CYBERSECURITY TRENDS 2020



VERODIN
NOW PART OF FIREEYE



Verodin reveals top trends that will shape the cybersecurity industry in 2020

Organizations' increased focus on cloud, business risk and data privacy, combined with election security concerns and the rise of deception are driving a more holistic approach to cybersecurity and the need for security effectiveness measurement.

Over the past few years, organizations have faced a growing challenge: while they have increased spending on cybersecurity infrastructure, the threat of attacks and breaches has continued to escalate at unprecedented speed. This conundrum is driving the need for business executives and security professionals to work in closer alignment to holistically address issues around cloud security, business risk and data privacy, as well as validate that security controls are offering necessary protection of critical assets, according to executives from security instrumentation provider Verodin.

Additionally, with the U.S. presidential election taking place in 2020, there are heightened concerns among the general public and state government institutions about the security of the country's electronic voting system. Verodin's leadership has insights into how state and local governments will address their own security infrastructure in the coming year.

Four key cybersecurity trends that will shape how users and vendors of security technology approach the evolving threat landscape, as described by Verodin's executive team, are outlined in the eBook.

© FireEye, Inc. 2020

CYBERSECURITY 2020 TREND:

Cyber Risk as a Measure of Business Risk – A Gap in Understanding Can Lead to Millions of Dollars Lost



When a breach or attack on a company's digital assets occurs, there is much more at stake than the loss of data – which, in itself, is significant. But there is also the greater impact on the brand and loss of trust, as well as the potential cost of millions (or billions) of dollars in lawsuits, fines and loss of revenues.

The recent Cyber Trendscape Report by FireEye states that while more than 90% of organizations surveyed believe that the cyber threat landscape will stay the same or worsen in 2020, just over half do not believe they are ready for, or would respond well to, a cyber attack or breach event. Moreover, 29% of organizations with cyber attack and breach response plans in place have not tested or updated them in the last 12 or more months.

Given all of this, C-level executives and Boards of Directors are demanding to understand in quantifiable terms the organization's cyber risk and its effect on business risk.

Currently, there is a gap between the C-suite and security teams, who aren't measuring cyber risk in terms of its impact on a company's financial, operational, and brand risk. They also aren't delivering quantifiable evidence to executives demonstrating that security controls are working as they should. As the stakes for poor cyber hygiene grow, the impact on business risk and pressure on business leadership to address security issues will also heighten.

90%

of organizations believe that the cyber threat landscape will stay the same or worsen in 2020.

29%

of organizations with cyber attack & breach response plans in place have not tested or updated them in the last 12 or more months.

© FireEye, Inc. 2020

VERODIN PREDICTS:

- Security leaders will be challenged to better align cybersecurity systems performance with the overall performance of the business, requiring evidence that people, processes and technology are directly impacting core functions – finance, legal/compliance, sales, HR, marketing, customers success and operations.

- Security teams will increasingly measure and report on cybersecurity effectiveness in quantifiable terms, using evidence-based data to demonstrate that the security infrastructure is providing the necessary protection, as required by the executive team.

- The C-Suite will continue to mature in understanding security's relevance and demand clear evidence that security investments are having a positive impact on key business areas:

BUSINESS CONTINUITY

An appropriate security infrastructure means ransomware and other types of attacks will not compromise how business decisions are made or how the business continues to operate.

REGULATORY COMPLIANCE

Companies across every vertical industry must be able to show adherence to government regulations, particularly with regard to security infrastructure and the protection of customer data.

COMPANY VALUATIONS

Companies need to demonstrate both an understanding of what determines their valuation and how critical assets are safeguarded against breach or attack to preserve that valuation.

RATIONALIZATION OF INVESTMENTS

Executives must be sure that IT and security investments are mapping to the company's operational framework, and that there aren't added costs stemming from unnecessary overlaps or gaps in security that weaken those investments.

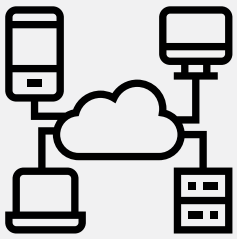
© FireEye, Inc. 2020

CYBERSECURITY 2020 TREND:

Increased Pressure on Security from Growth of Digital Transformation, IoT and the Distributed Cloud



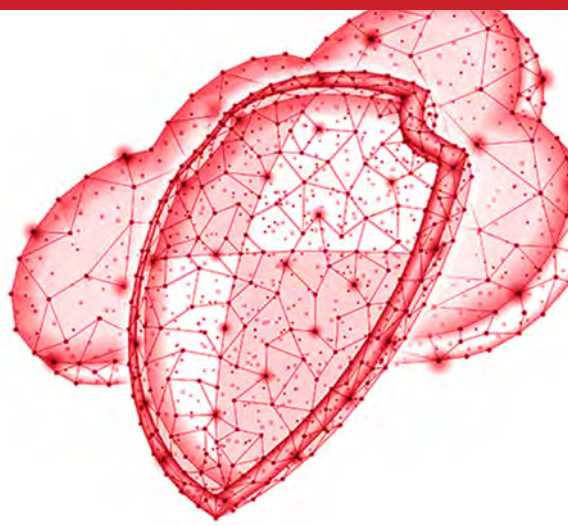
With the ongoing digital transformation of companies across all industries and the increasing use of IoT devices in the enterprise, organizations are moving more and more systems, applications and data to the public cloud. In particular, the distributed cloud is gaining prominence, as the ability to have data centers located anywhere offers added performance advantages. This cloud transformation and growing use of connected devices enables companies to cut costs, reduce infrastructure management and deliver a more engaging customer experience. But the benefits of the distributed cloud come with the need for increased vigilance.



The increasing number of devices and applications connected to the distributed cloud gives adversaries **a larger playing field on which to target attacks.**

Additionally, with cloud-hosted platforms and a decentralized infrastructure, security professionals have far less visibility into the security stack and how it's managed, forcing companies to rely on the promises made by cloud vendors that their environments are secure, without a way to know if assets are fully protected.

© FireEye, Inc. 2020



VERODIN PREDICTS:

- Companies will increasingly look to cloud-based security solutions to protect digital assets. This will come in the form of cloud providers forming partnerships with security vendors to bolster defenses of their platforms, or new cloud-based offerings directly from vendors that organizations can plug into their cloud environment.

- The trend toward cloud-based security solutions will drive a greater need for measurement of the effectiveness of security in the cloud to ensure that systems and controls are working as they should -- especially important given the lack of visibility and control security teams have when security is offered by their cloud provider.

- The growing use of IoT and mobile devices in the enterprise will push the need for application-layer security to ensure that cloud-connected devices and the applications that run on them don't pose new attack vulnerabilities.

> The ever-evolving threat landscape and new methods hackers use to conduct a breach, combined with the growing shortage of skilled security professionals, will cause more companies to turn to managed security services to ensure their defenses are appropriately looked after, and free up security teams to focus on aligning with business leaders to address cyber risk.

© FireEye, Inc. 2020

CYBERSECURITY 2020 TREND:

Customer Trust Will Become More Heavily Weighted in Compliance with Data Protection and Privacy Regulation



Formally instituted in May 2018, the European Union's General Data Protection Regulation (GDPR) was designed to establish uniform requirements around consumer data privacy for all member nations and businesses across the region. As data privacy becomes a growing concern for citizens of the U.S., it is expected that we'll begin to see legislation to establish similar protections to those specified by GDPR.

Currently, each of the fifty U.S. states has its own privacy regulations. This creates challenges in how companies address this important area, not to mention the added complexity of industry-specific regulations such as HIPAA and the Financial Privacy Act. While federal regulation may not take place immediately, companies in the U.S. will need to increase their focus on protecting customer data and ensuring enterprise systems have appropriate controls in place to demonstrate corporate governance and strengthen customer trust.

VERODIN PREDICTS:

- U.S. federal and state governments will complement their continued focus on data privacy through stronger regulation with a requirement to baseline and demonstrate evidence of compliance.
- Companies will pay greater attention to the protection of customer data as part of the organization's overall cybersecurity initiatives and corporate governance.
- Leaders from areas of the business not traditionally focused on cybersecurity that have a stake in data privacy compliance, such as CMOs, CFOs and CHROs, will gain greater influence over the company's approach to cybersecurity.
- The way companies protect customer data and demonstrate good 'cyber citizenship' will become an increasingly important factor among consumers in determining which brands to support and/or where to spend their dollars.

© FireEye, Inc. 2020

CYBERSECURITY 2020 TREND:

Increased Demand for Election Security – The Nation's Biggest Threat to Democracy in 2020



In 2018, new spending was made available by the federal government as part of the 2002 Help America Vote Act (HAVA), granting $380M in new funding for states to update the security of their election systems. Yet experts say this amount is a tiny fraction of what is needed to fully update the U.S. electronic voting system and protect this country from potential attacks. With the 2020 election cycle fast approaching, there is tremendous urgency to address the underlying issues that jeopardize the sanctity of U.S. elections. While Congress debates the need for more funding and how it should be applied, there are steps being taken by state governments to address the security of the election system and processes, which will become more prominent in 2020.

VERODIN PREDICTS:

- There will be increased collaboration between state governments and providers of cybersecurity software and hardware to ensure greater transparency in how systems are evaluated, their potential vulnerabilities and how those vulnerabilities are addressed.

- While security of the voter registration database and e-voting system are critical areas of the election process that need to be addressed, the biggest threat to the security and sanctity of the November 2020 election will be the growing manipulation of influence taking place by way of social engineering, which sways voters' opinions before they head to the polls. This includes viral sharing of deepfake videos, fictitious news stories and targeted, false content on social media networks and elsewhere.

- Currently, the Secretary of State in each state oversees the election process, independent of state CTOs and CISOs who are more familiar with the related cybersecurity challenges. There will be closer and more direct working relationships between the Secretary of State, CTO and CISO in implementing the people, processes and technology that will prevent malicious attacks on state voting systems.

- Continuous validation of security solutions that are part of the e-voting infrastructure will become a critical component of ensuring the election system is safeguarded from foreign or malicious attacks.

© FireEye, Inc. 2020



CONCLUSION:

The ability to measure and improve cybersecurity effectiveness is at the heart of the trends that will shape the security industry in 2020 and beyond.

With companies facing increasing regulatory pressures, as well as the widening attack surface and evolving threat landscape, investments in security tools must prove their value and give leadership confidence that the security team is doing everything it can to protect the organization's most critical assets.

Without ongoing validation that security solutions are working as promised, businesses can be caught off-guard when an attempted hack is successful, and the

financial impact and cost to brand reputation can be highly disruptive and long-lasting.

Verodin will play a central role in helping companies take a more holistic approach to cybersecurity by demonstrating effectiveness and the impact of cyber risk on the overall business, through testing and measurement that identifies misconfigurations, improper responsiveness and gaps in the security environment. When these issues are properly assessed and remediated, companies take great strides in protecting themselves from the long-lasting impact of a cyberattack and threat to their long-term viability.

© FireEye, Inc. 2020

VERODIN
NOW PART OF FIREEYE

ABOUT VERODIN

Verodin, part of FireEye, is a platform that has made it possible for organizations to validate the effectiveness of cyber security controls, thereby protecting their reputation and economic value. The Verodin Security Instrumentation Platform (SIP) proactively identifies gaps in security effectiveness attributable to equipment misconfiguration, changes in the IT environment, evolving attacker tactics, and more.

By measuring and testing security environments against both known and newly discovered threats, Verodin SIP identifies risks in security controls before a breach occurs and permits companies to rapidly adapt their defenses to the evolving threat landscape. Verodin SIP does this by instrumenting an IT environment to test the effectiveness of network, endpoint, email and cloud controls and provides quantifiable evidence that investments made in controls are actually delivering the expected business outcomes.

Find Verodin on:
Twitter | LinkedIn | YouTube | Facebook

A product demo can be scheduled at **Verodin.com/demo**

1-571-418-8684

© FireEye, Inc. 2020