EXECUTIVE SUMMARY

When it comes to cybersecurity, the constant, nagging question for enterprises is “Will the effort and strategy we are making protect the organization from an attack?” The soon-to-be-released Verodin 2020 Security Effectiveness Report, which compiles data from 100+ production environments, confirms that continuous validation of effectiveness is critical to performance.

2020 | SECURITY EFFECTIVENESS REPORT

DEEP DIVE INTO CYBER REALITY

We want to thank the Cyberhedge research team for sharing data from their series of 2019 reports to support our efforts to provide the most relevant and objective data to Enterprise CISOs and their teams.

VERODIN
NOW PART OF FIREEYE

ADDRESSING CYBER RISK AND SECURITY EFFECTIVENESS IN THE DIGITAL AGE

Digital transformation is sweeping the modern world of business as organizations become increasingly cloud-based, automated, and global. Even companies not historically associated with technology, such as those in industry and manufacturing, are implementing digital transformation strategies. As they do so, they must choose between top-line growth, cost-savings, and cybersecurity. Too often, organizations choose to prioritize growth and cost efficiencies over security, ultimately leaving their valuable digital assets unprotected, according to Cyberhedge, a financial services firm specializing in managing technology risk, in the latest issue of its Research Report.

Good cyber governance is now an essential part of any company's financial future. Yet in the Digital Age, the inherent complexity of enterprise IT environments combined with increased reliance on the cloud make it increasingly difficult to identify cyber risk. Digital transformation offers many benefits such as fueling economic growth and productivity and strengthening brand loyalty, but there are negative aspects as well. The technologies that power this transformation open up companies to greater risk of attack or breach, which is further heightened by the digital interconnectedness between companies and their partner ecosystem.

All of this is driving the need for tools that measure security effectiveness to help companies and investors understand and manage the associated risks of digital transformation.

To underscore the critical importance of understanding and improving a company's security effectiveness, Verodin, now part of FireEye, is releasing its newest 2020 Security Effectiveness Report [link to landing page], *A Deep Dive Into Cyber Reality.* The report details Verodin's findings* and offers some startling revelations — primarily, that a large percentage of companies believe their security investments are delivering expected value by protecting critical assets and data, when the reality is they have already experienced a breach without knowing. This scenario correlates with Cyberhedge data, which calculates the ongoing financial and operational impact when an undetected breach occurs. Both sets of data provide insights that have never before been available — security effectiveness combined with financial impact—all before a breach even occurs.

BLOAT

50-70

Average number of tools organizations report in their IT environment.

OVERLAP

35%

Average number of tools with overlapping capabilities.

MISCONFIGURATION

80%

Average number of tools left underutilized at default settings.

Sound cyber governance demands strong security effectiveness and close alignment between executives and security teams.

Looking at a company's cyber governance score is a good way to understand how well the business addresses systemic cyber risk. Cyberhedge created the performance metric of a cyber governance rating** as a way to compare how companies manage the operational risks and subsequent financial impact of their technology investments and network security. Through individual case studies and analysis of data from more than 5,000 public companies, the latest Cyberhedge report demonstrates the need to invest in securing data instead of prioritizing cost-savings and growth as companies execute their digital transformation strategies.

But it is not enough to simply invest in securing data. As the Verodin 2020 Security Effectiveness Report shows, organizations must prove that security investments are actually working. Given the complex IT environments with which companies operate, misconfigurations and regular environmental drift weigh heavily on the minds of executives. Additionally, as more companies migrate systems and operations to the cloud, they increase their vulnerability to attacks while also minimizing security teams' visibility into the security stack. Without ongoing monitoring and measurement, security teams have no way of knowing if tools are working as they should and lack an understanding of where there may be unnecessary overlaps in security infrastructure, and where there are gaps.

Beyond what security teams can accomplish, the path to good cyber hygiene lies in creating more alignment between CISOs and other C-level executives, along with ongoing evidence-based measurement and monitoring of security effectiveness. That is, by gaining a thorough understanding based on empiric evidence of how effective a company's security controls are at protecting them against an attack, rather than simply making assumptions based on what security vendors promise, CISOs can better communicate potential cyber risk to the C-suite and foster stronger collaboration in strengthening cyber governance.

This alignment between CISOs and other C-level executives is made easier when organizations can quantify cyber risk just as they would quantify any other systemic business risk—in financial terms. Cyberhedge's recent Research Report shows the importance of measuring the impact of technology on shareholder value, a measurement that helps bridge the gap between security teams and the C-suite, so the threat is better understood and organizations are better protected.

Reserve a copy of the full 2020 Security Effectiveness Report here →

GET REPORT

A data breach or cyber attack on corporate systems and networks can have a tremendous impact on a company's operational performance and financial position. When cyber risk is not addressed the same as other business risks from the executive level down to those on the front lines of cyber defense, the results can be disruptive if not disastrous. Multi-million-dollar lawsuits, government-issued fines, lost business and a deteriorating brand reputation can take a significant, long-lasting toll. The good news is that there is a path forward to optimized security effectiveness and good cyber governance, which starts with an understanding of what's at stake and the underlying causes, as well as following the example of companies that are getting it right. All of this is outlined in the latest report from Cyberhedge and Verodin.

Good cyber hygiene lies in creating more alignment between CISOs and other C-level executives, and ongoing evidence-based measurement and monitoring of security effectiveness.

* The statistics outlined in the Verodin Security Effectiveness Report were generated through careful analysis of 25,842 attack behaviors executed against 123 market-leading security technologies—including network, email, endpoint, and cloud solutions. The tests took place in 126 individual production environments that encompassed every major industry sector.

** Cyberhedge generated its cyber governance rankings by examining its proprietary CyFi scores (e.g., the composite Cyber + Financial metrics) for more than 5,000 U.S. companies over the last 12 months, determining how many companies per sector were ranked in the company's "worst-in-class" category on CyFi metrics. Beyond simple external cyber metrics, CyFi metrics include cash constraints companies face relative to cyber threats on a per sector basis.

About Verodin Security Instrumentation

The Verodin Security Instrumentation Platform (SIP), now part of FireEye, helps organizations demonstrate the value received from security through a data-driven, evidence-based approach. Verodin SIP enables customers to continuously validate that their cybersecurity controls are fully protecting their business-critical assets, identify and mitigate configuration issues, and optimize their people, processes, and technology.