Coalition for Fair Software Licensing

Coalition for Fair Software Licensing and Prescient Release Comprehensive Report Quantifying Link Between Restrictive Software Licensing and Cybersecurity Risks and Costs

Overview

The Coalition for Fair Software Licensing, in partnership with cybersecurity firm Prescient, published a comprehensive research report assessing the connection between legacy vendors' restrictive software licensing practices and their customers' cybersecurity risks and cost over time.

The Coalition's report found that legacy software vendors – like Microsoft – who engage in anticompetitive licensing practices levy a "cyber tax" on their customers by locking them into insecure environments. These unfair tactics make it significantly more difficult for customers to work with other infrastructure providers or implement cybersecurity solutions from the vendor of their choice. This licensing-enforced lock-in limits customers' ability to utilize multiple vendors and leaves their IT architecture particularly vulnerable to cyberattacks and increased maintenance. When these attacks occur, the customer bears the financial burden of mitigating the impact of these vulnerabilities and exploits.

This "tax" can be as high as 498% per incident of what a typical small- and medium-sized enterprise (SME) spends on Office 365 and Azure subscriptions and includes incident response costs, legal and regulatory expenses, additional security spend due to tiered pricing structures, added insurance costs, and security consultation which come as a result of reliance on legacy software vendors like Microsoft.

The Changing Cybersecurity Landscape & Its Consequences

- **Cyberattacks are on the rise:** "Throughout the last two decades, the number of data breaches has regularly increased exponentially. … 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. … 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."

- **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. However, the increase in

breaches and other cybersecurity incidents suggests that cybercriminals are outpacing and outmaneuvering their pursuers."

- **Microsoft continues to grow its cybersecurity practice and revenue at the expense of its own customers' cyber resiliency:** "The largest cybersecurity player in the market, Microsoft, grew its security-focused business by approximately 33% in 2022, generating approximately $20 billion. However, some of Microsoft's business practices that 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."

Risks & Costs of Tiered Pricing Tactics

- **Tiered pricing models can lead to cybersecurity gaps that expose businesses to risk and potential exploitation:** "Tiered offerings are typically sold as prepackaged bundles and often include different levels of security features, with more enhanced security features at the higher priced tiers. 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."

- **Customers' inability to select the cyber solution best-suited for their organization(s) leaves them susceptible to cyberattacks:** "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."

Restrictive Licensing Practices & Hidden Costs

- **Legacy providers restrict market competition and interoperability, leading to increased vulnerabilities and costs amongst customers:** "Legacy software providers often prohibit integration of 'non-authorized' external 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. … 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."

- **Many software customers find themselves subject to forced upgrades, locking them in to their existing cyber solutions:** "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."

Software Customers Pay the Price

- **Unfair software licensing tactics increase cyber vulnerabilities for customers:** "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."

- **These unfair licensing tactics result in a "cyber tax" for customers while legacy software providers pad their bottom lines:** "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."