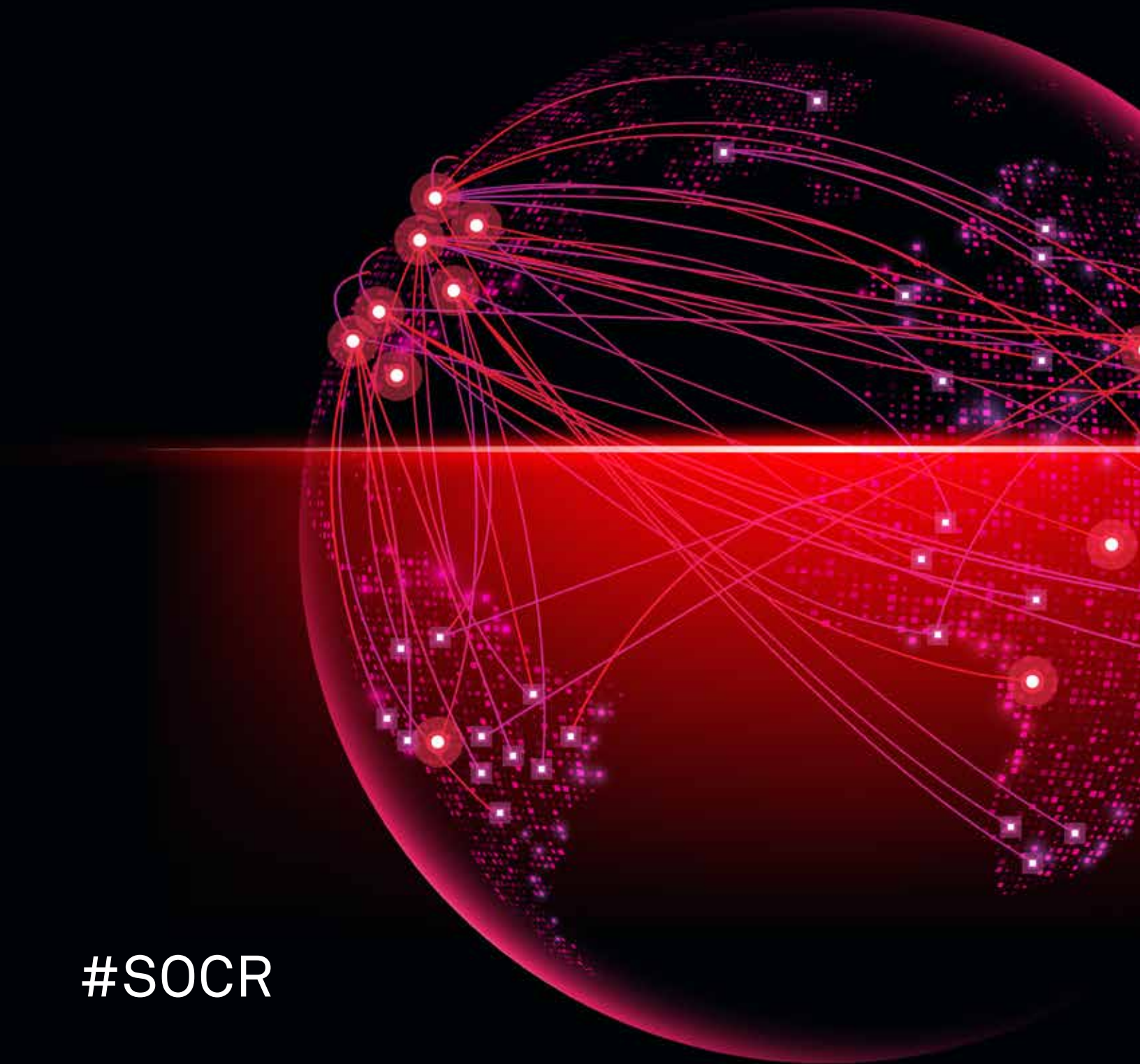
STATE OF CYBERSECURITY REPORT 2020



#SOCR

TABLE OF CONTENTS

FOREWORD

Welcome to the 4th edition of the State of Cybersecurity Report. In the last six months, the cybersecurity landscape has evolved considerably. We have come some way since the COVID-19 pandemic breakout. What started as a medical crisis and transformed into an economic and social crisis is being used by threat actors for targeted campaigns. Global trade wars are taking shape and could lead to cyber espionage. Stringent data privacy regulations and rising cybersecurity concerns in boardrooms are bringing more focus and accountability on executive management.

Our research findings this year offer insights into how organizations are trying to stay ahead of the curve in these demanding times. I notice businesses and organizations giving a lot of interest and attention to the following aspects:

- Defining minimum viable plans into critical business processes and supporting digital systems
- Continuously monitoring changing risks within units and supply chains
- Delivering secure IT services through multi-cloud and remote work enablement
- CISOs embracing collaboration for threat intel with ecosystem partners (ISACs, MSSPs, and even peers) to keep track of threat actors and their campaigns

Strategic focus and investments in cybersecurity will continue to increase. The CISO function will be a critical enabler for organizations as the economy picks up. Hence, our research not only focuses on what happened during the pandemic but also provides foresight toward future cyber strategies in a post-COVID world.

I wish to thank all our customers who participated in the primary research process and our valued technology and academic partners who contributed to the diversity of topics covered in the report. We believe that we have to give as much as we receive to make the world a safer place, and the State of Cybersecurity Report 2020 is a realization of that belief. Happy reading!

BHANUMURTHY B.M.

President and Chief Operating Officer

Wipro Limited

linkedin.com/in/bhanumurthy-ballapuram-080b7b

EDITOR'S NOTE

The four-year journey of Wipro's State of Cybersecurity Report has been exhilarating! The report's unique DNA has remained steadfast from its inception, providing readers with a unique construct of the changing macro, meso, micro, and future views of cybersecurity globally. Through this construct, we've continued to weave in refreshing insights on how threat actors are morphing themselves and how the defender stratagems are being redrawn.

This year's State of Cybersecurity Report is loaded with research and analysis that will appeal to executives and middle management alike. Nation-state attacks, classification of nearly 1.1 million intelligence alerts, top malware categories, worldwide regulatory heat maps, budgetary trends, cyber investment hotspots, security metrics, security patent trends, start-up technology spotlights, post-COVID-19 cybersecurity roadmaps, and more – we have it all!

I firmly believe that the points of view on the people's perimeter, zero trust security, cloud permissions risks, and container security will enrich the dialogues on these emerging areas. An academic viewpoint on the government's role in cyberdefense is expected to reignite the discourse on deterrence. The **Future of Cybersecurity** section highlights how cyber collaboration across critical infrastructure providers might need to leverage decentralized trustware networks during future disasters. The **Security Trends by Industry** section gives readers an industry benchmark of the cybersecurity landscape.

I want to thank the security leadership and researchers from our partner and Wipro Ventures ecosystems, who collaborated tirelessly with the research data and points of view woven into this year's State of Cybersecurity Report narrative. Read on and spread the good word!

JOSEY V GEORGE

Editor-in-Chief: State of Cybersecurity Report 2020

Practice Head, Strategic Initiatives, Cybersecurity & Risk Services

@joseyvg

linkedin.com/in/josey-george

Executive Summary

Cybersecurity is today a lever for competitive advantage in a world accelerating forward with intense digitalization. Along with being a shield that protects organizational innovation and intellectual property, it is foundational to digital trust, market making, and inclusivity. The state of cybersecurity is now a concern that transcends the interests of the CISO organization and holds the attention of executive management and the board. Over the course of the last four years, Wipro's State of Cybersecurity Report (SOCR) has grown leaps and bounds in the breadth of research, industry collaboration, and readership.

The noteworthy structure of the SOCR bringing forth the macro, micro, meso, and future views of cybersecurity makes it a unique, thought-provoking research publication. This year's report includes a cybersecurity perspective connected to COVID-19, which brings to the fore current cyber risks, IT security challenges, expected threat actor actions, and technology trends that could define the post-COVID cyber normal. The report is underpinned by primary research that covered 190+ corporations located in 35 countries, 1.1 million intelligence alerts, 6500+ incidents, 225 unique malware threats, and 30+ security products, and included collaboration with 21 technology and academic partners.

Presented below is a summary of key statistical findings grouped by the main sections of the report, which should strike a chord with the busy reader. For highly informative, relevant, and in-depth points of view on current and future cyber trends, we invite you to dive in.

State of **Attacks, Breaches, and Law**

This section presents a macro-level look at what happened in the cybersecurity ecosystem worldwide. It gives a big picture of how nation-state cyberattacks evolved during the past three years, the trends around data breaches, cybersecurity intelligence alerts, global malware statistics, vulnerabilities in security products and open-source projects, and changing regulations around the globe.

STATE OF

ATTACKS, BREACHES, AND LAW

1 Nation-State Attacks Target Private Sector

86%

of all Nation-state attacks fall under **ESPIONAGE** category

2 Attack Tactics: Rise in Botnet Malware-Based Attacks

BOTNET **MALWARE ATTACKS**

18% (2018) » 28% (2019)

3 Chink in the Armor: Human

86%

rated phishing as the biggest threat

4 Chink in the Armor: Technology

30+

Security products found with code execution & auth bypass vulnerabilities

*Analysis of CVE data

5 Attack Breach Rate

39%

of organizations had a breach in the **LAST 3 YEARS**

6 The Spoils of Breaches

WHAT WERE **ATTACKERS AFTER?**

67%

are after advanced PII

*Analysis of top 40 breaches

7 Monetization of Breach Spoils

41%

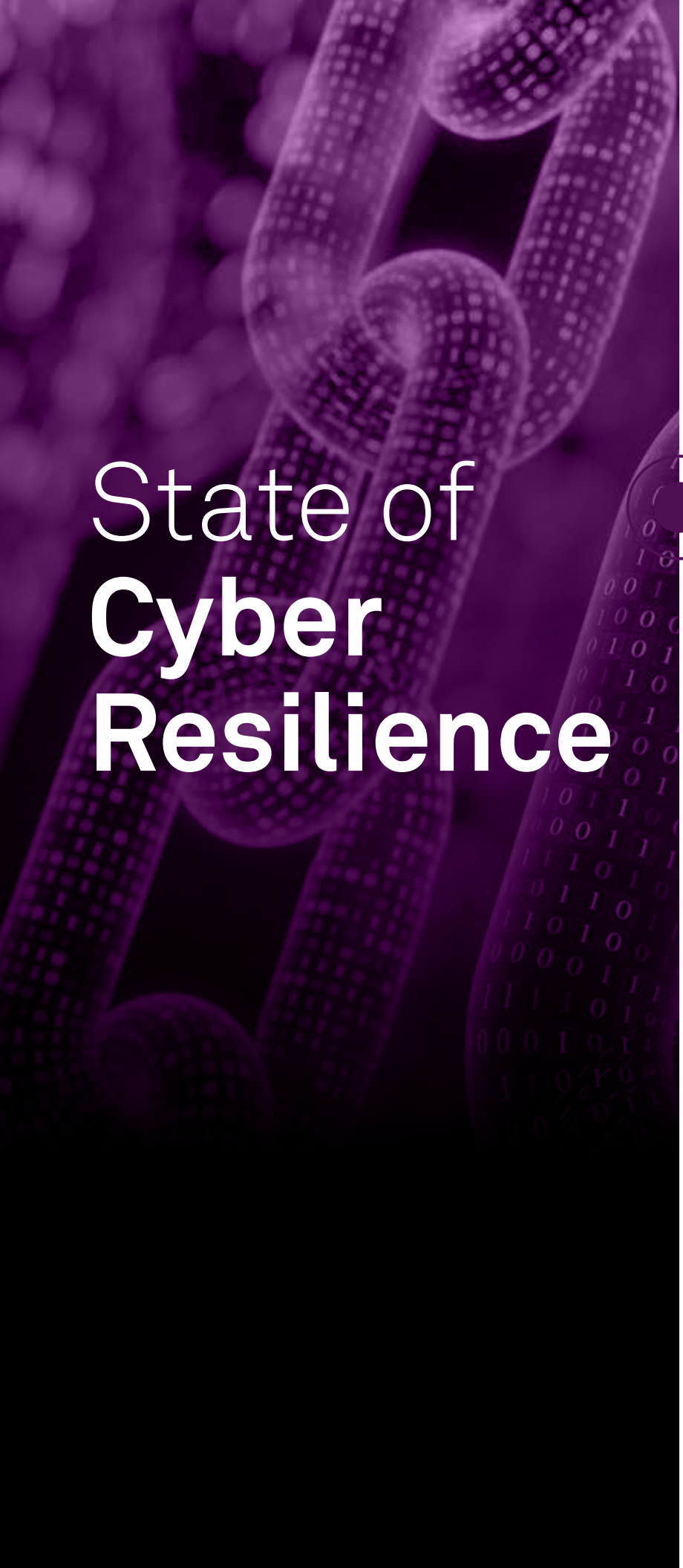
of black-market data sold belongs to BFSI sector

8 Public Policy Response

57%

of analyzed countries have strong breach notification laws

*Analysis of 23 countries



State of **Cyber Resilience**

This section takes a micro-level look at cybersecurity within the enterprise. This view gives an inside-out perspective about security governance, budget, investment priorities, domain-related metrics, and best practices across data security, application security, and endpoint security. The section also features our partners' viewpoints on topics like the people perimeter, zero trust, DDoS trends, cloud permissions, and container risks.

STATE OF CYBER RESILIENCE

1 Alignment of Cybersecurity to Business Risks

59%

UNDERSTAND their risks

2 Confidence on Resilience

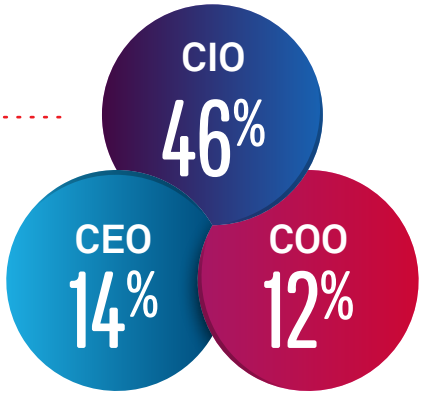
ONLY 23%

are highly confident about preventing cyberattacks

3 What are the TOP RISKS being battled?

- 86% Email phishing
- 57% Lack of employee awareness
- 54% Third-party risk

4 How are Governance Structures evolving?



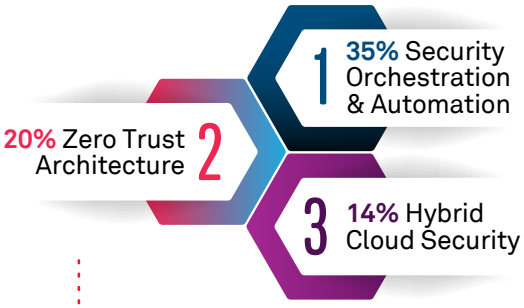
CISO roles are moving towards Risk Governance

5 % of IT Budget for Security

12%

14% of Organizations had >12% of IT Budget for Security

6 What are the TOP INVESTMENT PRIORITIES?



7 Top Security Metrics

64%

Report MEAN TIME TO DETECT (MTTD)

8 Cyber Talent Vacuum

Organizations **struggle to retain top talent**

STATE OF

CYBER RESILIENCE

Application Security

SECURE BY DESIGN

27%

Embed Security in DevOps

Organizations are shifting to the left by embedding security early on

SOC Capabilities

EVOLVE TO COGNITIVE SOC

49%

Organizations are looking to extend cognitive detection capabilities to their SOC

Employee Awareness

USE ADAPTIVE TRUST MODELS

Risk due to employee negligence

57%

Behavior-centric analytics provides adaptive risk-level ratings unique to each user

Data Security Controls

AUTOMATION IN DATA SECURITY

32%

Automated Data Discovery and Classification

Automation of data security controls from discovery to protection

Cloud Security

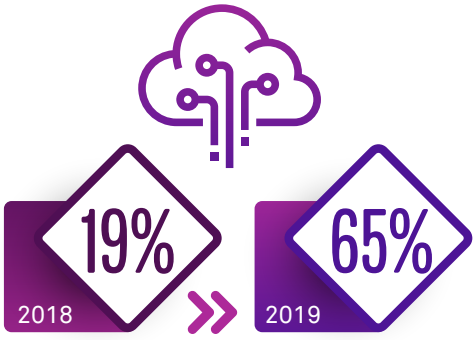
GOVERN OVER PERMISSIONS IN CLOUD

Cloud Identities Over Permissioned

Dangerous delta exists between permissions granted and used for cloud identities

IoT/OT Security

OT/IOT—IDENTIFY & MONTOR



OT/IOT Security Monitoring

Organizations stepping up on industrial asset identification & monitoring

State of **Collaboration**

This section emphasizes the importance of collaboration and represents the meso view. Security teams within organizations cannot exist by themselves and today need to depend on and collaborate with external stakeholders for threat intelligence, alerts, remediation measures, and general best practices. It also discusses governmental responsibilities toward private enterprises in the wake of nation-state attacks and highlights the growing importance of security within supply chains.

STATE OF
COLLABORATION

Peer Collaboration
Barriers to information sharing

43%
LEGAL BARRIERS

REPUTATIONAL RISKS
64%

Peer Collaboration
Information Sharing

57%

are willing to share only Indicators of Compromise (IoCs)

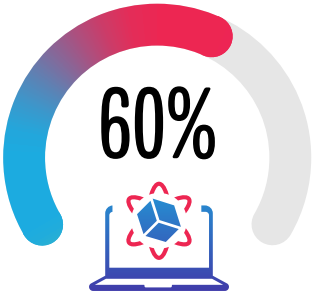
Internal Collaboration

In 34%
of organizations, the CPO/DPO are responsible for Data Privacy

Increased functional alignment with DPO, HR (Policies, Legal Action), General Counsel (Compliance, Breach Litigation), Risk Officer, CIO, CTO & CFO

Corporate Communications to build Stakeholder Trust

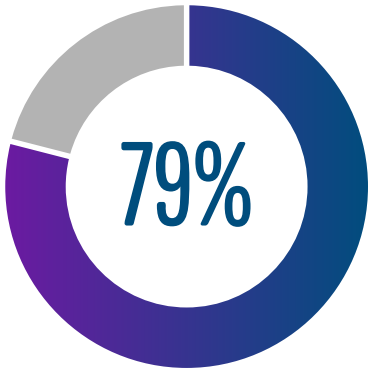
External Collaboration
Sectoral Simulation Exercises



PARTICIPATE
in Cyber Simulation Exercises

Organizations are increasingly participating in attack simulation exercises to assess preparedness

External Collaboration
Insurance-based Risk Transfer



of Organizations have Cyber Insurance

Cyber insurance as a partial risk transfer mechanism has seen a 14% increase

Future of **Cybersecurity**

New technology adoption as part of digital transformation is widening attack surfaces and expanding operational risks. The research on patent filings in cybersecurity presents trends in cyber research. We also analyzed key seed investment areas in security start-ups to identify emerging trends in security technologies. An academic point of view on leveraging decentralized trustware-based platforms for collaboration is also presented.

FUTURE OF CYBERSECURITY

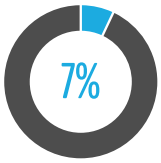
49% AI/ML

Leading Cyber Patent Category

of the Cybersecurity patent filings were in the AI/ML, and data science space

Emerging Patent Domain

5G Security



7% of the Cybersecurity patent filings were in the 5G space

AI/ML Leverage in Cyber

- Risk scoring
- Compliance management
- Threat detection
- Data discovery
- Threat intelligence
- Threat hunting
- Anomaly detection
- User behavior analytics
- DDoS mitigation
- Adaptive authentication

Top 3 Cyber Start-up Funding Categories

- IoT Device Security
- Payment Fraud
- Threat Detection

TOP 3 SEED FUNDING CATEGORIES

Cybersecurity start-up categories getting significant funding in last 3 years

Predictions (12-16 month horizon)

- Security attacks against Enterprise Cognitive systems
- Attacks on OT and Cyber Physical systems to escalate
- Penal attacks on private sector, triggered by global trade wars
- Espionage attacks on emerging Digital Twins
- Global Election attacks and disinformation campaigns
- API Abuse the Achilles heel of Cloud-driven digitalization
- AI/ML & SOAR to mainstream Cybersecurity automation
- Consumer IoT security legislation to emerge
- RPA/BOT security governance will move up priorities
- Board-inclusive wargaming on Cyber catastrophes


“
A lost battle is a battle one thinks one has lost.”
—Jean-Paul Sartre

1

STATE OF ATTACKS, BREACHES, AND LAW

This section presents a macro view of cybersecurity globally and explores trends in data breaches, cyber weapons, and insights from intelligence alerts.

We look at how nations are grappling with a spectrum of threats across digital battlegrounds and then venture into the complicated realm of commercial security products and their vulnerabilities. The last part of this section examines the relative stringency of breach notification laws and privacy laws across 23 countries. To start, how are nations, big and small, locking horns on the digital battlegrounds, and to what ends are these battles fought?

Nation-State Cyberwarfare

Cyberwarfare, categorized by different military doctrines as the fifth dimension of warfare, has attracted considerable attention in recent years. Direct nation-state attacks (and indirect ones through proxies) have increased as more and more countries are building offensive capabilities. In the domain of warfare, high-grade cyberweapon systems are not the sole purview of conventional military powers. Offensive cyber capabilities are highly technical and within the grasp of nations with lesser firepower than established military forces. In that sense, cyberwarfare is a great leveler. Data from the Center on Foreign Relations shows the types of nation-state attacks witnessed over the last three years, as reported in the public domain. Our analysis of the CFR data considered only countries with at least five attacks to derive trends. While attribution of these attacks is complex and sometimes contested, researching the data at a broader level helps identify macro trends.

Figure 1 represents attacks from source countries on the left, types and attack categories of cyber operations in the center, and targeted countries on the right.

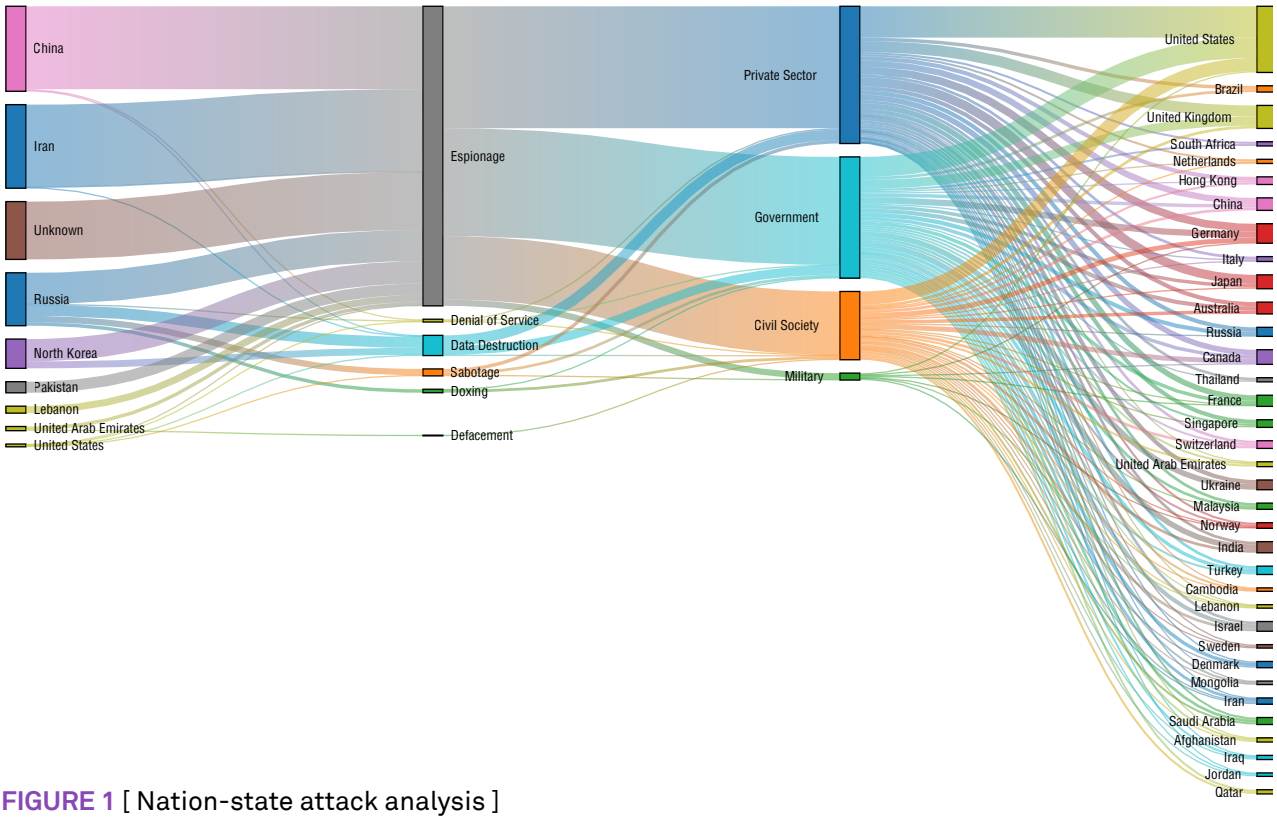


FIGURE 1 [Nation-state attack analysis]

While espionage appears as the most frequent cyber operation with the private sector bearing the bulk of the attacks, a significant number of attacks have an unknown source. Unlike a battlefield, where combatants are visible and identifiable, attribution in the cyber realm sometimes requires painstaking efforts over time.

Figure 2 shows an overwhelming 86% of the attacks in the espionage category, and nearly half of them targeted private companies.

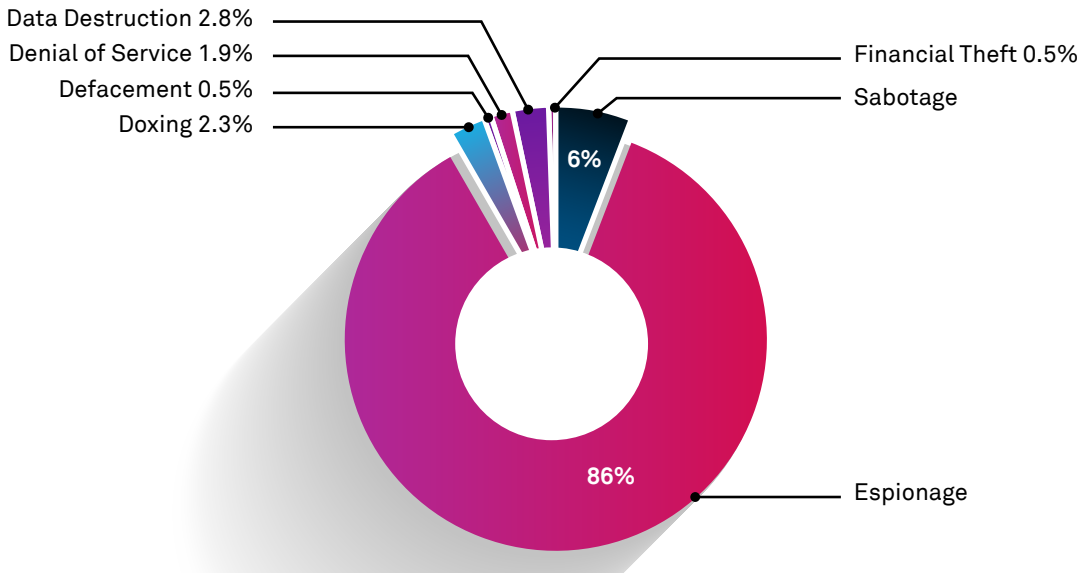


FIGURE 2 [Attacks by cyber-operation type]

Obtaining confidential information without the information holder's consent has serious business implications because the stolen data generally includes intellectual property, personally identifiable information (PII), or financial data.

Figure 3 shows attacks on civil society increased dramatically from 2018 to 2019.

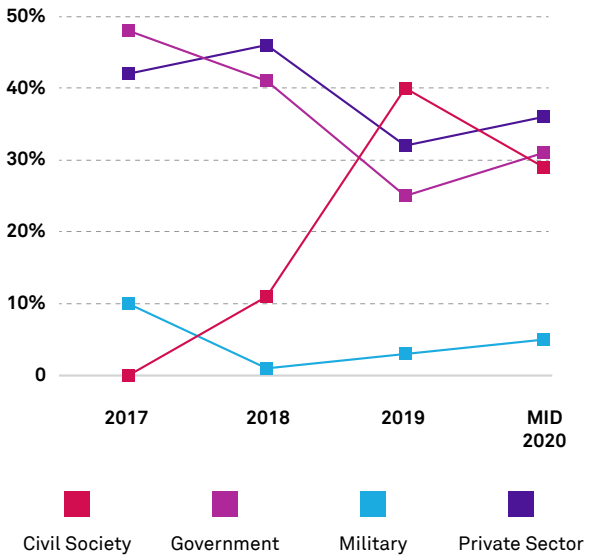


FIGURE 3 [Cyberattacks by sector]

Countries are leveraging firms specialized in mobile espionage to spy on their dissident citizens or persons of interest in other countries. Seemingly, attacks on military or government targets dipped during 2018. However, for 2020, attacks on these sectors are trending upward. The pandemic, escalating global tensions, and trade wars could be contributing to this trajectory.

These findings show that the private enterprise is enduring the most of nation-state attacks. Can private defense measures alone handle this problem? A viewpoint on nation-state attack response from ICRC, Tel Aviv University, appears in the **State of Collaboration** section.

In the ensuing section, find out how industry sectors fared with data breaches and know what kinds of data threat actors sought across the spectrum.

Data Breaches in 2019

Despite private enterprises stepping up measures to safeguard themselves, data breaches continue to surge in volume and affect the marketplace. Attackers continue to bypass preventive measures and defense strategies employed by organizations, unleashing economic fallouts, and raising the issue of cyber risk to the boardrooms for increased scrutiny. This year, Wipro asked its survey respondents whether they experienced significant data disclosure or breach. As shown in **Figure 4**, 39% of respondents indicated that they dealt with a breach at some level during the past three years. During last year, the top three verticals experiencing breaches were energy, natural resources, and utilities (38%), manufacturing (33%), and healthcare (29%).

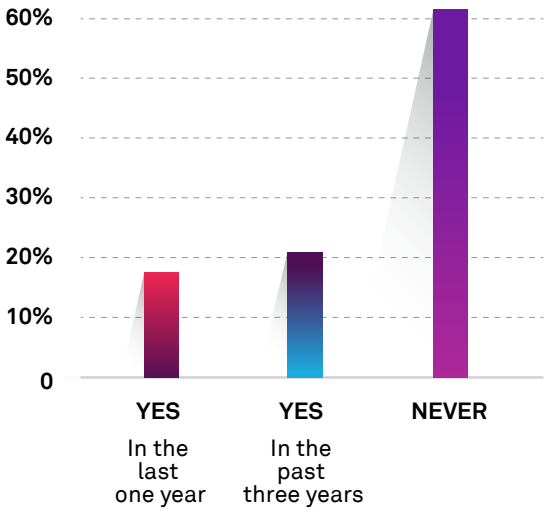


FIGURE 4
[Data breaches experienced by organizations]

What data do attackers seek?

Analysis of the top 40 publicly reported data breaches of 2019 classified the breached data sets into seven broad categories (**see Figure 5**):

- **Basic PII** (name, contact number, email address, physical address)
- **Basic PII + user credentials** (encrypted/unencrypted credentials)
- **Basic PII + user credentials + IP address**
- **Advanced PII** (Basic PII, gender, date of birth, identification numbers, driving license numbers)
- **Advanced PII + user credentials**
- **Advanced PII + user credentials + IP Address**
- **Advanced PII + financials** (tax information, payment card information, bank account statements)

39%

GLOBAL INSIGHT

of organizations surveyed have experienced a data breach in the last three years.

57%

VERTICAL INSIGHT

of healthcare organizations have experienced a data breach in the past three years.

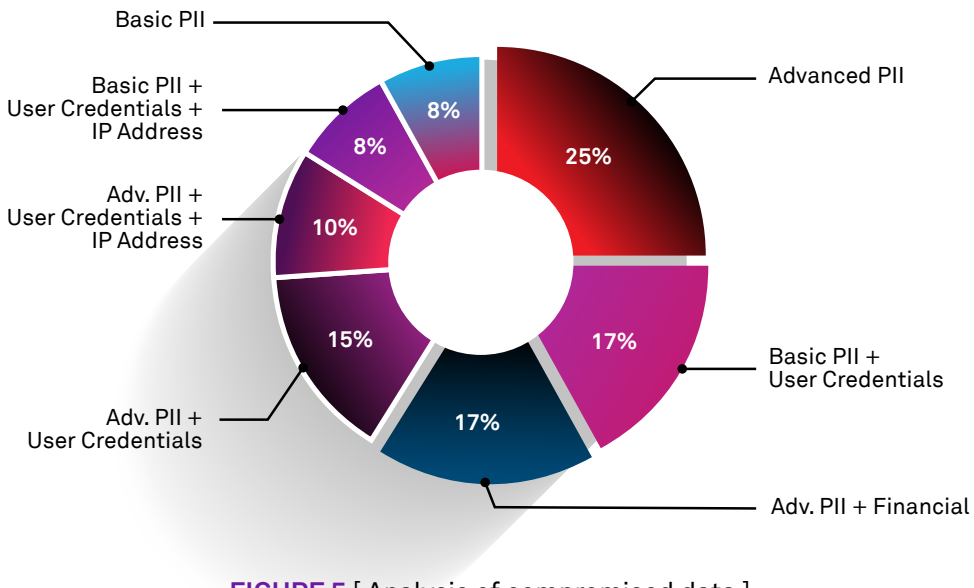


FIGURE 5 [Analysis of compromised data]

- 67% of all data breaches included advanced personally identifiable information (PII)
- Breaches involving only PII and user credential losses saw a year-over-year decrease of 20%
- Breaches involving advanced PII and IP addresses totaled 18%
- Breaches involving advanced PII and financial records saw a year-over-year increase of 4%

Across breaches, attackers seem motivated to harvest data for payment frauds, phishing attacks, and, in some cases, extortion. A large chunk of information is made available to be sold on dark web platforms. Attackers are continuing to focus on PII with user credentials as the latter tends to be reused across platforms for "credential stuffing" attacks. (More details on this can be found in the next section.)

The volume of breaches involving advanced PII indicates that attackers are gaining better intelligence on their targets and the increasing value of the data on the black market. The next section explores trends in threat intelligence available across industry segments from a defender standpoint.

Global Threat Intelligence Insights

This section explores threat intelligence trends globally across industry verticals targeted by different types of cyberattacks. Wipro's collaboration with its Ventures partner, IntSights—a top-tier cyber intelligence organization—led to some interesting findings in threat intelligence alert trends. IntSights threat researchers leveraged their dark/deep web analysis platform to analyze more than 1.1 million alerts to derive industry-wide threat intelligence trends. **Figure 6** shows the spread of cyber intelligence alert types across various industry verticals.

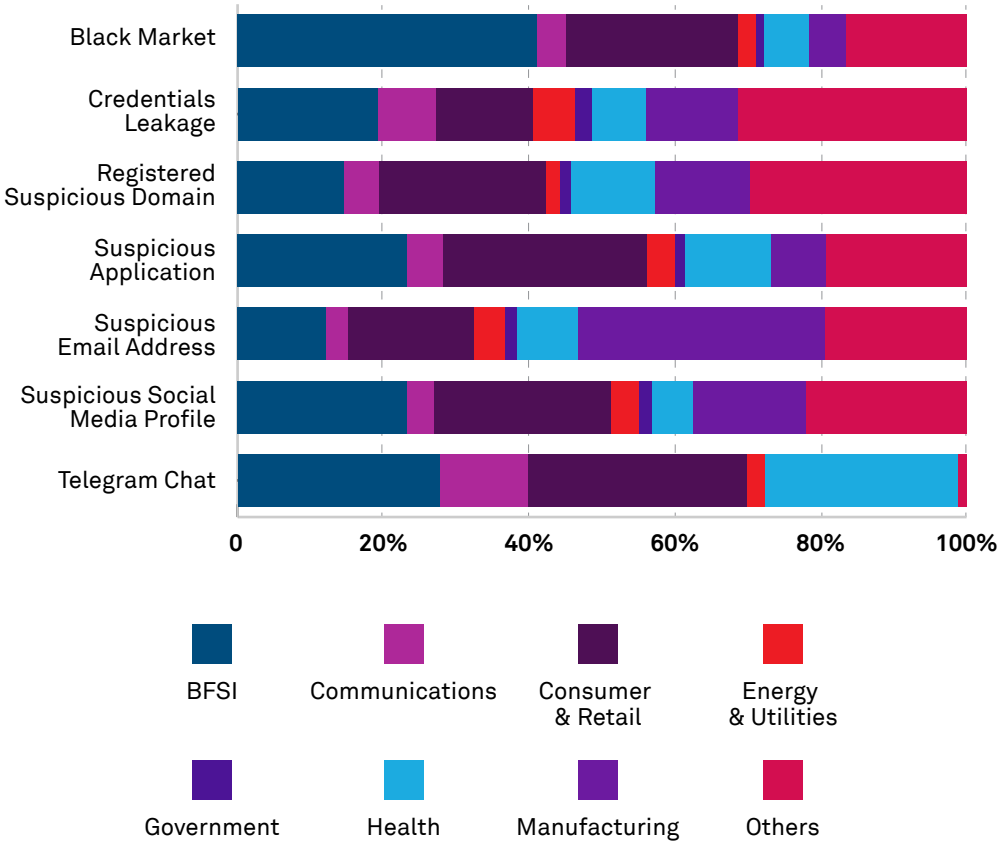


FIGURE 6 [Distribution of threat Intelligence alert types by Industry]

How targeted is your sector?

The nature of cyberattacks will differ from sector to sector, and the impact they cause can be differentially detrimental. The banking, financial services, and insurance (BFSI) sector has always been a prime target for social engineering attacks. The financial rewards and volume of PCI and insurance data available make the industry a tempting target for threat actors. IntSights indicates that about 41% of the information sold on the black market comes from the BFSI sector. Commonly compromised assets sold by threat actors on the black market include credentials, PII, server accesses, and databases.

In the world of manufacturing, customer trust relies on the brand, the value it provides, and the intellectual property the company owns. Any damage to the brand's reputation causes monetary losses and a loss of trust. Phishing attacks to acquire intellectual property and extract competitive pricing and sourcing information are very common. 34% of threats from suspicious email addresses target the manufacturing sector.

The consumer industry sector relies heavily on brand awareness to connect with its customers over digital platforms that host the widespread brand-related social media assets. The consumer goods and retail sector is the most sought after by attackers. 47% of suspicious social media profiles and domains detected over the last year were active within this sector.

Telegram chatter across "communities of interest" can indicate evolving threat patterns across other industry sectors. 27% of telegram chats focused on the healthcare and life sciences sector, and 12% discussed the communications sector.

Leaked credentials are a common way that threat actors access networks and systems. Leaked credentials are bought and sold on underground forums, but are freely available in paste sites and databases (like Collection 1-5, which surfaced early 2019). Some credentials in these databases are outdated, but, unfortunately, a certain percentage of users still reuse passwords on multiple sites and services, and many passwords are easy to guess using common brute force techniques.

In 2020, credential stuffing attacks gained in popularity and sophistication due to the COVID-19 situation, which increased the use of collaboration tools, such as Webex and Zoom.

In this section, we analyzed trends in threat intelligence available globally. However, to materialize these threats, malicious actors continuously evolve the tools of their trade. The next sections examine trends in cyberweapons leveraged by threat actors.

47%

GLOBAL INSIGHT

of suspicious social media profiles and domains detected in 2019 were active within the consumer goods and retail sector.

41%

VERTICAL INSIGHT

of information sold on the black market belonged to the BFSI sector.

Contributed by Wipro's Venture partner, IntSights (intsights.com).

Cyberweapons

Every year, new strains of malware emerge that attempt to exploit weaknesses in Enterprise IT defense mechanisms. While threat-hunting teams pool their energies toward identifying new persistent threats that are sometimes undetected by traditional toolsets, most Security Operations Center (SOC) teams need to also deal with the volume of regular threats that slip through the weak links in a layered defense. These cyberweapons cannot be ignored and consume SOC resources already crunched for time. This section presents findings from the analysis of traditional threats Wipro's Cyber Defense Center teams dealt with last year. The study examined ~6500 incidents across geographies. A thorough look at frequently deployed Trojans and worms provided trends across prevalent families.

Targeted ransomware on the rise

Ransomware continues to be an integral part of an attacker's strategy. It managed to shake up a few things at the start of 2019 after going through a relatively silent patch in the later stages of 2018. Since then, 51% of threats fall under the Trojan category (see **Figure 7**), indicating that Trojans continue to be the most favored agent to launch malware attacks. Targeted ransomware attacks increased to 15% from last year. Organizations need to minimize the availability of system/asset landscape data in the public domain and increase efforts to improve cyber hygiene. Worms, a tried and tested technique for attackers, totaled 14% of malware types.

51%

GLOBAL INSIGHT

of malware threats come from Trojans.

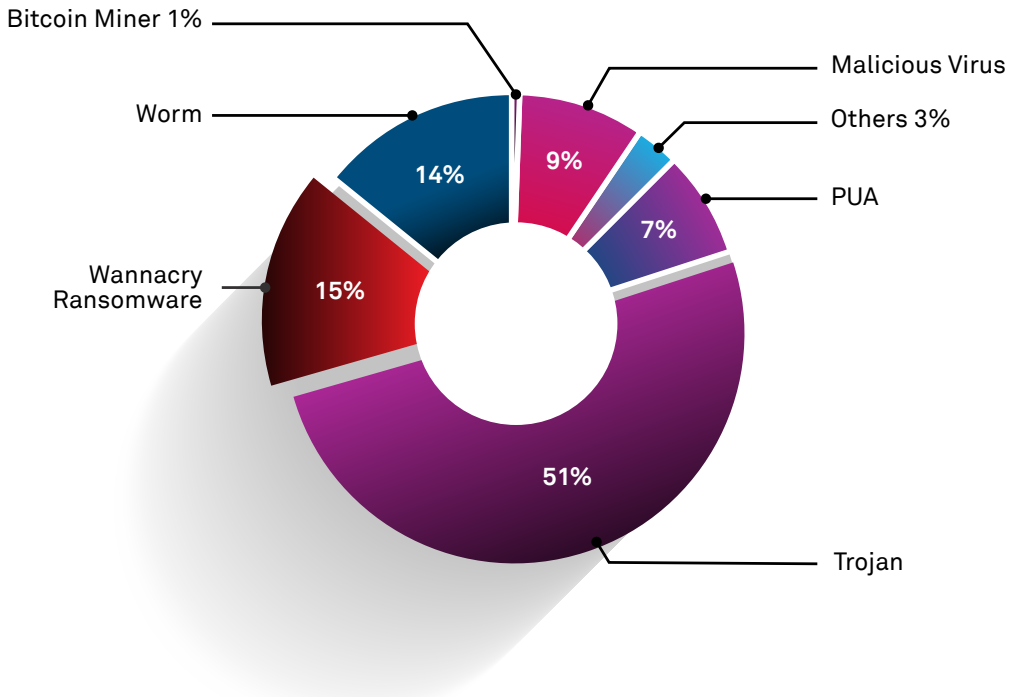


FIGURE 7 [Overall malware distribution, 2019]

FIGURE 7 [Overall malware distribution, 2019]

Figure 8 shows a quarterly distribution of malware types in 2019. An interesting finding is the ransomware spike in the Q1 of 2019, after a decrease in the last few quarters of 2018. Contrary to traditional methods, attackers used the novel technique of targeted campaigns that made ransomware attacks climb the charts.

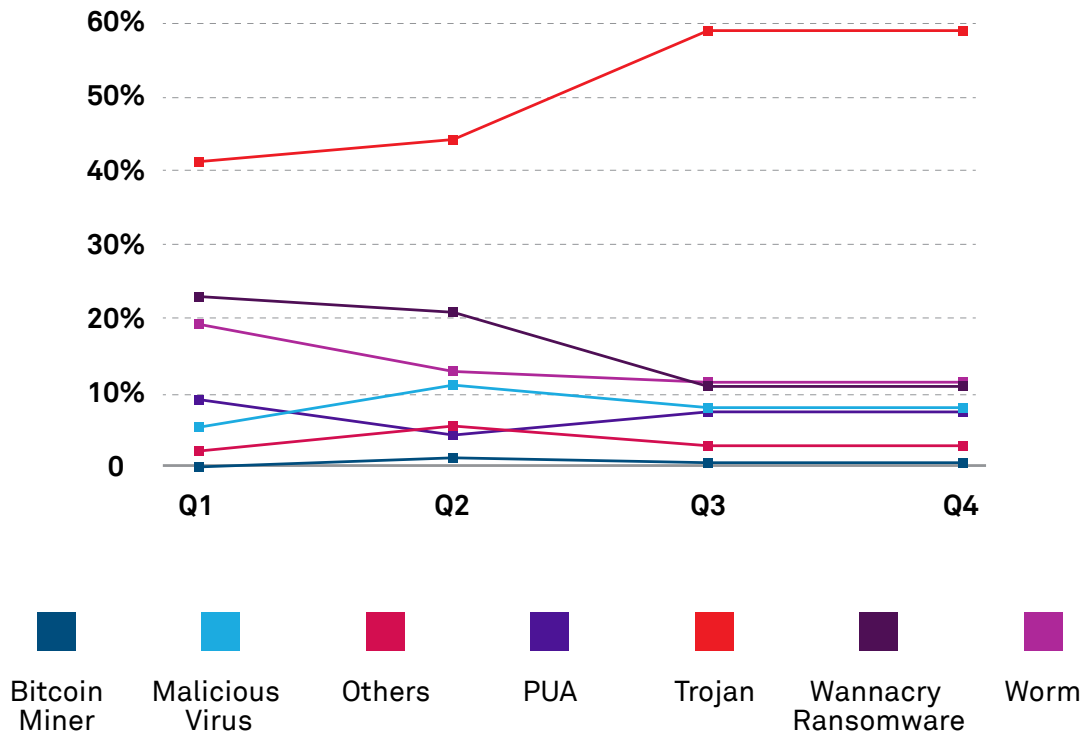


FIGURE 8 [Quarterly distribution by malware type]

Figure 9 shows the frequency of threats across Trojan and worm families in the sample analyzed. Heur.AdvML.C, Trojan.Gen.2, Heur.AdvML.B, W32.SillyFDC, W32.Mysracoin, and W32/HostInf-A dominated attacks. Nearly one-third of worm attacks belonged to W32/HostInf-A.

25%

GLOBAL INSIGHT

The top three Trojan families (Heur.AdvML.C, Trojan.Gen.2, and Heur.AdvML.B) are accountable for 25% of Trojan attacks.

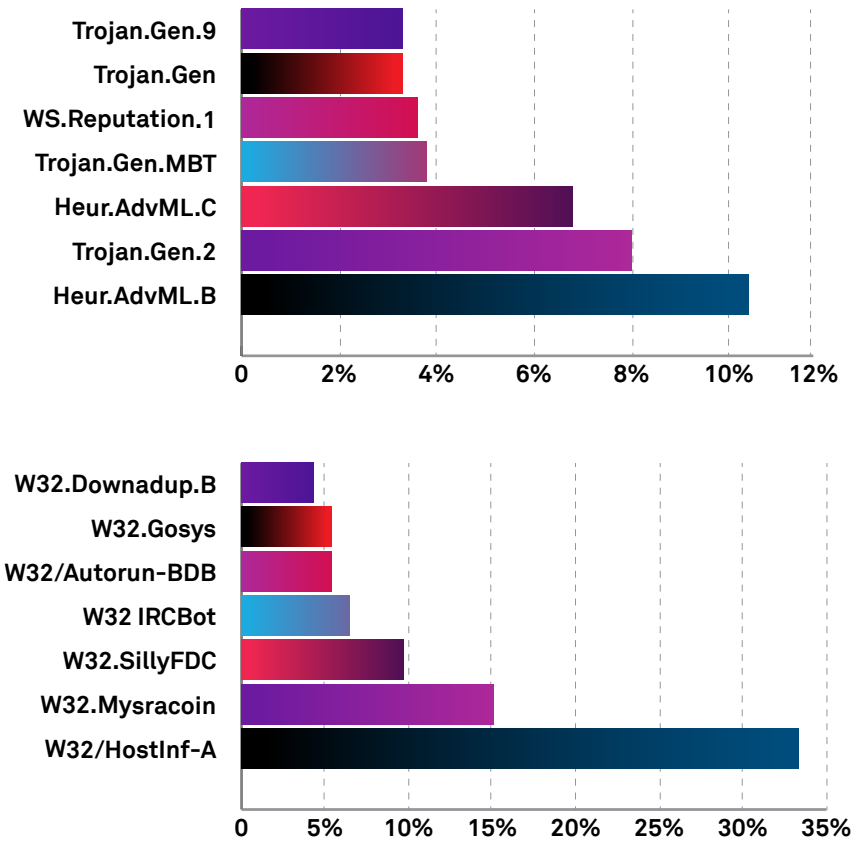


FIGURE 9 [Frequent threats per Trojans (top) and worms (bottom)]

Global Malware Statistics

The previous section focused on malware types encountered during regular operations across four quarters. To tie the analysis to an expanded global view, Wipro collaborated with Check Point Software Technologies Ltd. to further analyze malware patterns across geographies.

Cryptominer attacks have continued to dominate, with 38% of the attacks belonging to this category. This tried and tested technique has lured attackers to use it for financial gains. Also, attackers can easily embed cryptomining capabilities into the compromised machines handled by them, making these attacks a preferred choice.

The considerable increase in botnet attacks from 18% to 28% across geographies is an alarming concern. Bad actors are developing new techniques that impair identifying suspicious activity in hijacked systems and network devices.

Banking Trojans, a regular perpetrator over the years, continued to show steady growth in 2019. Banking Trojans have evolved from advanced plugins and distribution vectors, enabling them to carry out multiple tasks.

Figure 10 shows the distribution of dominant malware types in 2019.* An interesting finding is a spike in ransomware.

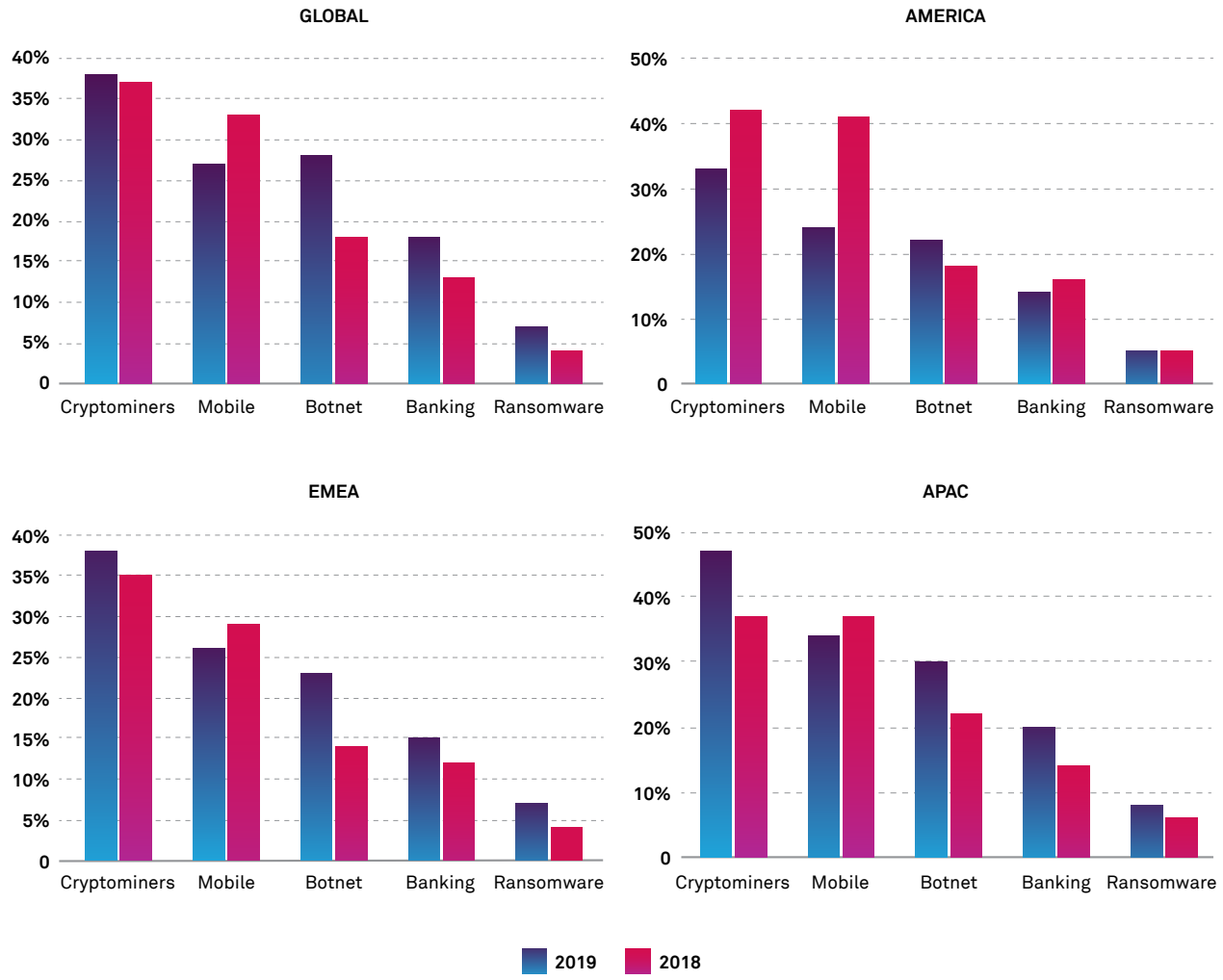


FIGURE 10 [Global malware patterns]

GLOBAL INSIGHT

18% » 28%

Botnet attacks increased from 18% to 28% last year.

REGIONAL INSIGHT

37% » 47%

Cryptominer attacks in the APAC region increased from 37% to 47% last year.

Wipro's partner, Checkpoint (checkpoint.com), contributed to this section.

* The sum of all attack categories exceeds 100% because certain attacks were attributed to multiple attack types.

Ransomware tactics have changed significantly during the last year. They are becoming more targeted on specific organizations and, upon successful encryption of vital infrastructure, are usually followed by significant ransom demands. State governments in some countries have declared emergencies while dealing with such attacks. Threat actors trying to make their entry into target environments through trusted service providers or supply chain dependencies bring supply chain risk management to the frontline of cybersecurity governance.

Another phenomenon observed during the year is the rise of Magecart attacks on e-commerce sites to steal credit card information. Unsecured cloud environments are stepping stones to attacks on large enterprises.

Distribution of Exploits

An analysis of cyber events by Wipro's CDC exposed the different types of exploits used by attackers in the previous year (**Figure 11**). Samba exploits increased from 5% in 2018 to 33% in 2019. Cross-site scripting jumped from 9% to 16% this year. Remote Code Execution and SQL Injection continue to remain among the top exploits.

33%

GLOBAL INSIGHT

of the exploits in 2019 were Samba exploits.

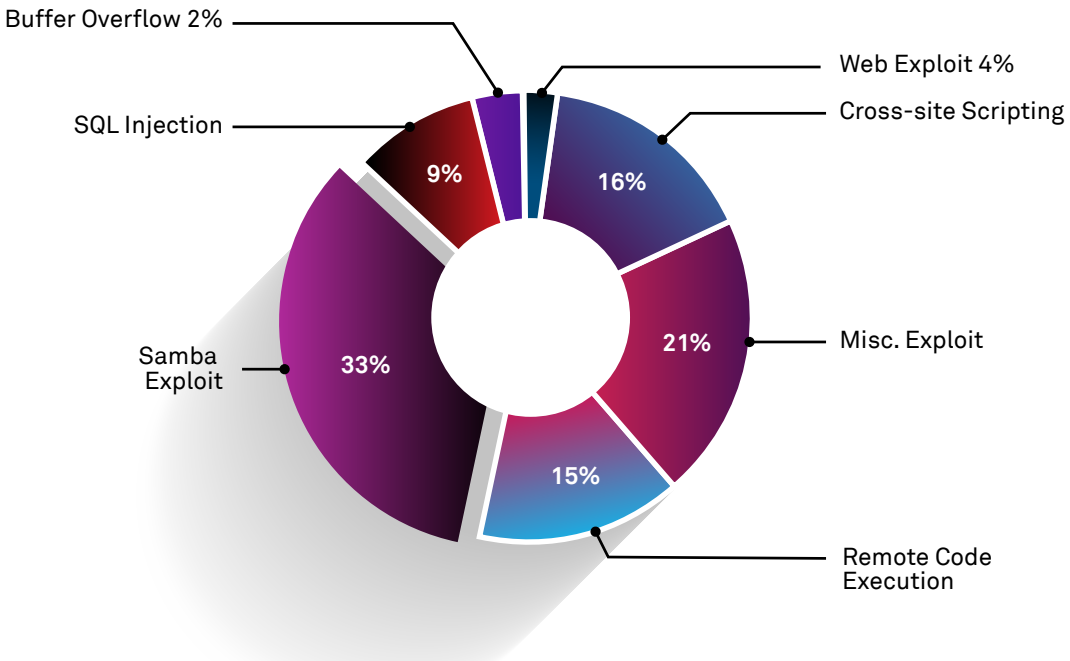


FIGURE 11 [Distribution of exploits]

Vulnerabilities in Cyber Defenders

Highlighting vulnerability trends in cyber defenders is a unique type of research in the SOCR. Conventional vulnerability management programs direct an organization toward detecting and mitigating weaknesses in the IT operating systems or applications. Lack of awareness of vulnerabilities in cyber defense systems can lead organizations into a false sense of security, which has been a long time struggle for security teams. Year on year detailed analysis of vulnerabilities reported against classes of security products revealed a consistently thorny problem. Can weaknesses in your security defenders tilt the balance further in favor of threat actors?

Vulnerability trend analysis

The research has been carried out based on the annual vulnerability scores available on the Common Vulnerabilities and Exposures (CVE®) website (cve.mitre.org). Security product vulnerabilities cover a wide range of product domains, such as Identity & Access Management (IAM), SAST/DAST, Firewall, Antivirus, VPN, Data Loss Prevention (DLP), and VPN. Across these product domains, vulnerabilities were analyzed in 13 categories:

- DoS
- Code execution
- Overflow
- Memory corruption
- SQL injection
- XSS
- Directory traversal
- HTTP response splitting
- Gain information
- Bypass something
- Gain privileges
- CSRF
- File inclusion

Figure 12 shows trends in the 13 vulnerability categories over the last four years. Last year, most categories declined in the number of reported vulnerabilities. Code Execution had the highest number of reported vulnerabilities, and Bypass Authorization witnessed the second-highest rise.

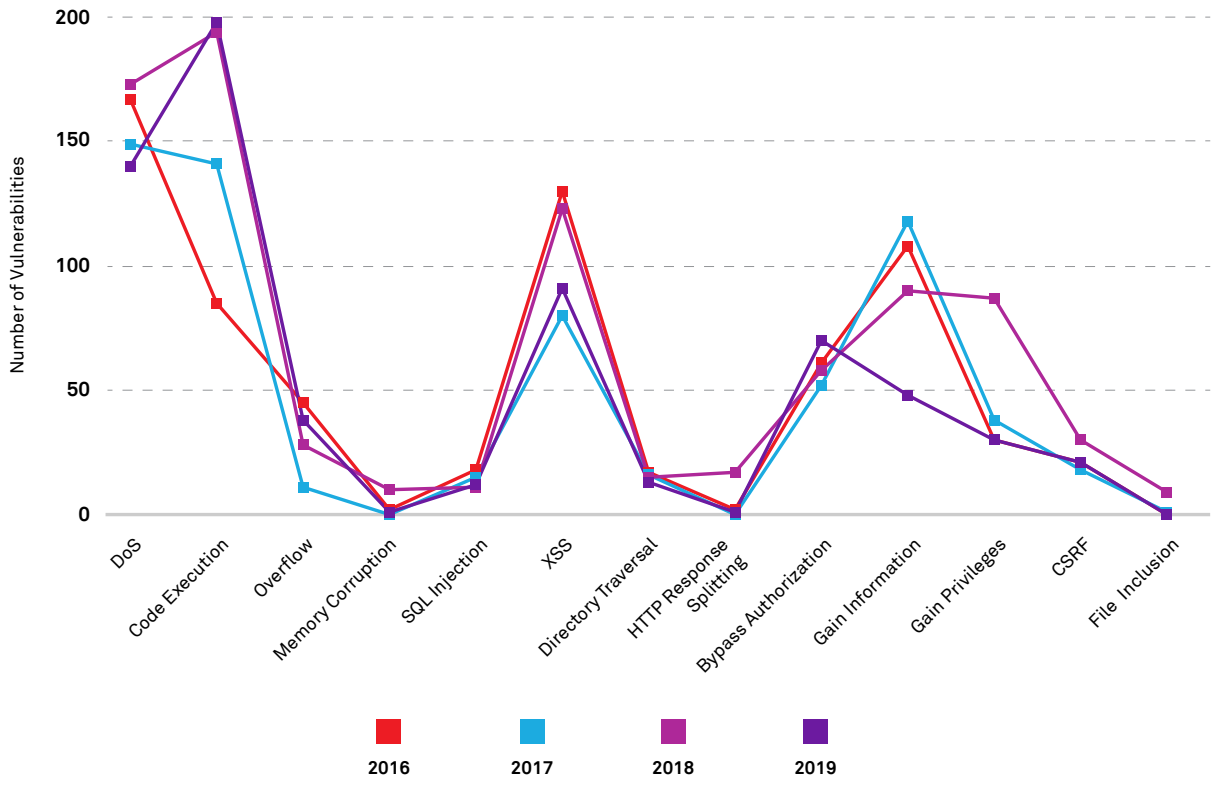


FIGURE 12 [Vulnerability categories in security products]

Vulnerabilities in security products

We analyzed common vulnerability categories across 30+ security products. Further, a weighted average vulnerability score was arrived upon for each product. The scores of similar products were then aggregated using a weighted average method to arrive at the final product category scores shown in **Figure 13**. Products with a high score indicate a higher propensity for vulnerabilities. Database Activity Monitoring topped the charts with a score of 7.08, which is significantly more than last year's score of 5.43. IDAM products also increased in score from 3.58 to 5.48. DLP and SIEM scores improved this year.

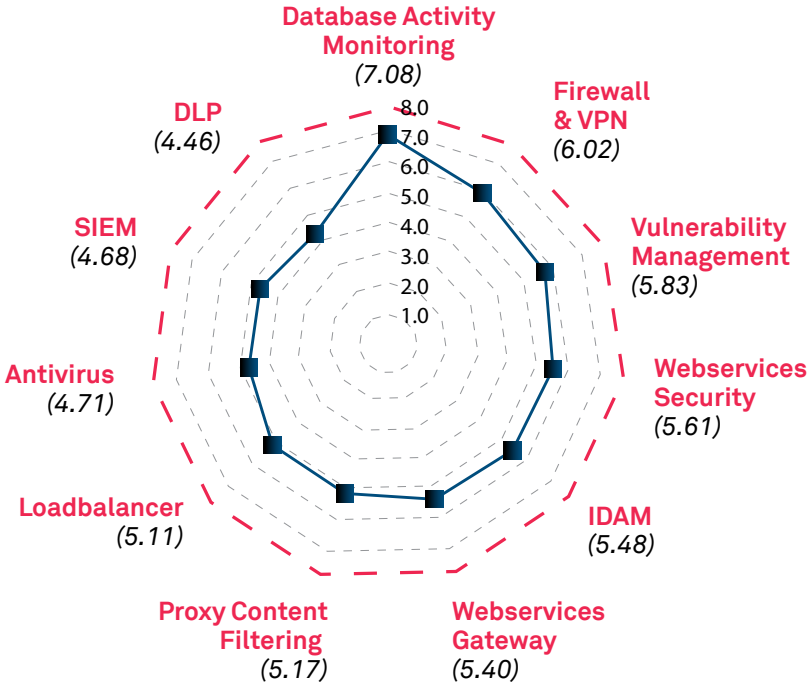


FIGURE 13 [Security product domain vulnerability scores, 2019]

GLOBAL INSIGHT

Database activity monitoring and IDAM product categories showed a higher propensity for attacks in 2019, while DLP and SIEM decreased considerably, implying a lower tendency for attacks.

Open-source security vulnerabilities

This year, in collaboration with our partner WhiteSource, we expanded the research scope of this report to include vulnerability trends in open-source ecosystems. The research analyzed data from multiple sources, including security advisory databases, the National Vulnerability Database, peer-reviewed vulnerability databases, and credible open-source-issue trackers.

This section focuses on security vulnerabilities in open-source libraries. The research scope covered lakhs of open-source projects. The number of reported open-source vulnerabilities has been rising significantly over the past few years, reaching ~6100 in 2019, as shown in **Figure 14**).

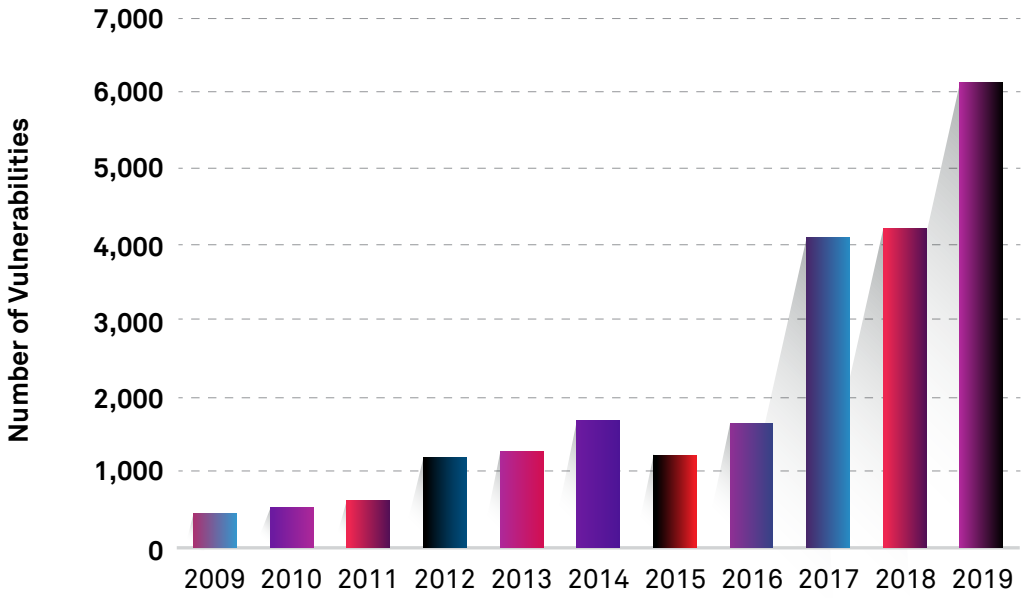


FIGURE 14 [Open-source security vulnerabilities]

This rise of nearly 50% compared to the previous two years is due to several developments in the open-source security ecosystem. The widespread use of open-source components, the growth of the open-source community, and numerous highly publicized data breaches have led to increased awareness of open-source security. All these factors have driven the open-source community, the security community, and the software development industry to invest more time and effort into the detection and remediation of security vulnerabilities within open-source components.

46%

GLOBAL INSIGHT

The number of reported open-source security vulnerabilities increased by 46% in the last year.

Common weakness enumeration in reported open-source vulnerabilities

The most common CWEs in 2019 are CWE-79 (cross-site scripting), CWE-20 (improper input validation), CWE-119 (buffer errors), CWE-125 (out-of-bounds read), and CWE-200 (information exposure), as shown in **Figure 15.**

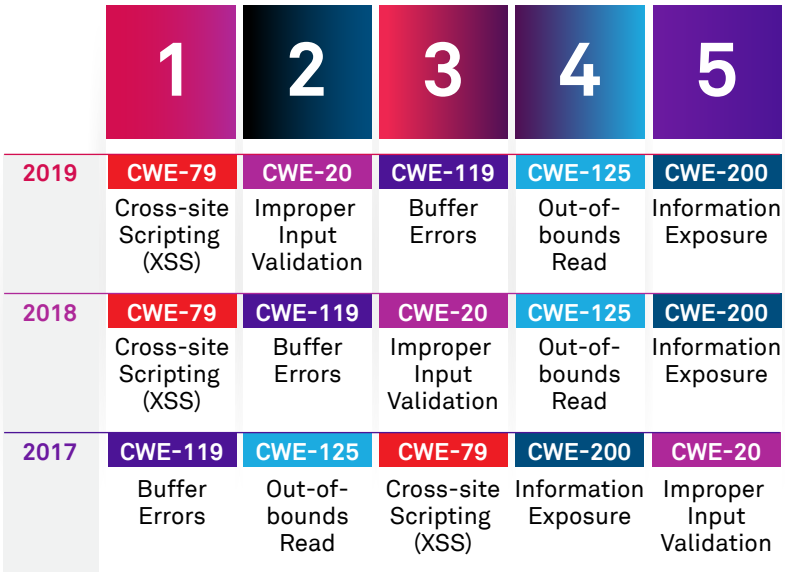


FIGURE 15 [Common weakness enumerations in reported open-source vulnerabilities]

Reasons for the high number of cross-site scripting (XSS) issues include the increased use of automated tools for their detection and the security community's focus on web application security where XSS issues are found. The prevalence of CWE-200 and CWE-20 is partly because they are both very general. As opposed to XSS, CWE-200 covers many consequences of a vast scenario.

The same is true for CWE-20, where input validation refers to a range of necessary security actions. Developers often forget to address all of them, resulting in improper input validation issues. Additionally, CWE-20 can mean anything from XSS to SQL injection to several other problems. A majority of CWEs are an outcome of coding errors, which can be avoided by adhering to basic coding standards and best practices.

Wipro's partner, WhiteSource (whitesourcesoftware.com), contributed to this section.

Cybersecurity Regulations

Laws and regulations play a pivotal role in the cybersecurity environment, helping shape rights, obligations, and behaviors. Thus, regulatory changes can have a macro-level impact across jurisdictions. Legal directives across the cybersecurity landscape are changing around the globe. The insights below are the output of detailed analysis and research by Wipro's SOCR team on breach notifications and cross-border, data-transfer laws in 23 countries: Australia, Brazil, Canada, China, Dubai, Finland, France, Germany, India, Ireland, Italy, Japan, Mexico, Norway, Poland, Russia Singapore, South Africa, Spain, Sweden, Switzerland, UK, and the US. Parameters used to evaluate the data appear in **Table 1**.

FOCUS AREAS OF ANALYSIS	PARAMETERS
Data breach notification requirements	• Mandatory notification to authorities • Breach categorization • Mandatory notification to affected parties • Financial penalty if notifications are not made
International data transfer restrictions	• Consent of data subjects • Whether outside jurisdiction provides adequate protection • Binding corporate rules (BSRs) • Standard contractual clauses (SCCs) • Permission of data protection authority

TABLE 1 [Analyzed breach and data-transfer parameters]

A score was assigned to each parameter based on a subjective analysis of each country's regulation stringency. A weighted average method blended parameter scores and arrived at a country-specific score for data breach notifications and restrictions on international transfers. A higher score implies a greater seriousness toward breach notifications and international data transfer laws. 13 out of 23 countries (57%) demonstrated stringency in the breach notification laws across the four parameters assessed. Ten countries demonstrated stringency related restrictions on international data transfers across five parameters assessed. **Figure 16** and **Figure 17** summarize the analysis.

REGIONAL INSIGHT

Japan, China, Singapore, Russia, Switzerland, Brazil, and Dubai amended their data protection regulations and international data transfer laws.

GLOBAL INSIGHT

More countries are adopting methods of imposing huge fines for non-compliance to data protection laws.

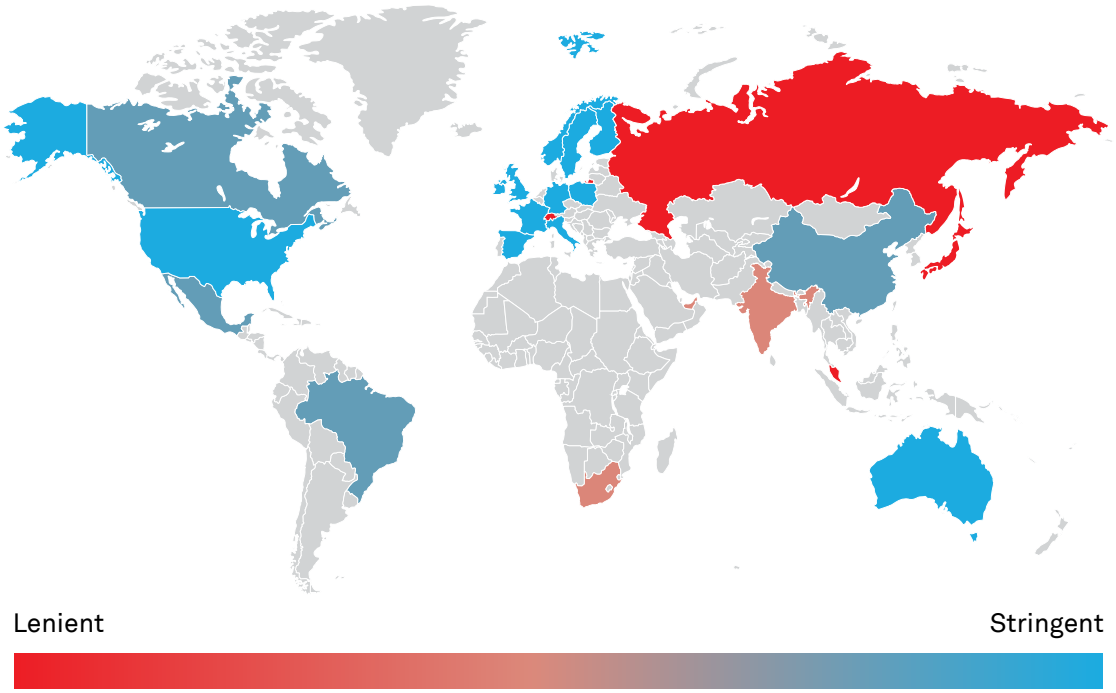


FIGURE 16 [Heat map of country-specific regulations relating to breach notifications, 2019]

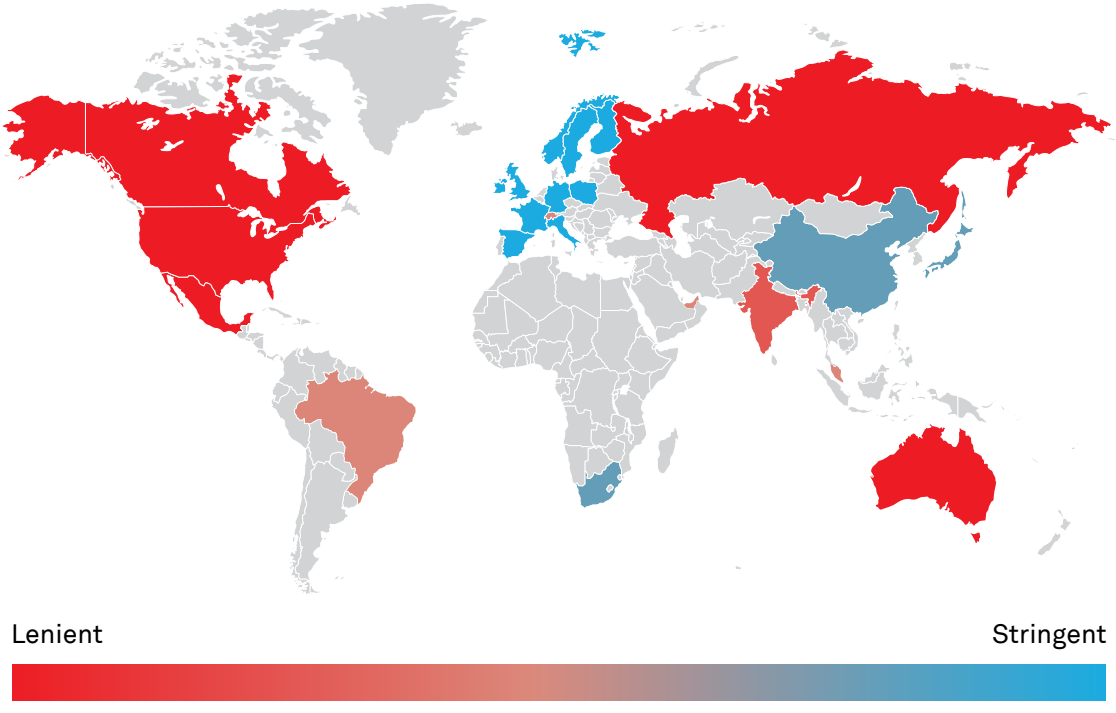


FIGURE 17 [Heat map of country-specific regulations relating to international data transfers, 2019]

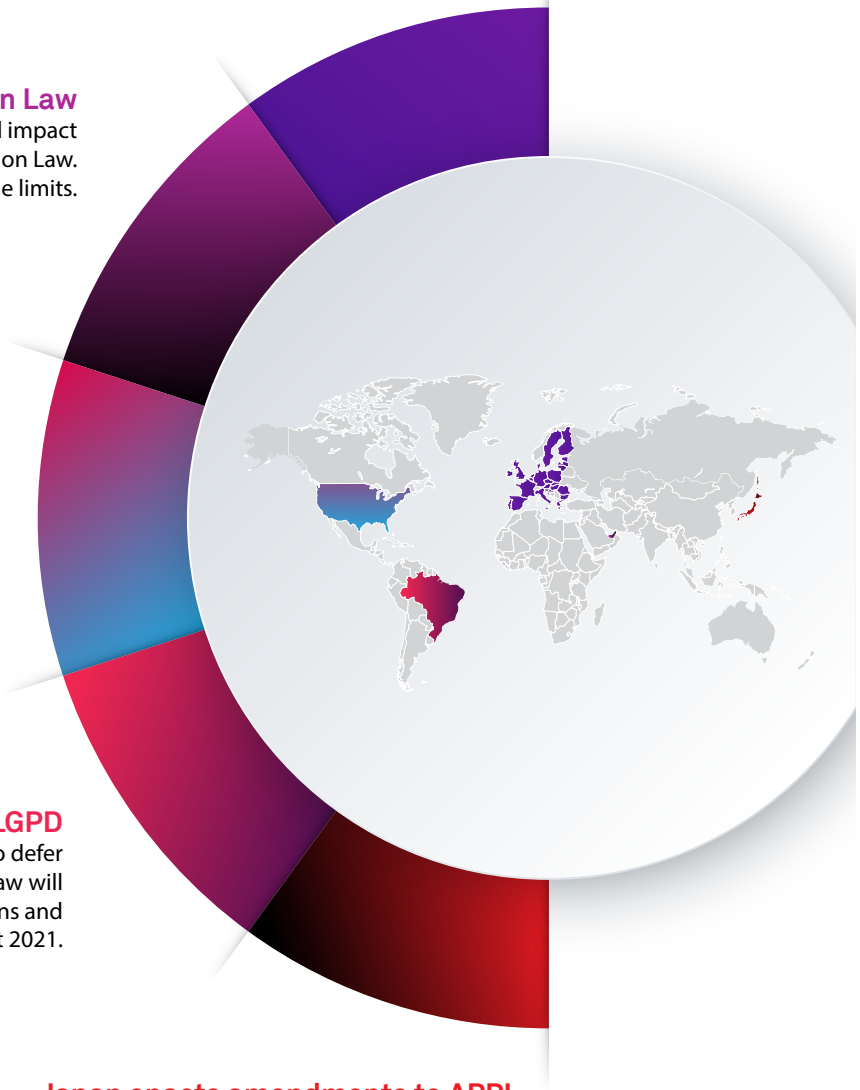
Countries across the globe are responding to citizen concerns, consumer demands, globalized trade imperatives, and geopolitics to strengthen their privacy and data security legal regimes every year. These changes could be incremental updates to existing legislation or completely new regulation necessitated due to various drivers. While presenting each of these changes is beyond this report's scope, a few updates that stood out amongst the 23 countries are captured below.

EU-UK Withdrawal Treaty

After the UK's exit from the EU on 31 January 2020, the EU-UK Withdrawal Treaty provides a transition period until the end of 2020. During this time, current GDPR laws and the UK Data Protection Act are in effect. After the transition period, EU law will no longer be applicable in the UK, unless any future agreement or evaluation under "adequacy decision" or "privacy shield" is agreed upon.

Dubai enacts new DIFC Data Protection Law

Appointment of DPOs, new compliance programs, and impact assessments are prominent highlights of DIFC Data Protection Law. Effective July 2020, the law increased maximum fine limits.



EU-US Privacy Shield struck down

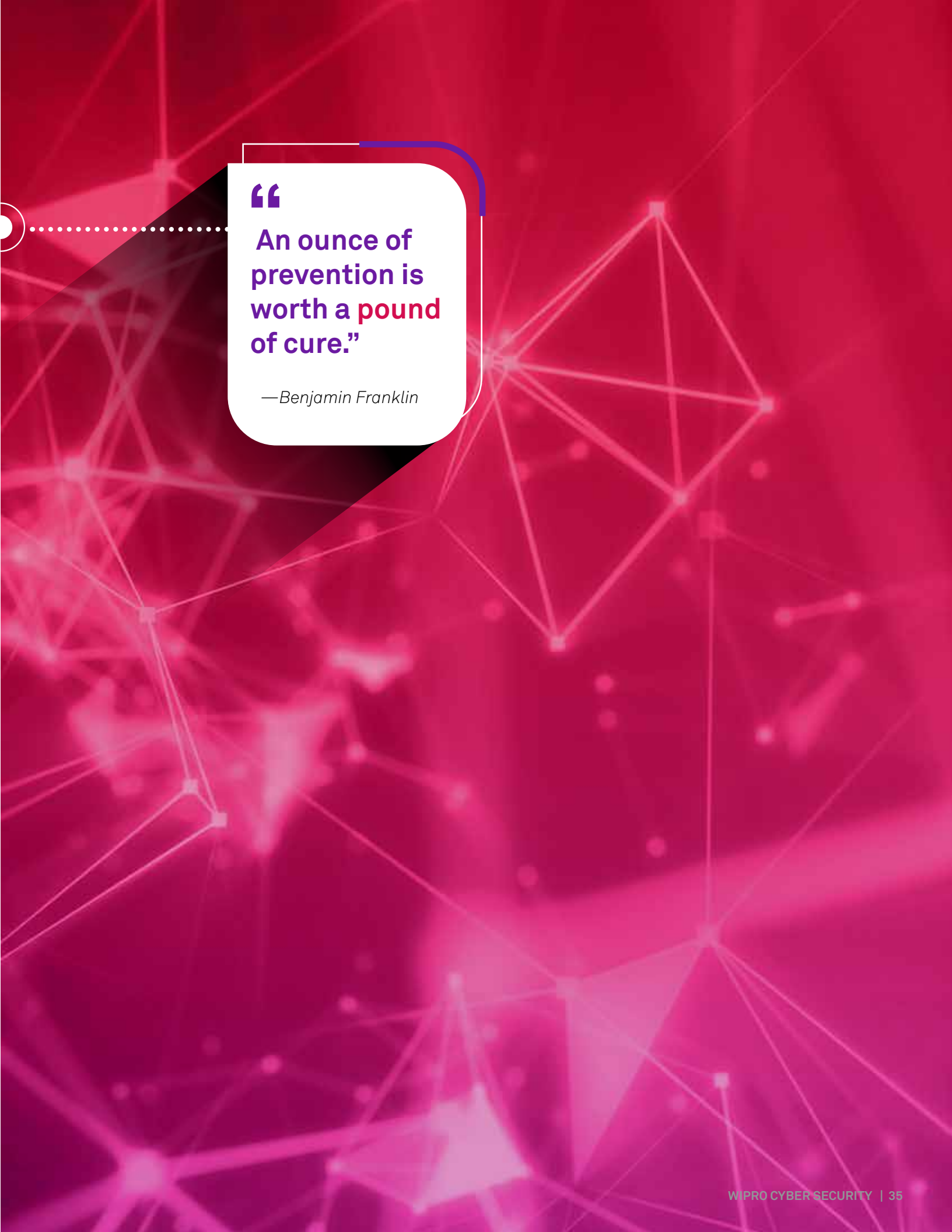
The European Court of Justice struck down the EU-US Privacy Shield, an agreement governing the transfer of personal data from the EU to the US. Standard contractual clauses (SCC) continue to be valid mechanisms to ensure data privacy laws' adequacy.

Brazil postpones LGPD

The COVID-19 pandemic forces the Brazilian Senate to defer the Brazilian General Data Protection Law (LGPD). The law will take effect in January 2021, while administrative sanctions and penalties will be applicable after August 2021.

Japan enacts amendments to APPI

Amendments to APPI were adopted on 5 June 2020, and the law will take effect in Q4 2021 or Q1 2022. Changes allow individuals to electronically retain their personal data and establish mandatory notifications of data breach incidents to PPC and affected parties. The bill introduced the use of pseudonymized information, with certain constraints. Also, fines for violating the order increased substantially.


“
An ounce of prevention is worth a pound of cure.”
—Benjamin Franklin

2

COVID-19 A CYBERSECURITY PERSPECTIVE

The COVID-19 pandemic disrupted the status quo to differing levels across many aspects of human existence in all parts of the world. Lockdowns resulted in remote work—a new normal across industry segments. Supply chain disruptions and less demand in sectors like oil, tourism, and automobile manufacturing devastated economies and led to uncertain futures.

While nations grappled with the pandemic, cybersecurity ecosystems also scrambled to manage new realities. The opportunities for profiting from espionage, IP theft, ransom, and other criminal actions increased while the world focused elsewhere.

New Realities for Enterprises

Keeping employees safe, securing business continuity with suppliers, maintaining relationships and fair prices with consumers, offering support for local governance, providing long-term viability to shareholders, and numerous other considerations required businesses to pivot as quickly as possible. In addition to these concerns, many technology-related challenges, as shown in **Figure 18**, rose to the fore.

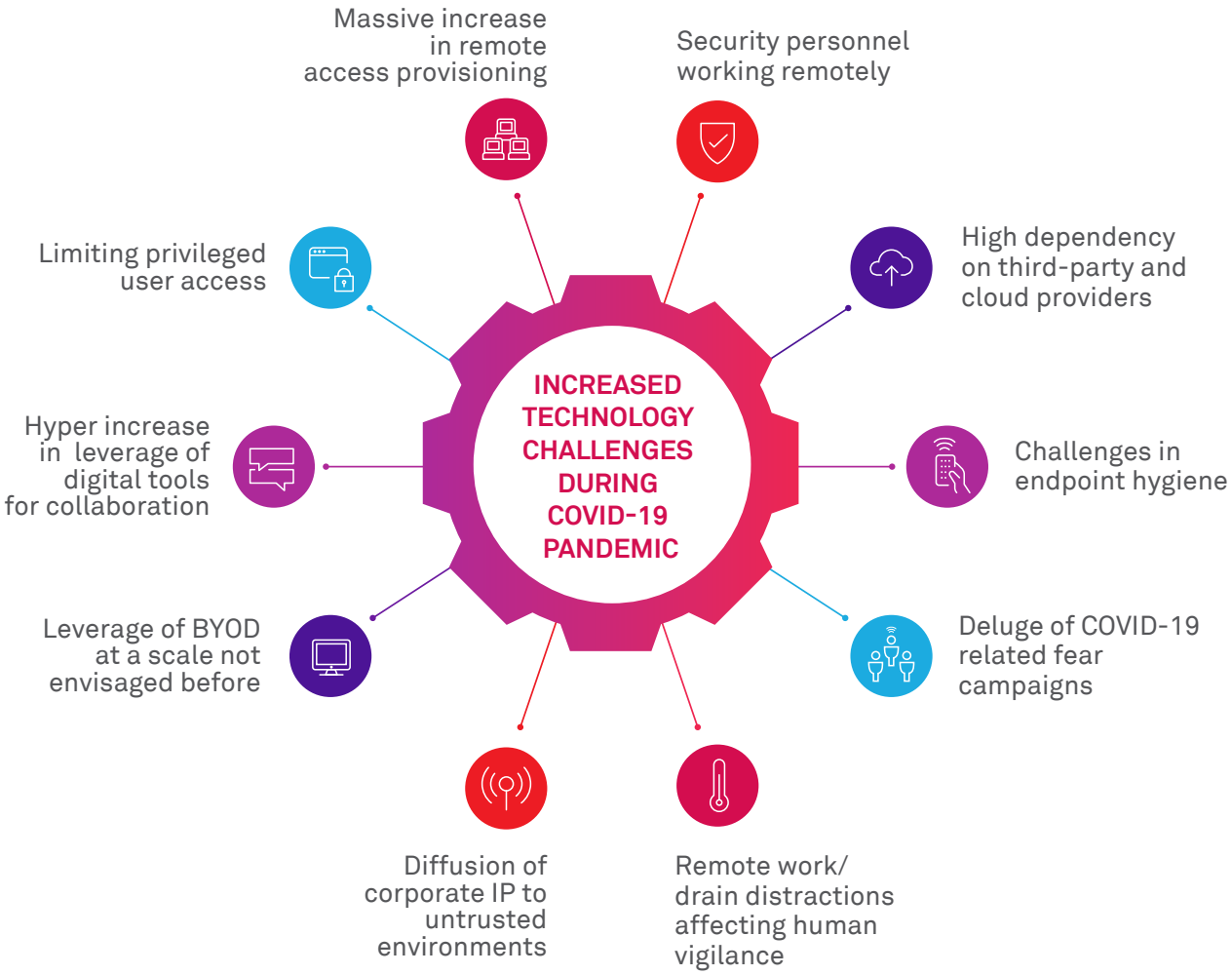


FIGURE 18 [Increased technology challenges during COVID-19 pandemic]

These circumstances heightened existing cybersecurity threats and created new ones. **Figure 19** represents cyber threats positioned by their impact and likelihood of occurrence based on historical learnings and emerging intelligence alerts.

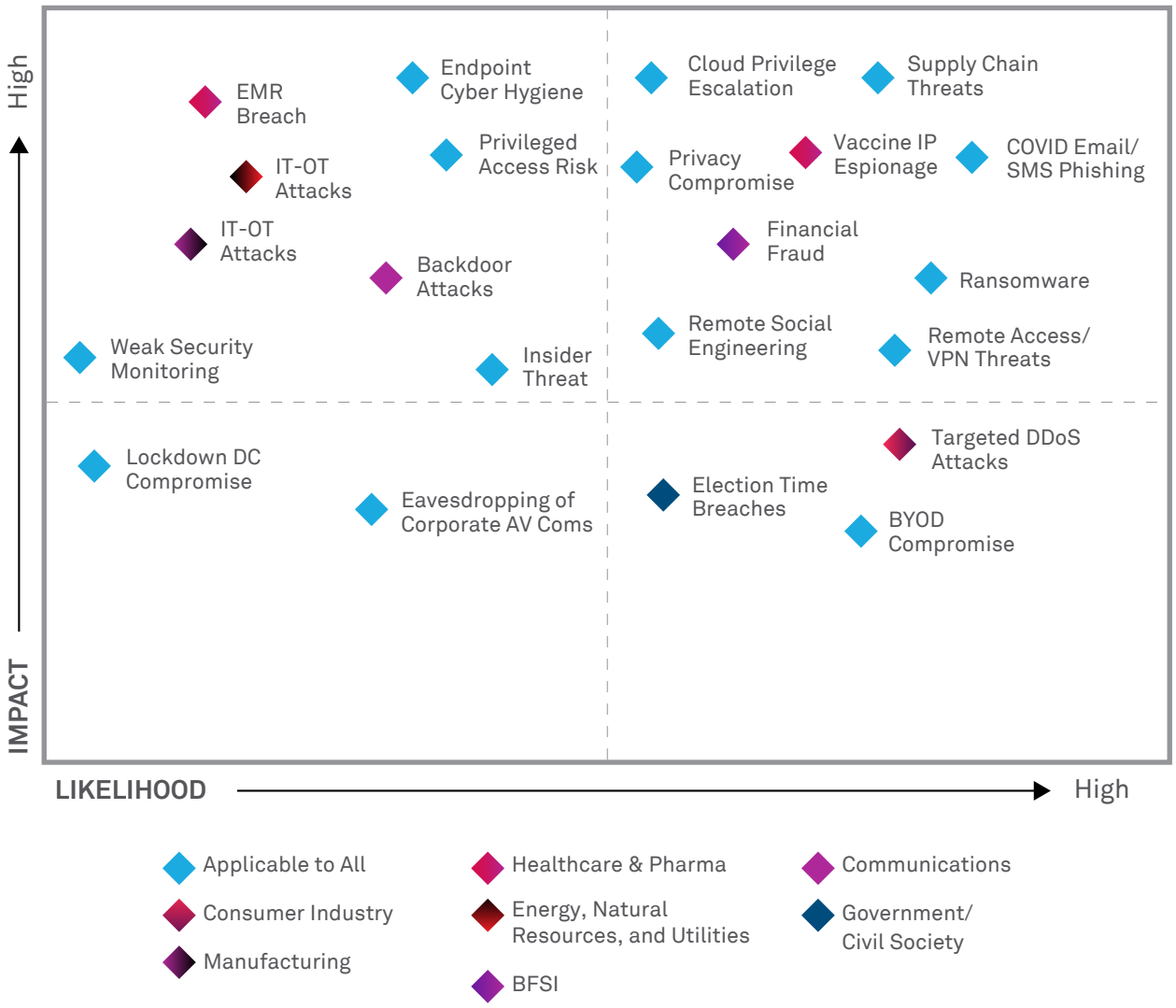


FIGURE 19 [Cyber threats across industry sectors during COVID-19 pandemic]

A significant portion of these threats apply to most industry sectors; for example, COVID-19-related phishing campaigns increased during the first two quarters of 2020 and continue to pose significant threats. An elaborate discussion on this trend and the challenges around human-centric security appears in the upcoming **Securing the People Perimeter to Move Left of Breach** section. Additionally, ransomware, supply chain threats, cloud-centric attacks, and remote-access threats continued to affect all sectors in differing proportions. During the first quarter of the year, targeted DDoS activity increased globally. The **DDoS Attacks: Shrinking in Size, Increasing in Impact** section sheds light on the distribution of DDoS attacks and their bitrates.

Some threats, however, manifested within specific sectors. For example, we saw campaigns targeted at the pharmaceutical sector, presumably for insights on vaccine development. Increased evidence of state-sponsored attacks on operational technology (OT) environments appeared in the manufacturing and energy, natural resources & utility sectors. The healthcare sector is becoming susceptible to EMR-related breaches and crippling ransomware attacks.

While the pandemic was escalating, as part of our research, we asked survey respondents which areas of their IT security were facing challenges. **Figure 20** shows that respondents were busy accommodating the new normalcy of remote working.

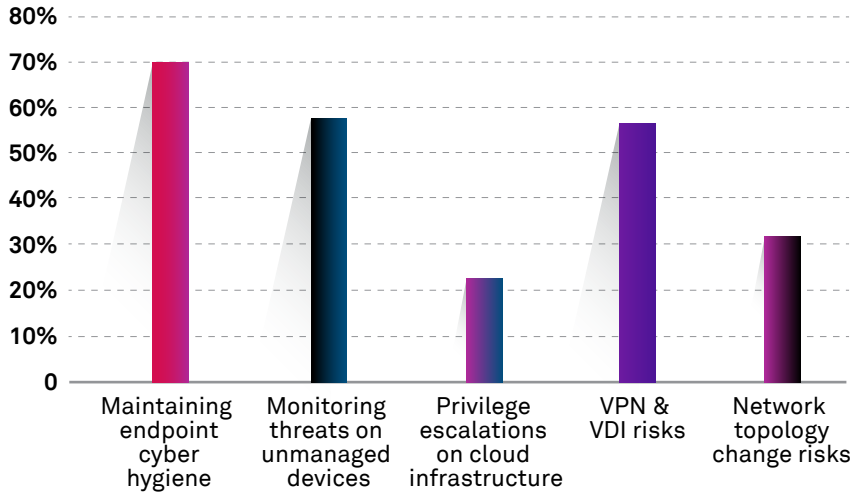


FIGURE 20 [IT Security challenges during COVID-19]

70% of the respondents highlighted challenges around maintaining endpoint cyber hygiene linked to the rapid increase in remote work. 57% of respondents were concerned about mitigating VPN and VDI risks as corporate systems connected to an expanded threat surface of outside networks.

We also asked survey respondents to name their cybersecurity priorities during the pandemic. As shown in **Figure 21**, 94% of respondents included increasing secure VPN/remote access capabilities. Enabling secure collaboration and multifactor authentication were also priorities.

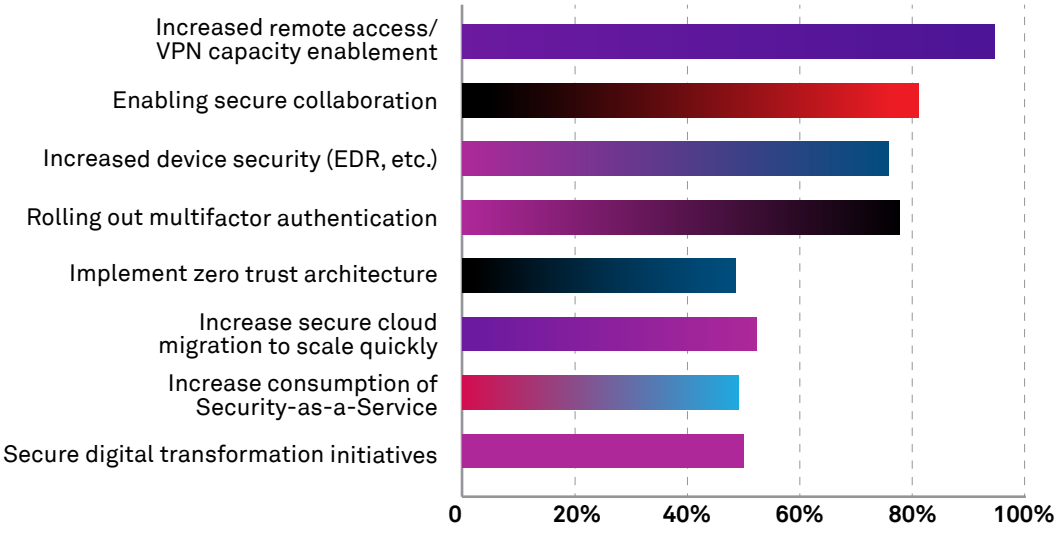


FIGURE 21 [Cybersecurity priorities during COVID-19]

Where Are We Heading Post-COVID-19?

How the world will collectively exit from the COVID-19 pandemic is uncertain at this time. Hence, it is challenging to hold a crystal ball and see how events will pan out in the months ahead.

The roadmap in **Figure 22** provides a potential evolution of the pandemic mapped to business events, cyber threats, and actions required from a cyber-response standpoint.

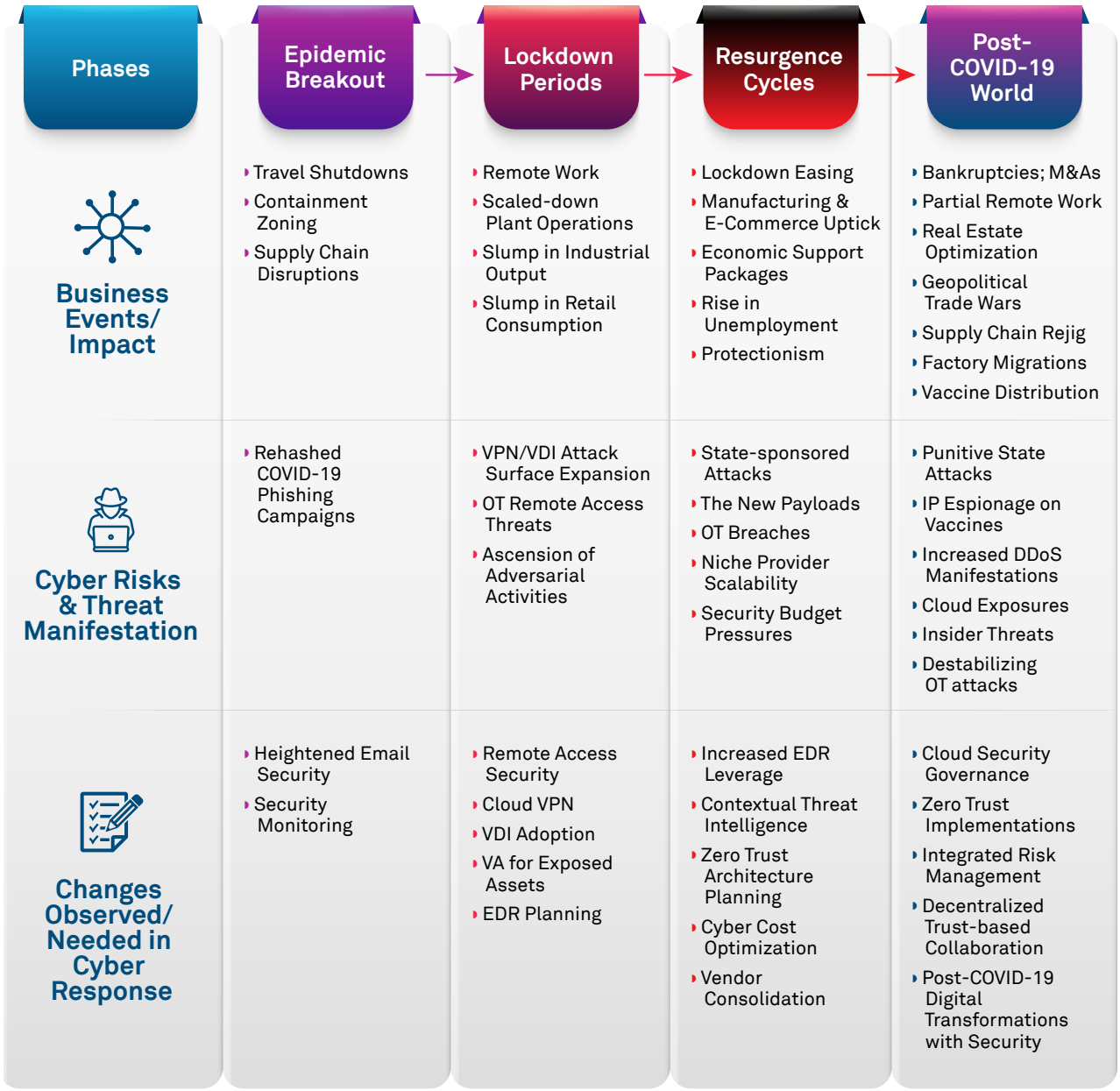


FIGURE 22 [Potential pandemic cycles and cyber responses]

Based on the geopolitical patterns playing out, it is evident that protectionism might rise, leading to global trade wars. Supply chains could potentially undergo restructuring, and manufacturing might see locational realignment. Some of these events might be transient, while others could have lasting effects. The resultant cyber threats could manifest in the form of increased multi-directional nation-state attacks on the government and private sectors, critical infrastructures, and, sometimes, civil society. Threat actors are exploiting the gamut of opportunities arising from the pandemic. Exposures through cloud environments, attacks on OT infrastructure, and DDoS manifestations are expected to increase.

Radical shift in cyber-resilience approach due to COVID-19

The COVID-19 outbreak has woken up organizations to plan for rapid digitization in a short span of time. With legions of employees working remotely, CISOs were overwhelmingly tasked with the dire need to create a secure remote work environment to ensure business continuity. This has instigated a radical shift in the traditional cyber-resilience measures deployed by the organizations, as conventional network monitoring and patching mechanisms might not be able to efficiently address the problems in this new reality. Organizations have increased the pace of adopting a cloud-based approach for patch management, security updates, etc.

Cloud adoption, digital transformation initiatives, and hyper-automation are expected to accelerate in the post-COVID-19 world. Cloud-enabled scalability and automation can address the need for future business resilience during similar disruptive situations. However, rapid migrations of enterprise services to the cloud need a secure foundation. Our survey responses align to this school of thought: 87% of respondents plan to scale up secure cloud migration, 89% plan to increase security-as-a-service consumption, and 94% plan to embrace secure digital transformation initiatives.

Zero trust architecture will play a critical role in managing threats as more and more organizations are unable to secure the data effectively as it flows outside the perimeter. **Figure 23** shows that 87% of the surveyed organizations are keen on implementing zero trust architecture post-COVID-19. The upcoming **State of Cyber Resilience** section lays out the beginning steps of orchestrating zero trust.

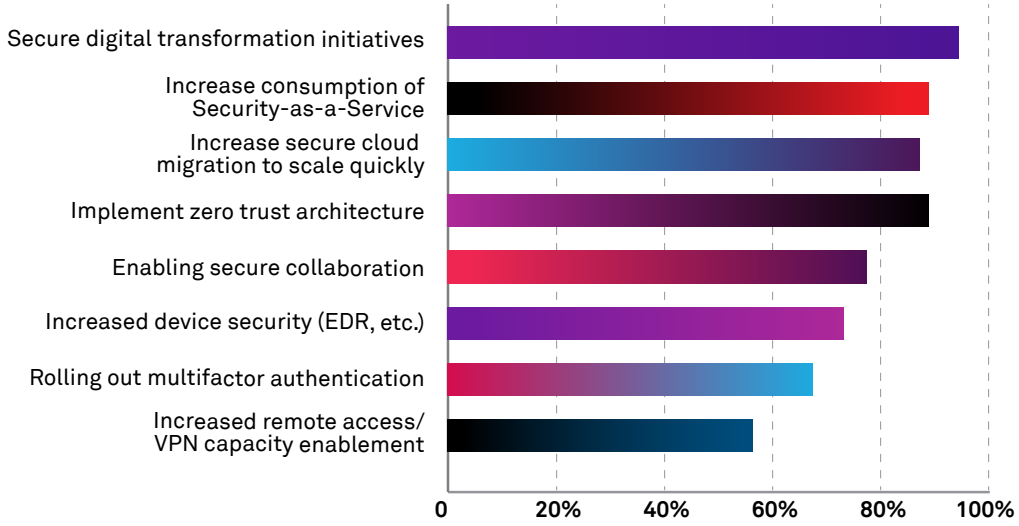


FIGURE 23 [Cybersecurity priorities post-pandemic]

The role of government agencies in aiding the private sector against state-sponsored attacks will be increasingly under scrutiny. A must-read on this line of inquiry is the **Recalibrating the Shared Responsibility to Secure, Protect, and Defend** section from our academic partner, Tel Aviv University. Additionally, our joint research with the Indian Institute of Technology Bombay on decentralized trustware-based collaboration during disasters appears in the **Future of Cybersecurity** section.

The next section from our partner, Google, discusses how organizations can leverage security as an enabler for digital transformation.

Security as an Enabler for Digital Transformation

As we entered the first few months of dealing with COVID-19, many organizations expected a slowdown in their digital strategy. Instead, we saw the opposite – most customers accelerated their use of cloud-based services. Ready or not, enterprises today have to manage a new normal that includes a distributed workforce and new digital strategies. A major trend over the next 6–12 months will be preparing companies to secure their employees and brand in the new normal.

While the companies that have been born in the cloud see VPNs as outdated, many others still rely on traditional VPN infrastructure. And with this rapid move to remote work, IT teams managing this legacy infrastructure struggled to deploy and manage so many new users in such a short period. These problems are exacerbated when organizations try to roll out VPN access to their extended workforce. They can also increase risk because they extend the organization's network perimeter, and many organizations assume that every user inside the perimeter is trusted.

The impact of the mobile workforce is not only changing traditional workflows but also how enterprises approach security. Companies have historically used firewalls to enforce perimeter security, an approach built on the assumption that all employees work exclusively on company-owned devices on company-managed networks, and therefore are safe and trustworthy. Now, it's not only employees who need to access internal apps remotely; it's also the extended workforce.

Like many have already pointed out, the world post-COVID-19 will look much different than it did just a few months ago. There will be employees that never return to the traditional office, with businesses having had their eyes opened to the fact that they can operate securely without being in a building.

There will also be businesses that do return to working side-by-side with their colleagues but with the understanding that disruption could happen again and that they must be equipped to quickly and efficiently switch back to working remotely. In order to prepare for a safer normal, here are some aspects for enterprises to consider as they think about their digital transformation journey over the next 6–12 months:

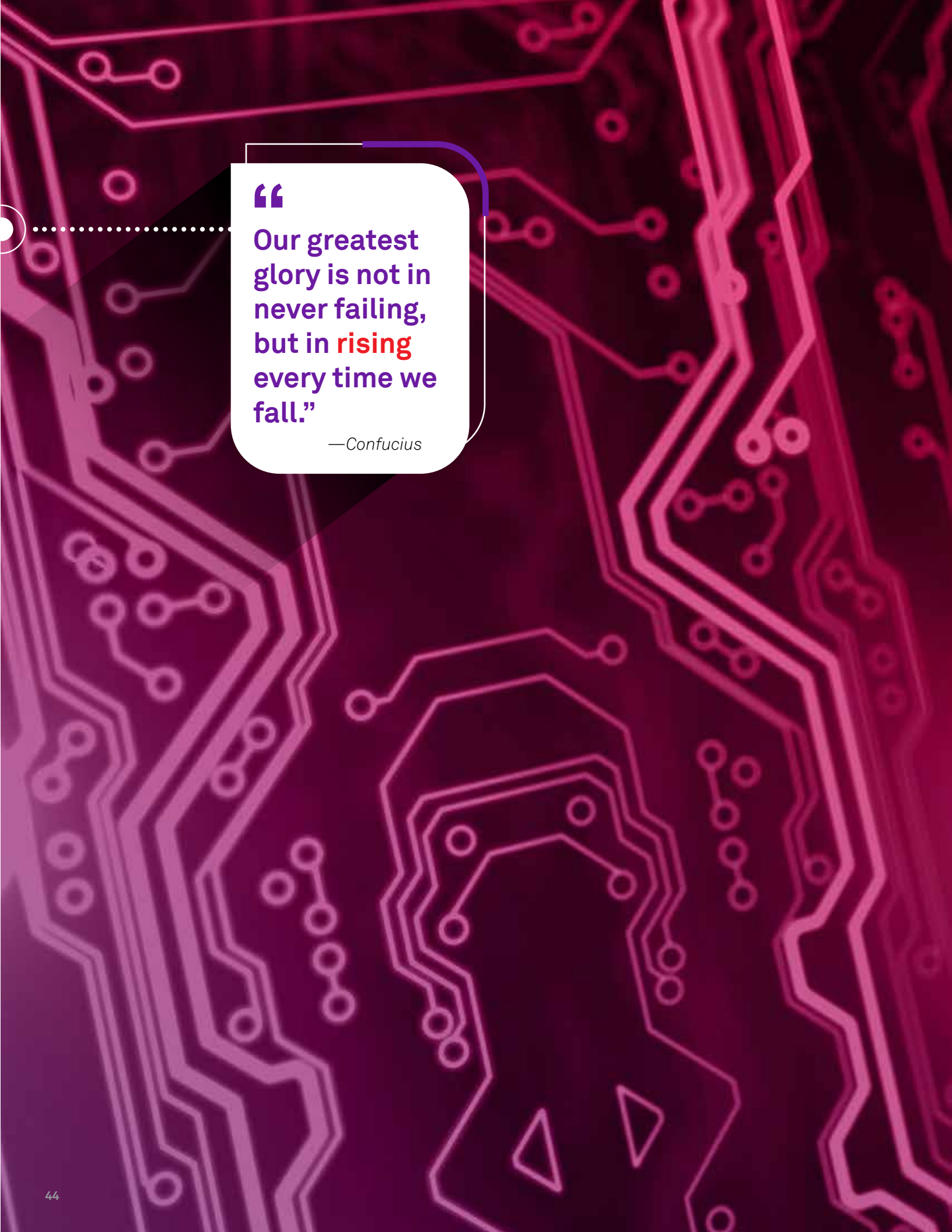
- Secure your endpoints, tied to a user's identity, that works anywhere and on any device.
- Adopt a zero trust access control system that adapts as remote workers change their environments.
- Deploy threat intelligence capabilities that apply new information to worker's activity to prevent account takeover and malicious attacks.
- Use a fraud prevention system, driven by threat intelligence, to protect your customers as effectively as you protect your employees.

- Use an app and data platform that identifies misconfigurations, exposed data buckets, unpatched systems, and actual attacks.

The current situation will persist for some time and will accelerate transformation away from the old model for user access and security – a model that spawned an add-on security industry, constant malware and breaches, and ongoing user frustration. This landscape will inspire enterprises to use security as an enabler for digital transformation beyond the new normal.

Authored by **Sunil Potti**, GM and Vice President of Cloud Security at Google Cloud.

The good work that organizations are doing to secure their digital assets and business continues despite the pandemic. The next section, **State of Cyber Resilience,** explores challenges and trends in governance and security practices within enterprises.


“
Our greatest glory is not in never failing, but in rising every time we fall.”
—Confucius

3

STATE OF CYBER RESILIENCE

This section focuses on organizations and their drive toward cyber resilience, providing a peek into the dynamics that play out as enterprises try to grapple with cybersecurity challenges. Contrasting against the earlier macro perspective presented in the **State of Attacks, Breaches, and Law**, this section brings together a micro view focused on cyber resilience actions within firms. Ultimately, cyber resilience is the sum of an organization's practices, governed by priorities laid out as part of the enterprise risk management framework. Technical practices covering data, application, network, and endpoint security are aspects of the broader security strategy.

This year, this section features relevant contributions from partners Forcepoint, Cloudflare, CloudKnox, Palo Alto Networks and ColorTokens on security challenges related to the people perimeter, DDoS attacks, cloud authorizations, container security and zero trust respectively.

Security Governance

Enterprise security governance goals must be aligned to corporate governance objectives to manage risks through the effective rollout of control measures. For organizations to achieve continuous cyber resilience, they need to assess maturity at the point of departure and draw short-term and long-term strategies to predict attacks, protect from attacks, detect intrusions, and activate timely response and recovery mechanisms. Given the governance strategies laid out across enterprises, what is the confidence level that organizations have in their cybersecurity measures?

Confidence in cyber-resilience measures

Wipro carried out the SOCR 2020 survey across 190+ CISOs and security leaders on security governance and security practices. In large firms, security governance is a complex issue with differing views on the function's roles, responsibilities, budget, investment priorities, success measurement, and metrics reporting. The survey extracted how firms globally and across sectors are grappling with cyber resilience.

We started by asking cybersecurity leaders how confident they felt about their resilience measures across three dimensions:

- Understanding/assessing cyber risks and threats
- Protecting/preventing cyberattacks
- Detecting/responding to cyberattacks

Figure 24 shows that although 59% of respondents indicated they had high confidence in assessing risks, only 23% claimed high confidence in preventing cyberattacks, and a mere 18% had high confidence in detecting them.

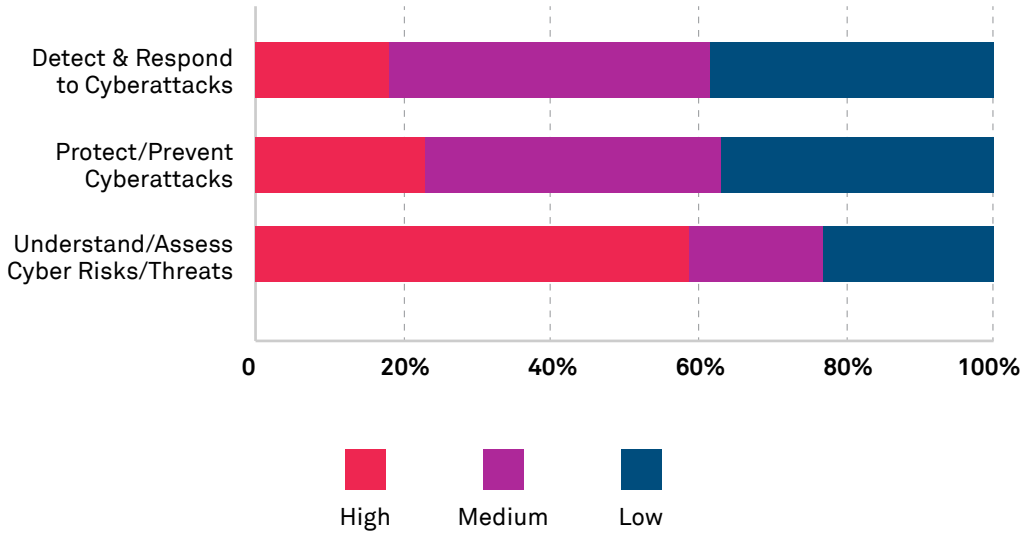


FIGURE 24 [Confidence in cyber-resilience measures]

The need for a cyber-resilience framework

Last year, we laid out a cyber-resilience framework that provides the mechanisms for communication of roles and responsibilities, feedback, and critical imperatives between various layers of the corporate hierarchy when strengthening the enterprise's posture. In the COVID-19 scenario, this framework will undergo stress tests as threats, events, and incidents will need to be identified and mitigated. But having this structure, depicted in **Figure 25,** is the best bet for an organization to make the resilience process sustainable.

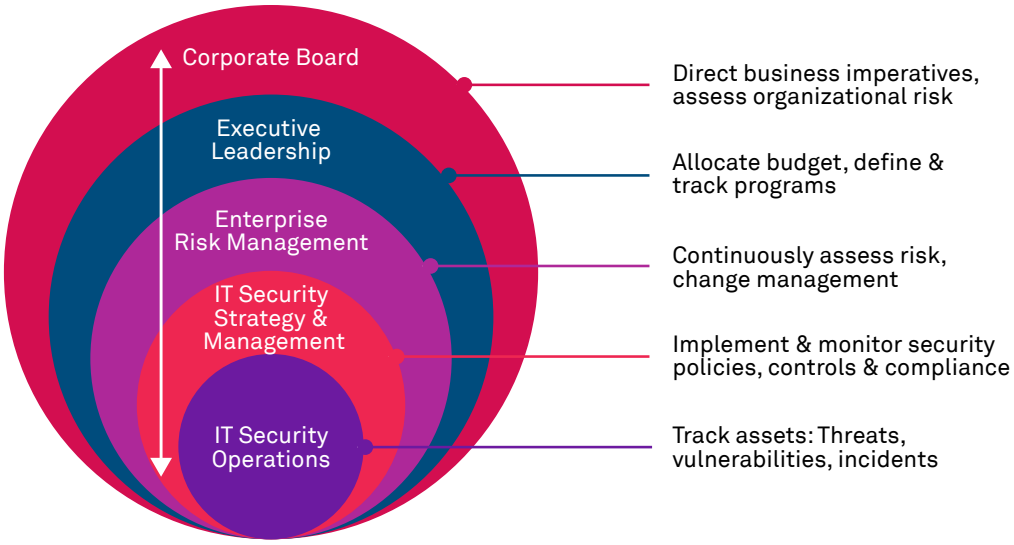


FIGURE 25 [Continuous cyber resilience framework]

The journey toward cyber resilience has to start with a continuous appreciation of cyber risks that can impact an organization's ability to thrive and deliver on its core business imperatives.

Cyber Risks that Organizations Face

The dynamic and evolving threat environment makes channeling efforts toward mitigating cyber risks imperative for organizations. According to the SOCR 2020 survey, 86% of respondents consider email phishing the top cyber risk; lack of security awareness amongst employees/employee negligence stands second at 57%. (**Figure 26** details more risks.)

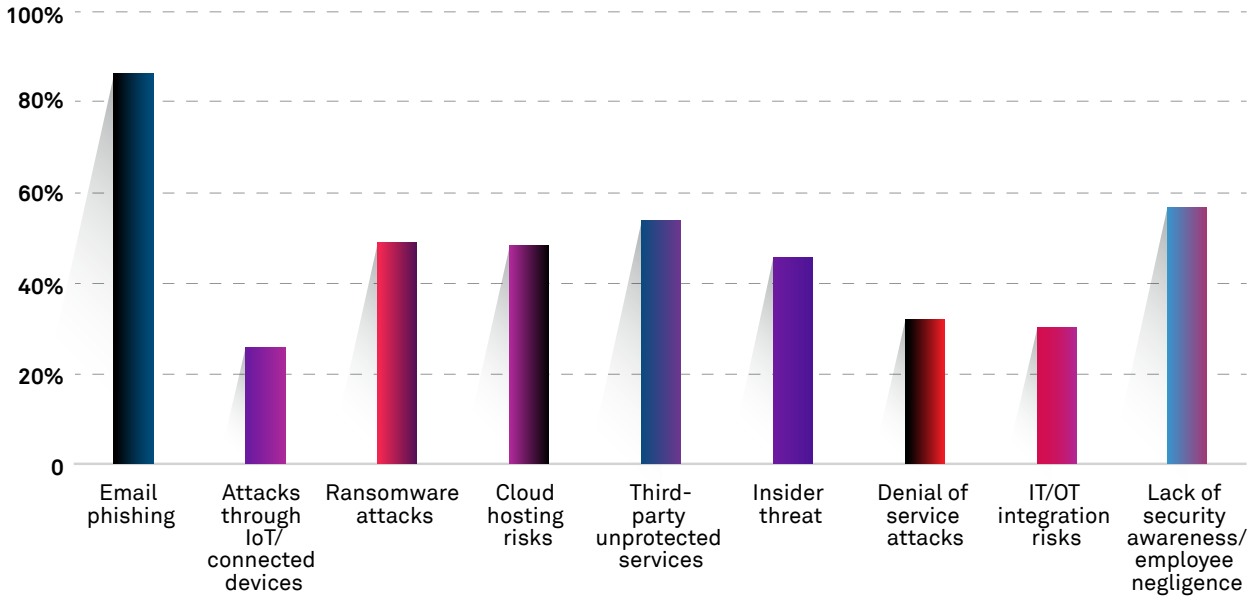


FIGURE 26 [Top cyber risks that organizations face]

Cyber risks continue to evolve, dovetailing with the emergence of new technologies and attack surfaces. The security industry has, mostly, responded with technology controls that can help prevent or detect such risks as they materialize. However, what continues to be the elephant in the room is the human dimension of the cyber problem. Organizations continue to grapple with how to protect the first line of defense. The next section features a point of view from our partner, Forcepoint, on this very important and challenging problem.

Securing the People Perimeter to Move Left of Breach

When I agreed to write this article, I had no idea that the state of cybersecurity, and indeed our working world, would be irrevocably changed in the months that followed.

As companies worldwide moved within a matter of days to a remote work environment, their networks and security capabilities were immediately pressure-tested beyond what most business continuity plans could have envisioned. Seeing a sizeable opportunity for exploitation of this new business reality, bad actors swiftly put in motion malware and spam campaigns to take advantage of this uncertainty and sudden change.

Forcepoint X-Labs research found that unwanted emails using Coronavirus-linked keywords rose from negligible values in January 2020 to more than half a million per day by the end of March 2020, settling down to around 200,000 per day right through until the end of May (**Figure 27**).

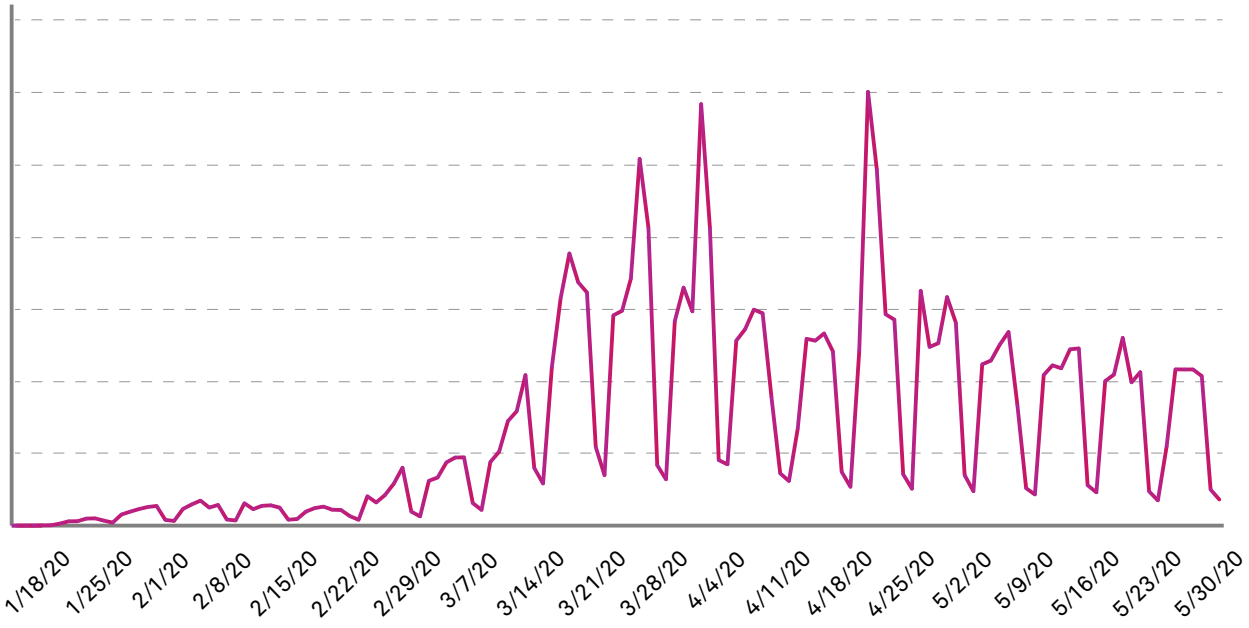


FIGURE 27 [Trend showing phishing emails containing links to malicious COVID-19-themed websites]

The hard truth is that this new reality has only exacerbated the status quo for cybersecurity professionals. Security leaders were already struggling to address the challenges of today's fluid network boundaries. This is now exponentially compounded as millions of workers connect remotely to corporate networks while working with critical data that has moved seemingly overnight to newly deployed software-as-a-service.

It's a fact now more than ever: your people are your new perimeter.

The old ways

Over the last four years, we've observed the industry starting to move away from the traditional reactive and threat-centric model that it's embraced for more than 20 years. The old-style business environment existed within walls and moats where security teams could control the perimeter by securing critical data within owned and managed data centers. But digital transformation, globalization, the cloud, and workforce mobility have spread data and users far beyond the perimeter of walled-off office networks and data centers.

Adding to these challenges are the new risks of large-scale remote work enablement. Consider enterprises adding thousands of device-busy home internet setups almost overnight: work systems became a shared family computer. This creates the perfect storm for security teams, delivering unlimited possibilities for bad actors to exploit new pathways onto enterprise networks. In this modern reality, security that isn't focused on understanding the behavior of people, and data at the edge opens the door for significant business risks.

Insider threat: Masquerading as your people

Modern cybersecurity understands that attackers will come through the digital door and find a way onto your network. Today's data protection model must keep those bad actors from leaving your network with critical data and IP. It is imperative to understand the constants, so you can protect both your people and digital crown jewels. Those constants are simply employees interacting with data.

When companies treat their people as their new perimeter, they replace broad, rigid rules with individualized, adaptive cybersecurity that enables employees to stay both productive and secure.

Adaptive trust security recognizes that risk is fluid and omnipresent and that removing risk wholesale is impossible. Instead, the goal should be to detect and respond to excessive risk, which can only be done through continuous evaluation of digital identities and their unique baseline behavior as they interact with business data day-to-day.

Adaptive trust means cybersecurity doesn't end after a user's behavior is labeled as "good" and access is granted, as would be the case with a traditional, static approach. Instead, the adaptive trust model continues beyond that initial decision, monitoring what a user does when granted access, and whether their behavior is trustworthy.

Behavior-centric analytics should provide adaptive risk-level ratings unique to each user that vary as behavior changes. For example, if a user accesses areas of the network not connected to their normal day job, or attempts to transmit an uncharacteristically large amount of data, the risk level should rise.

When only real risks are flagged and blocked, security friction for users and false positives for administrators are reduced. Overall, this leads to a more productive environment and more effective security.

Managing remote work in current business climate

Applying these principles to remote working at-scale, quite probably for the long term, requires some strategic thinking and forward planning. As enterprises assess the path forward within this "new normal," it is imperative to ensure that leaders have the tools and resources needed to achieve this while keeping employees productive, and without sacrificing security.

The remote workforce is now the new perimeter you have to secure.

We have now lived through a period where there has been a mass change to the way that business does business. The fundamental questions that IT and security leaders have asked themselves

are: "What have I learned about my people? Which data was I most concerned about?"

By answering these questions, you'll be preparing for a world where you make your people secure wherever they are, removing friction, allowing them to get their jobs done, and keeping your data protected. The shake-out from 2020 is going to be felt for years to come, but by applying lessons learned through the implementation of modern security best practices, businesses can come through these times with stronger security programs for today's unpredictable modern threat landscape.

Authored by **Matthew Moynahan**, CEO, Forcepoint (forcepoint.com).

How Cybersecurity Incidents Impact an Organization

A major cyber incident can have a cascading effect on an organization's brand and reputation, invite compliance fines, lead to erosion of customer trust, and impact the bottom-line. When we asked organizations about the impact a cyber incident could have, 72% of respondents said it would damage brand reputation, and 54% said the non-availability of services would lead to revenue loss (**Figure 28**).

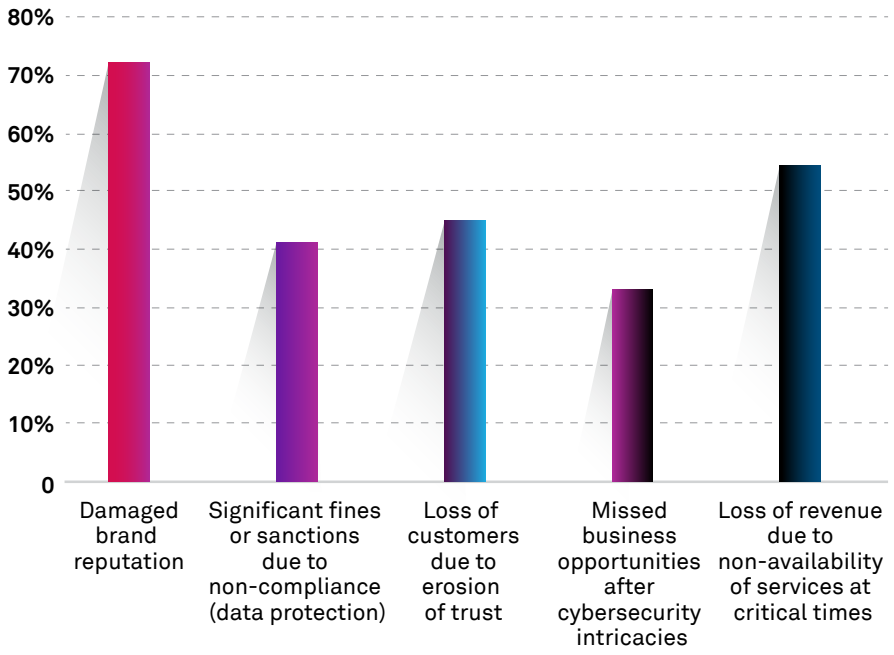


FIGURE 28 [Impact of a cyber incident on an organization]

75%

VERTICAL INSIGHT

of surveyed telecommunication organizations responded that cyber incidents would lead to missed business opportunities, and 64% of surveyed ENU organizations indicated that incidents could lead to loss of revenue due to non-availability of services at critical times.

The Evolving Role of the CISO

In an already volatile, uncertain, and complex world, executive management must be vigilant, continuously reviewing cyber risks and preparedness measures. The effects of recent cyber breaches have landed at the doorways of executive ownership. With leadership becoming accountable for any cyber incident, the spotlight has turned to the role of the CISO, whose widening responsibilities are moving toward all-round security governance, a noteworthy change.

Whom does the CISO report to?

Our survey analysis gathered that a majority (46%) of CISOs reported to the CIO; however, 14% reported directly to the CEO, and 12% reported to the COO, a sizable shift. **Figure 29** highlights the reporting structures of the CISO globally by sector.

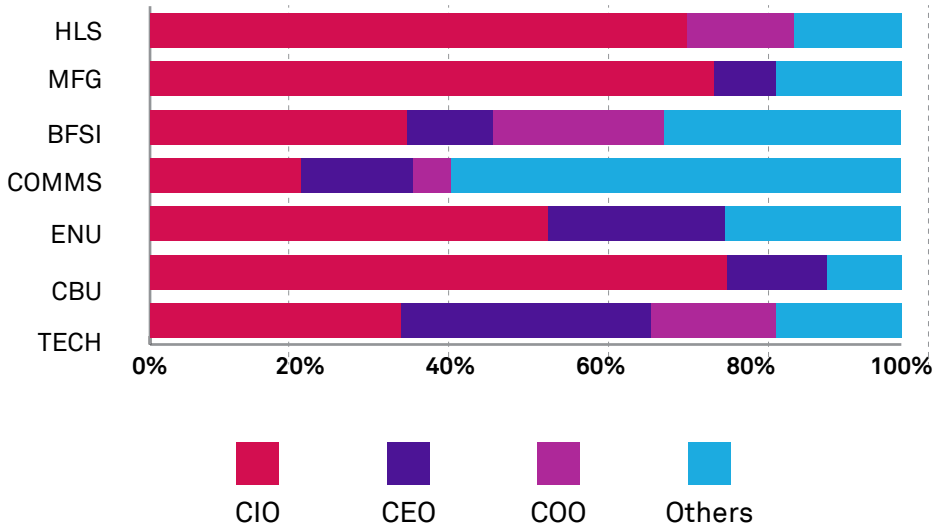


FIGURE 29 [CISO reporting by vertical]

No template for the CISO reporting structure exists for all organizations to leverage. Multiple factors, such as business goals, risks in the industry, organizational culture, and business unit diversity, need to be considered for CISO positioning. Most importantly, the evolving role should align enterprise risk priorities to business goals.

Ownership of Data Privacy

In the earlier **State of Attacks, Breaches, and Law** section, our research covered the more-stringent laws concerning breach notifications and restrictions on international transfers. More and more, countries require data controllers to act with due care on how they collect, process, store, and destroy personally identifiable information. Many new regulations also include heavy fines in the event of a significant data breach, requiring organizations operating in multiple jurisdictions to adhere to various mandates and work with regulatory authorities to report their compliance.

Who is responsible for data privacy?

Who in an organization is ultimately responsible for data privacy varies depending on the laws and regulations enacted by countries and regions, as shown in **Figure 30** and **Figure 31**. Globally, 34% of respondents indicated that data privacy was the responsibility of the CPO/DPO, and 45% indicated that either the CIO or CISO was responsible.

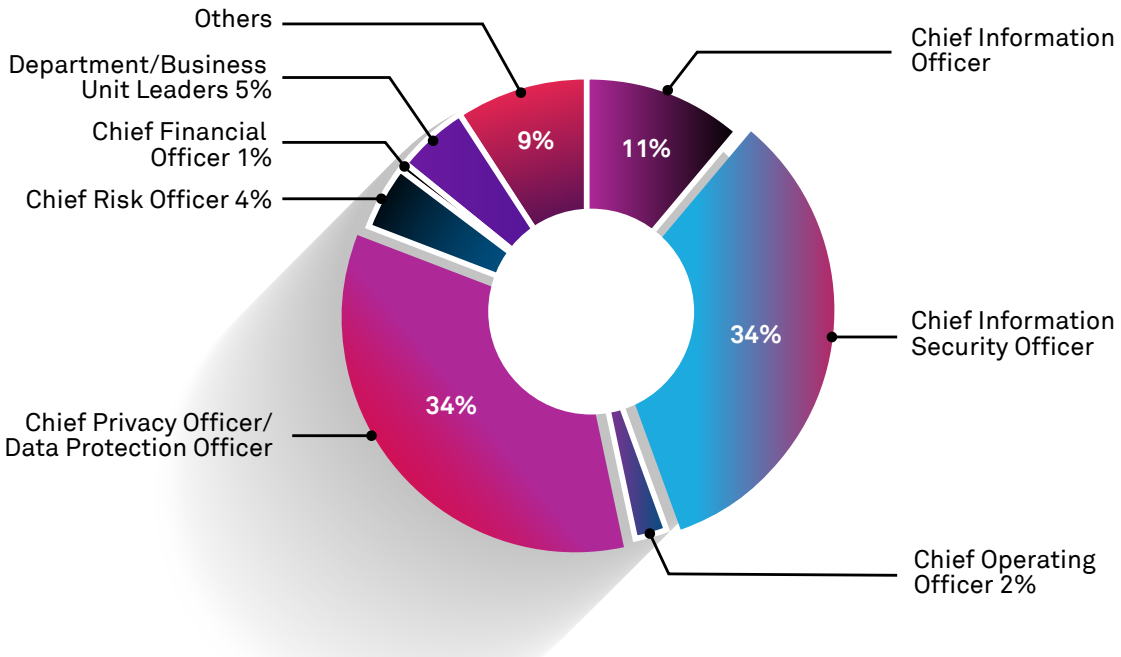


FIGURE 30 [Organizational responsibility for governance of data privacy – Global]

In Europe, organizations indicating that the CPO/DPO was responsible for data privacy was 57%, with 34% indicating that the CISO was responsible.

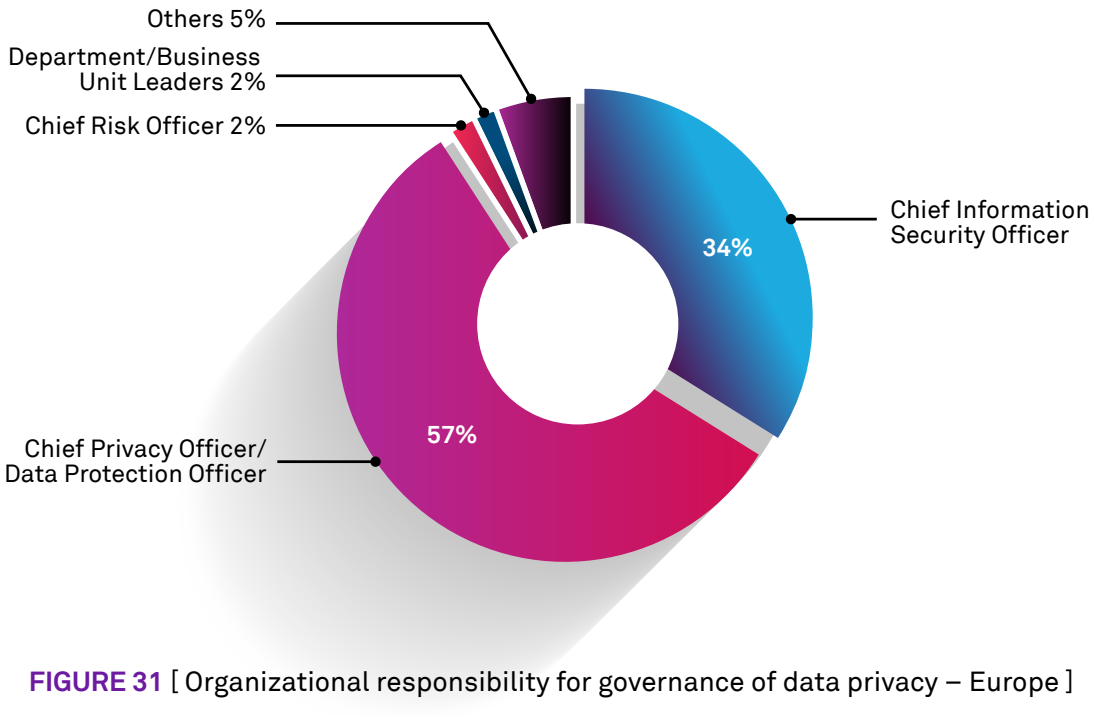


FIGURE 31 [Organizational responsibility for governance of data privacy – Europe]

Security Budgets

Organizations are investing continuously in cybersecurity to strengthen their security posture. The process of securing the requisite budget is affected by various factors, including new regulations, compliance mandates, board oversight on cybersecurity, and recent breaches. Security leadership must get their needs, based on risk evaluations across the enterprise's processes, on the boardroom's table.

68%

GLOBAL INSIGHT

Worldwide, 68% of respondents stated that the CISO or DPO/CPO is responsible for their organization's data privacy.

Factors driving increased security budgets

60% of CISOs surveyed cited new regulations as a significant factor behind increased budget allocations. Also, 56% stated that their board's oversight of cybersecurity had driven the budget increment. However, an interesting observation was that 46% of organizations saw their security budgets increase after their industry peers experienced a breach (**Figure 32**).

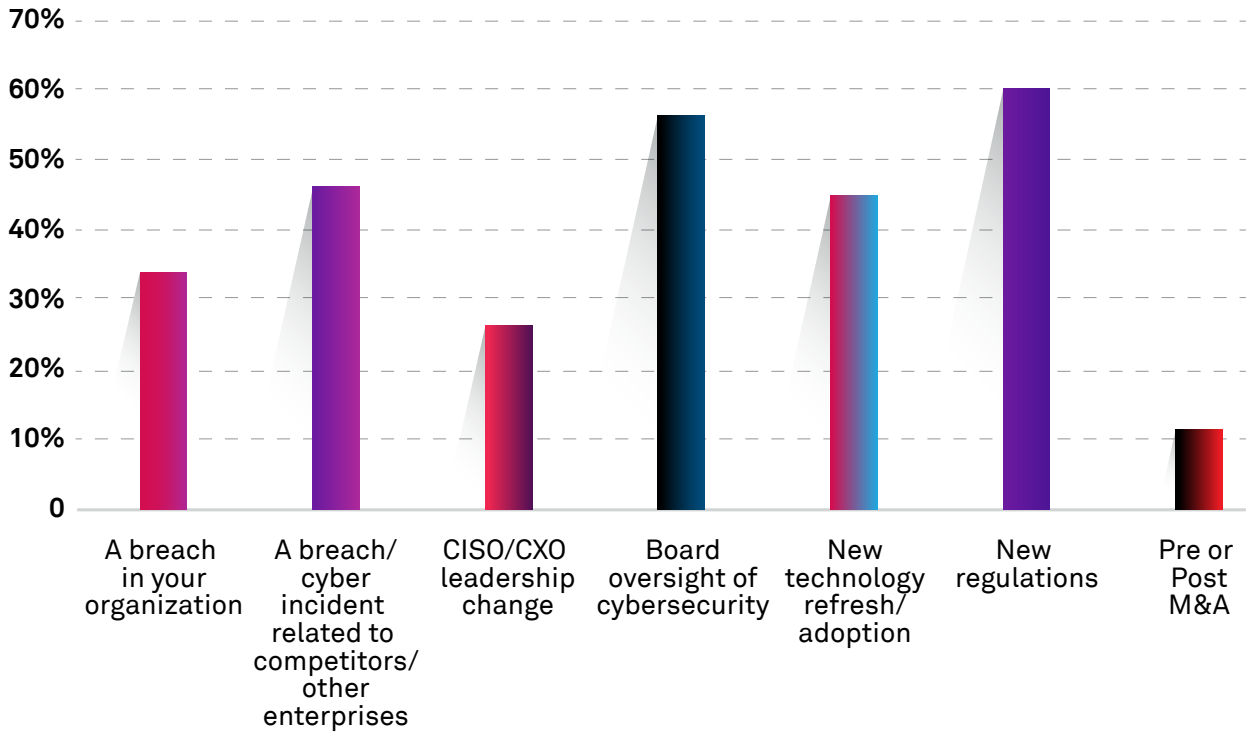


FIGURE 32 [Leading factors for increased budget allocation]

60% **GLOBAL INSIGHT**

of surveyed organizations consider new regulations to be the driving factor for increased security budgets.

71% **VERTICAL INSIGHT**

of surveyed HLS organizations consider a cyberattack on peers to be a driving factor for increased security budget.

One metric employed for comparing the availability of cybersecurity budgets across sectors is to look at relative allocations compared to overall IT budgets. Because attackers are unceasingly refining and intensifying their techniques, organizations need a thorough defense strategy, investments in advanced technology, and skilled professionals. Regardless of the percentage of budget allocated, organizations need to evaluate the money's use and effectiveness. When we asked security leaders what portion of their IT budget went toward security, 14% responded that they received more than 12%. An equal number of respondents indicated that their security spend was less than 4% of their total IT budget. **Figure 33** highlights the security budget posture.

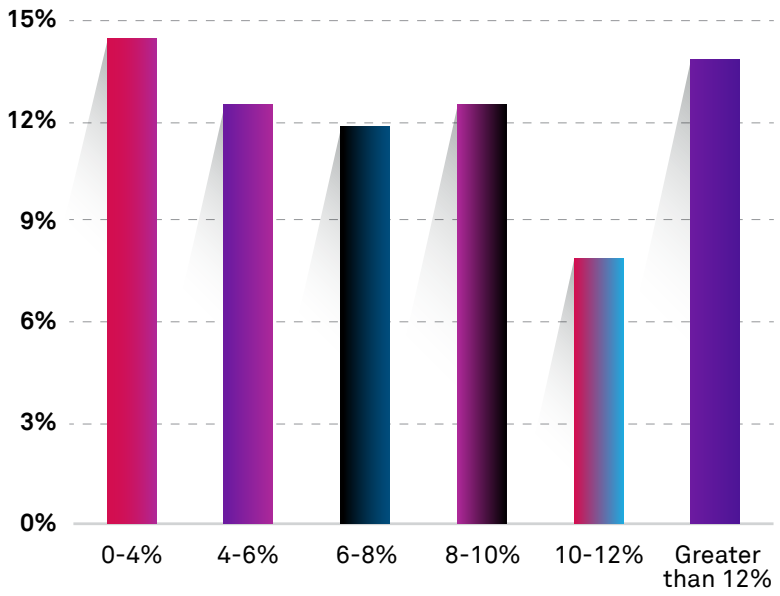


FIGURE 33 [Range of percentage of IT budget allocated for security]

Security Investment Priorities

We surveyed organizations about their investment priorities for the year ahead. 35% indicated that they would be investing in security orchestration and automation. 20% considered zero trust rollouts a priority, and 14% indicated hybrid cloud security. Along with investing in technologies, organizations have to invest in the human element to be more cyber resilient. An encouraging trend appears in **Figure 34**: 18% of organizations plan to invest in security awareness and training. The post-COVID-19 world is expected to see escalating supply chain attacks, and a worrying indicator is that 53% of organizations are not prioritizing investments in supply chain security.

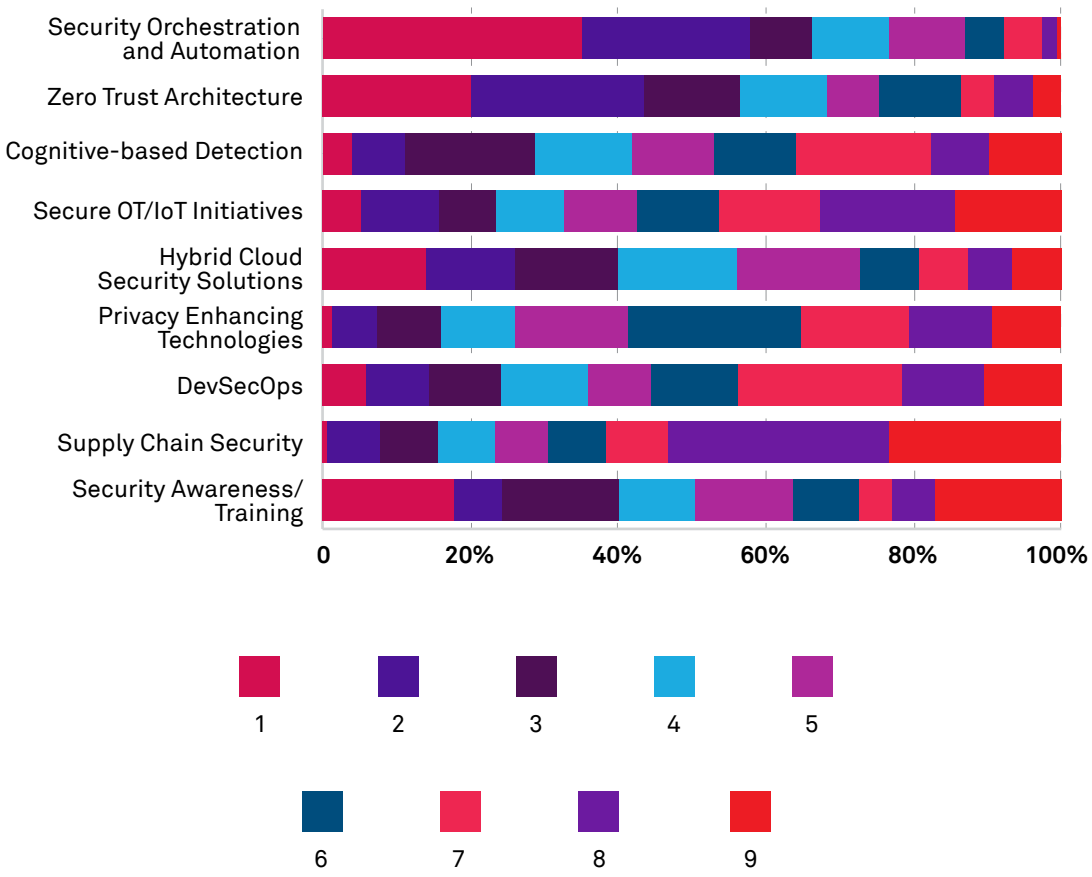


FIGURE 34 [Ranking of top investment priorities]

Security Metrics

As organizations utilize their allocated budgets on capital and operational expenditures, including the top investment areas indicated previously, the effectiveness of the spend needs to be measured and reported across the hierarchy.

Measure it to change it

In the survey, we asked organizations across industries about their metrics reporting in management, operational, and technical categories. 64% of respondents considered time to detect and remediate incidents the most critical management metric to track (**Table 2**). 62% stated that mean-time to mitigate vulnerabilities was the most important operational metric (**Table 3**), and 81% considered vulnerability scanning coverage an essential technical metric (**Table 4**).

Management Metrics	HLS	MFG	BFSI	COMMS	ENU	CBU	TECH	Global
Time to Detect and Remediate Incidents	83%	71%	72%	57%	33%	67%	67%	64%
Cost of Detection	33%	43%	38%	7%	17%	33%	22%	28%
Cost of Downtime	50%	49%	53%	29%	50%	48%	56%	48%
Cost of Incidents	17%	62%	47%	21%	25%	33%	33%	34%
Regulatory Compliance	50%	57%	73%	64%	50%	38%	78%	59%
Security Spending as % of IT Budget	33%	59%	43%	21%	25%	33%	44%	37%

Table 2 [Management metrics reporting across industries]

Operational Metrics	HLS	MFG	BFSI	COMMS	ENU	CBU	Global
Mean-Time to Patch	67%	33%	67%	54%	55%	67%	55%
Mean-Time to Incident Discovery	67%	67%	54%	62%	27%	43%	57%
Mean-Time to Incident Recovery	50%	44%	60%	62%	64%	67%	59%
Mean-Time to Mitigate Vulnerabilities	33%	67%	68%	69%	64%	76%	62%
% of Changes with Security Exceptions	17%	22%	25%	23%	9%	33%	20%

Table 3 [Operational metrics reporting across industries]

Technical metrics	HLS	MFG	BFSI	COMMS	ENU	CBU	Global
Patch Management Coverage	78%	80%	82%	75%	67%	91%	80%
Anti-Malware Compliance	83%	80%	65%	83%	58%	64%	68%
Vulnerability Scanning Coverage	81%	70%	85%	83%	75%	86%	81%
Configuration Management Coverage	47%	30%	53%	50%	33%	41%	43%
% of Systems with Known Vulnerabilities	51%	40%	68%	67%	50%	45%	55%

Table 4 [Technical metrics reporting across industries]

Cybersecurity Talent Management

The skills gap is a concern faced by most organizations around the globe. Cybersecurity skills across industries appear to have a demand versus supply mismatch. For executive leadership within the cyber ecosystem, attracting, motivating, and retaining the best talent is essential but not always easy.

We asked organizations to provide the top reasons for the existing cybersecurity skills gap. **Figure 35** shows that 42% of the respondents found it challenging to retain cyber talent, and 41% didn't find enough qualified applicants for the job. However, 17% of organizations felt that applicants needed to improve their cybersecurity expertise.

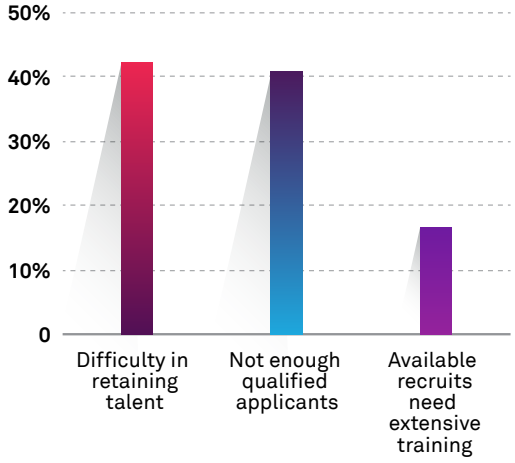


FIGURE 35 [Reasons for the existing skills gap]

What factors motivate cyber talent?

As part of our research, we asked global cybersecurity leaders what factors motivated their teams. **Figure 36** shows 68% responded that participation in external cybersecurity conferences and training (allowing for learning and growth) was the best motivator. 62% considered cross-functional training and defined career roadmaps as a critical motivating factor. A relatively lesser 33% of organizations indicated that differentiated compensation structures helped to motivate and retain talent.

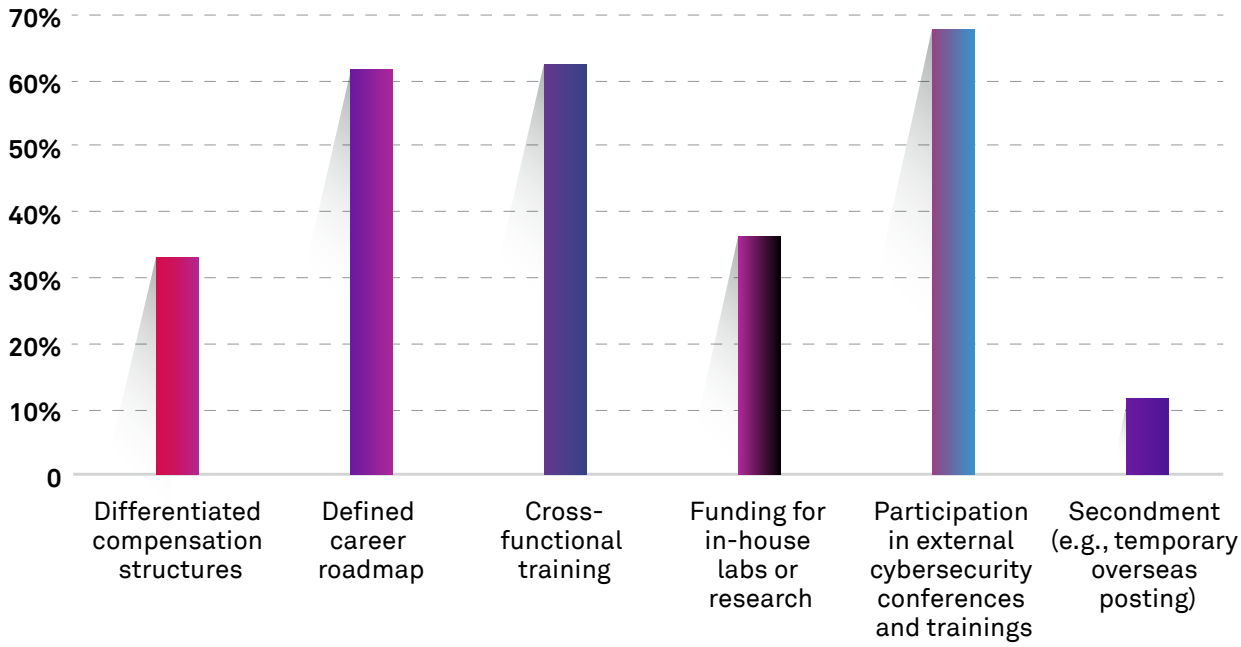


FIGURE 36 [Cyber talent motivation factors]

68%

GLOBAL INSIGHT

of organizations consider participation in external cybersecurity conferences and training as the best way to motivate teams.

42%

VERTICAL INSIGHT

of the BFSI organizations highlighted differentiated compensation structures for talent motivation and retention.

Security Practices

A broad spectrum of research from our survey focused on trends in security practices that organizations were employing. The research identified significant trends over the past three years in selected domains, including data security, application security, edge security, endpoint security, DDoS prevention, security monitoring and analytics, cloud security, and IoT security.

Data security

The enterprise perimeter has been expanding, and data has been steadily leaving the shores to foster collaboration and exchange. Data migrations to SaaS applications, cloud infrastructures, and mobile devices, coupled with stringent regulations, such as CCPA and GDPR, forced organizations to implement robust data privacy and security measures.

The number and types of IT assets holding sensitive data expanded, and mapping the flow of data has been a challenge for enterprises. We asked organizations which enterprise systems stored their data and whether they encrypted it. **Figure 37** indicates that enterprise databases held a large amount of sensitive information, but only 70% of those environments were encrypted. 80% of respondents indicated that their big data stores held sensitive information, but more than one-third of them were not encrypted.

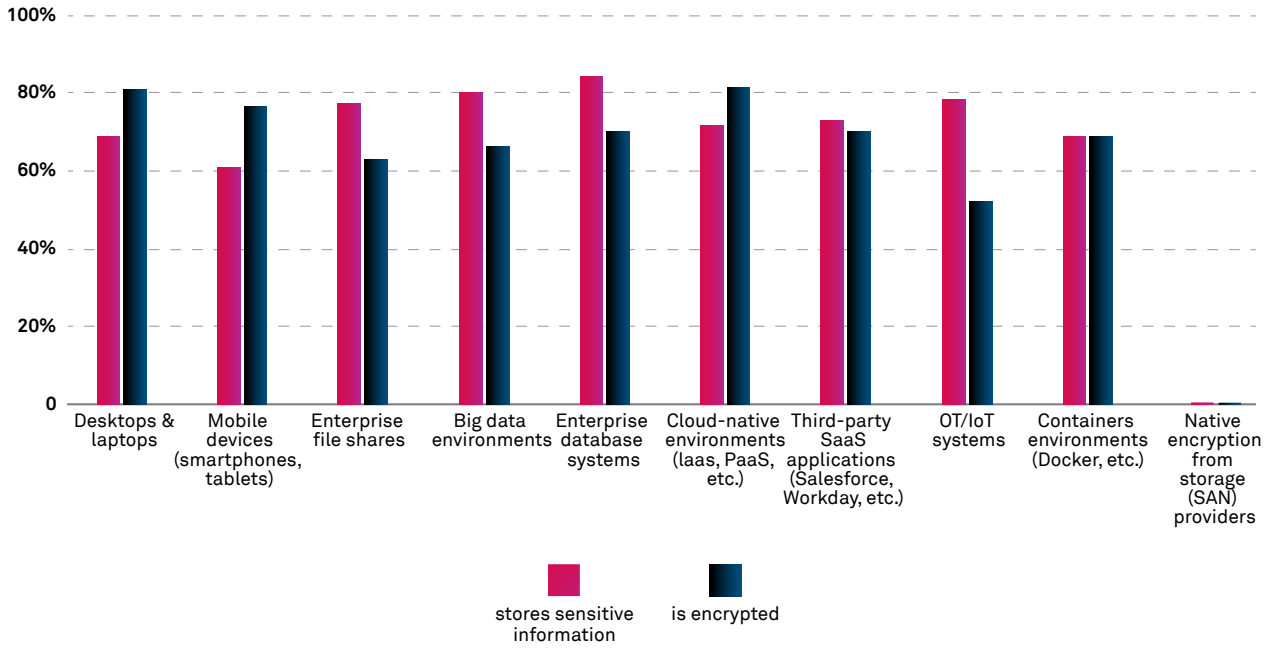


FIGURE 37 [Data storage strategies and encryption priorities]

New data privacy regulations gave consumers leverage to seek compensation for the improper management, use, and disclosure of their data. When we asked security leaders to rank the data security controls they implemented (**Figure 38**), 32% said automated data discovery and classification was the most efficient (a rise of 16% from last year). This is not surprising because IT teams must identify the dispersion of sensitive data before they can apply encryption or compensating control policies. 23% of

respondents ranked privileged access management (PAM) as a top data security control. Additionally, data leak prevention and encryption of data across the databases were among the top security controls implemented by organizations.

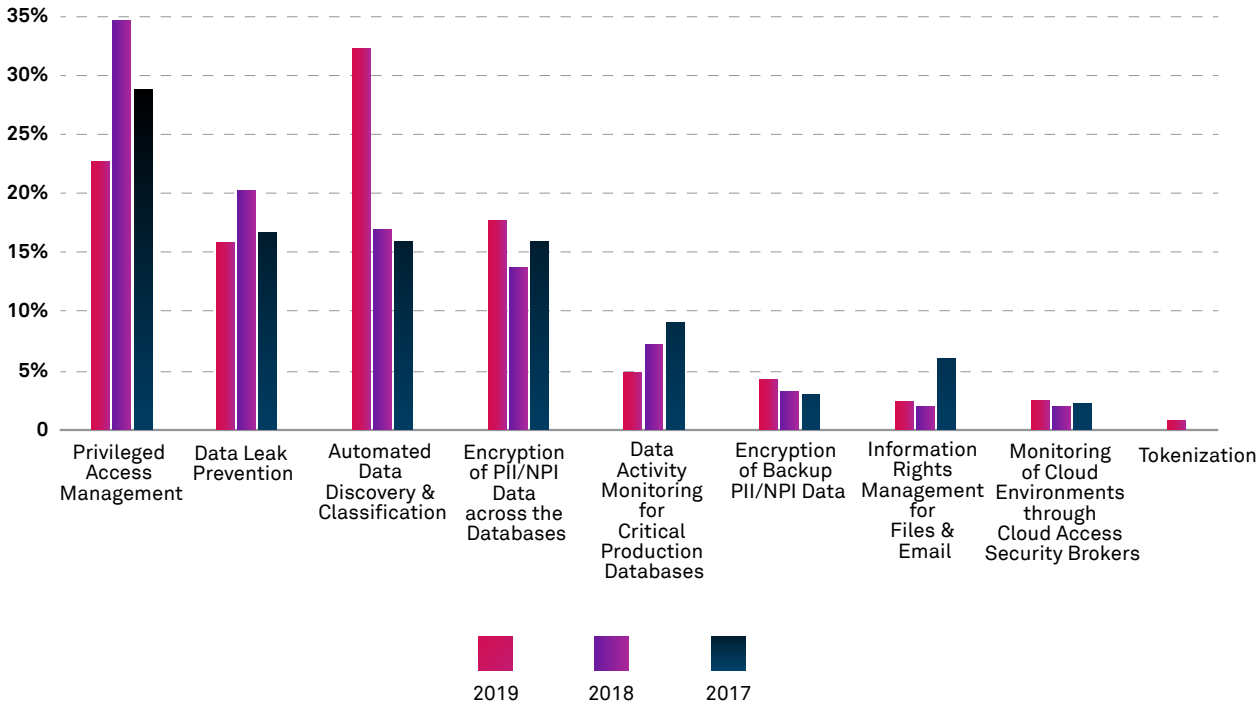


FIGURE 38 [Data security control trends]

32%

GLOBAL INSIGHT

of respondents chose automated data discovery and classification as the most effective data security control.

88%

VERTICAL INSIGHT

of BFSI enterprises that hold sensitive data in cloud-native environments encrypt them.

Application security

Application security management in enterprises has been a casualty of arduous enhancements to the classic waterfall software development lifecycles that had not been wholeheartedly accepted by development teams. However, the advent of DevOps has been an opportunity for advancement because of the way DevOps leverages automation. Integration of security checks in DevOps has been made possible by automating security code reviews or penetration

tests seamlessly. This has triggered incremental movement toward improving application security posture over the past 2–3 years.

During primary research, we asked organizations about their security assessment frequency for business-critical applications. 27% said that they carry out security assessments in every build cycle, an increasing trend over the past three years. We attribute the acute decrease in security assessments of applications post-launch (see **Figure 39**) to the fact that organizations are moving toward the adoption of DevSecOps practice.

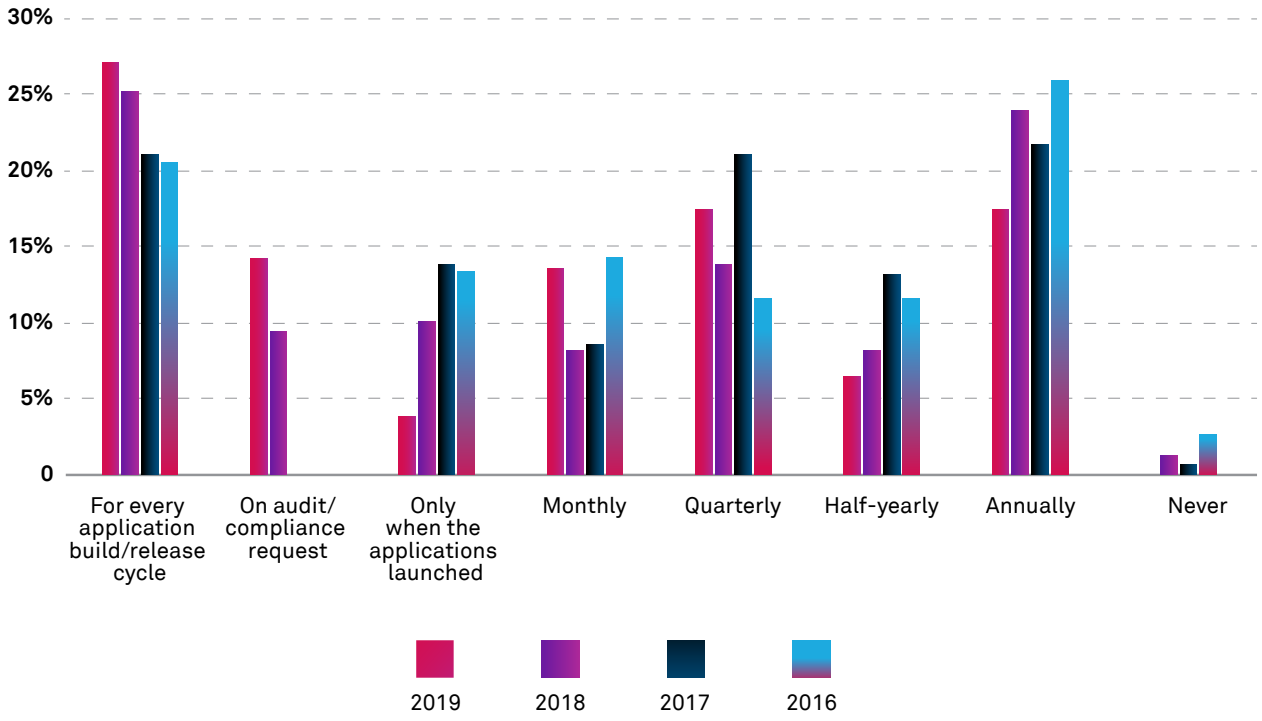


FIGURE 39 [Frequency of security assessment of business-critical applications, 2016–2019]

27%

GLOBAL INSIGHT

of respondents conduct security assessments in every build cycle.

VERTICAL INSIGHT

Communications and BFSI verticals took the top spot in conducting security assessments for every application in the build/release cycle, with 44% and 37%, respectively.

Although applications and data can be protected from a confidentiality perspective to minimize the impact of cyberattacks, organizations may still have to deal with maintaining the availability of their services in the event that threat actors launch distributed denial of services (DDoS) attacks on their exposed asset base. In the next section, we explore trends in DDoS attacks.

DDoS attacks: shrinking in size, increasing in impact

The rise of DDoS attacks in the wake of increased internet use during a global pandemic is no surprise. To avoid significant revenue loss, keeping services up as the world entered into lockdown was of prime importance. Wipro asked organizations about the average duration of the DDoS attacks they faced. Responses to the survey indicated that 27% of organizations that faced DDoS attacks saw durations of less than 60 minutes (**Figure 40**).

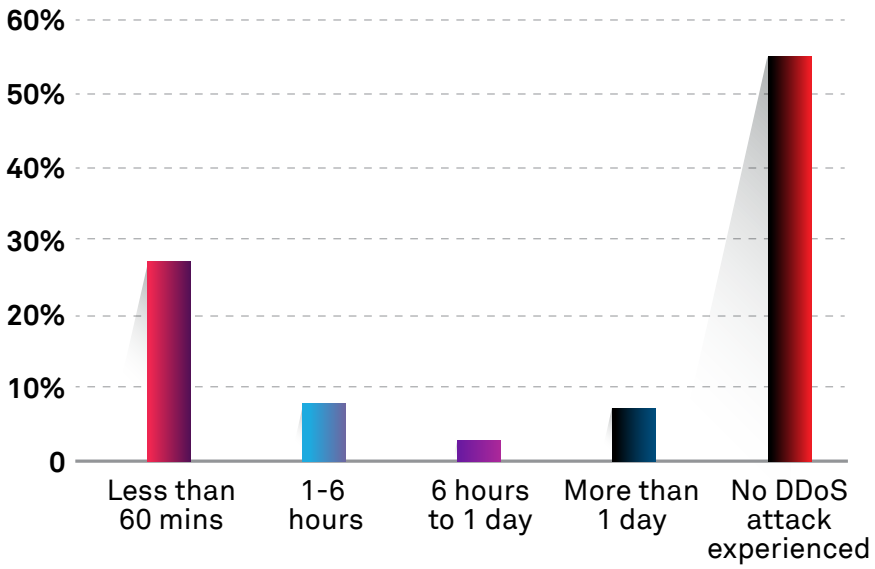


FIGURE 40 [Duration of DDoS attacks]

Analysis of worldwide DDoS attack patterns

Working with our global alliance partner, Cloudflare, we derived worldwide trends on DDoS attacks from mid-2019 through the first two quarters of 2020. This data, based on analysis of patterns across Cloudflare's global network, spanned more than 200 cities in more than 95 countries.

Voluminous attacks with the potential to disrupt business operations persisted. **Figure 41** from

Cloudflare highlights the highest bit rate of network-layer DDoS attacks spanning 12 months. The highest bit rate observed, 550 Gbps, was in March 2020.

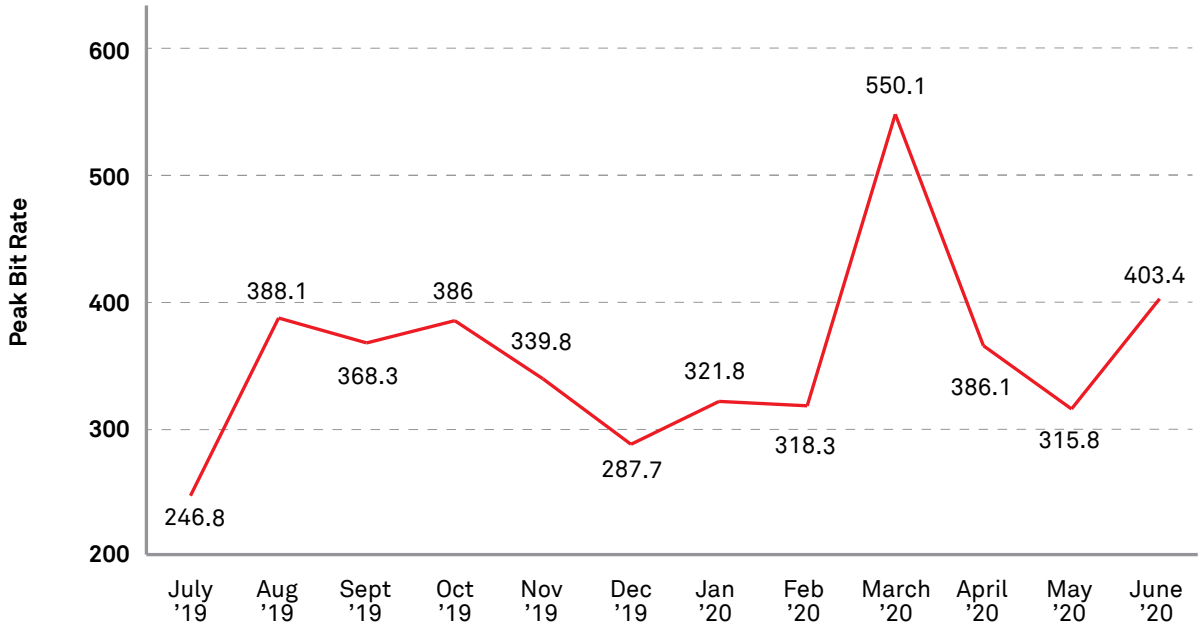


FIGURE 41 [Peak bit rate by month]

While the peak bit rate per month gives us the extreme scenarios, the number of attacks by bit rate provides a more holistic perspective of the attacks' distribution. **Figure 42** shows that in Q1 2020, 92% of the attacks detected by Cloudflare's network had a bit rate of less than 10 Gbps, compared to 84% in the previous quarter.

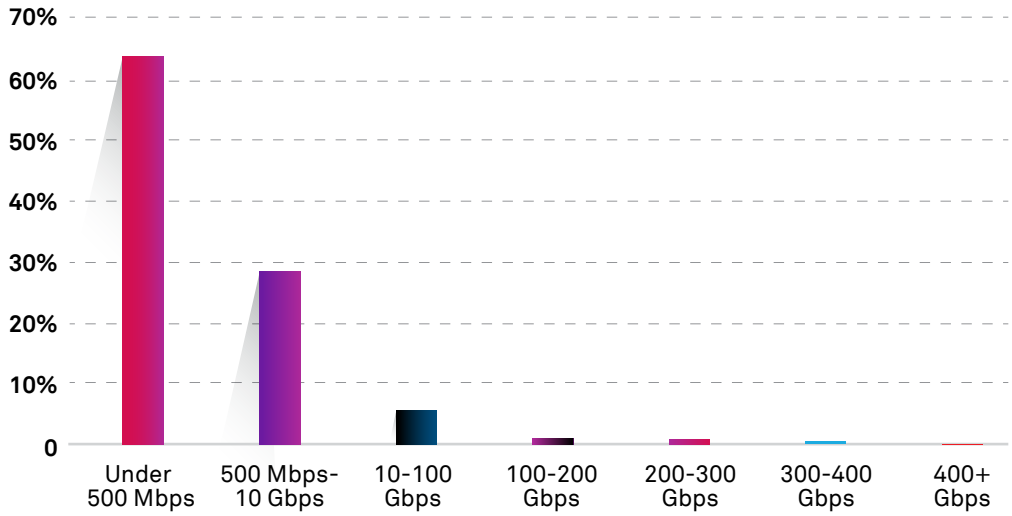


FIGURE 42 [Attacks by bit rate]

With the availability of DDoS-as-a-service tools, amateur attackers are launching DDoS attacks economically with limited bandwidth. Worth pondering is whether these small attacks are designed distractions for the security operation center (SOC) while threat actors are attempting other network penetrations and exfiltrations.

45% **GLOBAL INSIGHT**

of organizations experienced a DDoS attack in 2019.

73% **VERTICAL INSIGHT**

of manufacturing respondents didn't experience a DDoS attack in 2019.

Wipro's partner, Cloudflare (cloudflare.com), contributed this subsection.

Endpoint security

A combination of BYOD, shipped desktops, and fully managed devices facilitated the explosion of remote work enablement for many employees in numerous enterprises across geographies, and security teams struggled to maintain endpoint hygiene across assets.

Compromised endpoints of remote privileged users lead to entryways for threat actors. We asked CISOs to rank the vectors through which threat actors were successfully compromising endpoints. 73% ranked phishing emails as the biggest culprit, while 18% ranked USBs as the second-most compromised vector (**Figure 43**).

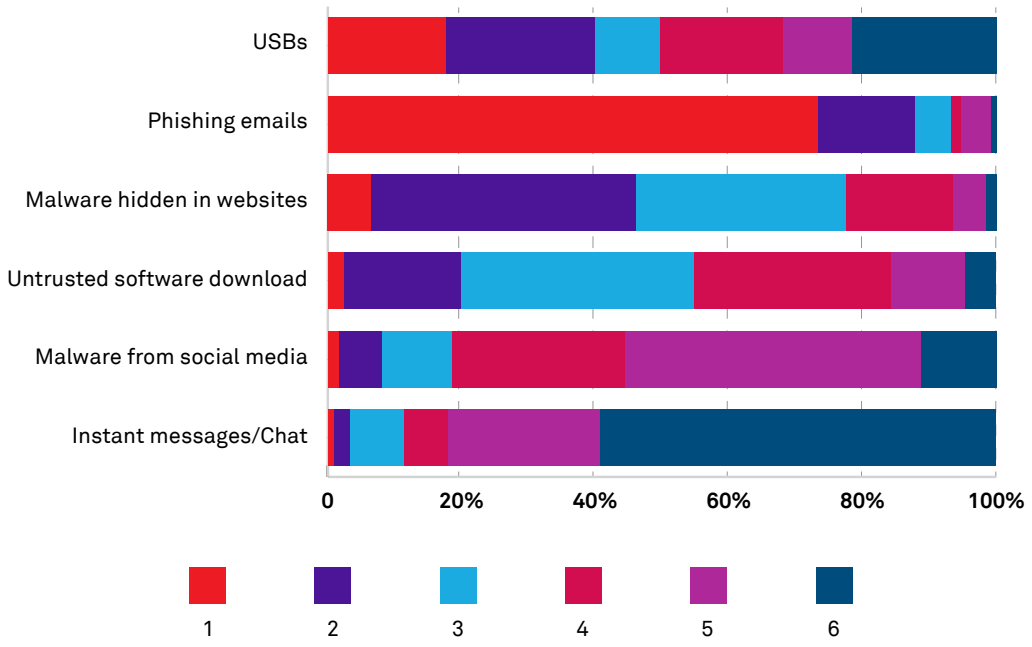


FIGURE 43 [Ranking of endpoint attack vectors by frequency, 2019]

73%

GLOBAL INSIGHT

of organizations ranked phishing email attacks as the top vector of endpoint compromise.

50%

VERTICAL INSIGHT

of surveyed ENU organizations responded that USBs were the top vector for endpoint compromise.

The battle for endpoints cannot be won through technology alone. The final line of defense is the employee. Recurring employee awareness and training must complement any technical measures in place.

Security monitoring and analytics

SOCs are a critical building block of an organization's all-round cybersecurity risk mitigation capability. Although layered defenses have their use, enterprises must be able to detect and contain an intrusion early. SOCs need to be able to extract insights with context across multiple layers of defense, deal with "alert deluge," and winnow true positives from the rest of the noise. Are enterprise SOCs today equipped to handle this deluge? What kind of tooling will be required to improve performance?

We asked organizations what key capabilities they needed in their SOC. Nearly 50% of survey respondents identified adding cognitive detection capabilities to tackle unknown attacks and threat hunting as a critical capability. Other findings shown in **Figure 44** include:

- **Organizations struggle with all-round visibility of all IT assets across the data centers, cloud, mobile, and social environments.** 18% of respondents are planning to widen the asset visibility from the conventional data center to the cloud, OT/IoT, and connected devices.
- **SOC teams need continuous learning on new threat scenarios, detection use cases, and response procedures.** A few respondents indicated that they needed to leverage cyber range capabilities to administer crisis simulation exercises to staff.

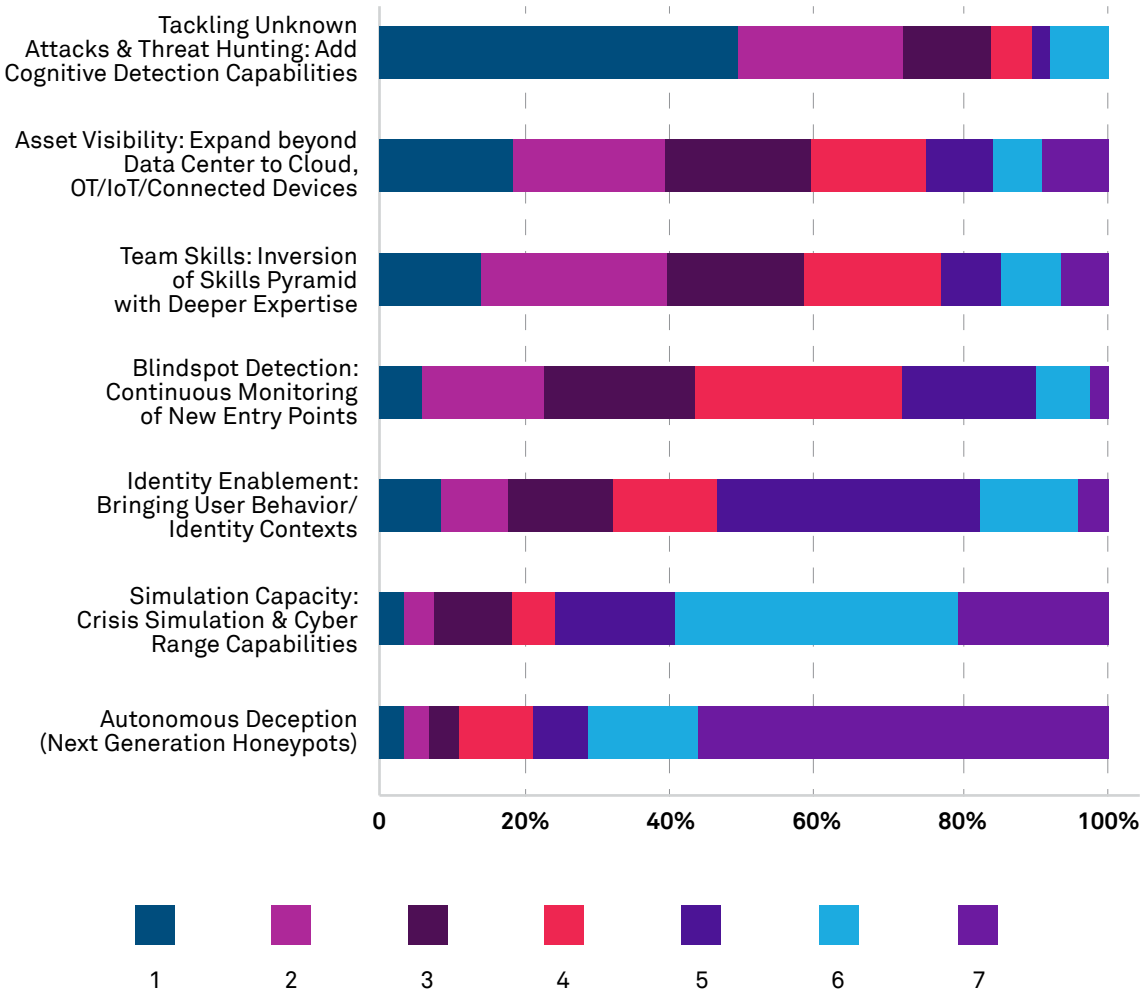


FIGURE 44 [Needed security operation center capabilities]

49%

GLOBAL INSIGHT

of organizations are prioritizing cognitive detection capabilities to enhance their SOC.

36%

VERTICAL INSIGHT

of manufacturing organizations are expanding asset visibility of the SOC to OT/IoT and cloud environments.

Cloud security

With the growing adoption of cloud-based services, we see organizations increasingly willing to manage sensitive information in cloud environments, such as Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), and Platform-as-a-Service (PaaS). 72% of organizations that responded are storing sensitive data on cloud environments (refer to Figure 37).

With the COVID-19 situation in the background, we asked a few questions about current and future data migration priorities. 52% of respondents prioritized scaling up secure cloud migrations during the COVID-19 crisis, while 87% of respondents stated they would continue to scale up secure cloud migrations after the COVID-19 crisis (refer to Figure 21 and Figure 23).

To enable data mobility and enhance cost efficiency, 74% (**Figure 45**) of responding organizations are migrating employee information to cloud environments. The migration of business finance records has also seen growth from last year's 41% to 54% this year. Organizations are now considering migrating payment card information (PCI) to cloud systems, with 25% of responding organizations preferring it compared to 19% last year.

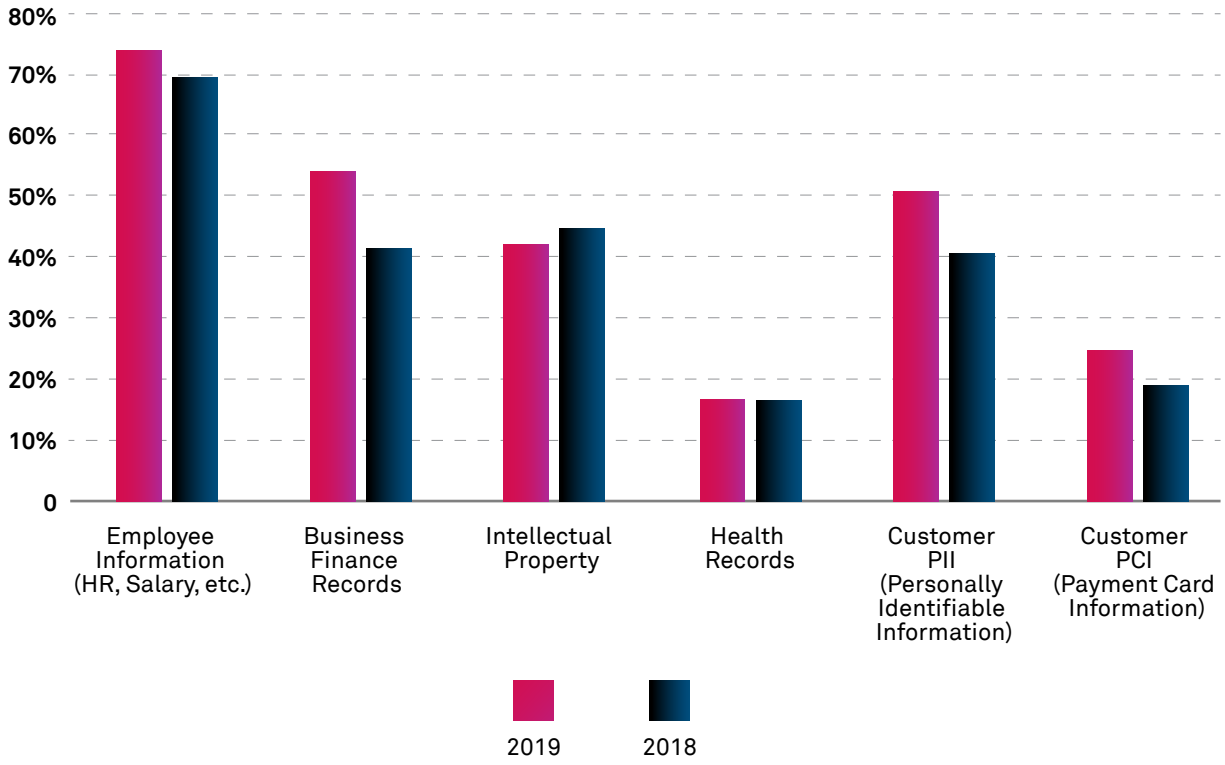


FIGURE 45 [Data migrating to the cloud]

Also, a rising 23% of responding organizations considered privilege escalations on cloud infrastructure to be among the top IT security challenges experienced during the pandemic. The difficulties around privilege management and authorization governance in multi-cloud deployments are complex because of the permissions layers buried deep within. Our partner, CloudKnox, conducted some interesting research on the extent of the permissions problem, which is presented in the next section.

Risks of Over-provisioned Permissions in Cloud Environments

As organizations modernize IT and adopt hybrid and multi-cloud infrastructure and support more distributed business processes involving human and non-human identities, the traditional security perimeter becomes outdated. Identities today are the new security perimeter and have become the new attack vector to exfiltrate business-critical data. Moreover, with the accelerated adoption of public cloud workloads, the number of identities with privileged access to infrastructure is increasing exponentially. This trend has rendered high-risk identity permissions to be one of the most menacing threat vectors to cloud infrastructure for years to come. This emerging threat will force enterprises of all sizes to rethink how they grant, manage, and monitor permissions and secure their cloud resources from accidental misuse and intentional exploitation across their environments.

As a result, the problem of cloud infrastructure permissions management has become very critical. At publication, over 40,000 permissions could be granted to identities across the key cloud infrastructure platforms (AWS, Azure, GCP, and VMware vSphere), and nearly 50% of these permissions can be classified as high-risk with the ability to cause catastrophic damage if used improperly (Figure 46). High-risk permissions are defined as any action that can cause service disruption, service degradation, or data exfiltration, as was in the case of a large banking breach recently.

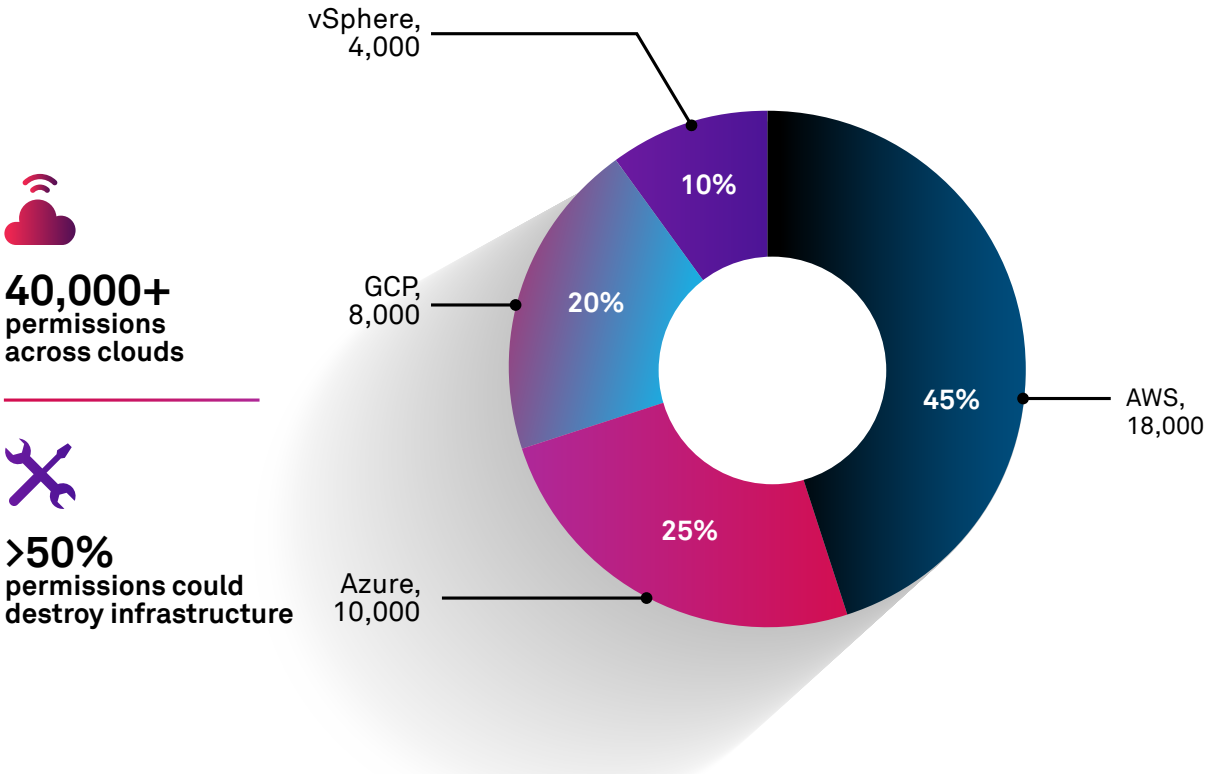


FIGURE 46 [Cloud infrastructure permissions]

We collected data from over 125 risk assessments, and what we discovered is that over 95% of all identities are grossly over-provisioned (i.e., granted a substantial number of high-risk permissions). What was even more alarming was the fact that these identities used less than 10% of the permissions granted to perform their daily tasks (**Figure 47**). This leaves a significant permissions gap, exposing enterprises globally to high risk that malicious attackers can exploit or can be inadvertently misused. The dangerous delta between permissions granted and permissions used is what we refer to as the *cloud permissions gap*. This gap has quickly emerged as the number one risk to public and private cloud infrastructure and proving to be fertile ground for both accidental and malicious permissions misuse and exploitation. As more identities (human and non-human) leverage the cloud infrastructure and deploy exponentially more workloads, the cloud permissions gap is growing wider and is exposing global enterprises to higher risk. The inability to properly grant, manage, and monitor these permissions across a multi-cloud environment is accelerating the permissions creep, which in turn has resulted in over-permissioned, privileged identities becoming the number one security risk for public and hybrid cloud infrastructures.

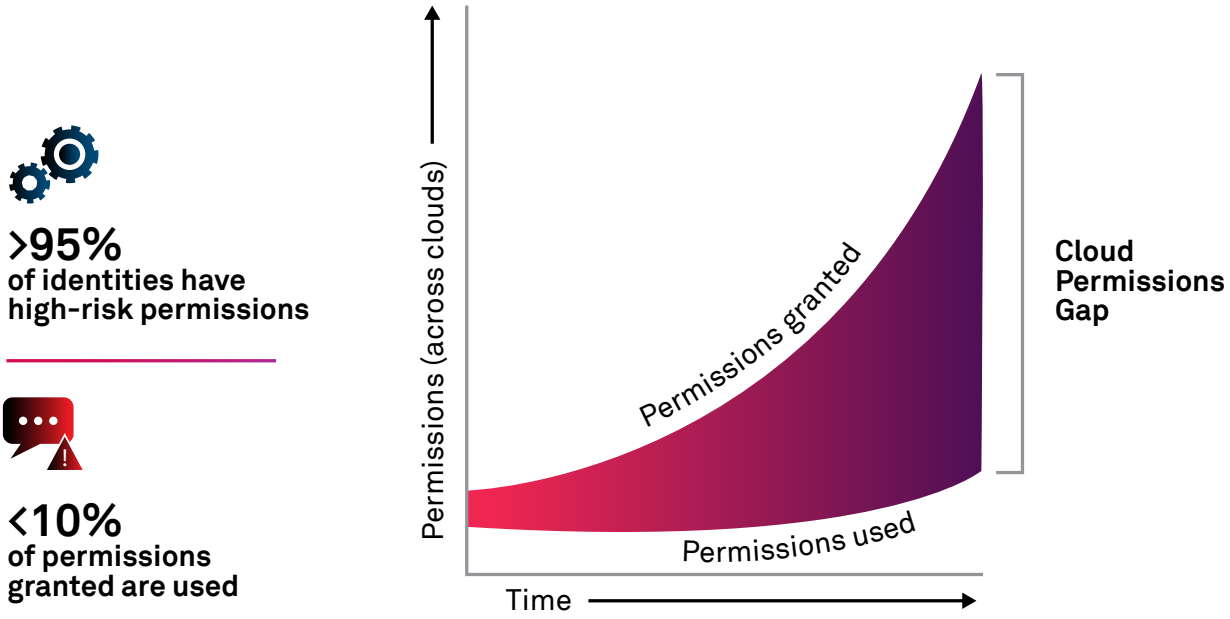


FIGURE 47 [Cloud permissions gap]

Security and infrastructure operations teams are being asked to do the impossible and are finding it increasingly difficult to manage and secure the dynamic nature of multi-cloud infrastructure platforms (**Figure 48**) while keeping up with the explosion of new over-permissioned machine and human identities, accounts, resources, and services.

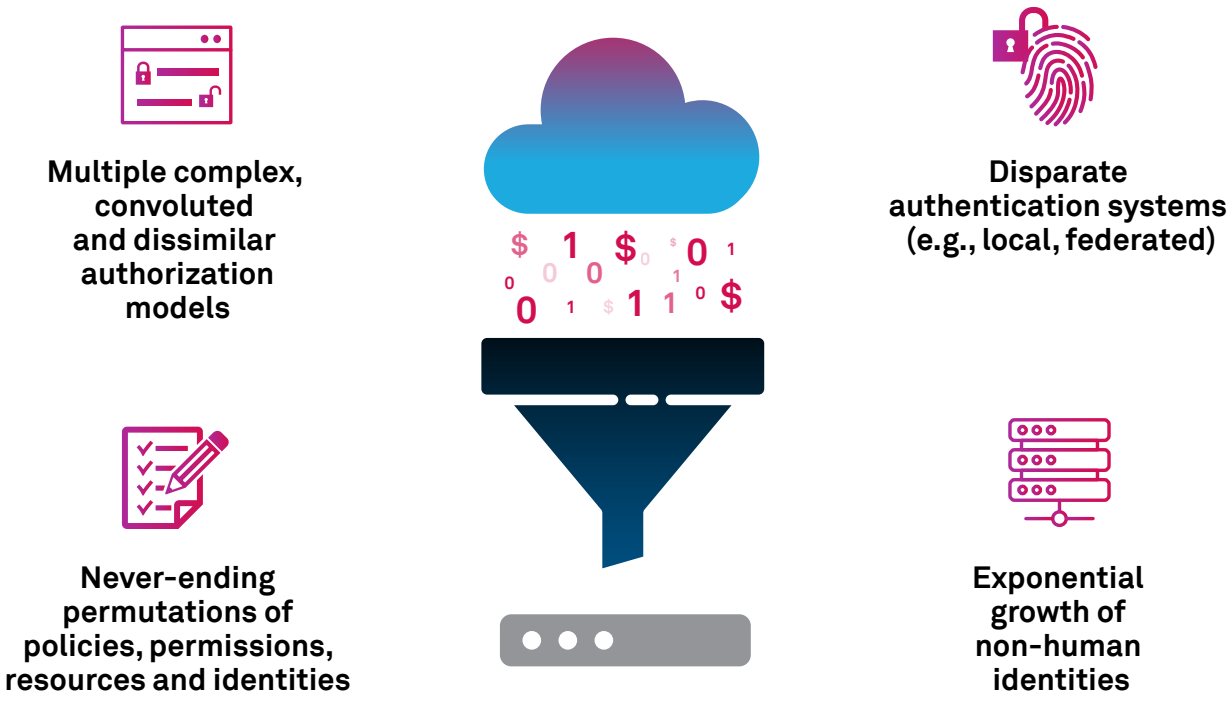


FIGURE 48 [Managing complexity across clouds]

The risk management strategy around cloud hosting will have a gaping hole if security and risk teams do not evolve a clear strategy to handle this problem as they plan to increase the pace of digitalization and cloud migration.

Wipro's partner, CloudKnox (cloudknox.io), contributed this subsection.

48% of responding organizations still consider cloud hosting risks among one of the top cyber risks.

The next research-based point of view from Wipro's partner, Palo Alto Networks, draws out the risks of unsecured container environments in the cloud.

Containing Risks in Containers

Many enterprises that are adopting a cloud-first strategy are embracing container technologies to build, deploy, and roll out new applications. Container platforms are thus becoming the new extended attack surface for most organizations. Attackers are targeting docker engines as a host for launching attacks and for installing rootkits on host systems. Exposed logs from insecure docker hosts can reveal critical data like infrastructure configuration and application credentials. Business IT and Security teams are grappling with understanding the risks posed by insecure containers and in developing an effective strategy to mitigate the threats.

We collaborated with Wipro to present a contemporary analysis of the tools and techniques that attackers are using to compromise docker environments. A docker daemon is a process that runs in the background, which communicates with REST API to manage objects such as containers, networks, images, and other daemons through a single host system. The research spanned across publically exposed insecure docker hosts across the Americas, EMEA, and APAC regions during late last year. This included 1400 docker hosts, 8600+ active containers, and 17900+ docker images that were publically visible.

The metadata collected from the compromised docker engines revealed some malicious activities, attacker's tools, techniques, and procedures (TTP), exposed docker versions, and locations. **Figure 49** shows how the exposed docker hosts were spread across different geographical regions.

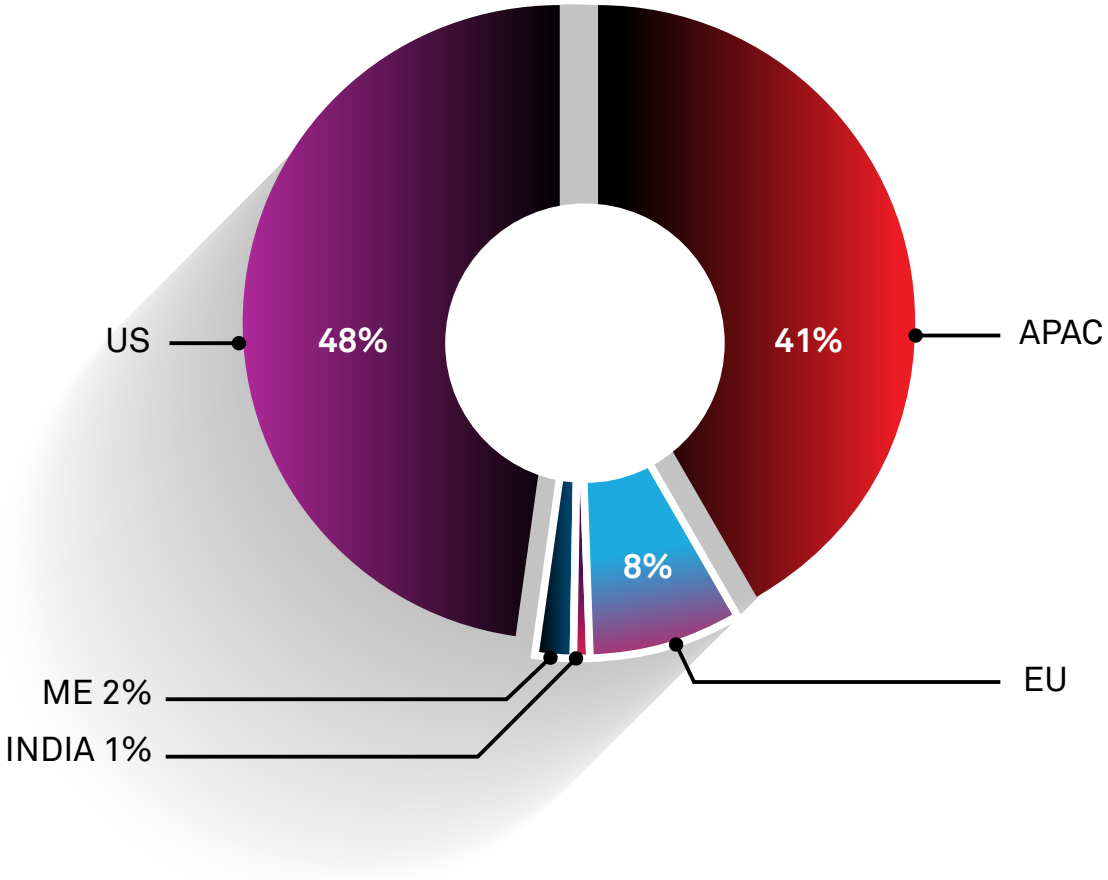


FIGURE 49 [Insecure docker environments by region]

The observations from malicious activities were classified into four categories that followed a typical pattern. **Figure 50** shows the category and the technique, along with potential mitigation strategies.

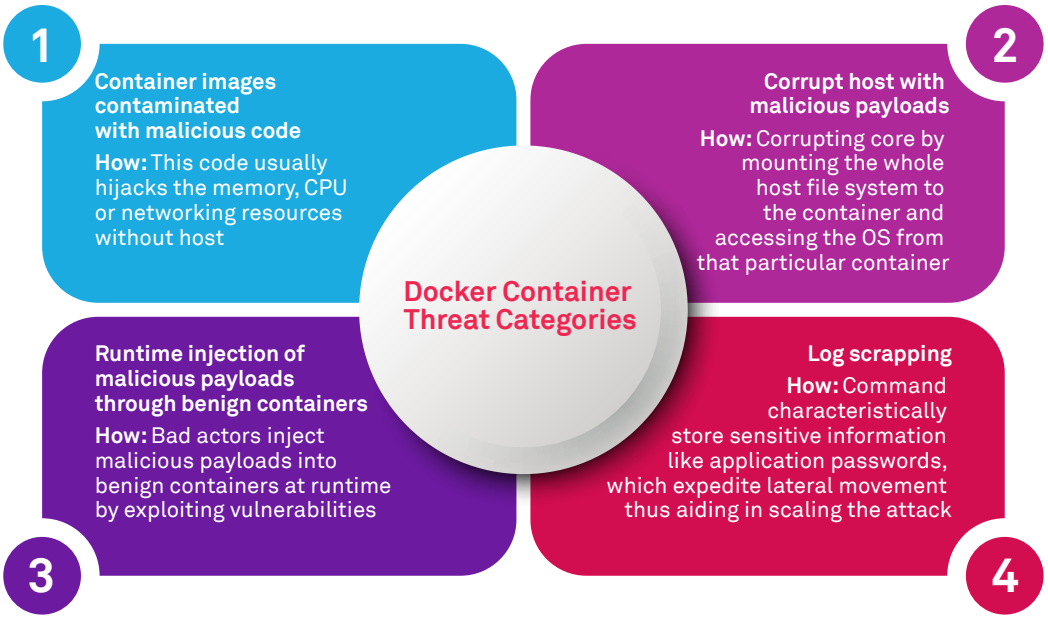


FIGURE 50 [Container threat categories and mitigation strategies]

Wipro's partner, Palo Alto Networks (paloaltonetworks.com), contributed this subsection.

IoT security

The early rollout of Industry 4.0 use cases and the continued fusing of OT and IT environments have brought many benefits around visibility, intelligence, proactive interventions, and operational efficiency in the manufacturing, oil and gas, utilities, and pharmaceutical sectors. The specialized hardware and software components of integrated OT environments are now a ripe target for threat actors who seek to disrupt operations or steal confidential information.

Although there has been a universal increase in the deployment of all core organizational control areas, this should not be mistaken for a significant increase in the maturity of organizational capability. Indeed, based on our client interactions over the past 12 months, we see

this increase in organizational control deployment as representative of the first step on a long journey for many organizations as they consider the needs of the new cybersecurity landscape, a journey that is often 2–3 years in fulfillment and aligned to wider industry digital transformation programs. The organizational control deployment is shown in **Figure 51**.

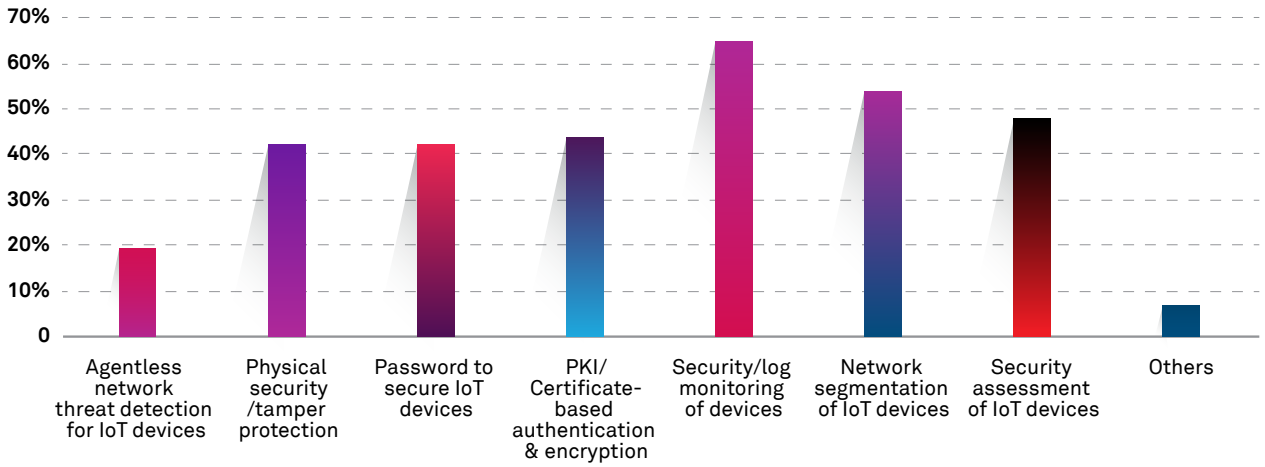


FIGURE 51 [Controls planned to mitigate IoT risks]

The traditional gaps between Enterprise IT and OT/IoT landscapes are fast eroding, and convergence is the key challenge for CIOs and CISOs as they transition to delivering digital transformation and cyber resilience across their operations. This assessment is backed by 78% of organizations recognizing that sensitive information, often business-critical, is stored within their OT/IoT systems. Yet, only 19% of businesses have adopted the asset detection and monitoring capabilities central to an effective, holistic, industrial security capability.

The vendor ecosystem in industrial security is significantly changing with the consolidation of vendors when IT-focused providers acquire traditional OT/IoT security vendors. While this consolidation should deliver an accelerated and enhanced solution capability in the medium term, client organizations must focus on the critical differences between the security management of Enterprise IT and OT/IoT landscapes. Partnering with specialist providers who can provide a proportional and pragmatic response to industrial security is essential to ensure that organizations benefit from targeted investment in the deployment of technology solutions to deliver enhanced organizational controls to manage OT/IoT risk. CIOs and CISOs, therefore, should ensure that when making buying decisions, they remain focused on the core business needs delivered by the OT/IoT environment and avoid slavish alignment to traditional Enterprise IT cybersecurity approaches.

Edge security

SOCR 2019 covered the emerging challenges in security as the 5G ecosystem evolved. Consumption of edge computing is expected to grow exponentially in tandem with worldwide 5G rollouts. With the expected growth of field devices, edge computing will help mitigate bandwidth constraints associated with a traditional centralized computing environment. Edge computing with 5G will help remove latency constraints

by placing resources close to the edge devices and increasing resiliency with alternate data routing capabilities. However, this highly fragmented system might pose a risk for the security of the systems, data, and applications.

For edge computing to work effectively, sufficient bandwidth would be required to access and manage the devices or endpoints. Cybersecurity controls near the user or edge devices could then leverage SaaS security services to secure data and identities. Many applications used by edge devices or cloud endpoints currently leverage APIs that are usually neither authenticated nor encrypted and might leak confidential data. Securing these access points with proper controls and strong authentication mechanisms is a critical enabler for the success of edge computing.

Network edge devices provide access using SD-WAN, CDN, Network-as-a-Service offerings, bandwidth aggregators, and networking vendor services. Each of these components can integrate with SaaS-based security services to provide security controls for edge devices and avoid routing of traffic back to traditional data centers. Integration with the edge devices or cloud endpoints is usually done with agents to carry secure traffic to cloud provider environments with strong authentication and encryption of data. Future edge-security services will need to follow a zero-trust security approach to ensure access validation and identity verification. The zero trust model should allow complete visibility and insight into the activities, isolate legitimate or malicious activities, and enforce security controls automatically to contain any attack or breach.

Figure 52 depicts a conceptual edge security framework showing the different security services available on the cloud, such as secure web access, identity security, and data security. As cloud migration and 5G induced edge computing volumes increase, organizations will have to start factoring edge security into their security strategies.

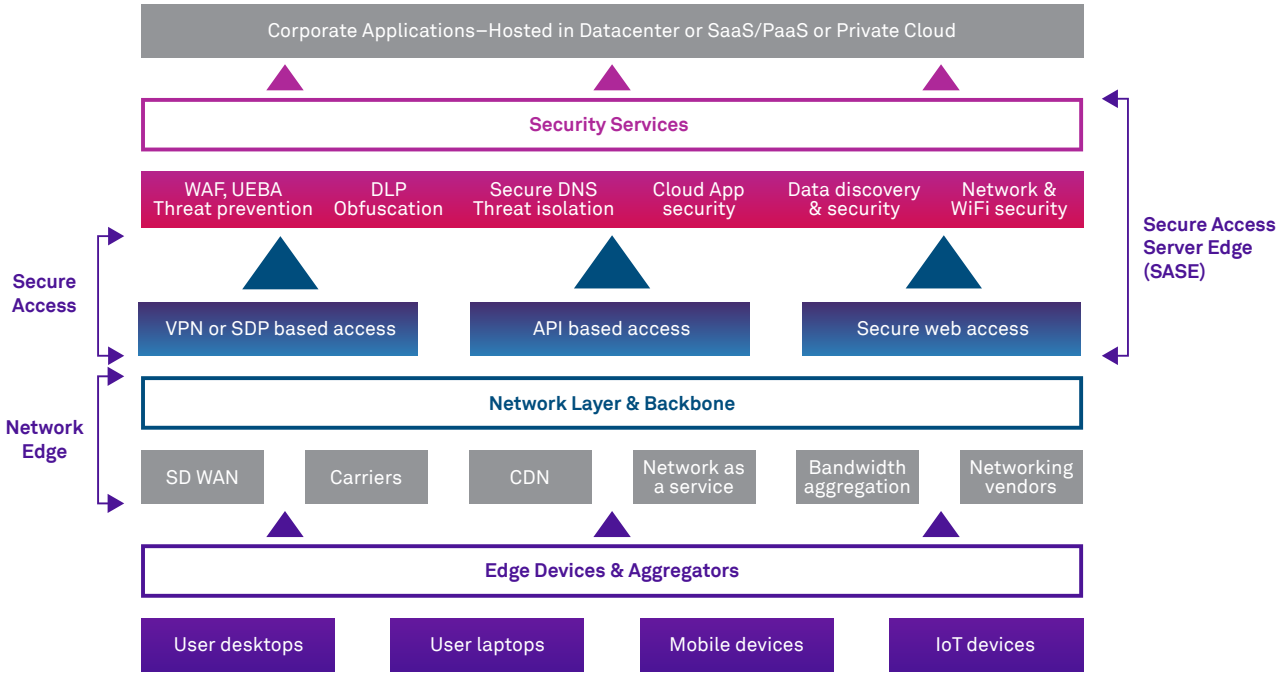


FIGURE 52 [Edge security framework]

Zero Trust: A paradigm shift

Many enterprises have enabled the process of allowing their data and applications to flow into multi-cloud environments, satellite offices, and traditional remote endpoints. OT and IoT environments are fusing to harness real-time data, derive analytics, and orchestrate business actions. In many ways, the old perimeter has broken down into smaller perimeters. However, the implicit trust that existed once you were inside the perimeter has become a millstone around the neck for most enterprises. Advanced persistent threats can lurk within the perimeter and move laterally with abandon once an entrance path is achieved. Zero trust is a paradigm shift that challenges the traditional perimeter model and demands changes in engagement rules.

In zero trust-centric approaches, the trust zone is compressed to narrow segments where continuous decision-making occurs. This approach works under the assumption that the threat actor is already present in the environment. The NIST 800-207 draft specification suggests that zero trust can roll out using different approaches. A few examples of zero trust-based models include zero trust through identity governance, zero trust through micro-segmentation, and zero trust through SDN.

The next section from Wipro's partner, ColorTokens, discusses how organizations can embark on the zero trust journey leveraging the micro-segmentation approach.

Zero Trust with micro-segmentation

The recent rise in security incidents can be largely attributed to the emergence of advanced persistent threats (APTs). In an APT-style attack, a bad actor can infiltrate the network, remain undetected for an extended period, and inflict large-scale damage.

APTs are particularly dangerous for three main reasons:

1. Organizations aren't aware that perimeter firewalls inspect at most 25% of overall traffic.
2. Many common security implementations assume that internal network traffic is trustworthy.
3. Even organizations that do scrutinize internal network traffic may be relying on outdated security tools.

It shouldn't come as a surprise, then, that APTs are inflicting severe damage to organizations around the globe. Clearly, organizations need to change the way they defend against APTs.

What is micro-segmentation?

Micro-segmentation, a key pillar of the zero trust security framework, is a security practice that divides the network into granular and mostly isolated segments. Inter- and intra-segment traffic can then be more easily monitored and controlled. In the process, organizations proactively remove built-in trust assumptions by evaluating and authorizing every network communication – a highly effective strategy to thwart APTs.

Other key benefits of micro-segmentation include:

- **Protection for business-critical applications:** Reduce the attack surface for your most vital applications and sensitive data.
- **Compliance assurance:** Simplify compliance – and cut costs and time – by reducing the scope of an audit.
- **Environment separation:** Ensure hygiene of your production environment by segregating environments in shared infrastructure.

- **Breach containment and future-proofing:** Stop breaches from spreading laterally and protect your business from future attacks.

Most micro-segmentation implementations fall into one of two categories:

- **Hybrid data center implementation:** Where the organization's infrastructure is in one or more data centers or distributed between their data center and public cloud.
- **Cloud-native implementation:** Where the organization has zero data center footprint and runs all infrastructure on one or more public clouds. In such scenarios, one must deal with not only VM-based workloads but also container and serverless workloads across multiple public cloud platforms.

In addition to the support for the spectrum of workloads as described above, organizations should also evaluate their micro-segmentation solution for these critical attributes:

- **Deep visibility:** You can't protect what you can't see. Hence, it's critical to gain deep visibility into assets and lateral traffic, along with contextual data that helps make policy decisions (see **Figure 53**).

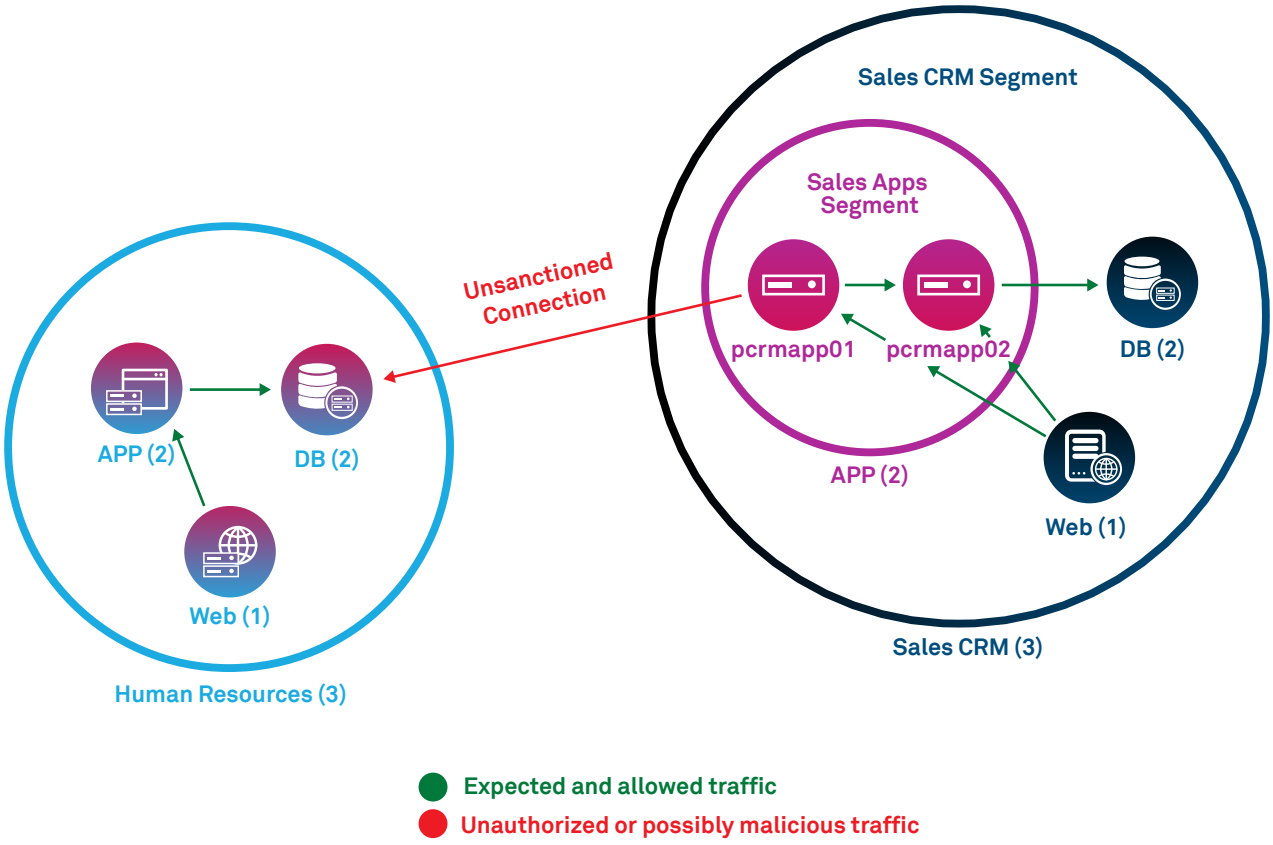


FIGURE 53 [Internal traffic visualization – Crucial for micro-segmentation]

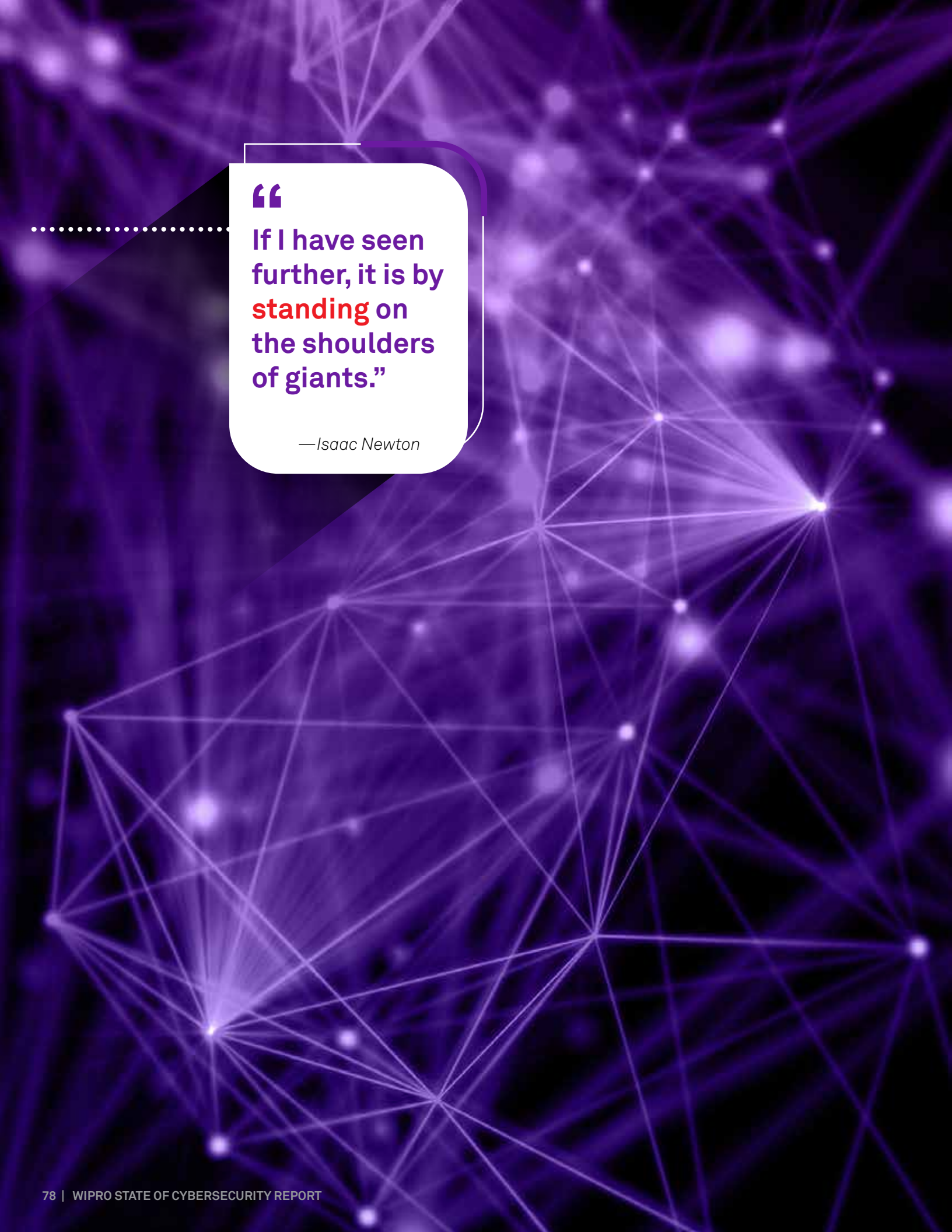
- **Adaptability:** The approach should adapt to infrastructure changes with little to no human intervention to keep operational costs down.
- **Time to value:** Organizations should plan to deploy micro-segmentation in a hybrid model with co-existing perimeter defenses as the transition happens.
- **Non-disruptiveness:** The approach should be minimally invasive to your users.

APTs will likely only continue to grow in efficacy and complexity, but the right micro-segmentation solution provides powerful capabilities to identify and thwart potentially damaging attacks. Micro-segmentation is also a key component of a strong zero trust architecture because it applies a "never trust, always verify" approach to evaluating and authorizing network communication.

Wipro's partner, ColorTokens (colortokens.com), contributed this subsection.

Security governance is a complex endeavor that needs to be driven top-down in an organization with roles and responsibilities defined down the chain of command, with relevant and timely metrics to measure its effectiveness. The flavor of the governance framework that was outlined at the beginning of the section needs to be implemented within organizations with underlying processes, procedures, and supporting functions. In addition to the governance framework, organizations need to pay attention to improving their technical controls' effectiveness as a continuous process. With ongoing governance and effective implementation of controls, organizations can elevate themselves to become more resilient to adversarial actions.

While internal enablement is supreme and needs the maximum focus, organizations cannot build up the defenses in isolation. The next section explores collaboration in the field of cyber with the external ecosystem.


“
If I have seen further, it is by standing on the shoulders of giants.”
—Isaac Newton

4

STATE OF COLLABORATION

Strong collaboration between the public and private sectors is a necessary enabler for identifying new threats in cyberspace and evolving strategies to counter them. Collaboration becomes even more pertinent when it comes to protecting national, critical infrastructure operated by the private sector. Governments worldwide are attempting to facilitate this collaboration through legal and quasi-legal constructs, including sharing networks. Given various factors, such as reputational risks and reservations around working with competitors, the private sector has been cautious in their participation. As cyber threats emanate more and more from nation-state actors, the home government's role and military doctrine around cyberattack response is coming under increasing pressure.

This section examines the sources of effective threat intelligence in enterprises and barriers in information sharing between organizations. Further on, we discuss aspects of collaboration from a supply chain standpoint and the confidence that organizations have in dealing with them. Lastly, we preview trends in cyber insurance as a risk-transfer mechanism.

To dissect the policy imperatives around attack response, we collaborated with the Blavatnik Interdisciplinary Cyber Research Center (ICRC) at Tel Aviv University for this perspective on the role of governments in active defense against external cyber aggression directed at the private sector.

Recalibrating the Shared Responsibility to Secure, Protect, and Defend

A foreign adversary contemplating an attack on a developed nation's homeland faces definite state-grade military defenses on land, sea, and air. A foreign adversary launching a direct cyberattack on a non-military homeland target will meet none. No wonder the dictum, "In cyberspace, the offense has the upper hand" has taken over.

Tel Aviv University's Blavatnik Interdisciplinary Cyber Research Center conducted major research on cyberdefense, drawing on fundamental and applied social and management science, and unique ties

with practitioners. Our findings highlight that cybersecurity requires radical, structural innovation. Some of the insights are below.

The world's major powers are failing to protect their societies and economies from cyberattacks. Recently, ransomware campaigns hit Japanese, European, and Indian firms and even entire American cities. Ransomware is ostensibly a criminal for-profit phenomenon, below the national security threshold. However, the damage is real, its operators tend to reside in adversarial jurisdictions, and their target selection and timing often resembles coercive bargaining. Commercial cybersecurity can always do better. The crux of the problem is the lack of state-grade cyber defenses that undermines the "shared responsibility" strategy.

We must accept the complex coalitions of criminal and political threat actors behind cyberattacks and innovate our defenses accordingly.

Toward sovereign cyberdefense

Israel's cybersecurity strategy, as well as the US Cyber Command, usefully distinguish three related tiers: secure, protect, and defend.

SECURE
Threat-agnostic

PROTECT
Threat-specific but passive

DEFEND
Pro-active counter-adversary strategy and capability

The five functions of the NIST Cybersecurity Framework are Identify, Protect, Detect, Respond, and Recover. The NIST Cybersecurity Framework does not include defense, and for a good reason: no functioning state expects its citizens to defend themselves. Universally, states hold a monopoly on using force and forbid their citizens from violating another nation's sovereignty. Developed nations have long-established and deployed state-grade defenses on land, sea, and air. When deterrence fails, a country's armed forces combat the attackers and shield the citizens at home.

However, states have yet to deliver on cyberdefense. Little suggests that India's forthcoming 2020 cybersecurity strategy will include defense. The UK's 2016 National Cyber Security Strategy, and the £1.9 billion of investment that came with it, reaches its conclusion in 2021. Media speculation about drawing together GCHQ and Ministry of Defense offensive cyber capability aside, British future cyberdefense posture outside the critical national infrastructure sectors is vague. The heightened threat perception may affect Australia's forthcoming 2020 strategy; its 2016 version does not mention whether, or how, its defenders will act. The US and Israel suggest some military cyberdefenses. The March 2018 "Achieve and Maintain Cyberspace Superiority" US Cyber Command vision statement declares for the first time that the American military will "defend forward." The commander of US Cyber Command claims, "We must take this fight to the enemy, just as we do in other aspects of conflict." American "persistent engagement" may mean that foreign adversaries contemplating a direct cyberattack on a non-military homeland target no longer will have it so easy. Israel's cyber defense posture has been similar for much longer: intelligence-driven pre-emption and disruption of adversarial capabilities underpin whole-of-society cybersecurity.

We should not confuse cyberdefense with militarization. Cognizant of the serious obstacles precluding military cyberdefense, several countries opt for establishing civilian cybersecurity organizations.

The short term goal: Join forces and scale up

The "In cyberspace, the offense has the upper hand" dictum is accepted. It does not have to be. While the private sector will continue to perform the lion's share of the secure and protect tasks, nation-states must accept their share of responsibility: active defense. Once governments deliver active cyberdefense, the civilian cyber burden will dwindle, liberating human, managerial, and fiscal resources to boost your core business.

Business leaders should press their relevant governments – but cannot afford to wait. Joining forces and pooling resources is a promising strategy for cost-effective business security. Some not-for-profit initiatives offer tangible business value. American Information Sharing and Analysis Centers (ISACs) offer threat and mitigation information to their respective members. Israel's National Cyber Directorate has developed the CyberNet information sharing network and stood up sectoral SOCs that offer superior situational awareness and incident management capabilities. Moreover, large managed security service providers (MSSP) are already at the frontlines of civilian cybersecurity. MSSPs can correlate huge datasets from various entities to enhance situational awareness across sectors or geographies, automate security operations at scale, and support temporary surges in demand.

Threat intelligence and incident response populate the higher-end of the services. These threat and capability-focused services resemble defense but fall short of defense in scope, capability, and authority. Private cyberdefenders do not operate to disrupt adversaries in "red space" persistently; neither can they realistically compete with state-grade adversaries. Even though the best private-sector efforts fall short of defense, global MSSPs, with their superior scale and know-how, are the toughest opponent for threat actors conducting offensive cyberspace operations (OCO) against private corporations.

Shared responsibility is the foundational principle in cybersecurity. Your security journey will be smoother with a global MSSP. However, the sooner governments take a larger responsibility for their respective citizens' cybersecurity, the brighter our common future will be.

Authored by Dr. Lior Tabansky, Blavatnik ICRC, Tel Aviv University.

Internal Organizational Collaboration

Before embarking on collaboration between the firm and external entities, the house must be in order internally. The applicability of a cyber-resilience framework was discussed in the previous section, and the significance of communication protocols through the hierarchy, including reporting of cyber risks and actions into the board of directors, was highlighted. The changing role of the CISO into a governance function with higher visibility into executive management was also a noteworthy trend. These changing dynamics have increased the stakes on the need for collaboration with other functions, such as Human Resources, Legal, CTO, CFO, Risk Management, Corporate Communications, and the CIO.

Collaboration with HR is increasing across policy definitions, employee awareness, and disciplinary actions. The Legal/General Counsel office is integral to driving regulatory compliance, post-breach response mechanisms, and the safeguarding of certain actions under attorney-client privilege. Corporate Communications is increasingly playing a critical role in customer awareness of security practices, targeted fraudulent schemes, and post-breach communications to affected parties. Above all, collaboration between business units and the CISO office is on an upward trend due to the growing instances of shadow IT and the need for security enablement for new business opportunities in the digital era.

Supply Chain Security

Businesses that depend on their supply chain for core business sustenance will need to understand and mitigate risks associated with the chain. Additionally, supply chains are essential when businesses enter new markets and need local partners to increase the speed of access.

Recently, cyberthreats have been moving up the index of general supply chain risks, as demonstrated by multiple incidents. Supply chain cyber risks can impact the cyber posture of the host company itself (cyberattacks *through* the chain), but a destabilizing cyber incident on a critical partner (cyberattacks *on* the chain) can impact the enterprise's business continuity as well. Organizations need to extend the threat intelligence they gather to their supply chain partners and conduct regular risk assessments across their chain. Supply chain access and data flows need to be segmented and monitored for anomalous activities. Organizations also need to be prepared with a response plan for an adverse scenario.

We asked respondents about their confidence in preventing attacks from within their supply chain elements. **Figure 54** shows that 94% of organizations indicated some confidence in preventing attacks through their technology providers (managed services, cloud service providers, SaaS, etc.).

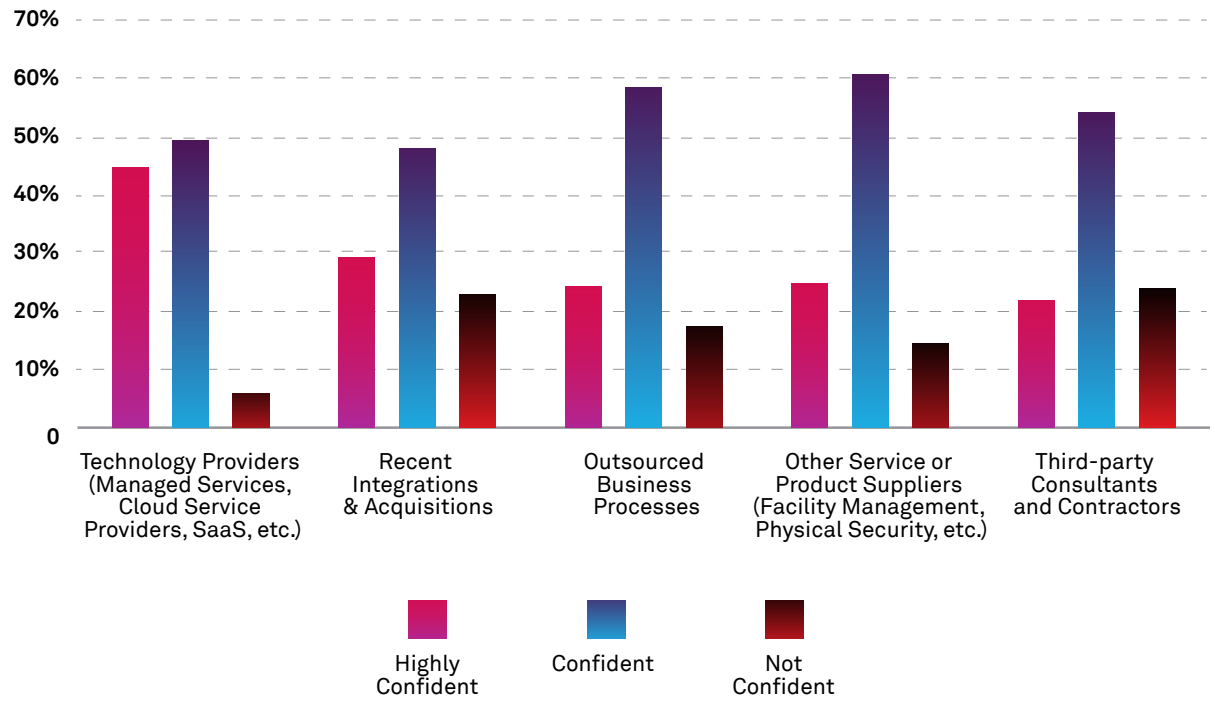


FIGURE 54 [Confidence level in preventing cyberattacks]

Many enterprises are beginning to offer the supply chains some basic security capabilities, including subscribing to security services as-a-Service to reduce risks and improve availability. Organizations need to move from treating supply chain risks as a third-party issue to dealing with them collaboratively in a holistic manner.

45%

GLOBAL INSIGHT

of respondents are highly confident in mitigating risks coming from their technology providers..

Threat Intelligence Feeds

Enterprise security teams and the monitoring systems they operate need continuous real-time data streams to retrieve information on potential threats. Knowledge about attackers' tactics, techniques, and procedures helps mitigate risks and serves as a healthy prescription for the cyber immune systems to scale up their defense mechanisms. Increasingly, security defense mechanisms have automation capabilities. Feeding real-time data into security systems, such as SIEM, to block blacklisted entities helps increase response speed and accuracy. Threat intelligence feeds serve organizations with vigilance and help narrow the window of opportunity for attackers. An organizational threat-intelligence strategy should include an array of sources and a balance of general and contextual threat intelligence.

What are the sources of threat intelligence?

In our primary research, we asked organizations to rank threat intelligence sources in order of their reliability. Gaining their lost momentum of 2018, commercial, third-party threat intelligence suppliers topped the charts with 41% while intelligence provided by SIEM vendors ranked second with 23% (**Figure 55**). 15% of respondents still rely on the National CERT Association (NCA) or a similar organization for their threat intelligence feeds.

41%

GLOBAL INSIGHT

of respondents consider commercial, third-party threat intelligence suppliers as the top source of threat intelligence feeds.

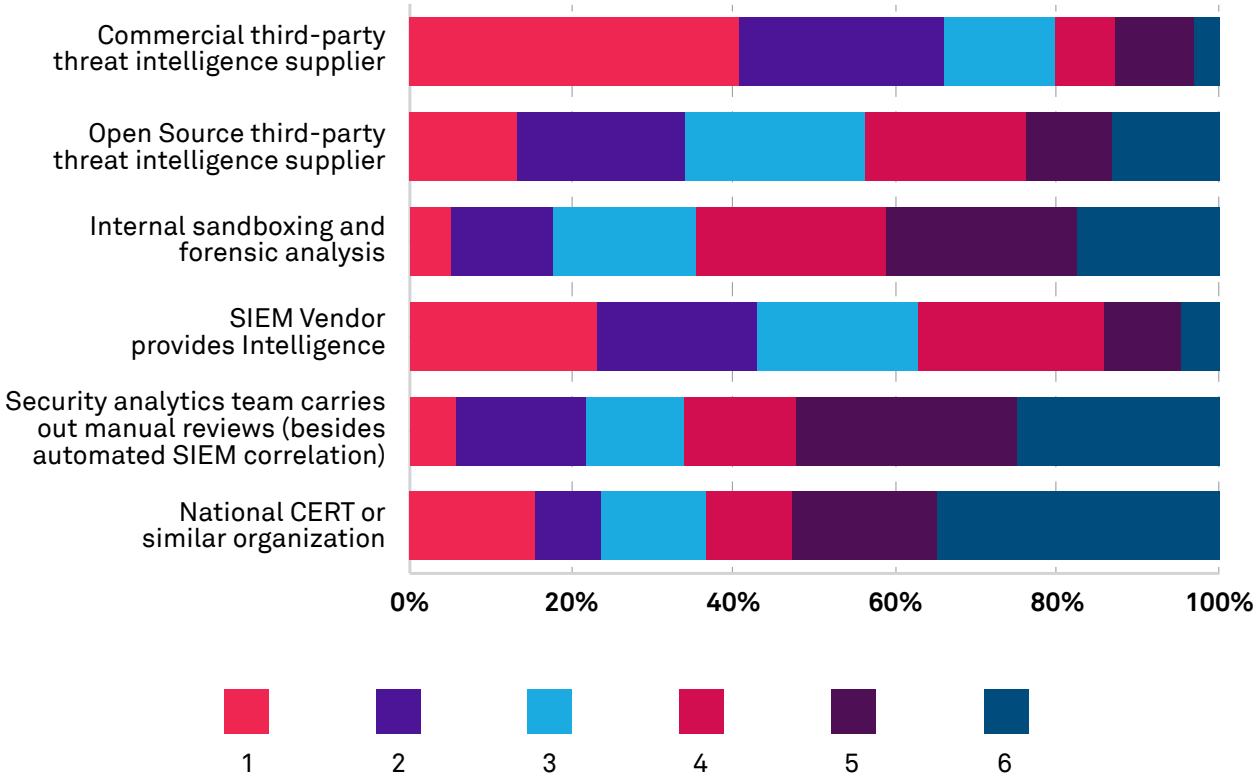


FIGURE 55 [Sources of threat intelligence for organizations]

Information Sharing

Information sharing between organizations in the private sector directly or through government intermediaries is critical to stay abreast of threat actor actions. The sharing process becomes enriched and valuable to all only when consumers become producers of intelligence, and sharing becomes bidirectional. We asked organizations about the nature of threat intelligence information they are willing to share over common forums. **Figure 56** shows an encouraging trend, where 43% of respondents were comfortable sharing the tactics, techniques, and procedures employed by threat actors in their environments – a 10% increase from the previous year. Interestingly, 57% of respondents are comfortable sharing only indicators of compromise (IoC) compared to 67% in 2018.

43%

GLOBAL INSIGHT

of responding organizations are comfortable in sharing the tactics, techniques, and procedures of attackers.

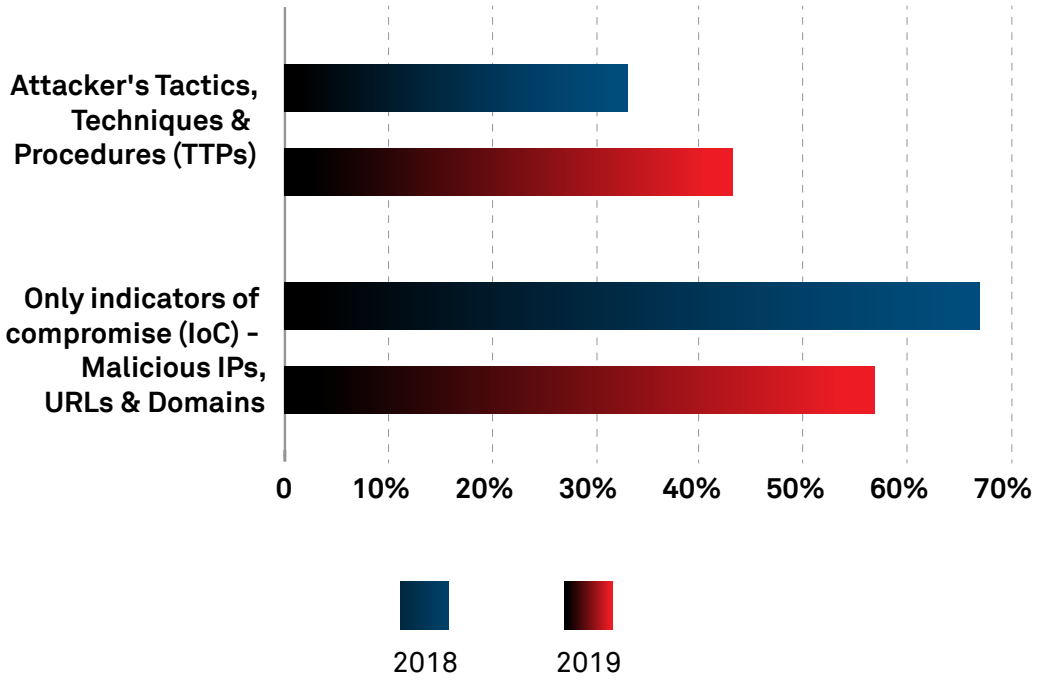


FIGURE 56 [Information organizations are willing to share]

Barriers to sharing

The above research highlights reluctance among organizations to share attack information with peers or a sharing network. We asked organizations what barriers to information sharing exist. **Figure 57** shows that 64% of survey respondents considered reputational risks the most significant obstacle to sharing threat information. 43% responded that legal barriers to public sharing existed, while 41% stated that the lack of a standard format for information exchange is critical.

64%

GLOBAL INSIGHT

of responding organizations consider reputational risk the most significant barrier against the sharing of threat information.

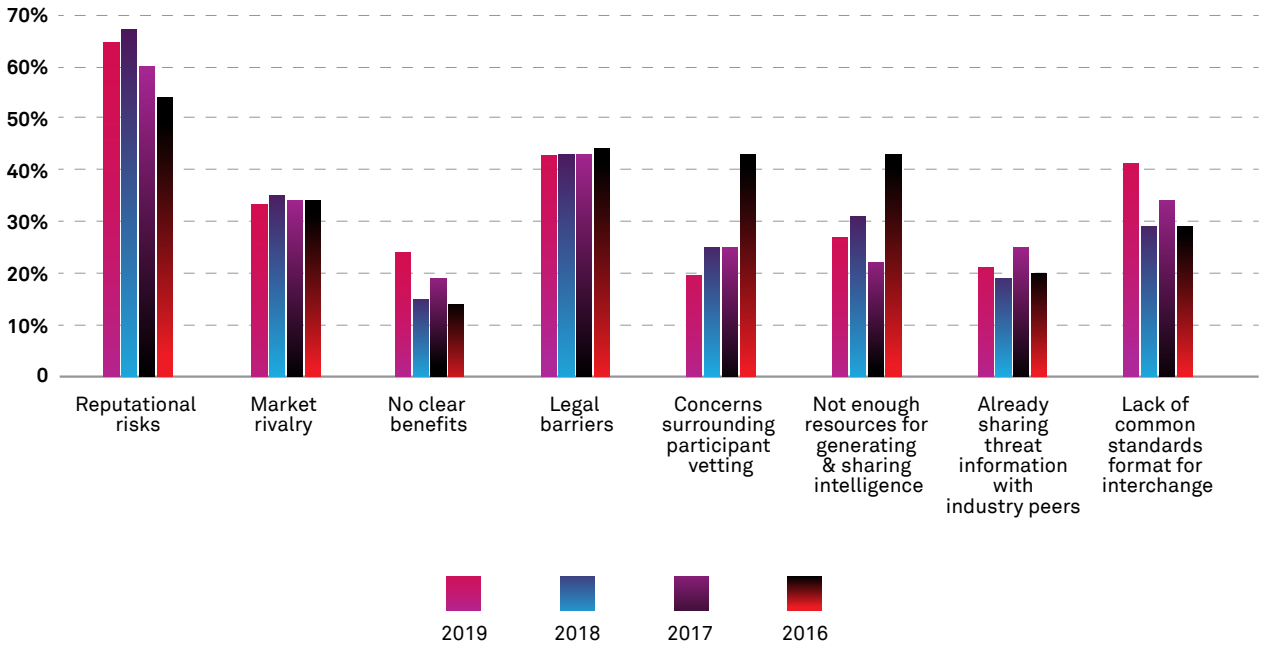


FIGURE 57 [Challenges related to sharing threat information in peer networks, 2016–2019]

Cyberattack Simulations

Cyberattack simulation exercises gauge an organization's preparedness against real-life attack scenarios. Simulations that involve multiple players in the economy across industry sectors can also test the preparedness against dovetail effects and assess collective resilience. Cyberattack simulation exercises are usually designed to imitate real-world scenarios with the intent of organizations to learn from the outcomes and recalibrate their defense strategies.

Industry simulation exercises on the rise

Wipro's research on organizational participation in simulation exercises globally revealed that 82% of the surveyed organizations participated

in cyber simulation exercises to test their defense strategies' robustness. However, 60% of respondents participated in simulation exercises coordinated by third-party service providers. Cyberattack exercises coordinated by NCA/CSIRT saw 39% participation, nearly a 10% increase from the previous year. Participation in attack simulation exercises organized by industry regulators has dipped from 28% last year to 20% currently, as shown in **Figure 58**.

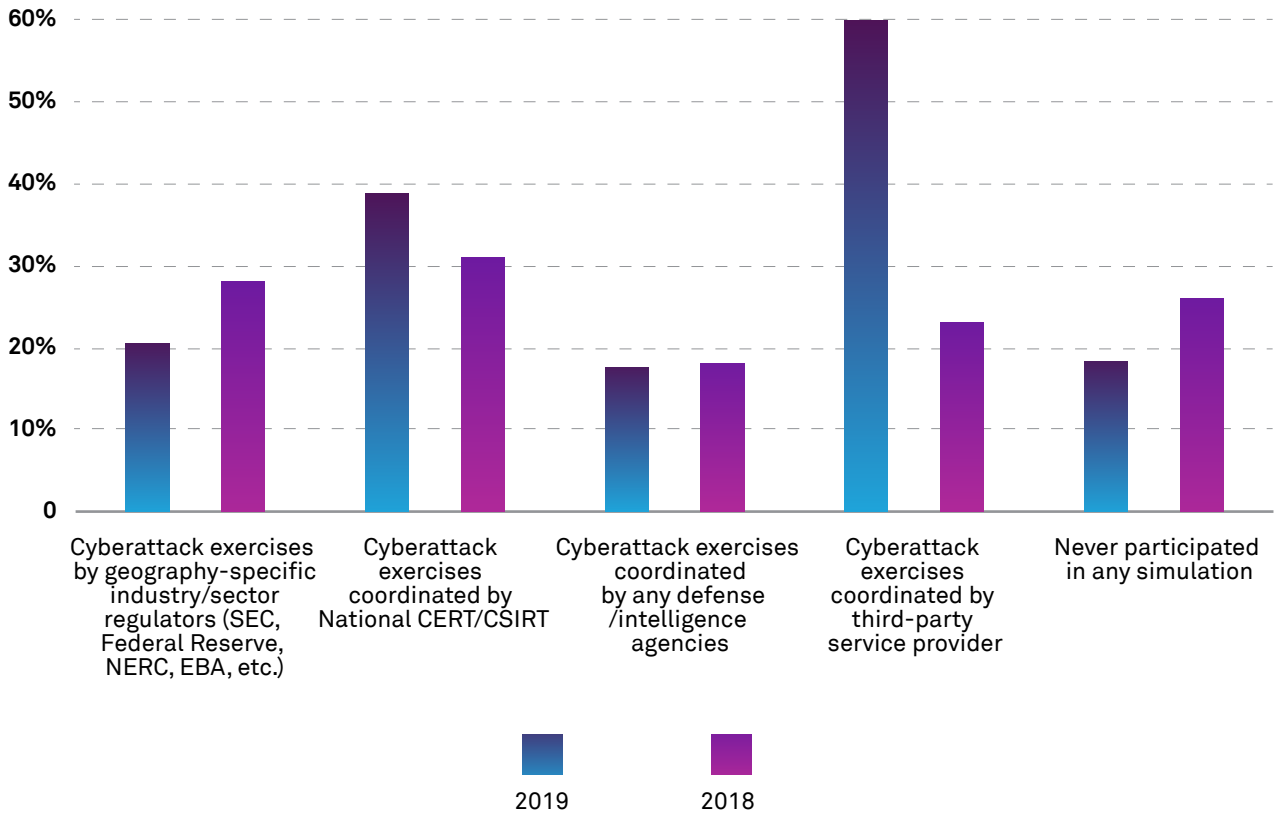


FIGURE 58 [Organizational participation in cyberattack simulation]

39%

GLOBAL INSIGHT

of responding organizations participated in simulation exercises coordinated by their National CERT/CSIRT.

86%

VERTICAL INSIGHT

of HLS respondents, 70% of CBU respondents, and 58% of MFG respondents participated in simulation exercises coordinated by third-party service providers.

Cyber Insurance

Enterprises are adopting cyber insurance as a risk transfer mechanism to hedge against the losses that unexpectedly arise from cyberattacks. With the advent of cloud and IoT and the resultant increase in attack surfaces, organizations are becoming more susceptible to cyberattacks. While a cyberattack can lead to erosion of trust and negative publicity resulting in broader business losses, organizations can leverage cyber insurance policies to cover some portions of legal and recovery expenses. Depending on the severity of the breach, insurers have various coverage policies. Typical cyber insurance policies cover costs incurred in investigations, legal processes, lawsuits, and IT recovery.

Our survey results (**Figure 59**) showed promising trends in this area. 79% of responding organizations indicated that they have cyber insurance in place, which is a 14% increase from the previous year. In this year's research, 43% of respondents indicated they carry a dedicated cyber insurance policy, which is a 4% year-over-year growth. Organizations buying multiple cyber insurance policies are trending upward, with 18% opting for this compared to 7% in 2018.

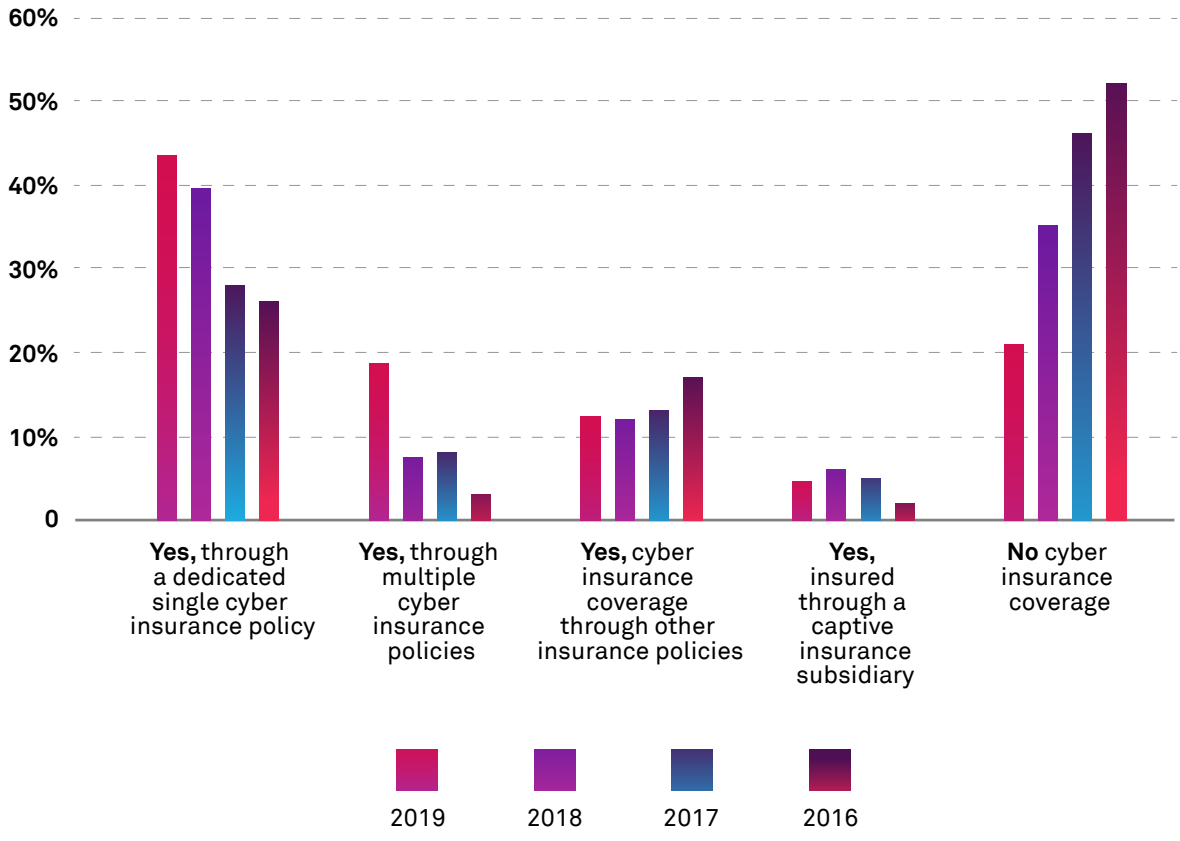


FIGURE 59 [Cyber insurance policy adoption, 2016–2019]

A word of caution

Cyber insurance policies should complement the overall risk management plan. Regard them as a fallback strategy, not a primary risk management strategy. Thoroughly understanding the finer details of the coverage, including exceptions, which vary based on geographical jurisdiction and credibility of third-party vendors, is of utmost importance.

79%

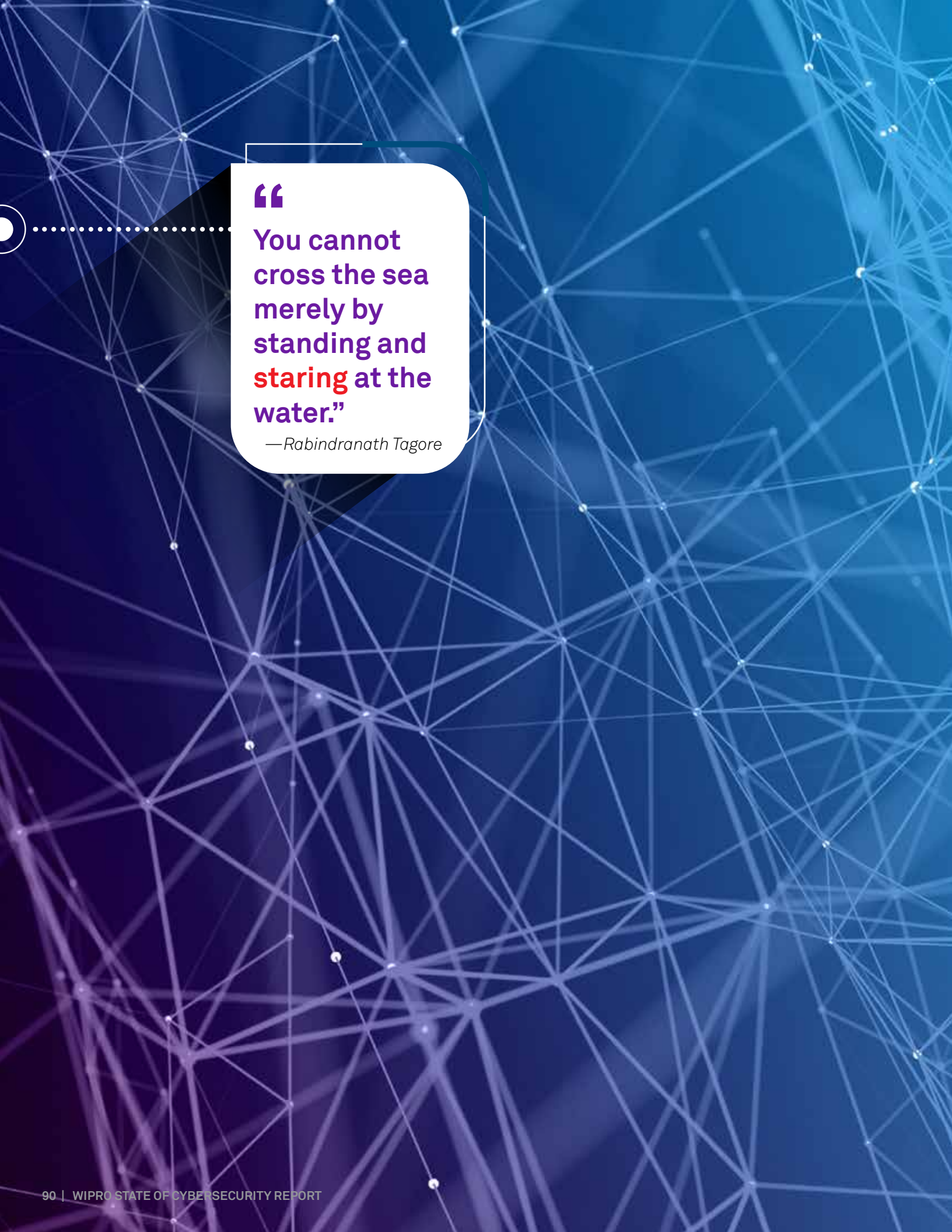
GLOBAL INSIGHT

of organizations indicated that they possess cyber insurance.

52%

VERTICAL INSIGHT

of consumer business organizations and 50% of manufacturing organizations have dedicated cyber insurance policies.



> **“You cannot cross the sea merely by standing and staring at the water.”**
>
> *—Rabindranath Tagore*

4

FUTURE OF CYBERSECURITY

The previous sections looked at the macro, meso, and micro views of cybersecurity, largely deriving trends from the last year. This section lays out a future perspective on cybersecurity by analyzing leading indicators derived from trends in academic research and venture capital investments in this space. Additionally, a point of view on the potential for decentralized trustware-based collaboration for sharing skilled resources across critical infrastructure providers during disasters is presented – based on a joint research effort between Wipro and IIT Bombay. In closing, we lay out a few cybersecurity predictions for the year ahead.

Patent Trends in Cybersecurity

One mechanism of identifying technology insights and market adoption in the cybersecurity space is to analyze the patent landscape and derive trends and insights. These insights highlight research activities, growth, and adoption of relevant technologies by different entities, such as corporations, governments, and academia. Additionally, insights from cross-sections of cybersecurity provide evidence of the use or potential use of emerging technologies in addressing problems faced by cybersecurity ecosystems.

Our cyber patent research methodology and scope have changed from the SOCR 2019 approach; hence, the findings are not directly comparable. In this year's research, we examined six emerging technologies: artificial intelligence (AI)/machine learning (ML), blockchain, internet of things (IoT),

5G, quantum computing, and digital twin across security practice areas, such as data security, application security, network security, cloud security, and endpoint security. We scanned patents filed in the past five years covering all geographies and focused our trend analysis on 20 countries: Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, Korea, Mexico, Norway, Russia, Singapore, South Africa, Sweden, Switzerland, UK, and the USA.

Cybersecurity patent filings

Since 2015, we found 9000+ cybersecurity-related patent family (technology inventions) filings, and each year saw an increase in patent filings compared to the prior year (based on standard scope of filings). A nearly 350% increase in patent filings from 2015 to 2018 indicates a rapid increase in cybersecurity research, technology growth, and adoption. **Figure 60** depicts the yearly cybersecurity patent filing trends.

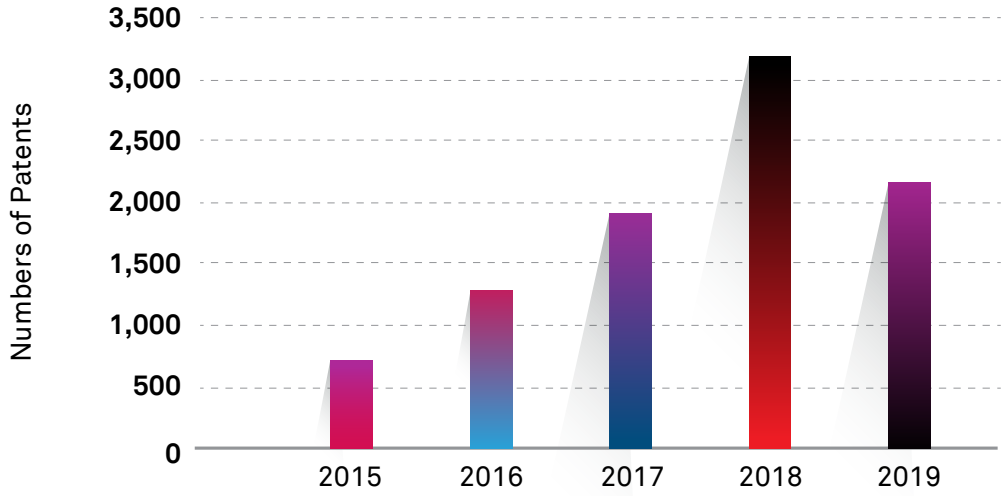


FIGURE 60 [Yearly cybersecurity patent filings*]

* Due to procedural delays in publishing patent filings across the world, the data for 2019 is incomplete.

Cybersecurity patent filings by geography

Cybersecurity patent filing analysis indicates that China has, by far, surpassed all other countries in the number of patentable inventions (**Figure 61**).

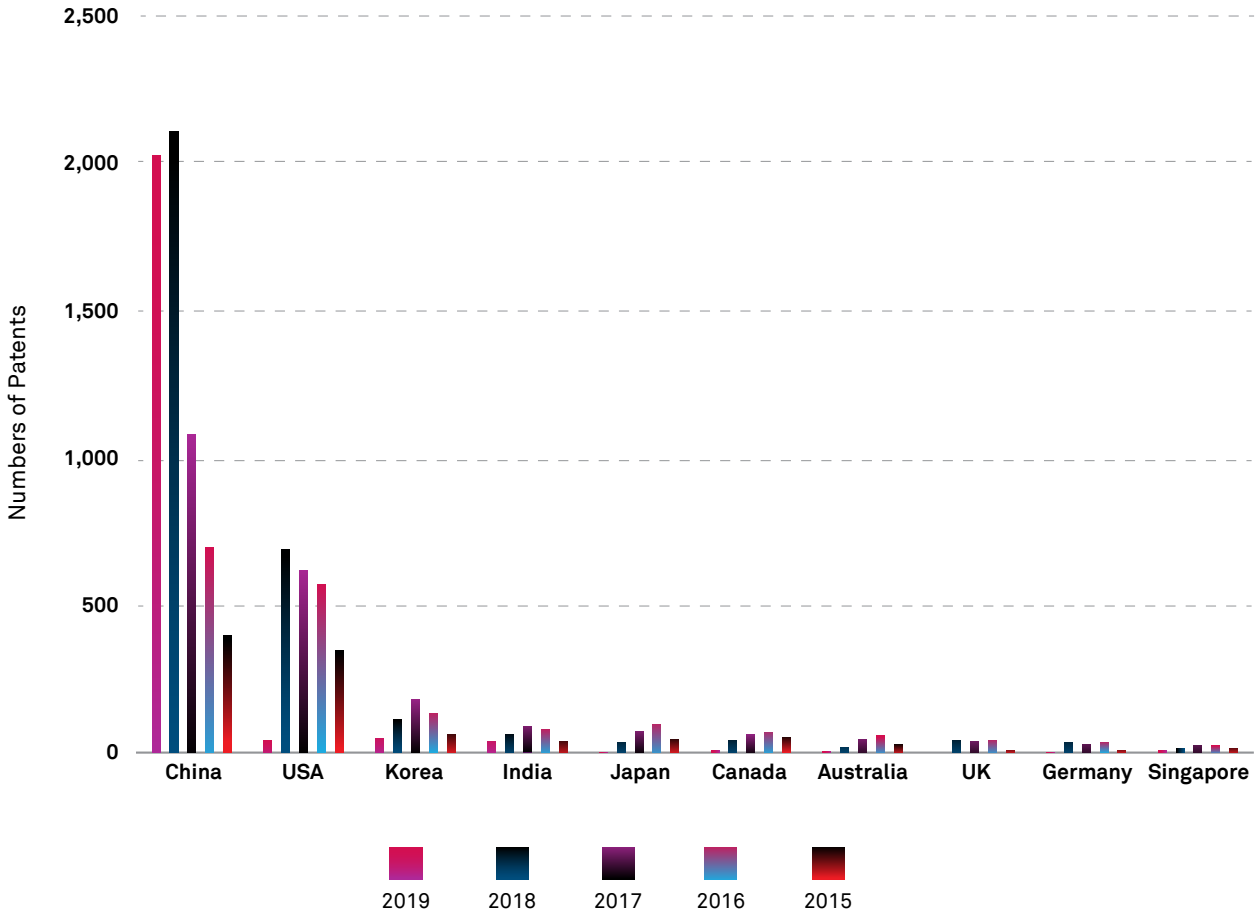


FIGURE 61 [Cybersecurity patent counts by country]

Country	2019	2018	2017	2016	2015
China	2027	2108	1080	698	397
USA	42	688	617	571	346
Korea	47	114	181	134	63
India	39	63	87	80	39
Japan	2	33	71	97	45
Canada	7	41	61	69	50
Australia	3	18	43	57	29
UK	0	41	39	40	8
Germany	1	36	29	35	6
Singapore	6	14	25	23	13

China and the US accelerated patent filings in 2018 and 2019, which is likely to continue in 2020. Six corporations and five universities of Chinese origin filed a majority of the patents in China, indicating collaboration in developing unique technology solutions for industry problems in the cybersecurity space. Figure 61 shows analysis for the top 10 countries, as the patent count was significantly less for the rest. The remaining countries appear to have stabilized or slightly reduced cybersecurity patent filing rates. Although the quality of these patents was not within the scope of our study, the trend in patent filings shows the growing importance of cybersecurity research.

Cybersecurity practice areas and emerging technologies

We further dissected the patent filing data by cross-sectioning cybersecurity practice areas and emerging technology areas, laying out a cybersecurity practice area as one dimension and selecting an emerging technology as the second dimension (**Figure 62**).

The data indicated a significantly high number of patents filed in the data security and device security areas followed by network security. When cross-sectioning cybersecurity patents with emerging technologies, we found that the majority of patents filed were in the AI/ML space. Additional findings included

- Patent filings in the data security area further broken down by emerging technologies were as follows: blockchain (1813), AI/ML (1519), IoT (441), 5G (196), quantum computing (40), and digital twin (36).
- Patent filings in the device security area broken down by emerging technologies were as follows: AI/ML (1502), IoT (616), blockchain (603), 5G (243), quantum computing (28), and digital twin (16).
- In the network security area, the splits were AI/ML (1130) followed by IoT (376), blockchain (343), 5G (198), quantum computing (21), and digital twin (6).
- Cybersecurity patent filings involving quantum computing, 5G, blockchain, and AI/ML were 1%, 7%, 25%, and 49%, respectively.

From a technology implementation point of view, AI/ML topped all cybersecurity practice areas, followed by blockchain. Among selected emerging technologies in cybersecurity, adoption of AI/ML, blockchain, and the intersection with IoT witnessed significant growth.

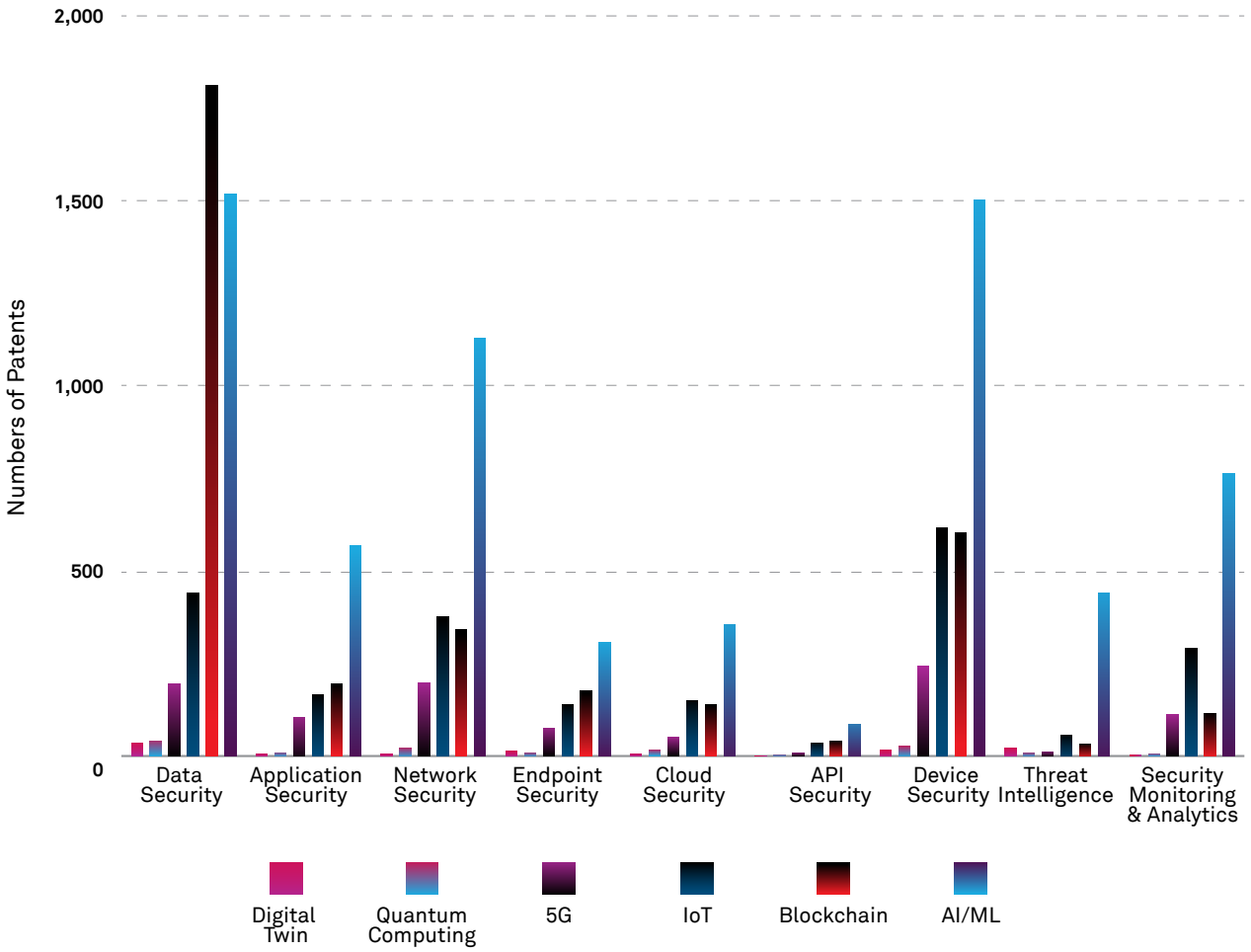


FIGURE 62 [Patents by cross-sections of cybersecurity practice areas and emerging technologies]

Functional Areas / Technology	Digital Twin	Quantum Computing	5G	IoT	Blockchain	AI / ML
Data Security	36	40	196	441	1813	1519
Application Security	5	9	104	167	194	569
Network Security	6	21	198	376	343	1130
Endpoint Security	14	8	76	140	177	307
Cloud Security	6	16	51	151	139	354
API Security	1	4	8	36	39	85
Device Security	16	28	243	616	603	1502
Threat Intelligence	21	8	10	56	31	440
Security Monitoring & Analytics	4	5	113	290	115	764

Patent filings in the AI/ML domain indicate their usage for different functions, such as risk scoring, compliance management, data discovery, threat detection, threat intelligence, threat hunting, user behavior analytics, anomaly detection, DDoS mitigation, and adaptive authentication. Cybersecurity is witnessing a rapid increase in technology research, development, and adoption because of collaborative participation among governments, industry, and academia to devise unique solutions that address emerging threats.

The proliferative growth of AI/ML- and blockchain-related research seems to reflect the need to solve problems in new and innovative ways. Although technology areas like AI/ML, blockchain, and IoT will continue to drive innovation, areas such as 5G, quantum computing, and digital twin will probably see an uptick in research focus in the coming years. API security and threat intelligence could also see more research output in the future.

Seed Investment Trends in Cybersecurity Start-ups

Start-up funding patterns by venture capitalists around the world indicate trends in promising areas that could produce disproportionate economic returns. Start-ups typically go through different stages of capital accumulation, such as Seed, Early Stage, Expansion, and Pre-Public. Although many ventures fail for various reasons, clusters of investments in similar technologies indicate market potential, and such areas need to be on cybersecurity teams' radars when laying out their roadmaps, with necessary caution. Within cybersecurity, disruption is quick, and acquisitions occur frequently. Many enterprise security teams are willing to dabble with emerging tools and technologies to mitigate new threats. The last section presented an analysis of where cybersecurity research and resultant patent filings worldwide were focused. This section identifies patterns related to seed investments in cybersecurity.

For this research, we partnered with Tracxn to gather data around cybersecurity-related seed investments during the past three years. The Wipro SOCR team classified companies into various domains based on technology and focus areas and examined the top 50 start-ups that received maximum funding. Although our coverage is not exhaustive, the research aimed to identify macro investment trends. **Figure 63** depicts the security domain categories in which companies received seed funding.

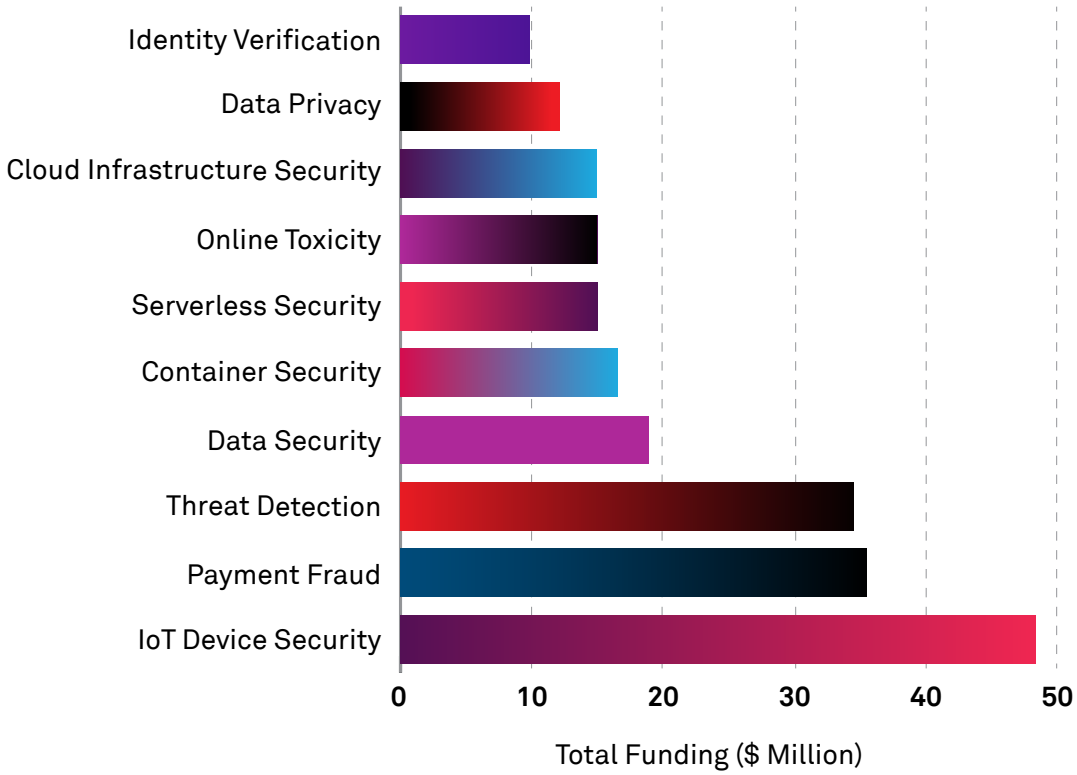


FIGURE 63 [Seed funding by category, 2016-2019]

Although the graph gives a numerical representation of the top-funded technology areas, we can highlight some patterns:

ML-BASED IDENTITY VERIFICATION
Remote identity verification is critical for the digital economy. Computer vision and ML-based solutions continue to evolve for identity verification.

SERVERLESS SECURITY
Serverless risks remain poorly understood. Serverless security solutions with function firewalling, code execution monitoring, and vaults can address the gaps.

DECENTRALIZED IDENTITY VERIFICATION
Where trust relationships do not exist, community-based vetting can help. Decentralized, consensus-based identity verification solutions are emerging.

CONTAINER SECURITY
solutions that provide guardrails for DevOps processes and runtime security continue to attract funding.

IOT DEVICE SECURITY
Key management for IoT devices becomes challenging at scale. IoT device security solutions using quantum driven key management look promising.

ONLINE TOXICITY
is a substantial problem for gaming platforms and other services consumed by children. Solutions that can track and report online toxicity will be complementary.

Wipro produced this research in collaboration with Tracxn (tracxn.com).

Decentralized Trustware-based Collaboration

Pandemics and natural disasters cause abrupt restrictions on people's movement and resources, thus creating roadblocks in addressing cybersecurity incidents. The availability of services from sectors like healthcare, transportation, communication, power, et al., is even more important in such times. To ensure the availability of critical services during exceptional times, there is a need of realigning sector-wise business processes toward a common minimum standard such that an expert from one organization can operate on the process of another organization under a well-defined, constrained, trusted, and auditable environment.

A different approach to conventional threat modeling

The current sensitive processes in critical infrastructure are typically role-based with strict separation-of-duty constraints. Maintaining the availability of experts handling these processes is a challenge. COVID-19 has forced us to rethink cybersecurity assurances by introducing a new angle to the typical threat modeling. Threat modeling usually considers the external factors impacting a system or, at most, the internal malicious activities. An open governance model where organizations allow a transparent, capability-based (instead of role-based) access to their business processes by entities verified on the trusted network can be a different approach.

Even before the pandemic hit us, there were initiatives to extend the monolithic access control model of an organization to a federated setup where more than one organization can collaborate. Such extensions of traditional access control models are known as trust management frameworks whose objective is to help the participants of the framework manage their risk while opening up their resources for external access. As organizations deploy resources (IoT) with a constrained scope of computation and storage, traditional access control models fall short of efficiently enforcing access control. There is a need for an internet-scale trust management service. The paradigm of zero trust is a step in this direction.

Trust-as-a-service using blockchain

The Linux Foundation has constituted the Trust over IP initiative to deliver trust as a service by combining cryptographic trust at the machine layer and human trust at the business, legal, and social layers. These initiatives aim to abstract out resources and users of independent organizations into a consortia-supported overlay network such that a user from one organization on the network can act on a resource from the other; provided, the users furnish their capabilities to the resource. Capability-based access control models are well studied for their suitability in a distributed environment, and it is known that they lack in communicating the state-change of a user's capability to resources. However, due to the advent of technology platforms like blockchain, it is worth revisiting these models with the help of a blockchain-based state-communication channel.

Blockchains are effective state-change communication platforms in distributed environments for various applications that are either purpose-specific or general-purpose. Any client connected to a blockchain platform can be assured of the state-change in the most reliable fashion known to us so far.

Capability based models using blockchain

With the gamut of new and old technological models available to us, it is possible to address the impact of the COVID-19 scenario on prevalent threat models by realigning the existing business processes of an organization from

role-based models to capability-based models with support from blockchain platforms.

Should there have been a wide-scale acceptance and deployment of DID (Distributed Identity Network), it would have been possible to address the crunch on expert human resources by allowing them to participate in process execution beyond their routine scope of work. This assumes that there is a redesigning of business processes in such a modular way that the experts familiar to a sector-specific business process in a host organization can operate upon a module of a process hosted in a foreign organization while revealing only the data relevant to the operations assigned to the external expert. Trust plays a significant role in realizing this vision.

The key challenges in realizing this futuristic vision of cybersecurity are:

- **Formation of a platform:** Motivating sector-specific players to form a platform for exchanging their requirements and available expertise to others
- **Identification of modular boundaries** of sector-specific business processes (health, transport, power, etc.)
- **Overlay network of segmented services:** Integration of service platforms like identity, event orchestration, escrow, payment
- **Zero Trust–based** minimalistic access enablement
- **Protection of internal processes** from networked and non-networked entities
- **The anonymity of organizations** affected by an incident
- **Reliability of patches** developed by an external expert
- **Privacy of experts** participating on the network
- **Escrow facility** via contracts to capture conditions of deliverables and payments

Addressing the new normal

Cybersecurity in the context of COVID-19 is a human-centric problem. Assuming that a consortia-supported trust management network is in place, identification of the parts of a business process that can be automated as a smart contract and its execution that can be controlled by an entity verified by the network is an area that demands further investigation.

In the post-COVID-19 era, cybersecurity implementations will have to rely on trustware – technologies and governing models that allow organizations to supplement their prevalent access control mechanism – to adapt to its collaborative needs and give assurances to the trust it is placing on the external entities. **Figure 64** depicts a trustware-assisted relationship between two organizations that allows each party to rely upon technological and non-technological means to derive a level of trust to agree on a decision.

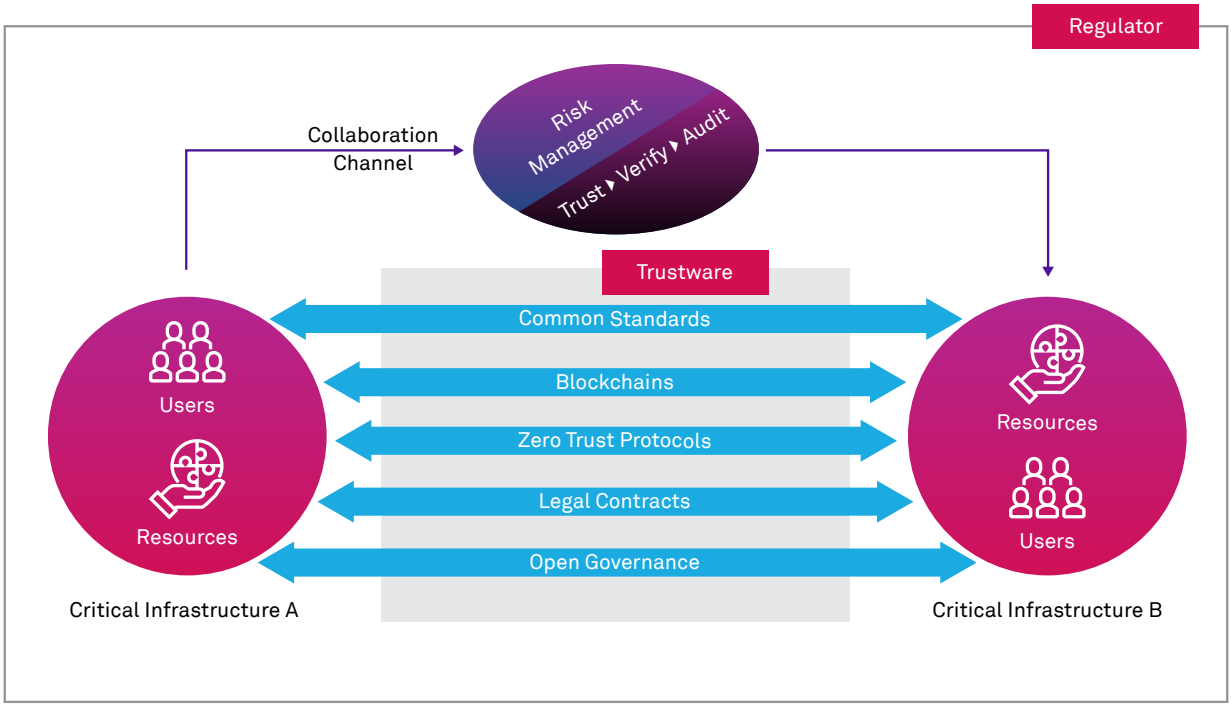


FIGURE 64 [Trustware-based collaboration mechanism]

The technological means may encompass various blockchain-based networks used for identity or attestation, for example; and the non-technological means, like legal contracts, help complement incomplete conditions (unforeseen) that cannot be effectively addressed by technological means. The figure highlights a setup of collaborators being observed by their regulator, implying that only need-to-know data is being exposed to the regulator. Trustware encapsulates a broad set of trust-enhancing technologies, frameworks, and standards. Trust-as-a-service will be a pressing demand, and organizations will have to realign their business processes to take advantage of this service. This brings us to a new challenge – guaranteeing security and governance assurances once organizations start deploying trustware into their business processes.

In a joint research collaboration, Wipro Technologies (a member of ToIP Foundation) and IIT Bombay are devising a framework to help system designers to juxtapose security properties for a new or re-engineered business process that rely on blockchains (a type of trustware) to derive digital trust amongst distributed entities. This is an important step in assessing the security assurances of a newly composed business process and its effective governance with a clear understanding of the ramifications of each design decision.

Authored by **Professor R. K. Shyamasundar** and **Dr. Vishwas Patil**,Department of Computer Science and Engineering, Indian Institute of Technology, Bombay and Vinod Panicker, Sr Member, DMTS, CRS, Wipro.

Cybersecurity Predictions

It is sometimes hard to carry out a post mortem analysis of cybersecurity-related events, given the challenges in attribution, the availability of reliable data, and the secrecy surrounding this space due to legal challenges. Making predictions is an even more difficult task. The trends presented here are evident from emerging intelligence patterns and collective patterns of organizational behavior.

1. Security attacks against cognitive systems

Adversaries are increasingly interested in targeting ML systems through traditional attacks leading up to opportunities for data poisoning, extraction of confidential ML model data, etc. Such attacks, if successful, can be leveraged to effect favorable transactional outcomes for adversaries.

2. Attacks on OT and cyber-physical systems to escalate

Attacks on national, critical infrastructure, such as utilities, telecom, power, healthcare, emergency services, etc. are expected to increase, fueling changes in national cyber doctrines and the defense measures that states will take.

3. Penal attacks on the private sector, triggered by global trade wars

As countries emerge from the ravages of the pandemic-induced recession, trade protectionism is expected to rise due to geopolitical tensions. Cyberattacks are an expected lever for nation-states through their proxies to impose punitive damages on enterprises involved in the trade scenarios.

4. Espionage attacks on emerging Digital Twins

As the world economies push for reducing carbon emissions, lean manufacturing, and net-zero goals, the role of digital twins that replicate real-world physical systems will become increasingly critical to model system behavior. Such digital twins will become the target of attacks to leapfrog technology development cycles or serve as a training ground prior to actual attacks on physical systems.

5. Global election attacks and disinformation campaigns

Disinformation campaigns orchestrated by nation-states to influence public perception and attacks on election infrastructure and political outfits to leak information and influence outcomes are expected to rise as multiple countries head for their national and local elections.

6. API abuse: the Achilles heel of cloud-driven digitalization

APIs have become the glue connecting business services within and outside enterprises. Insecure APIs will expand the attack surface of organizations significantly with cloud and IoT expansion.

7. AI/ML and SOAR to mainstream cybersecurity automation and reduce skill gaps

The need for speed in detection, triage, and response and the evident shortage in technical cyber skills will see AI/ML and automation step in to fill the gaps.

8. Consumer IoT security legislation to emerge

Countries are expected to push for minimum security and privacy standards for consumer IoT devices through recommended security practices. These practices are expected to evolve into full-scale legislation, as is already evident in North America.

9. RPA/BOT security governance will move up priorities

Mushrooming of RPA and other forms of technical and business process automation expand risks through digital identities and authorizations that BOTs possess.

10. Board-inclusive wargaming on cyber catastrophes

Boards will need to move from being appraised of changing cyber risks to being an inclusive participant in risk management.

Security Trends by Industry

SECURITY TRENDS BY INDUSTRY

BANKING, FINANCIAL SERVICES & INSURANCE

SECURITY GOVERNANCE

42% of CISOs are responsible for ownership of data privacy.

SECURITY BUDGET

40% of organizations have a security budget that is more than **8%** of the IT budget.

FACTORS DRIVING BUDGET

70% said that new regulations are the reason for increase in budget allocation.

54% said that board oversight of cybersecurity is the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

44% said that security orchestration and automation is a top priority.

18% said that hybrid security solutions are a top investment priority.

TOP 2 CYBER RISKS

87% said email phishing is a top risk.

54% said third-party unprotected services are a top risk.

SUPPLY CHAIN SECURITY

54% said they are highly confident about preventing risks from technology providers.

CYBERATTACK CONSEQUENCES

74% said a bad cyber event causes damage to brand reputation.

SIMULATION EXERCISES

54% said they participate in cyberattack exercises coordinated by a third-party service provider.

52% said they participate in cyberattack exercises coordinated by National CERT/CSIRT.

11% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

73% said maintaining endpoint cyber hygiene has been a challenge.

66% said VPN & VDI remote access risks have been a challenge.

TOP PRIORITIES DURING COVID-19

- Increase remote access/ VPN capacity enablement
- Enabling secure collaboration

TOP PRIORITIES POST-COVID-19

- Secure digital transformation initiatives
- Increase consumption of Security-as-a-Service

SECURITY TRENDS BY INDUSTRY
COMMUNICATIONS

SECURITY GOVERNANCE

40% of CPO/DPO are responsible for ownership of data privacy.

SECURITY BUDGET

20% of organizations have a security budget that is more than **15%** of the IT budget.

FACTORS DRIVING BUDGET

69% said that board oversight of cybersecurity is the reason for increase in budget allocation.

63% said that new regulations are the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

50% said zero trust architecture is a top priority.

25% said that security orchestration and automation is a top priority.

TOP 2 CYBER RISKS

100% agree email phishing is a top risk.

71% said cloud hosting is a top risk.

SUPPLY CHAIN SECURITY

47% said they are highly confident about preventing risks from technology providers.

CYBERATTACK CONSEQUENCES

74% said a bad cyber event causes missed business opportunities.

SIMULATION EXERCISES

46% said they participate in cyberattack exercises coordinated by a third-party service provider.
38% said they participate in cyberattack exercises coordinated by National CERT/CSIRT.
15% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

50% said privilege escalation on cloud infrastructure has been a challenge.

50% said maintaining endpoint cyber hygiene has been a challenge.

TOP PRIORITIES DURING COVID-19

Increase remote access/ VPN capacity enablement

Increased device security (EDR, etc.)

TOP PRIORITIES POST-COVID-19

Implement zero trust architecture

Increase secure cloud migration to scale quickly

SECURITY TRENDS BY INDUSTRY
CONSUMER

SECURITY GOVERNANCE

77% of CISOs report to CIO.

SECURITY BUDGET

9% of organizations have a security budget that is more than **10%** of the IT budget.

FACTORS DRIVING BUDGET

67% said that board oversight of cybersecurity is the reason for increase in budget allocation.

54% said that new technology adoption is the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

29% said that zero trust architecture is a top priority.

21% said hybrid cloud architecture is a top priority.

TOP 2 CYBER RISKS

86% said email phishing is a top risk.

67% said lack of security awareness/employee negligence is a top risk.

SUPPLY CHAIN SECURITY

57% said they are somewhat confident about preventing risks from technology providers.

CYBERATTACK CONSEQUENCES

75% said a bad cyber event causes damage to brand reputation.

SIMULATION EXERCISES

70% said they participate in cyberattack exercises coordinated by a third-party service provider.

15% said they participate in cyberattack exercises coordinated by National CERT/CSIRT.

30% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

57% said monitoring threats on unmanaged devices has been a challenge.

57% said changing network topology has been a risk.

TOP PRIORITIES DURING COVID-19

- Increase remote access/ VPN capacity enablement
- Enabling secure collaboration

TOP PRIORITIES POST-COVID-19

- Secure digital transformation initiatives
- Increase secure cloud migration to scale quickly

SECURITY TRENDS BY INDUSTRY

ENERGY, NATURAL RESOURCES & UTILITIES

SECURITY GOVERNANCE

24% of CISOs report to CEO.

SECURITY BUDGET

33% of organizations have a security budget that is more than **10%** of the IT budget.

FACTORS DRIVING BUDGET

54% said that new regulations are the reason for increase in budget allocation.

69% said that board oversight of cybersecurity is the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

43% said that security orchestration and automation is a top priority.

36% said that IT/OT initiatives are a top investment priority.

TOP 2 CYBER RISKS

71% said email phishing is a top risk.

71% said IT/OT integrations is a top risk.

SUPPLY CHAIN SECURITY

54% said they are not confident about preventing risks from third-party consultants and contractors.

CYBERATTACK CONSEQUENCES

64% said a bad cyber event causes loss of revenue due to non-availability of services at critical times.

SIMULATION EXERCISES

64% said they participate in cyberattack exercises coordinated by National CERT/CSIR.

55% said they participate in cyberattack exercises coordinated by a third-party service provider.

9% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

80% said maintaining endpoint cyber hygiene has been a challenge.

80% said monitoring threats on unmanaged devices has been a challenge.

TOP PRIORITIES DURING COVID-19

Increase remote access/ VPN capacity enablement

Increased device security (EDR, etc.)

TOP PRIORITIES POST-COVID-19

Secure digital transformation initiatives

Increase secure cloud migration to scale quickly

SECURITY TRENDS BY INDUSTRY

HEALTHCARE & LIFE SCIENCES

SECURITY GOVERNANCE

52% of CISOs report to CIO.

SECURITY BUDGET

14% of organizations have a security budget that is more than **12%** of the IT budget.

FACTORS DRIVING BUDGET

71% said that a breach related to peer/competitor is the reason for increase in budget allocation.

43% said that a change in CISO/CXO leadership is the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

44% said that security orchestration and automation is a top priority.

17% said that DevSecOps is a top priority.

TOP 2 CYBER RISKS

71% said cloud hosting is a top risk.

72% said lack of security awareness/employee negligence is a top risk.

SUPPLY CHAIN SECURITY

43% said they are not confident about preventing risks from third-party consultants and contractors.

CYBERATTACK CONSEQUENCES

40% said a bad cyber event causes loss of business due to erosion of trust.

SIMULATION EXERCISES

86% said they participate in cyberattack exercises coordinated by a third-party service provider.

29% said they participate in cyberattack exercises coordinated by defense/intelligence agencies.

29% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

83% said maintaining endpoint cyber hygiene has been a challenge.

67% said monitoring threats on unmanaged devices has been a challenge.

TOP PRIORITIES DURING COVID-19

- Increase remote access/ VPN capacity enablement
- Enabling secure collaboration

TOP PRIORITIES POST-COVID-19

- Increase consumption of Security-as-a-Service
- Secure digital transformation initiatives

SECURITY TRENDS BY INDUSTRY

MANUFACTURING

SECURITY GOVERNANCE

71% of CISOs report to CIO.

SECURITY BUDGET

46% of organizations have a security budget that is less than **6%** of the IT budget.

FACTORS DRIVING BUDGET

54% said that new regulations are the reason for increase in budget allocation.

54% said that board oversight of cybersecurity is the reason for increase in budget allocation.

TOP INVESTMENT PRIORITY

40% said that security awareness and training is their top most investment priority.

50% said that zero trust architecture is a top priority.

TOP 2 CYBER RISKS

100% said email phishing is a top risk.

77% said lack of security awareness/ employee negligence is a top risk.

SUPPLY CHAIN SECURITY

58% said they are not highly confident about preventing risks from supply chain providers.

CYBERATTACK CONSEQUENCES

74% said a bad cyber event causes loss of revenue due to non-availability of services at critical times.

SIMULATION EXERCISES

58% said they participate in cyberattack exercises coordinated by a third-party service provider.
17% said they participate in cyberattack exercises coordinated by National CERT/CSIRT.
42% said they never participated.

IT SECURITY CHALLENGES DURING COVID-19

67% said monitoring threats on unmanaged devices has been a challenge.

67% said maintaining endpoint cyber hygiene has been a challenge.

TOP PRIORITIES DURING COVID-19

Rolling out multi-factor authentication

Increase remote access/ VPN capacity enablement

TOP PRIORITIES POST-COVID-19

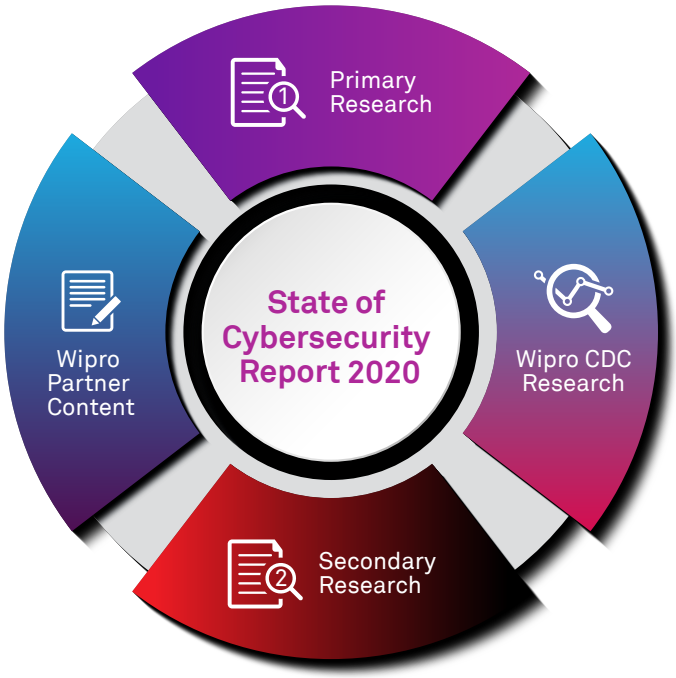
Increase secure cloud migration to scale quickly

Secure digital transformation initiatives

METHODOLOGY & DEMOGRAPHICS

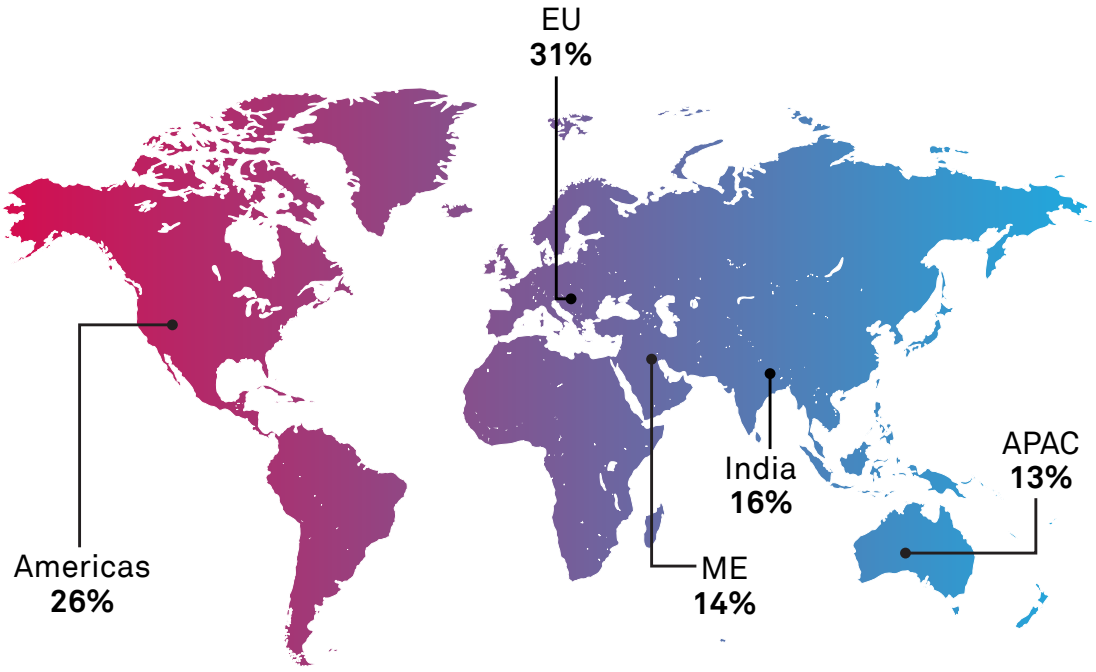
Wipro developed the State of Cybersecurity Report 2020 over four months. The methodology applied was four-pronged:

1) Primary research (external)
2) CDC research (primary research through our Cyber Defense Centers)
3) Secondary research
4) Wipro product, academia, and industry collaboration



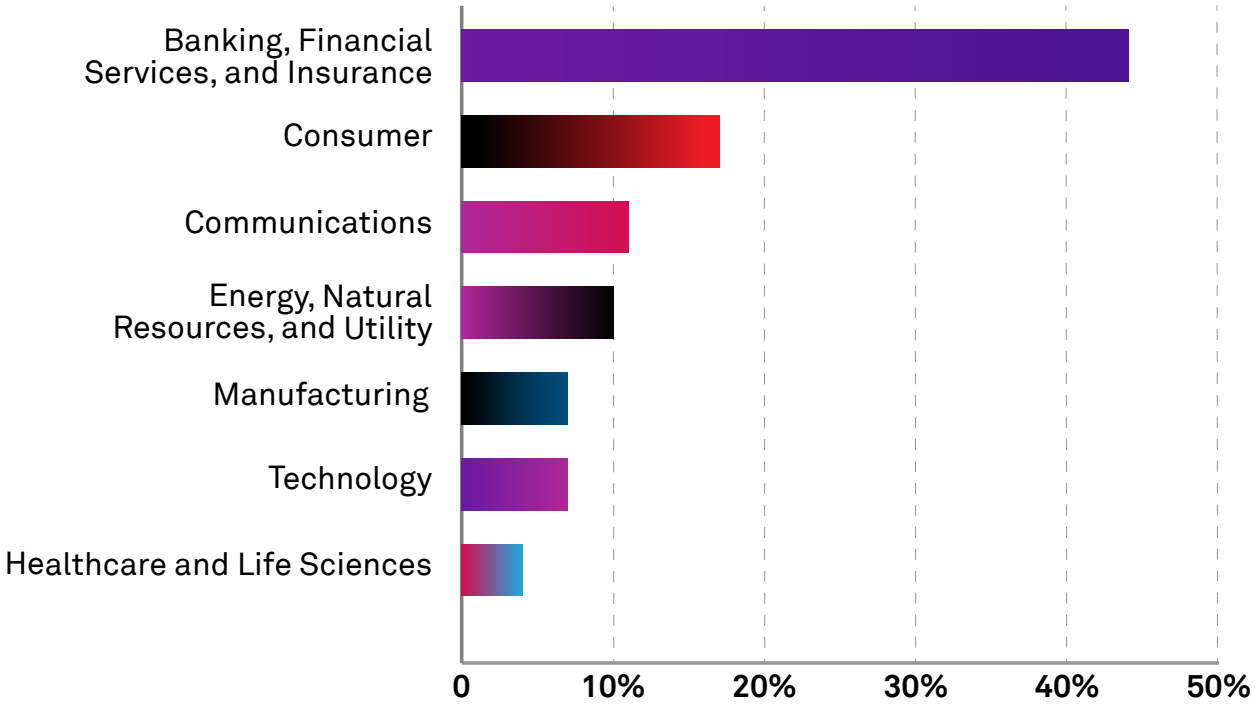
The primary research (external) involved surveying security leadership throughout Wipro's customer base. A questionnaire with 30+ questions around trends, governance, security priorities, and best practices was administered over two months. The survey was anonymous, and the responses were processed at an aggregated level to arrive at insights. The CDC research was conducted on aggregated data from Wipro's CDCs across North America, Europe, India, Middle East, and the APAC region.

The secondary research, carried out by the SOCR core team, involved various public databases and research platforms to supplement the primary research and CDC data analysis and correlate trends in the cybersecurity domain. This year, Wipro collaborated with our Ventures partners, security product partners, and academia to bring together their perspectives on the changing cybersecurity landscape.

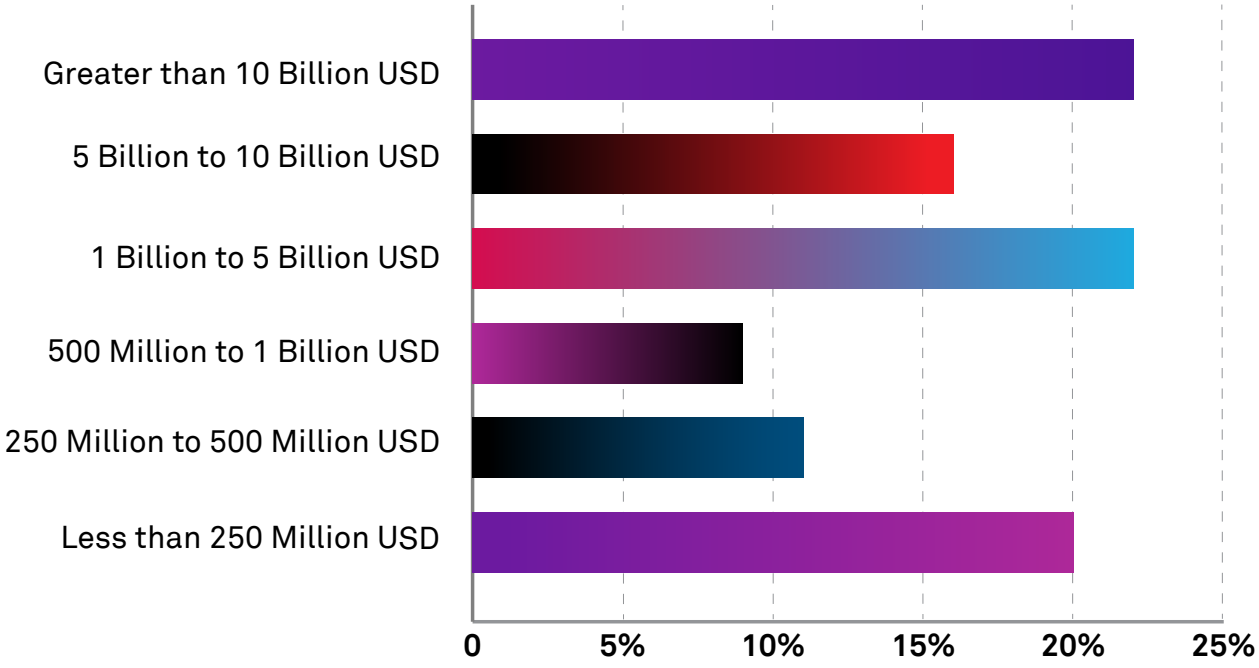


Respondent's Geography

Organizations surveyed by vertical



Organizations surveyed by revenue



CLASSIFICATION OF INDUSTRY VERTICALS IN THE REPORT

BANKING, FINANCIAL SERVICES, & INSURANCE (BFSI)

Banking, insurance, capital markets, and financial institutions

COMMUNICATIONS

Telecommunications, network equipment providers

CONSUMER

Retail, consumer goods, travel & transportation, hospitality

ENERGY, NATURAL RESOURCES & UTILITIES (ENU)

Natural resources, oil and gas, utilities

HEALTHCARE & LIFE SCIENCES

Healthcare, medical devices, pharmaceutical

MANUFACTURING

Industrial and process manufacturing, engineering, automotive

KEY STATISTICS: MAKING OF SOCR 2020

35 countries covered

194 Organizations Surveyed

225
unique malware risk/ threats analyzed

6,500+
CDC incidents analyzed

23
countries breach notification & cross-border transfer laws analyzed

30+
security products analyzed for vulnerabilities

1.1 M
cyber intelligence alerts analyzed by our venture partner insights

CONTRIBUTING PARTNERS

CREDITS & KEY CONTRIBUTORS

Core Research & Editorial Team

Josey V George
Editor-in-Chief & Distinguished Member of Technical Staff, Wipro | Chevening Fellow for Cybersecurity

Kartik Upadhyay
Sub-Editor & Cybersecurity Consultant, CRS, Wipro

Niraj Patil
Sub-Editor & Cybersecurity Consultant, CRS, Wipro

Marketing & Content Team

Vamsi Krishna Vinjamuri
Global Head, Strategic Marketing, CRS, Wipro

Nicole Sholly
Editorial Director, Wipro

Christopher Dutton
Global Head of Marketing Operations, Wipro

Mohona Mukhopadhyay
Assistant Manager, Strategic Marketing, CRS, Wipro

Lia Parisyan
Director of Content Marketing, Wipro

Gurvinder Sahni
General Manager, Strategic Marketing, Wipro

Content & Research Inputs

Sudheesh Babu
General Manager, Head of Strategy and M&A, CRS, Wipro

Mark Brown
Practice Head, IoT / OT, CRS, Wipro

Angshuman Chattopadhyay
Practice Director, Infra Security, CRS, Wipro

CDC Team, CRS, Wipro
Radhakrishna P S, Sankaranarayanan, Cheshta Batra

Vinod Panicker
Chief Architect, CRS, Wipro and DMTS, Senior Member

Deepak Kothari
Lead Architect, Cyber Defense Platform, CRS, Wipro

CTO Office, Wipro
Sudipta Ghosh, A. Raju

Institutional Contributors

Dr. Lior Tabansky
Blavatnik Interdisciplinary Cyber Research Center,
Tel Aviv University

Professor R. K. Shyamasundar and Dr. Vishwas Patil
Indian Institute of Technology, Bombay

ABOUT WIPRO CYBERSECURITY & RISK SERVICES

Wipro's Cybersecurity & Risk Services (CRS) enables global enterprises to enhance their business resilience through an integrated risk management approach. Wipro empowers customers to rethink their cybersecurity strategy through our expertise and experience with best practices across people, process, and technology. Leveraging a large pool of experienced security professionals located across our global Cyber Defense Centers (CDC), we provide consulting and advisory, system integration, and managed services to help customers transform their security posture. Through our venture capital arm, Wipro Ventures, we've invested in leading-edge cybersecurity start-ups, each one building advanced products that address the biggest challenges in the world today. Our deep network of technology partners, experienced staff, and flexible service models make us a partner of choice for customers to manage their cyber risks.

Contacts

CRS Marketing
cybersecurity.services@wipro.com

Previous editions of State of Cybersecurity Report

REFERENCES

- https://www.cfr.org/cyber-operations/
- http://cve.mitre.org
- http://www.cvedetails.com
- https://www.dlapiperdataprotection.com/
- https://www.khaleejtimes.com/news/government/sheikh-mohammed-enacts-new-difc-data-protection-law
- https://www.lexology.com/library/detail.aspx?g=27e0f500-7819-41ab-8b9f-91cdd7924f8a
- https://www.bbc.com/news/technology-53418898
- https://iapp.org/news/a/japan-enacts-the-act-on-the-protection-of-personal-information/
- https://www.helpnetsecurity.com/2020/03/27/ddos-attacks-increase-2020/>
- https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019
- https://www.upguard.com/blog/biggest-data-breaches
- https://csrc.nist.gov/publications/detail/sp/800-207/draft
- https://www.forbes.com/sites/oracle/2019/01/17/chief-information-security-officer-priorities-for-2019/#5fa926046937