Infrastructure Security Agency ("CISA") likewise issued a Cybersecurity Advisory regarding the increased globalized threat of ransomware.[23]

Likewise, more data means an increase in software and its complexity, which in turn becomes that much more subject to vulnerabilities that go unnoticed by developers prior to public release. A study by Mandiant analyzing 200 zero-day vulnerabilities between 2012 to 2021 found that these exploits are expected to continue to grow from year to year, partially because of "the continued move toward cloud hosting, mobile, and Internet-of-Things technologies [that] increases the

[15] Juliana De Groot, *The History of Data Bridges*, DataInsider (Digital Guardian Blog), available at: https://www.digitalguardian.com/blog/history-data-breaches (Aug. 22, 2022).

[16] Statista, *Cyber crime: Number of compromises and impacted individuals 2005*-2022, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (Aug. 29, 2023).

[17] Niall McCarthy, *Chart: The Biggest Data Breaches in US* History, Forbes, available at: https://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/?sh=4004981d7735 (Aug. 29, 2014).

[18] Abi Tyas Tunggal, *The 72 Biggest Data Breaches of All* Time, Upguard Blog, available at: https://www.upguard.com/blog/biggest-data-breaches (Aug. 3, 2023).

[19] Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st* Century, CSO Online, available at: https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html (Nov. 8, 2022).

[20] De Groot *supra* note 15.

[21] Sophos, State of Ransomware 2022, available at: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf.

[22] Sophos, State of Ransomware 2023, available at: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf.

[23] Cybersecurity & Infrastructure Security Agency, *2021 Trends Show Increased Globalized Threat of* Ransomware, available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a (Feb. 10, 2022).

volume and complexity of systems and devices connected to the internet—put simply, more software leads to more software flaws."[24]

A Data Breach Chronology Database from the nonprofit Privacy Rights Clearinghouse includes information on more than 20,000 data breaches dated between 2005 and February 2022.[25] Breaches can be sorted by the number of reported records impacted; firms such as Epsilon and Marriot / Starwood, for example, have suffered breaches affecting over 200 million customers.

However, such breach statistics—which are regularly limited to the U.S., and which most often focus only on the entities affected and the magnitude or sensitivity of their breached records—belie the fact that breaches regularly occur due to the involvement of an organization's vendors, partners, and other service providers, particularly those which interface with IT functions such as data storage. Indeed, the 2022 CISA advisory observes a recent increase in "malicious cyber activity targeting managed service providers."[26]

> *"Customers are often at the mercy of service providers to inform them of vulnerabilities in the service providers' software or platform."*

Based upon research on vulnerabilities between 2006 and 2016, Cybersecurity Help ("CH") reported Microsoft as the vendor with the largest number of zero-day vulnerabilities, 46% of those reported. (The second-closest vendor was Adobe, with 18.26%).[27] Similarly, data from 2020 through 2023 reveal Microsoft as the vendor with the most vulnerabilities (25.63%), followed by Apple Inc (18.49%), and then Google (16.81%).[28] Vendor software can be further subcategorized; for instance, Microsoft Windows represents 68.85% of the vendor's 2020-2023 vulnerabilities, followed by Microsoft Exchange Server (11.48%), and so on.

Other databases compiling vulnerabilities confirm the findings from CH's database. Since 2021, CISA has reported more than 930 known vulnerabilities, with nearly 30% of which are attributable to Microsoft—more than the next five providers combined.[29]

[24] James Sadowski, *Zero Tolerance: More Zero-Days Exploited in 2021 than Ever Before,* Mandiant Blog, available at: https://www.mandiant.com/resources/blog/zero-days-exploited-2021 (Aug. 10, 2023).
[25] Privacy Rights Clearinghouse, Data Breach Chronology, available at: https://privacyrights.org/data-breaches.
[26] Cybersecurity & Infrastructure Security Agency, *Protecting Against Cyber Threats to Managed Service Providers and Their* Customers, available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a (May 11, 2022).
[27] Zero-Day.CZ Tracking Project *supra* note 10.
[28] *Id.*
[29] Cybersecurity & Infrastructure Security Agency *supra* note 10.

This disproportionate share of vulnerabilities might be most readily attributed to a similar disproportionate market share. Indeed, according to aggregate data collection firm StatCounter Global Stats, Windows accounts for 69.51% of the desktop operating system market share worldwide. The second-highest market share belongs to Mac OS X, with 20.43%.[30] As such, it is reasonable to assume that unknown software vulnerabilities and related breaches will affect Microsoft and other software market leaders at comparably proportionate rates.

However, certain sources draw attention to disproportionately high instances of ransomware, malware, and other breach incidents for market leaders even when adjusted relatively against their smaller competitors. According to Datto's 2020 Global State of the Channel Ransomware Report, for instance, 91% of Windows desktops, 76% of Windows servers, and 8% of Windows tablets were reported by 1,000+ managed service providers as targets of ransomware attacks. The desktop and server numbers were significantly higher than the 7% infection rate reported for MacOS X.[31] Similarly, a study by Mandiant analyzing zero-days from a dozen software vendors in 2021 found that 75% of those reported were attributed to products from only three providers: Microsoft, Google, and Apple (the study was conducted prior to Mandiant's subsequent acquisition by Google).[32] [33]

The Cybersecurity Market is Evolving, But Not Fast Enough

Of course, the cybersecurity market is evolving as well. Indeed, in the first quarter of 2023, spending on cybersecurity increased by 12.5% compared to the same period a year earlier, outpacing the rest of the tech sector.[34] However, the increase in breaches and other cybersecurity incidents suggests that cybercriminals are outpacing and outmaneuvering their pursuers.

A closer look at the players in the field indicates that some of this growth has not necessarily led to innovation or effective solutions to the emerging challenges. The largest cybersecurity player in the market, Microsoft, grew its security-focused business by approximately 33% in 2022, generating approximately $20 billion.[35] However, some of Microsoft's business practices that

[30] StatCounter, Desltop Operating System Market Share Worldwide, available at: https://gs.statcounter.com/os-market-share/desktop/worldwide.

[31] Datto, Datto's Global State of the Channel Ransomware Report, available at: https://www.datto.com/resource-downloads/Datto-State-of-the-Channel-Ransomware-Report-v2-1.pdf.

[32] Sadowski *supra* note 24.

[33] Thomas Kurian, *Google + Mandiant: Transforming Security Operations and Incident* Response, available at: https://cloud.google.com/blog/products/identity-security/google-completes-acquisition-of-mandiant (Sept. 12, 2022).

[34] Stephen Weigand, *Cybersecurity market grew 12.5% in first quarter, outpacing overall tech* market, SC Media, available at: https://www.scmagazine.com/news/cybersecurity-market-grew-12-5-in-first-quarter-outpacing-overall-tech-market (June 20, 2023).

[35] Sam Boughedda, *Microsoft the largest cybersecurity player in the market – CFRA* Research, Investing, available at: https://www.investing.com/news/stock-market-news/microsoft-the-largest-cybersecurity-player-in-the-market--cfra-research-432SI-3080399 (May 11, 2023).

contributed to this growth and position in the market have been criticized as anti-competitive and stifling innovation. For example, Microsoft's vendor lock-in and bundling of products has been a thorn in the eye of some of its competitors and the subject of legal battles for more than a decade.[36] [37] [38] Of course, using a single vendor can have benefits, including better integration of single-vendor solutions.[39] However, single vendor lock-in presents significant risks to customers when the vendor is in the position of assessing and reporting the vulnerabilities in its own software and operating system. This creates a conflict of interest and misaligned incentives for the vendor; and, ultimately increasing cybersecurity risk borne by the customer. In addition, restricting interoperability and services to those allowed only by the service provider may ultimately prevent the agility necessary to tackle the everchanging cybersecurity challenges.

Another trend that is prevalent today and directly affects the customers has emerged with the advent of hybrid and cloud-based IT infrastructure. Providers of hybrid and cloud-based services began to offer tailored services and features to consumers. This pricing strategy is commonly referred to as **tiered pricing**. Tiered pricing allows providers to sell their products or services at different price points by restricting or expanding certain features of their products. This allows consumers to select the services they want at a price they can afford. However, this tiered pricing may lead to hidden vulnerabilities, leave the customers with inadequate protection, and ultimately lead to greater direct and indirect damages and costs.

[36] Matt Ashare, *Cloud tensions flare as Google accuses Microsoft of vendor lock-in,* CIO Dive, available at: https://www.ciodive.com/news/Google-battles-Microsoft-cloud-SaaS-Federal-Trade-Commission/653816/ (June 26, 2023).
[37] Melanie Chernoff, *The European Commission Stands Against Vendor Lock*-In, OpenSource Blog, available at: https://opensource.com/government/09/12/european-commission-stands-against-vendor-lock (Dec. 23, 2009).
[38] Kyle Rankin, *Vendor Lock-In: Now in the* Cloud, Linux Journal, available at: https://www.linuxjournal.com/content/vendor-lock-now-cloud (Apr. 1, 2018).
[39] Peter Zaitsev, *Understanding the Potential Impact of Vendor-Lock on Your* Business, Forbes, available at: https://www.forbes.com/sites/forbestechcouncil/2021/03/30/understanding-the-potential-impact-of-vendor-lock-in-on-your-business/?sh=5956cb0d5455 (Mar.30, 2021).

PART II
TIERED PRICING, RISKS, & COSTS

Tiered offerings are typically sold as prepackaged software bundles and often include different levels of security features, with more enhanced security features at the higher priced tiers. Unfortunately, the lower-level tiers are significantly more susceptible to data breaches and/or incident response hindrances due to cybersecurity gaps and limited response features. During a cyber-attack, some customers may feel the need to remain with their current software vendor but upgrade into a higher tier with more security features. With the lion's share of this industry's market, we will use Microsoft's tiered pricing strategy for this discussion. It is important to note, however, that most hybrid and cloud-based IT providers also offer tiered pricing models, though key differences exist between each.

Cybersecurity Gaps

Limiting cybersecurity options to tiered pricing models contribute to greater occurrence of cybersecurity gaps that expose businesses to risk and potential exploitation. Naturally, companies are primarily focused on generating revenue and reducing costs. Because of this, customers may be more inclined to choose a lower tier that includes fewer and more basic security features. Although most tiers provide standard security features (e.g., email filtering, password policies, multifactor authentication, etc.), advanced cybersecurity features (e.g., endpoint security, data loss prevention, auditing, etc.) are often only available in the higher tiered packages. Customers who either 1) choose a lower tier, or 2) have security needs that fall in between two tiers and opt for a lower tier will find themselves under-protected from cybersecurity risk and subsequently vulnerable to risk and exploitation. Unfortunately, many customers do not realize the extent to which they are under-protected until a cybersecurity incident occurs.

This tiered pricing strategy is akin to a scenario in which an individual purchases a vehicle with brakes and a seatbelt but learns they need to pay an additional cost for items such as anti-lock brakes and airbags. Allowing a customer to choose between different safety devices rather than standardizing features across all vehicles could have detrimental effects as the absence of anti-lock brakes and airbags during an accident could impact whether passengers survive a collision. United States Senator Ron Wyden of Oregon used the same car analogy when he criticized Microsoft in a *Wall Street Journal* ("WSJ") article.[40] Specifically, Senator Wyden noted that customers who had not purchased Microsoft's premium tiered service were unable to detect a state sponsor attack.

[40] Robert McMillan and Dustin Volz, *China Hacking Was Undetectable for Some Who Had Less Expensive Microsoft Services*, Wall Street Journal, available at: https://www.wsj.com/articles/china-hacking-was-undetectable-for-some-who-had-less-expensive-microsoft-services-58730629 (July 13, 2023).

"Service providers foster insecure environments when they fail to provide critical cybersecurity features across all tiers or allow customers to opt out of cybersecurity features."

Senator Wyden stated that "Offering insecure products and then charging people for premium features necessary to not get hacked is like selling a car and then charging extra for seatbelts and airbags."[41] The WSJ article also quoted an anonymous Senior CISA official who advocated for standardizing cybersecurity features across product offerings: "Every organization using a technology service like Microsoft 365 should have access to logging and other security data out of the box to reasonably detect malicious cyber activity."[42] Indeed, under the leadership of Jen Easterly, CISA has been pushing for making software secure-by-design and putting the liability on the vendors to sell better products:[43] [44]

> "Technology providers and software developers must take ownership of their customers' security outcomes rather than treating each product as if it carries an implicit caveat emptor. To achieve this, every technology provider must begin by creating products that are both 'secure by default' and 'secure by design.'"[45]

Service providers using tiered packaging strategies foster insecure environments when they fail to provide critical cybersecurity features across all tiers or allow customers to opt out of essential cybersecurity features via purchase of a lower tier package.

In addition to tiered security features, legacy software providers often present customers with a complex array of choices that can be difficult for customers to understand and make informed decisions to select the right tier to protect their business. As such, customers often need to spend a considerable amount of time researching the different features in each tiered package and mapping these offerings to fit their cybersecurity needs. For example, Microsoft has several 365 offerings for business customers. There are basic, standard, and premium, as well as apps for business tiers. For enterprise-level customers, there are enterprise levels 1, 3, and 5, as well as apps for enterprise tiers. In addition, there are frontline workforce (e.g., M365 F1 and F3), government (e.g., O365 G3, O365 G5, M365 G3, and M365), and nonprofit (basic, standard, and premium) tiers.

[41] *Id.*
[42] *Id.*
[43] CISA Director Jen Easterly and Executive Assistant Director Eric Goldstein, *Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products*, Foreign Affairs, available at: https://www.cisa.gov/sites/default/files/2023-04/foreign-affairs_stop-passing-buck-on-cybersecurity_508.pdf and https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity (Feb. 1, 2023).
[44] Jessica Lyons Hardcastle, *US Cybersecurity Chief: Software makers shouldn't lawyer their way out of security* responsibilities, The Register, available at: https://www.theregister.com/2023/02/28/cisa_easterly_secure_software/ (Feb. 28, 2023).
[45] Easterly and Goldstein *supra* note 45.

Reviewing the different tiers and features can be a daunting task. This is especially true for novice or non-cybersecurity personnel (i.e., CEOs, CFOs, procurement officers, etc.) who are tasked with tier selection on behalf of their organization.

These tiers can be confusing to understand and often provide ambiguous information about their security features. The wrong selection could have catastrophic results, affecting the confidentiality, integrity, and/or availability (commonly referred to as the CIA Triad by information security professionals) of the customer's data. Customers who select a tier that does not meet their cybersecurity needs may learn they do not have the capabilities within their tier to address a cybersecurity incident and are forced to upgrade to a more expensive tier or find another solution to address the issue. Moreover, alternative solutions may be limited or restricted to only services or vendors approved by the service provider, thus limiting the customer’s options and reducing competitive opportunities for outside, or non-approved, vendors to address security flaws.

Lastly, some of the cybersecurity features offered in tiered packages require setup, configuration, and training. Many features are not “plug and play” nor are they turned on by default. Expert assistance (either internally or externally) may be required to implement these security features or controls. Customers who lack the knowledge or personnel to configure these features often need to purchase additional services from the service provider or authorized partner. In addition, these support packages are often presented in the form of tiered pricing levels.

> *“Alternative solutions may be limited or restricted to only services or vendors approved by the service provider, thus limiting the customer’s options and reducing competitive opportunities for outside, or non-approved, vendors to address security flaws.”*

Data Breaches, Incident Response, & Hindrances

Tiered pricing models can contribute to hybrid and cloud-based breaches because customers cannot pick and choose which security and auditing features they need. Security features are often sold in prepackaged tiers and do not allow customers to select features from higher tier packages or tiers that do not include upgrading.

One such feature is Microsoft’s “Impossible Travel.” Impossible travel is an anomaly detection tool used to identify account compromises. It detects when a user connects from two different countries (e.g., New York and Montenegro) and determines if the time between connections (e.g., 1:00 PM EST and 9:00 PM CET) is possible. If the time between those connections cannot be made through conventional air travel, the account is flagged as "impossible travel". This would be an important and helpful feature to be included in all tiers. However, if a customer has a Microsoft Business Standard license, they will need to upgrade to a higher tier product (e.g., Microsoft 365 Business Premium, Microsoft 365 Enterprise 5, Azure, etc.) that includes Impossible Travel. As a result of a forced upgrade, the customer further binds or ties their IT security to Microsoft and possibly extends their licensing period. It is worth mentioning that Prescient has observed that a large percentage of its business email compromise (BEC) clients, including those that were breached using Microsoft's MFA, upgraded their license immediately after the incident to a package that includes Impossible Travel. Consequently, if these clients had Impossible Travel embedded in the lower tier or if they had the ability to add it at the time of purchase, many of the BECs may not have occurred.

A second feature often overlooked by tiered customers is logfile retention. Most of Prescient's Microsoft breach clients were unaware that their logs were retained for 90 days for lower tier users (i.e., non-E5 users and/or guest users).[46] According to an IBM report, it may take approximately 197 days to discover a breach. As such, 90-day retention period was grossly inadequate to assist victims of data breaches.[47] Facing pressure from policymakers, customers, and industry, Microsoft recently announced changes to their audit log retention policies to extend the retention period from 90 to 180 days for audit logs generated after October 17, 2023.[48] However, as the extension falls short of the average time to discover a breach, it is unclear how much this extension will help. Tiered customers who identify a breach after the logs have been purged find themselves in a guessing game as to how long the threat actors were in their system and what data was accessed or exfiltrated. This is a nightmare scenario for companies that fall under breach reporting guidelines as they often need to spend considerable amounts of money and resources to answer these two questions for regulators and their customers. These victims will often upgrade to a higher tier during a data breach in the hopes that they can recover the missing or purged logs. It is important to note that this log retention tier issue applies to other vendors and not just Microsoft.

Data loss prevention ("DLP") is a third feature that is not often available at lower tiers offered by hybrid and cloud-based service providers. DLP features are tools used to 1) detect potential data breaches and data exfiltration, and 2) prevent sensitive data loss. These are typically available to customers who select higher tier options. DLP features can help customers monitor which users are accessing and transmitting sensitive information in an organization. They are also designed to prevent access to sensitive data while in use, in transit, or at rest. Deploying tools of this nature could help reduce the number of data breaches in the United States. Unfortunately, service providers require their customers to pay an additional cost for these features.

[46] Microsoft, *Manage audit log retention* policies, available at: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies (Oct. 24, 2023).
[47] IBM, Cost of Data Breach Report 2023, available at: https://www.ibm.com/reports/data-breach.
[48] Microsoft *supra* note 46.

PART III

RESTRICTIVE LICENSING PRACTICES & HIDDEN COSTS

The restrictive licensing practices of legacy vendors often lead to locking customers into their uniform ecosystem. While a uniform or identical IT architecture allows service providers to efficiently manage and maintain their clients' cloud-based infrastructure, it also provides a roadmap or single attack vector for hackers to exploit all of the service provider's customers en masse each time a vulnerability is discovered. Additionally, it puts the service provider in a position of assessing and reporting the vulnerabilities in its own software and operating system rather than relying on a third-party vendor to provide objective feedback. Of note, this threat is amplified exponentially when segments considered critical infrastructure (e.g., healthcare, transportation and logistics, energy, defense, and financial services) rely on a limited number of cloud service providers. This was demonstrated in a recent attack on U.S. government agencies by nation-state actors.

In July 2023, the email accounts of several U.S. government agencies were breached by a hacker group affiliated with the Chinese government, stealing 60,000 emails.[49] The Chinese hacker group, Storm-0558, was able to exploit Microsoft's "GetAccessTokenForResourceAPI", which allowed the group to forge signed access tokens, impersonate customer accounts, and gain access to 25 organizations and government agencies.[50] [51] The threat actors discovered this security flaw after successfully compromising a Microsoft engineer's corporate account.[52] Once the flaw was discovered, the threat actors were able to compromise several U.S. government agencies that used Microsoft's Exchange Online and Azure Active Directory services. As demonstrated in this example, the government's reliance on a single vendor created a weakness and a single point of failure that diminished the government's cyber-resiliency against a cyber-attack.

"Uniform IT architecture also provides a roadmap or single attack vector for hackers to exploit all of the service provider's customers en masse each time a vulnerability is discovered."

[49] Karoun Demirjian, *Chinese Hackers Stole 60,000 State Department Emails in Breach Reported in July*, New York Times, available at: https://www.nytimes.com/2023/09/27/us/politics/chinese-hackers-state-department.html

[50] Sergiu Gatlan, *Stolen Microsoft key offered widespread access to Microsoft cloud* services, Bleeping Computer, available at: https://www.bleepingcomputer.com/news/security/stolen-microsoft-key-offered-widespread-access-to-microsoft-cloud-services/ (July 21, 2023).

[51] Demirjian *supra* note 50.

[52] Phil Muncaster, *Microsoft Breach Exposed 60,000 State Department Emails,* InfoSecurity Magazine, available at: https://www.infosecurity-magazine.com/news/microsoft-breach-60000-state (Sept. 29, 2023).

Limited Integration Capabilities

In our experience, legacy software providers often prohibit integration of "non-authorized" external security solutions (presumably those offered by competing service providers) into their platforms. This restriction is in direct opposition to the "defense in depth" strategy, which is a best practice in cybersecurity. Defense in depth is a multi-layered approach to cybersecurity that incorporates different defense mechanisms at varying layers to protect systems and the data contained therein. These different defense mechanisms increase the efficacy of blocking an attack at a deeper layer of security should the previous security layer fail. Restricting integration of external solutions creates more vulnerable environments because threat actors can apply what they have learned from the environment of one service provider's customer to the environments of that provider's other customers. There have been a few limited instances where legacy providers have allowed some "authorized" external solutions (e.g., Endpoint Detection and Response systems) to be integrated into their environment. However, several of these external solutions have been proven to be ineffective in blocking cyber-attacks or they conflicted with the provider's operating system or solutions (e.g., Microsoft's Defender, etc.) and subsequently did not perform as expected.

> *"The closed software environment forces the customer to use the service providers' tools that are often hard to interpret, produce false positives, and do not work as well as some industry standard tools."*

Ultimately, the uniform architecture and limited integration capabilities contribute to the cyber tax as they create more vulnerable environments that are more easily exploited, increasing the likelihood of devastating breaches and contributing to increasing breach remediation costs.

Tool Dependency

Legacy software providers boast about available tools for customers to manage and address their cybersecurity needs when subscribing to their tiered service. However, there is little information about the expertise needed to properly implement and utilize these tools. In addition, the closed software environment forces the customer to use the service providers' tools that are often hard to interpret, produce false positives, and do not work as well as some industry standard tools. For instance, in a recent court case, a Special Master determined that Microsoft Purview tool did not "satisfy the duty of reasonable inquiry under Federal Rule of Civil Procedure 26(g)(1)."[53] The Special Master stated that Microsoft's 365 Purview tool does not 1) "fully index" documents in its cloud environment, 2) does not accommodate complex Boolean searches, and 3) does not allow users to validate their search and production results. As a result of these flaws, customers that rely on Microsoft's Purview tool for eDiscovery might miss critical data needed for a legal matter, which can adversely affect their case.

Forced Upgrades & Vendor Lock-In

As previously mentioned, most breach victims upgrade their tier during a cyber incident in the hope that it will help them respond to and/or mitigate the incident. In addition, on-premises victims typically opt to move their entire infrastructure to the cloud service offered by the legacy software vendor. This transfer to the cloud results in the customer shifting more control and data to the same service provider and operating systems involved in the cyber incident. This is especially true for Microsoft victims in Prescient's DFIR practice who have often moved their entire on-premises Active Directory (AD) to Microsoft's Azure Active Directory (also known as Microsoft Entra).[54] Unfortunately, this move often transfers (or syncs) the same settings that caused the original breach. Additionally, Azure Active Directory features new settings that create new vulnerabilities, as noted by discoveries from cloud security providers Wiz and Tenable.[55] [56]

While these forced upgrades are perceived as necessary to restore security and operations, many customers fail to understand that the shift does not protect the customer from future hacks or breaches. According to Palo Alto's *Cloud Threat Report*, the "fast evolution and growth of cloud workloads—as well as the complexity of managing hybrid and multi-cloud environments—cause many organizations to fall behind the curve and inadvertently introduce security weaknesses into their environments, as evidenced by the many legacy resources, vulnerabilities, and insecure configurations [they've] witnessed. These gaps give adversaries significant opportunities to gain a foothold in the cloud."[57]

[53] John Patzakis, *Special Master Determines Microsoft Purview Does Not Comply with FRCP 26(g) Due to Unreliable and Incomplete Search Results,* X1: NextGen GRC & EDiscovery Law Blog, available at: https://www.x1.com/2023/08/01/special-master-determines-microsoft-purview-does-not-comply-with-frcp-26g-due-to-unreliable-and-incomplete-search-results/ (Aug. 1, 2023).

[54] Active Directory (AD) authenticates and authorizes all users and computers in a Windows computer network. It assigns and enforces security policies for all computers. Visit the following link for more information about AD: https://en.wikipedia.org/wiki/Active_Directory

[55] Rob Wright, *Wiz warns of exposed multi-tenant apps in Azure* AD, TechTarget, available at: https://www.techtarget.com/searchsecurity/news/366547696/Wiz-warns-of-exposed-multi-tenant-apps-in-Azure-AD (Aug. 9, 2023).

[56] Ernestas Naprys, *Expert voices pile up on Microsoft's "negligent" security* management, Cyber News, available at: https://cybernews.com/news/microsoft-azure-negligent-security-management/ (Sept. 22, 2023).

[57] Palo Alto Networks, Cloud Threat Report: Navigating the Expanding Attack Surface, available at: https://start.paloaltonetworks.com/rs/531-OCS-018/images/4.13PM_unit42-cloud-threat-report-volume7-final.pdf.

Unfortunately, these forced upgrades during a time of a cyber incident further enmesh these customers with service providers, and, in essence, lock them into their services, which makes it difficult and expensive for customers to shift to a new service provider. This dynamic also reduces the opportunity for non-legacy providers to break into the market and introduce newer, and possibly more secure, solutions. Once customers transition their operation to the cloud, they often learn of additional fees and/or hidden costs related to networking, processing, and storage. As such, customers can quickly exceed their anticipated costs.

Cyber Insurance Premiums

The increase in cyber incidents has led to an increase in demand for cyber insurance. At the same time, the growing costs of these incidents are driving up the premiums. Indeed, between 2020 and 2022, premiums increased by a median of 50%.[58] In addition to the increasing premiums, insurance companies are increasing their requirements and list of exclusions. In some cases, this leads to more time and effort spent by the companies to obtain insurance. According to Delinea's 2023 State of Cyber Insurance report, "the percentage of respondents reporting that the process to get cyber insurance took more than six months increased from 0.46% in 2022 to 7% in 2023."[59]

In much worse cases, rising premiums and restrictive coverage leave many companies uninsured.[60] A 2022 BlackBerry and Corvus Insurance study found that nearly half of the surveyed companies

> *"These forced upgrades further enmesh customers with service providers, and, in essence, lock them into their services, which makes it difficult and expensive for customers to shift to a new service provider. This dynamic also reduces the opportunity for non-legacy providers to break into the market and introduce newer, and possibly more secure, solutions."*

[58] Judy Greenwald, *Company cyber budgets jump 70% in four years: Moody's*, Business Insurance, available at: https://www.businessinsurance.com/article/20230929/NEWS06/912360168/Company-cyber-budgets-jump-70-in-four-years-Moody%E2%80%99s- (Sept. 29, 2023).

[59] Michael Hill, *Time and effort to obtain cyber insurance increasing for US* businesses, CSO Online, available at: https://www.csoonline.com/article/650609/time-and-effort-to-obtain-cyber-insurance-increasing-for-us-businesses.html (Aug. 29, 2023).

[60] Bob Ackerman, *Making Cyber Risk Insurable: Cyber Insurance Industry in 2023*, Forbes, available at: https://www.forbes.com/sites/forbesfinancecouncil/2023/04/27/making-cyber-risk-insurable-disrupting-the-cyber-insurance-industry-in-2023/?sh=36c6c44958eb (Apr. 27, 2023).

did not have insurance and of those insured, over one third were not covered for ransomware payments.[61] The same study found that more than one third of respondents were denied cyber coverage specifically for not meeting the requirement of deploying Endpoint Detection and Response ("EDR") solutions.[62] Notably, Microsoft's endpoint security solution Defender for Business is offered in its Microsoft 365 Business Premium package but has to be purchased separately in its more basic tiers.[63]

[61] Bruce Sussman, *The State of Cyber Insurance*, Blackberry Blog, available at: https://blogs.blackberry.com/en/2022/11/the-state-of-cyber-insurance-2022-research (Nov. 21, 2022).

[62] *Id*.

[63] Microsoft, *Find the Best Microsoft 365 Plan for Your* Business, available at: https://www.microsoft.com/en-us/microsoft-365/business/compare-all-microsoft-365-business-products?tab=2.

CONCLUSION

The changing cybersecurity landscape is putting pressure on the leaders in both the public and private sectors to scrutinize their current cybersecurity infrastructure and procedures and look for new solutions. The landscape of cybersecurity challenges has grown even more complex with the collective shift away from traditional on-premises security infrastructure into hybrid or fully cloud-based solutions from external providers.

Legacy software providers, taking advantage of their dominant market share, engage in practices that may ultimately expose their customers to greater cybersecurity risks and costs over time. The costs – direct breach remediation, security upgrades, legal fees, loss of time, reputational and IP damages – associated with these practices can be thought of as a “cyber tax.”

These practices can especially affect small and medium-sized businesses, who collectively form the foundation of the U.S. economy. While legacy providers strengthen their market share, their expanded control and handling of financial, medical, and other critical data only further incentivizes the malicious actors behind an increasingly complex and prevalent landscape of ransomware and other cybersecurity incidents.

The tradeoff is seasonal returns for a minority of tech shareholders at the cost of mass data exposure, personal and corporate, from a larger majority of affected individuals, both directly (through their own firsthand organizational involvement) and indirectly (when their own customer data, interpolated into the larger landscape of vendors and organizations that make up the U.S. economy, is breached). This is a shortsighted exchange, compromising personal and organizational security for marginal gains of “too-big-to-fail” legacy software providers, who will in turn likely face stricter regulations in the years to come, when governmental incentives have more closely aligned against these factors.