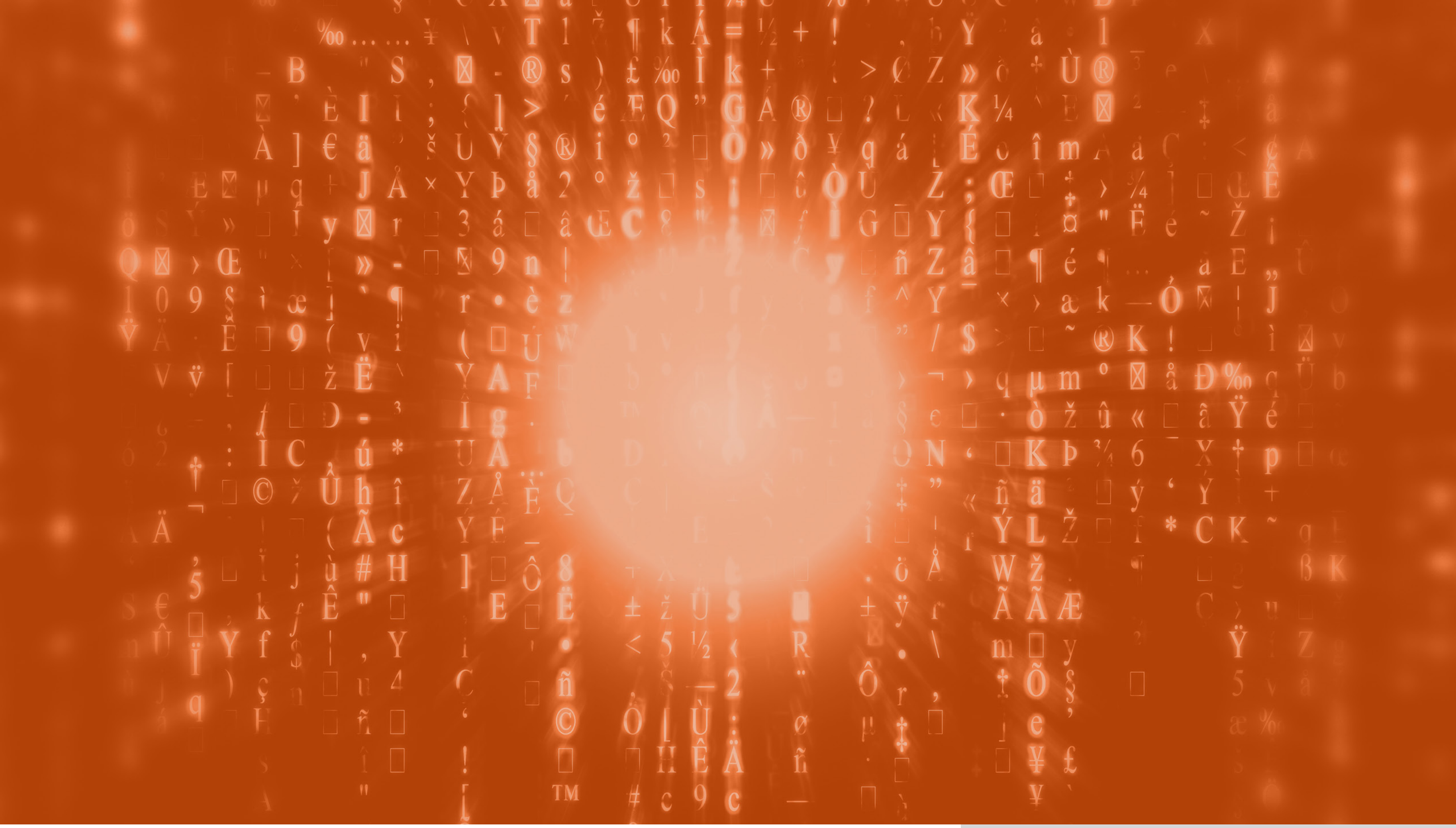
# NEW SECURITY CHALLENGES REDEFINE RISK AND VULNERABILITY

## What Security Leaders Need to Know

WHITE PAPER



**The onslaught from cybercriminals did not let up this past year. Rather, the attacks increased in volume and sophistication, impacting global economies, nation state relations, political elections, and critical infrastructure. Cybercriminals with relatively small resources took down banking and healthcare systems, held entire companies hostage for ransom, and disrupted large sectors of commerce and communications.**

The cost of cyberattacks is a significant problem. Estimates peg the cost of cybercrime to businesses at $400 billion annually, a number that continues to grow. Indeed, some projections indicate it will hit $6 trillion by 2021—a 15-fold jump![1]

To keep pace with this changing threat landscape, enterprises will spend over $1 trillion on cybersecurity between now and 2021. This equates to an increase of 15 percent year-over-year.[2] This growth is evident in a number of ways. For example, the U.S. government alone accounts for $19 billion in cybersecurity spending; Microsoft invests over $1 billion annually on cybersecurity research.[3] And enterprises are worried about the risks of cyber threats, accounting for upwards of a 50 percent annual growth rate in cyber insurance.[4]

The constant noise around cybersecurity and its dynamic evolution makes it difficult for enterprises to keep up and to hone their focus around what is really important—namely, what will enable them to improve their risk threshold. In the analysis below, we look at the reasons security remains a major problem for many enterprises today.

**76 percent** of enterprise cybersecurity professionals fear they will fall prey to **cyberattacks** this year.[5]

Multi-vector attacks increased **322 percent** last year[6]

**4.2 billion** data records were stolen last year.[7]

SCADA bugs now comprise **30 percent** of all vulnerabilities.[8]

## IMMATURE SECURITY POSTURE

The speed of transformation and intensity of cyber risks dictates that organizations search for new ways to automate aspects of cyber-threat detection and prevention. Relying on traditional signature-based threat protection solutions leaves large gaps in an organization's security posture.

And while we have seen significant advancements in cybersecurity technologies and services over the past few years, the reality is the security postures for many enterprises lack maturity. For example, a study by the Online Trust Alliance found that 9 out of 10 data breaches that occur could have been easily avoided.[9] Security professionals are concerned: 8 in 10 believe that cost pressures and the need to generate revenue in their organizations have increased their exposure to threats, and 7 in 10 say their enterprises have experienced a security issue in the past 18 months.[10]

**So, what are some of the reasons this is the case?**

**First,** security is too reactive. Evolution of business requirements and accompanying technology disruption, along with the growing intensity of the cyber-threat landscape, surpasses the protection and compliance capabilities of traditional security infrastructures. Organizations with the best endpoint security and security firewall technologies cannot extend to combat the different attack vectors.

While these technologies form a critical part of an enterprise's security strategy, they are no longer able to deliver levels of protection demanded by today's business requirements. Instead, as noted by Accenture, "state-of-the-art in cybersecurity is an approach, a mindset—not an implementation or technological end-state. It evolves and adapts as the value of assets shift and the type or level of threat changes."[11]

**Second,** many enterprises lack appropriate levels of security awareness and preparedness. And it is not simply business leaders who indicate that this is the case; security leaders lack confidence as well, with less than half of security operations professionals reporting that security processes at optimal levels.[12]

There are various reasons for this deficiency. One is a need to evolve and mature security processes further. A second relates to a lack of vetting of business partners and their security postures—more than 40 percent of enterprises do not vet their ecosystem partners for cyber readiness. A third reason is that too many enterprises maintain inconsistent security processes among business units, geographies, and vertical industries, resulting in cybersecurity postures fraught with deficiencies and gaps. A final issue is that organizations lack transparent security visibility, often failing to actively monitor and analyze for security threats.

**Third,** finding, recruiting, and hiring cybersecurity professionals with the experience and expertise to manage security technologies, as well as craft, implement, and manage security policies and processes required by the business, is becoming increasingly difficult. One of the problems is that the number of security technologies a typical enterprise has in place continues to grow in number and complexity. The other reason is that there simply are not enough cybersecurity professionals to go around. Estimates pinpoint the shortage of workers today at around 1 million, with projections showing the number will top 1.5 million by 2020.[13]

**42 percent** of enterprises did not know the source of security incidents eight years ago. Today, that number has fallen to **10 percent**.[14]

**Training** is an area where enterprises could offset some of the worker and skills shortages. However, only **60 percent** of enterprises express that they are even slightly open to investing in security training for their cybersecurity teams; **one-fifth** are not willing to fund security training at all. It is no surprise that **70 percent** of cybersecurity professionals say they hold no professional certifications.[15]

## LOSS OF CONTROL DUE TO IoT

Internet of Things (IoT) devices are growing at a 50 percent annual rate. Projections show the number of IoT devices will double between now and 2020, hitting 30.7 billion—and increase five-fold by 2025 to exceed 75 billion. Sam Lucero, "IoT Platforms: Enabling the Internet of Things," IHS White Paper, March 2016.[16]

IoT is transforming certain industry segments such as healthcare, utilities, transportation and shipping, manufacturing, automotive, among others. It is not just businesses that benefit from IoT devices. Consumers are being offered new conveniences, such as the ability to integrate automotive experiences, in-home digital services, smart shopping experiences, and more.

But as often happens with digital transformation and growth, the challenges concurrently multiply. The cybersecurity risks of IoT are substantial, and enterprises need to heed the potential impacts to their organizations carefully. One recent study found that 70 percent of the most commonly used IoT devices contain security vulnerabilities.[17] Thus, it should not be a surprise that 25 percent of all attacks on enterprises in the near future will target IoT devices.[18] And in the event of a sophisticated attack, organizations admit they are unlikely or highly unlikely to detect it before systems and data are impacted.

Take the automotive space as an example. IoT-connected vehicles offer consumers everything from autonomous driving, to smart traffic management and routing, to intelligent safety and maintenance systems.[19] While these offer consumers a vast array of new vehicle experiences and safety improvements, they also create immense cybersecurity risks, which are much broader in scope than hacking of personal and private data flowing between the vehicle and cloud apps. Rather, cybercriminals could hack into the actual IT systems of the vehicle to initiate ransomware attacks, make the vehicle inoperable, or disable critical systems—which could lead to accidents and even fatalities.

The 2015 cyberattack on the Ukrainian power grid demonstrates the potential repercussions on a nation state level, where bad actors rewrote firmware on the SCADA network to take control of the network and shut down electrical services in 130 different cities.[20] Another area with the potential for dire consequences is healthcare, where cybercriminals could feasibly infiltrate IoT devices used to deliver patient care with ransomware and hold them and data hostage until the healthcare company pays a specified ransom.[21]

Automotive, utilities, and healthcare are just a few of the industries where IoT security concerns are real; other industries such as manufacturing, warehousing, and transportation present comparable cybersecurity risks.

Enterprises saw a **152 percent** jump in **IoT attacks.**[22]

The number of **IoT botnets** are growing in leaps and bounds, with a **130 percent** increase occurring over a three-month timeframe last year.[23]

## FLEXIBILITY VIA THE CLOUD

Even though the cloud comprises less than 15 percent of total IT spend,[24] estimates show that nearly half of IT services are delivered via the cloud today.[25] And this number is going to jump to 75 percent by 2020 according to Microsoft.[26] A parallel projection indicates that 92 percent of workloads will be processed in the cloud (versus 8 percent by traditional data centers) within that same time frame.[27]

Greater flexibility is at the top of the list of reasons organizations typically cite for their adoption of the cloud. Growth in the use of software-as-a-service (SaaS) applications, and their transmission of data to and from the cloud, is pushing cloud security to the forefront for many enterprises. Additionally, as the number of SaaS applications grow, so do the interdependencies—and thus security liabilities—between them.

Enterprises simply cannot approach cloud security in the same ways they address traditional infrastructure security. They will do well to heed the differences:

**First**, cloud solutions redefine the network perimeter. Traditional infrastructure security solutions have a well-defined network perimeter. The cloud deconstructs this by stretching security to the edges of the network (e.g., IoT devices). And as organizations need a transparent view of cloud services, the risks they pose, and how they are being managed, cloud security data must be synthesized with other forms of external and internal data to create a proactive security posture.

**Second**, stewardship and controls change with the cloud. Encryption of data in transit and at rest and what cloud providers can see and cannot see become very important. Data controls, monitoring, and system logs also play a role. Existing regulations such as the Health Insurance Portability and Accountability Act (HIPPA) and Health Information Technology for Economic and Clinical Health (HITECH) Act serve as a lens for the development of data stewardship and controls. The EU General Data Protection Regulation, which supersedes the existing Data Protection Directive and will go into effect in May 2018, is certain to drive any number of data governance initiatives for enterprises as they relate to the cloud.

**Third**, shadow IT cloud services—where the average employee uses up to 27 different cloud applications and the average enterprise has 897 different cloud applications in use—present significant risk issues.[28] These shadow IT services present significant risk, starting with the fact that security leaders have no idea which users and business units are using which cloud services, and the risk of each of the services. And when it comes to data—both in transit and at rest—there are varied questions involving cloud services such as their security protections and policies in relationship to industry regulations.

**22 percent** of files uploaded to file-sharing cloud services contain sensitive or confidential data such as PII, payment information, or PHI.[29]

Only **22 percent** of enterprises have **cloud awareness** training programs.[30]

## NEED FOR CONSOLIDATION

As the attack surface expands, so does the number of different security solutions that an enterprise must manage. Just a few years ago, a cybersecurity organization needed to manage a handful of security solutions. Today, this number has grown into a substantial snowball for many organizations. Multiple point solutions are layered on top of each other to fill potential gaps. And though it may vary from one organization to the next, the number of point products many enterprises use ranges between 6 and 50.[31]

Many enterprise security leaders add these different layers on the basis that they make it more difficult for a bad attacker to succeed. However, as Forrester argues, point-product solutions point-product solutions can add complexity and obstruct cybersecurity professionals from detecting and preventing attacks in some instances.[32] They also add cost and require more staff resources.

In the first case, a patchwork of point solutions prevents cybersecurity teams from seeing across their entire enterprise. Each solution may have their own visibility, but this is only in their own individual silos. What organizations need is an integrated, global view across all of their security infrastructure.

Managing all of the different moving pieces of a security infrastructure also becomes increasingly difficult with point solutions. One aspect involves the need for universal policies that enable organizations to maintain consistent security enforcement and management—something not possible with point solutions. Instead, enterprises must create—and manage—policies unique to each one of them. Not only is this inefficient, but it creates security gaps that can be exploited.

The separate silos of data sets that reside within each point solution impede real-time communication and collaboration between solutions. Without an aggregate data record, it becomes very difficult for an organization to possess full intelligence, which is required in a world of zero-day attacks. Most point solutions also lack automated artificial intelligence and machine learning technologies such as whitelisting and sandboxing to identify known and unknown threats. Not only does this generate inefficiencies, it also creates added risks.

The number of **point-security solutions** managed by the typical enterprise has spiraled from a handful to as many as **50** in some instances.[33]

## LACKING A COMPLETE PICTURE OF RISK EXPOSURE

Historically, many cybersecurity organizations sprung from IT and remain contained within them. Though it varies from one report to the next, only about one-quarter of CISOs report to the CEO or board, with over half reporting to the CIO today. However, without visibility at the executive level, CISOs lack the influence and management scope to affect necessary change—and the outcomes support this contention. For example, in instances where the CISO reports to the CIO versus the CEO or board, downtime caused by security incidents is 14 percent higher and financial losses are 46 percent higher.[34]

At the same time, with many CISOs coming up through the ranks of IT, most are technologists at heart. Enterprise security is viewed foremost as a technology challenge, and not a business issue. As a result, less than half of security leaders view security as a risk-management issue and admit they do not understand their organization's business issues and competitive environment.[35] In this context, security becomes a checkbox, an afterthought once the business requirements of speed, optimization, automation, innovation, and other business issues are addressed.

Enterprises predominantly rely on qualitative guidance to determine vulnerability based on estimates that lump together both frequent and rare large losses. But this risk assessment model fails to provide accurate direction, leading companies to size their security investments incorrectly and to obtain insufficient cybersecurity insurance protection.[36] Admittedly, while it is impossible for any company to eliminate cyber risks completely, enterprises can do much better.

The problem is that too many organizations determine their risk postures based on an incomplete or inaccurate understanding of their vulnerabilities. Companies typically calculate risks in terms of operational risks, focusing on direct revenue losses rather than a broader set of factors. The reality is that cybercriminals can harm an enterprise even if they exact no financial gain.

Risks fall into two buckets: 1) those where services are shut down, and 2) those where information is compromised (private data, personal information, bank accounts, passwords, etc.). The impact of these risks can run the gamut—from lost revenue, to brand degradation, to service interruptions. It also can involve remediation fees such as offering credit monitoring services to impacted customers, legal fees, compliance penalties, and class-action lawsuits.[37] See Table 1 below for more details.

| | How to Respond | Revenue | Cost-Fines | Brand |
|---|---|---|---|---|
| **Operations Disruption** | Customer experience is degraded as a result of being unable to have questions answered and service-related issues resolved. | Loss in commerce transactions, productivity inefficiencies, and delays that translate into lost revenue. | Lost productivity while systems are down. | DDoS attacks create brand awareness problems; delays in product shipments or service delivery also impact brand reputation. |
| **Information Theft** | Privacy and data theft requires customers to monitor credit and identities in the event they have been hacked. | Brand degradation deriving from publicized data theft and the release of private information leads to lost revenue. | Non-compliance with data privacy regulations and laws results in fines, penalties, and even class-action lawsuits. | Publicity surrounding data breaches and losses directly impacts brand reputation. |

TABLE 1: CYBERSECURITY RISK SCENARIOS

## SECURITY IN A NEW DIGITAL WORLD

In a digital world where the attack surface is rapidly expanding and pushing the edges of the network into new territories, enterprises must rethink cybersecurity strategies. The breadth of devices and data involved, the number of applications residing in the cloud combined with the amount of data crisscrossing on-premise and cloud systems, as well as the ability to employ advanced threat intelligence technologies such as artificial intelligence and machine learning are transforming how enterprises think about cybersecurity.

[1] Steve Morgan, "Cybersecurity Spending from 2017 to 2021," CSO Magazine, June 15, 2016.

[2] "Cybersecurity Market Report," Cybersecurity Ventures, Q1 2017.

[3] Ibid.

[4] "2017 Cybersecurity Predictions: Attacks Intensify and Regulation Emerges from the Shadows," Stroz Friedberg, January 2017.

[5] Dean Alvarez, "Enterprises Fear Brand Damage—More Than Breaches—Due to Lack of Risk Management Strategy," IT Security Guru, February 3, 2017.

[6] Lindsay Stares, "Growth of Cyberattacks Explored in New Report," Upside, January 13, 2017.

[7] Herb Weisbaum, "More Than 4 Billion Data Records Were Stolen Globally in 2016," NBC News, January 30, 2017.

[8] Bharat Mistry, "The Biggest Security Threats in 2017," Betanews.com, accessed March 11, 2017.

[9] "90% of data Breaches Are Avoidable," Cyber Security Intelligence, February 2, 2016.

[10] "As Hyper-Extended Enterprises Grow, So Do Security Risks," Market Pulse, RSA, April 2016.

[11] "The State of Cybersecurity and Digital Trust 2016: Identifying Cybersecurity Gaps to Rethink State of the Art," Accenture, 2016.

[12] "Tackling the Cybersecurity Maturity Challenges to Succeed with Digital Transformation," i-Scoop.eu, accessed March 14, 2017.

[13] Michael Suby, et al., "The 2015 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan, 2015.

[14] "Toward New Possibilities in Threat Management: Key Findings from the Global State of Information Security Survey 2017," PwC, February 2017.

[15] Peter Tsai, "The Alarming Cybersecurity Skills Gap," Network Computing, September 29, 2016.

[16] Sam Lucero, "IoT Platforms: Enabling the Internet of Things," IHS White Paper, March 2016.

[17] "Cybersecurity and the Internet of Things: Insights on Governance, Risk, and Compliance," EY, March 2015.

[18] "Understanding the IoT Explosion and Its Impact on Enterprise Security," Fortinet, February 2017.

[19] Richard Vierecki, et al., "Connected Car Report 2016: Opportunities, Risk, and Turmoil on the Road to Autonomous Vehicles," PwC, Strategy&, September 28, 2016.

[20] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 3, 2016.

[21] "Internet of Things Triggers Healthcare Security Concerns," Healthcare IT News, March 31, 2015.

[22] "IoT-powered Attacks Gain Ground While Financial Sites Plagued," Orbit News Online, March 9, 2017.

[23] Ibid.

[24] Clint Boulton, "6 Trends That Will Shape Cloud Computing in 2017," CIO, November 2, 2017.

[25] "Toward New Possibilities in Threat Management: Key Findings from the Global State of Information Security Survey 2017," PwC, February 2017.

[26] "Emerging Era of Cyber Defense and Cybercrime."

[27] Joe McKendrick, "With Internet of Things and Big Data, 92% of Everything We Do Will Be in the Cloud," Forbes, November 13, 2016.

[28] "Cloud Adoption & Risk Report Q4 2016," Skyhigh Networks, 2016.

[29] "Cloud Computing Trends: 2016 State of the Cloud Survey," Right Scale, February 2016.

[30] Ibid.

[31] Patrick Moorhead, "With a Few Surprises, Cisco Releases 2017 Annual Cybersecurity Report," Forbes, February 14, 2017.

[32] Rick Holland, "Point Solutions Must Die," Forrester, August 18, 2013.

[33] Morehead, "With a Few Surprises."

[34] "Eight Reasons the CISO Should Report to the CEO and Not the CIO," CIO, January 6, 2017.

[35] "Toward New Possibilities in Threat Management: Key Findings from the Global State of Information Security Survey 2017," PwC, February 2017.

[36] Leslie Chacko, et al., "Can You Put a Dollar Amount on Your Company's Cyber Risk?" Harvard Business Review, October 5, 2016.

[37] Ibid.

FORTINET®

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990