State of Cybersecurity Report 2018

Foresight for the global cybersecurity community

Contents

Foreword

Sheetal Sharad Mehta

Global Head and VP – Cybersecurity & Risk Services, Wipro Ltd.

Twitter@Sheetal_S_Mehta

linkedin.com/in/sheetal-mehta-026aa34

Welcome to the 2nd edition of the State of Cybersecurity Report from Wipro. The year that has gone by has witnessed some of the most visible cyber-attacks in recent times through ransomware that propagated as the world media reported on it, making this menace very real to society, large corporations and governments, all at the same time.

Today, cybersecurity has become a boardroom concern for organizations across verticals, revenue bands and geographies. Governments have been strengthening regulations to force data owners to exercise their responsibility to protect the privacy of data. In addition to this, in the event of a data breach or loss, regulations across world are forcing companies to own up and report breach incidents to regulators and the affected public. Attackers are getting increasingly sophisticated. They use machine learning to increase the sophistication of attacks and IOT botnets as launch pads to create domino effects. Organizations across the globe realize the need to join hands to share data, anticipate the next attack and increase the costs for adversaries. It is no longer about protection of infrastructure alone. Now, it's generally accepted that we need to be ready to detect an incident and respond in a timely manner and address the challenge.

Wipro's Cybersecurity & Risk Services (CRS) through its people-process-technology framework and a 'Simplify, Secure and Sustain' service approach strongly believes in standardization at the core and differentiation at the front. Our CyberDefense Platform (CDP) offering enables customers to differentially consume services to enable their digital transformation strategies. We have been collaborating with regulators, industry bodies, CERTs, academic institutions and technology partners to gear up the defenses and response mechanisms to better handle recurring cyber-attacks and incidents. In this report we have not only pulled in forces to carry out secondary research on global trends but also leveraged the knowledge gained from our shared CyberDefense Centers (CDC) to correlate the research findings with what we saw on the ground. We also carried out a survey with our customers, reaching out to the senior and middle management layers engaged with cyber risk mitigation, in order to hear from the frontline on real issues that matter. In this edition of the report, we have also gone a step further and included contributions from our partner companies IntSights, Demisto and Denim Group. These partners bring in rich expertise in their specific domains such as threat intelligence, security automation and Secure DevOps. Their contributions have strengthened the insights available to the reader.

I am confident that the report will provide useful operational and strategic insights to security teams and professionals across customer organizations. Together we can strive to make our digital journey an exciting yet safe one!

Editor's note

Josey V George

Editor – State of Cybersecurity Report 2018
Practice Head, Solutions Engineering at Cybersecurity & Risk Services, Wipro Ltd.

Twitter@joseyvg

linkedin.com/in/josey-george

Welcome to the 2018 edition of State of Cybersecurity Report from Wipro. We are indebted to customers, partners, industry analysts and fellow professionals in the global cybersecurity community who encouraged us with an overwhelming response to the first edition of the report last year. I sincerely believe that this edition, with the breadth of topics covered, will have some interesting takeaways for all to cherry-pick from and assimilate back into their enterprise contexts!

The four-pronged approach of macro, micro, meso and future views of cybersecurity presented in the first edition have become genetic identifiers that differentiate this Report from others in the market. Thus, we have decided to retain the four-section format for the second edition as well. Section 1 of the Report is titled State of Attacks, Breaches and Law, and it provides a macro view of cybersecurity trends related to breaches, vulnerabilities, weapons of cyber destruction, active APT groups and changing regulations. Section 2, titled State of Defense Mechanisms, provides a micro environment or inside view of how the CISO organization within companies is approaching governance around security budgets, metrics and control practices across layers like endpoint, data, application, network, cloud and IOT. Section 3, titled State of Collaboration, provides a meso view of how the internal security teams are collaborating with the external environment consisting of regulators, CERTs and other agencies, to anticipate attacks and reduce risk. Lastly, Section 4 titled Future of Cybersecurity talks about emerging trends that impact cybersecurity. Additionally, in this edition, we have covered quantum computing, blockchain and security response automation as pertinent topics.

This year we had 203 organizations from the Wipro customer base responding to our primary research survey compared to 139 last year – a phenomenal increase in participation! We also analyzed a sample of 9,749 security events visible to our CyberDefense Centers (CDC) through the four quarters of the year gone by. This generated some interesting insights on malware trends. As part of the secondary research, we reviewed 2700+ breaches that were reported publicly in 2017 due to regulatory mandates. Out of them, we examined the top 40 breaches for the nature of data breached and patterns that emerged from that analysis are presented in this report. Like last year, we also took a critical view of the security industry and extended our analysis of CVE (Common Vulnerabilities and Exposures) vulnerabilities reported against enterprise-grade security products in the market. The not so comforting lessons from the vulnerabilities study is that security vendors themselves need to do more to keep their products secure. But the heavens are not crashing down yet – customers are maturing on how they track and monitor the effectiveness of security controls across preventive, detection and response realms. This makes a holistic approach to cybersecurity seem like the best way to minimize the risks and allow businesses to scale new heights!

Happy reading and we look forward to serving you again through the year!

Methodology & demographics

The State of Cybersecurity report 2018 from Wipro was developed over a period of three months. The methodology that was followed for developing the report was four-fold:

1) Primary Research (external)

2) CDC Research (primary research through our Cyber Defense Centers)

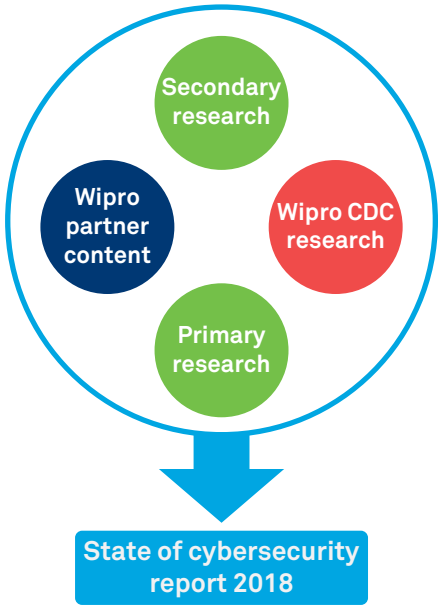
3) Secondary Research

4) Wipro Partner Content

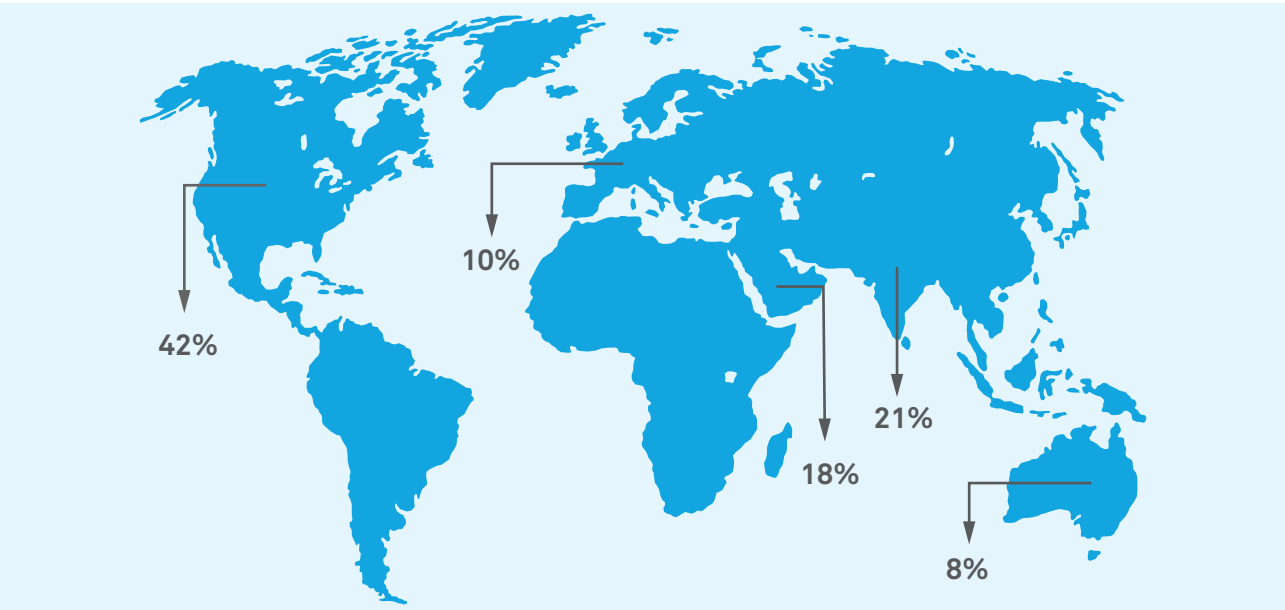
The primary research (external) was driven through surveys of security leadership, operational analysts and architects from Wipro's customer base. The survey was conducted through direct interviews and limited online surveys over a period of two-months, till March-end 2018, with a detailed questionnaire that respondents were required to fill out anonymously. The CDC Research was conducted on aggregated data from Wipro's CDCs across North America, Europe, India, Middle-East and the APAC region. The data analyzed ranged from incident tickets, malware analysis reports, vulnerability analysis and threat intelligence feeds across these regions, over four quarters of 2017.

The secondary research was carried out by a core team of CRS COE analysts who brought in various strategic perspectives from academic, institutional and industry research, to supplement the primary and CDC research and help connect trends in the cybersecurity domain.

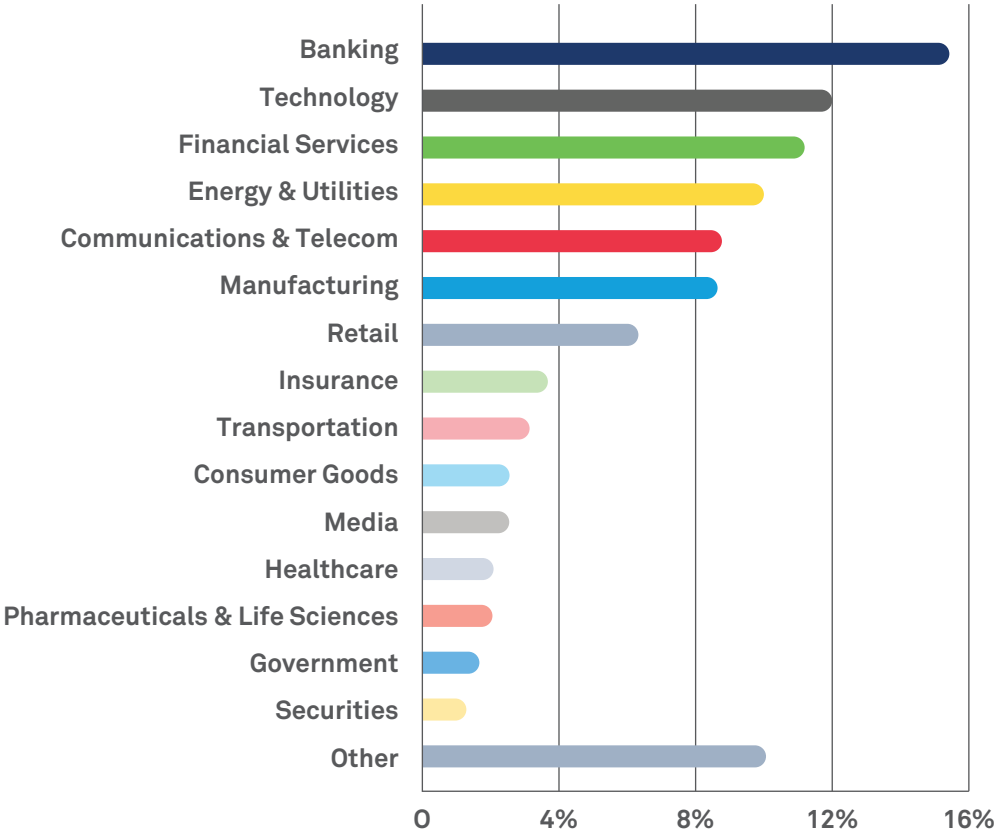
Lastly, Wipro partner content was contributed by three of Wipro's partners – IntSights, Denim Group and Demisto. IntSights, Denim Group and Demisto have core competencies around cyber intelligence, application security services and automated incident response and security orchestration, respectively.



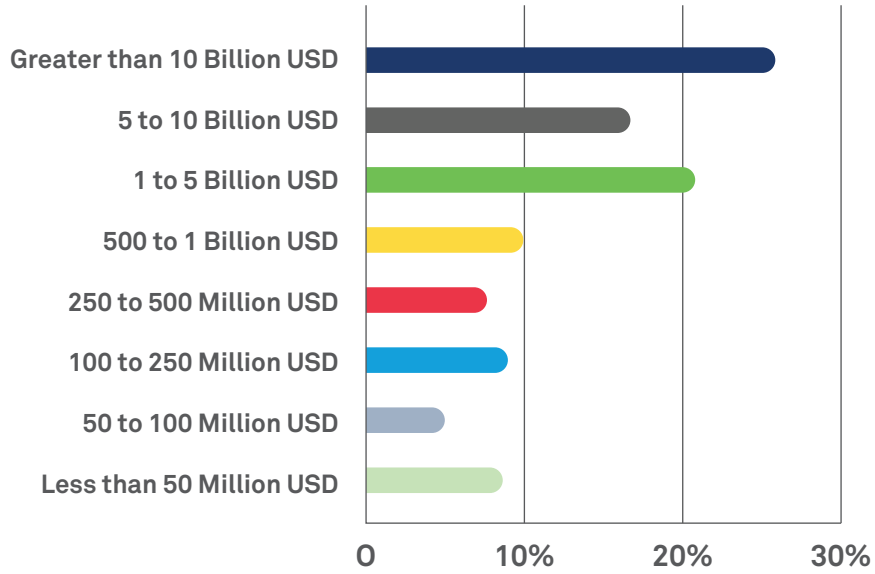
Percentage of survey respondents across different geographies



Organizations surveyed by vertical



Organizations surveyed by revenue



203	Organizations surveyed
11	Countries covered
9,749	CDC incidents analyzed
283	Unique malware risk/threats analyzed
111	Security products analyzed for vulnerabilities
18	Countries breach notification and cross-border transfer laws analyzed
40	Top breaches analyzed in detail

Technology partners

DENIM GROUP — https://denimgroup.com/

DEMISTO — https://www.demisto.com/

INTSIGHTS — https://www.intsights.com/

Structure

DNA of the report

The first edition of the "State of Cybersecurity report" was well received by customers, industry analysts and cybersecurity professionals. The 2018 edition of the Report maintains the same unique structure to build on the first edition's ethos and bring in new viewpoints and findings. The rest of this section is reproduced from last year's report for the benefit of first-time readers.

Through this edition, we want to cover and provide a perspective of **1) The Macro Environment** around the globe in relation to cybersecurity – an outside-in view of cybersecurity, **2) The Micro Environment** as it relates to how organizations are implementing, operating and optimizing security controls as a holistic industry trend – an inside-out perspective, **3) The Meso Environment** on how organizations and the external world are collaborating to allow information flows – detailing connections between the Macro and Micro Environments and **4) Disruptions that can affect the equilibrium** between Macro, Micro and Meso Environments.

With these objectives in mind, Section 1: State of attacks, breaches and law addresses the Macro Environment needs, followed by Section 2: State of defense mechanisms that maps to the inside-out view or the Micro Environment, followed by Section 3: State of collaboration that addresses the Meso Environment and culminating in Section 4: The Future of Cybersecurity which takes a view on possible disruptions in the future. Further details on each of these sections are given below.

Section 1: State of attacks, breaches and law

This section illustrates the research around major breaches that happened during 2017 and analyzes the profile of data elements that hackers were after. Section 1 continues with the attack analysis on the weapons of cyber destruction from our CyberDefense Centers (CDC) around the globe. The section also includes a contribution from a partner on active APT groups of 2017. This section also analyzes the vulnerability trends of security products, how breach notification regulations are changing and becoming more stringent and the implications of the same.

Section 2: State of defense mechanisms

This section is borne out of the primary research that Wipro carried out with 203 customers across North America, Europe, APAC, Middle East and India and thought leadership content from partners and the practice. The primary research was carried out by direct interviews and an online survey with key stakeholders such as the CISO or from the CISO organization. The research focused on the current state of defense mechanisms around endpoints, network, applications, cloud, IOT environments and the use of security monitoring controls. This year we have also added a sub-section on security governance covering security budgets, metrics and privacy governance.

Section 3: State of collaboration

This section is based on the primary research carried out with the CISO organization and focuses on the readiness of security organizations to collaborate with the external cybersecurity ecosystem to better manage the risk. The collaboration here would typically be with regulatory bodies, CERTs and often with competitors in the same business market.

Section 4: Future of cybersecurity

The last section focuses on the future and is largely based on secondary research and viewpoints garnered from within the cybersecurity practice and partners. The topics covered range from quantum cryptography, blockchain and security automation for the future.

Executive summary

"There are only two types of companies: those that have been hacked, and those that will be."
– Robert Mueller (FBI Director 2001-13)

The year 2017 was witness to some of the most dangerous and blistering attacks across the spectrum of industries, ever recorded in the history of cybersecurity. The WannaCry ransomware attack was a bolt from the blue and many organizations were exposed for their lack of sound threat response controls. Per our estimates based on the study of public disclosures, approximately 2.7 billion data records were stolen in 2017, more than twice the total number of records stolen in 2016. DDoS attacks maneuvered into more sophisticated attacks, both in terms of scale and frequency. Unfortunately, the defense mechanisms employed by organizations were still not able to square up with the growing threat landscape. The anticipation of the next wave of WannaCry type of attacks remains a real threat. The challenges of building resilient infrastructure for containing today's threats as well as deflecting tomorrow's new wave of cyber-attacks is driving organizations into funding, planning and operationalizing their response to this growing global menace.

The State of Cybersecurity report 2018 brings together an interesting mix of research and analysis on attacks, vulnerabilities, cyber weapons and contrasts their impact on existing defense mechanisms. The Report also explores how organizations are grappling with the problem of getting timely intelligence and mechanisms of collaboration around the same. Last but not the least, the report also looks at the future with emerging disruptions that can strengthen the hands of the cybersecurity teams.

State of attacks, breaches and law | State of defense mechanisms | State of collaboration | Future of cybersecurity

In this section of the report we present secondary research findings about globally reported data breaches of 2017, weapons of cyber destruction monitored through Wipro's CDCs, active APT groups, vulnerabilities in security products and the cybersecurity regulatory landscape across 18 countries. A few key takeaways from this section are presented below:

High tide to monster wave of breaches in 2017

88 records were lost or stolen every second in 2017 as per our estimates (43 records/sec in 2016)

Ransomware went pandemic in 2017 – more to come?

43% increase in detected ransomware variants in 2017 from 2016 (based on annualized CDC estimates)

Security products need more body armor

DOS, Code Execution & Gain Information were the most common vulnerabilities in security products

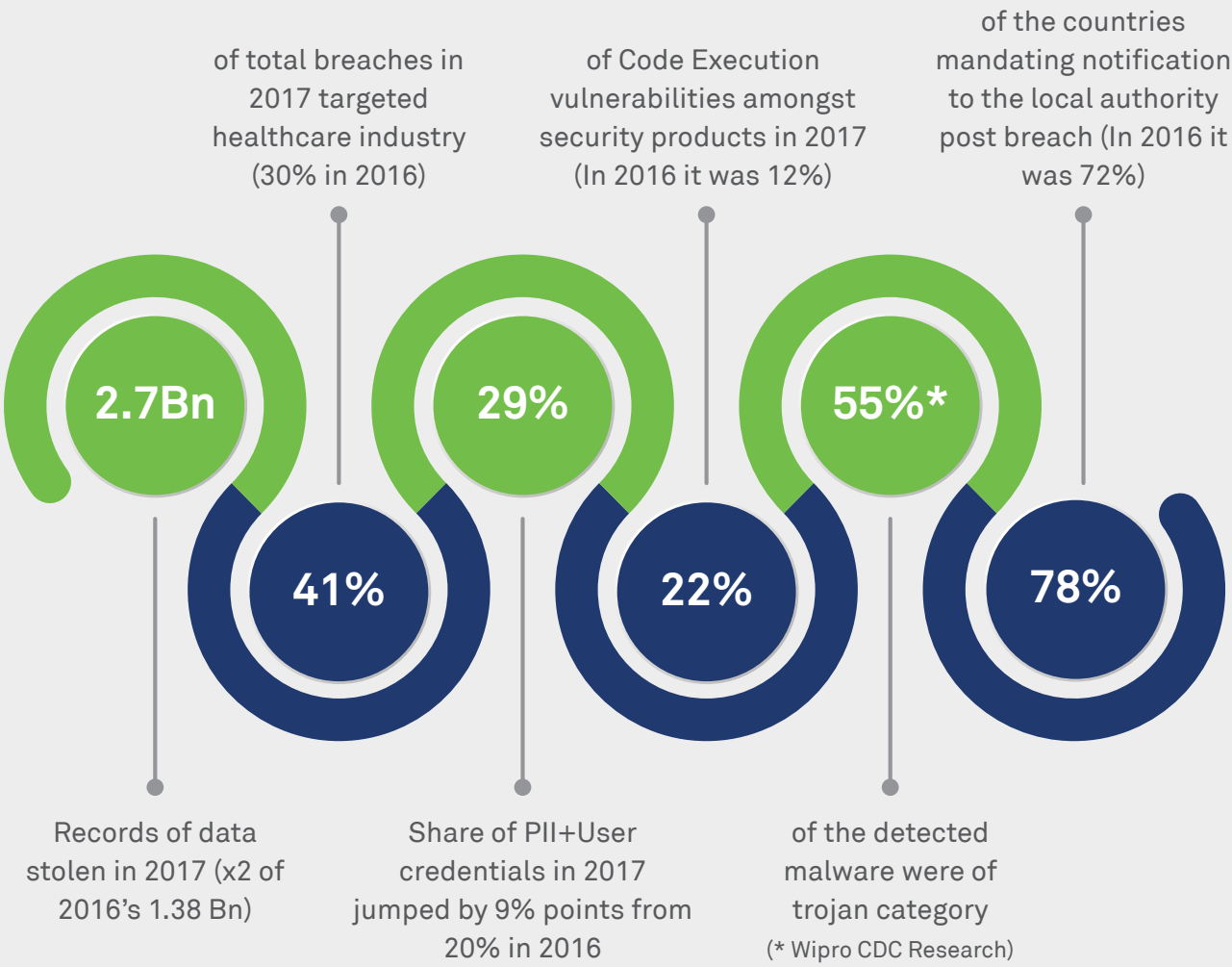
Spreading wildfire of breach notification laws

50% of the 18 countries analyzed in 2017 have clearly defined laws which mandate notifying concerned data subjects upon detection of a data breach (in 2016 it was 44%)

Organized threat actors in play

Active APT Groups: **APT 1, APT 29, Lazarus Group** – Based on research by IntSights, a Wipro Ventures partner

A few more highlights from section 1



Section 2 of the report presents interesting insights and findings from the survey conducted with CISOs about the state of security management and governance, data security, application security, network security, endpoint security, security monitoring and analytics, cloud security and IOT security in enterprises. A few key takeaways from this section are presented below:

Are the boardrooms listening?

4% was the maximum share of overall enterprise IT budget allocated for security in 2017 as per 39% of the organizations in 2017

If it's not on the RADAR, no one will see it coming!

Only **36%** of organizations tracked how much of the IT estate/asset base was effectively monitored by their SOC

Protect the keys to your kingdom

29% of organizations ranked PAM (Privileged Access Management) as their first choice amongst data security controls

Applications are the soft underbelly

Only **21%** of the organizations were doing security assessment of business-critical applications for every application build/release cycle

Are you ready for the DDoS garden hose?

45% of organizations faced some form of DDoS attack in 2017

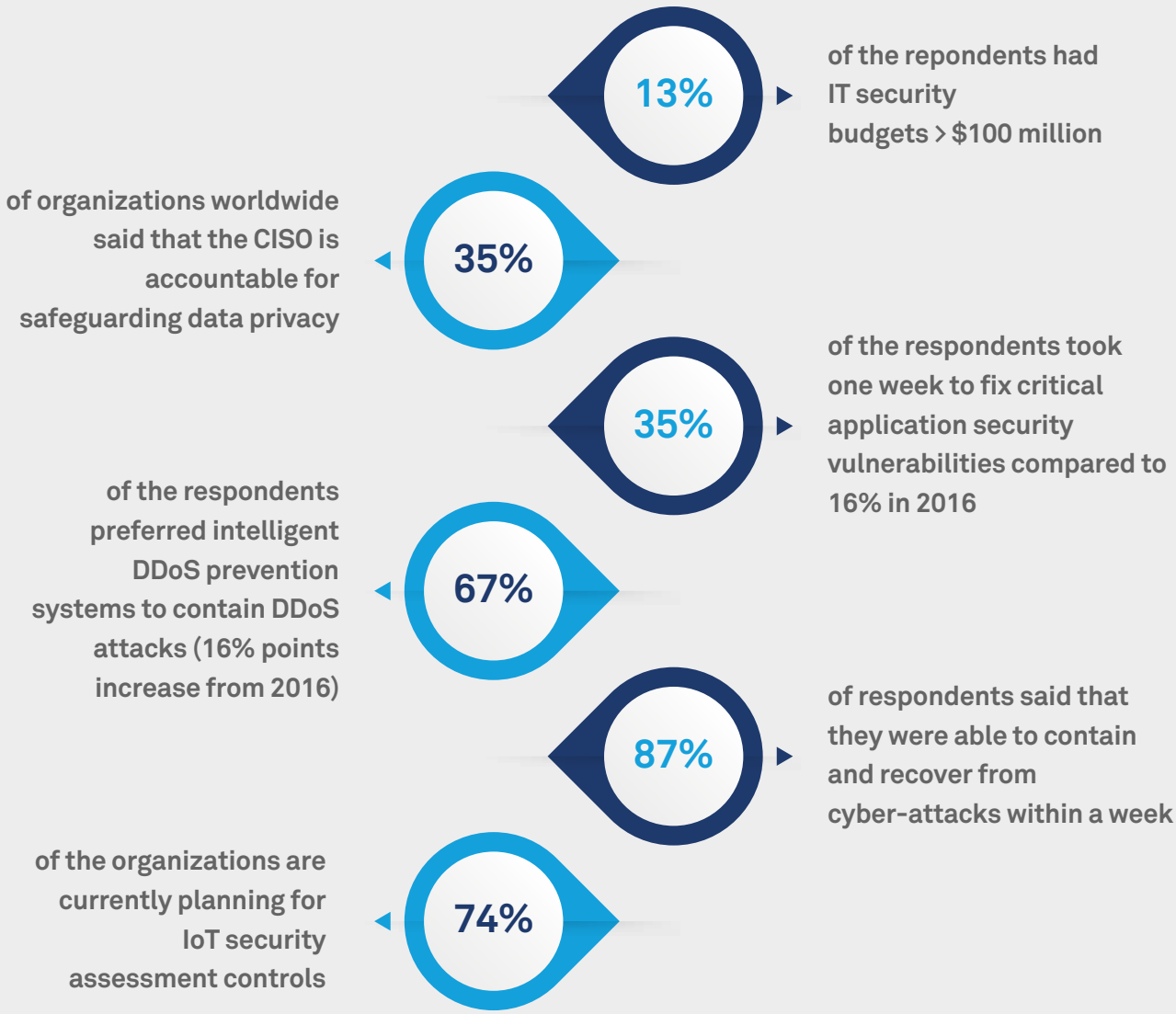
Users are still the weak link

60% of organizations ranked phishing emails as the primary vector of endpoint attack

Serverless computing cannot be security less!

44% of organizations polled minimal control of security as the main hurdle preventing them from migrating applications to a Serverless model (FaaS – Function as a Service)

A few more highlights from section 2



The state of collaboration section explores the extent of collaboration between enterprises and industry ecosystem in cybersecurity. Broadly, through primary research, we gathered insights on organizations' threat intelligence, cyber-attack simulation exercise coordination, information sharing and cyber insurance practices. A few key takeaways from this section are presented below:

Generic threat intelligence is getting commoditized

68% of organizations, when compared to 60% in 2016, have opted for SIEM vendor providing TI

Threats by state sponsored actors driving cyber war gaming

11% points jump in participation in cyber-attack exercises, organized by geo-specific industry/sector regulators, as compared to 2016

Sharing – it's about giving and taking!

70% of organizations were willing to share Malware URLs, Blacklisted IPs and Phishing email addresses with their peers (provided there is approval from legal)

Risk Transfer – still a limited option

46% of organizations in 2017, compared to 52% in 2016, have no cyber insurance

A few more highlights from section 3

60%

of organizations were reluctant to share intelligence with sharing groups mainly due to reputational risks

33%

of organizations participated in simulation exercises coordinated by national CERT/CSIRT (up from 25% in 2016)

22%

of organizations said that they have never participated in any simulation exercise in 2017 (down from 31% in 2016)

28%

of organizations said that they have a dedicated Cyber Insurance policy in 2017 (26% in 2016)

Section 4 of the Report focuses on the future and is largely based on secondary research and viewpoints derived from within cybersecurity practice and partners. The topics covered range from quantum cryptography, blockchain and security automation for the future.
A few key takeaways from this section are presented below:

72 qbits: Quantum computing is steadily growing towards breaking traditional encryption methods

42% of the respondents chose criminal activity to be the most worrying risk w.r.t. blockchain

The future of security automation: **Unifying disaster and security recovery, regulation and compliance, and melding digital with physical security measures**

State of attacks, breaches & law

The state of attacks, breaches & law section lays out the broad environment that defined cybersecurity around the globe in 2017. In this section, we will re-visit key data breaches of 2017 and the type of data that was stolen in those breaches. This section also analyzes the 'cyber weapons of 2017' that were developed by hostile elements in digital underworld and how they were used to perpetuate various attacks on commercial IT infrastructure. This is followed up with an interesting analysis on 'Active APT groups of 2017'.

Further, the section weaves its way into the troublesome territory, and analyzes the security weaknesses in commercial security products and what that holds for CISOs and their teams as they leverage these products to fortify their defenses. Last but not the least, this section surveys the evolution of breach notification and privacy laws in 18 countries. It calls out countries that have stringent norms to protect consumer data, and limit the overseas cross-border flow of information.

Analysis of 2017 data breaches

The year 2017 saw vicious and crippling cyber-attacks across the globe, causing financial and reputational losses to the general public and businesses. Approximately 2.7 billion data records were stolen based on estimates of publicly reported incidents, which is twice the number of records stolen in 2016. The frequency of attacks and the stature of the victim enterprises are sending signals to escalate cybersecurity as a governance issue. Amongst the types of data stolen, there is a clear trend that customer information is the most sought-after target by hacking syndicates. Over 143 million customers were impacted by the Equifax breach, which occurred due to a vulnerability found in an open source software, allowing attackers to access sensitive files. During the first half of 2017, major breaches hit organizations in a variety of industries, exposing the records of millions of individuals. Our research indicates that even though 2015 and 2016 have seen some of the most successful breaches of high-value targets, the story has only gotten progressively worse.

Relative impact of data breach across verticals

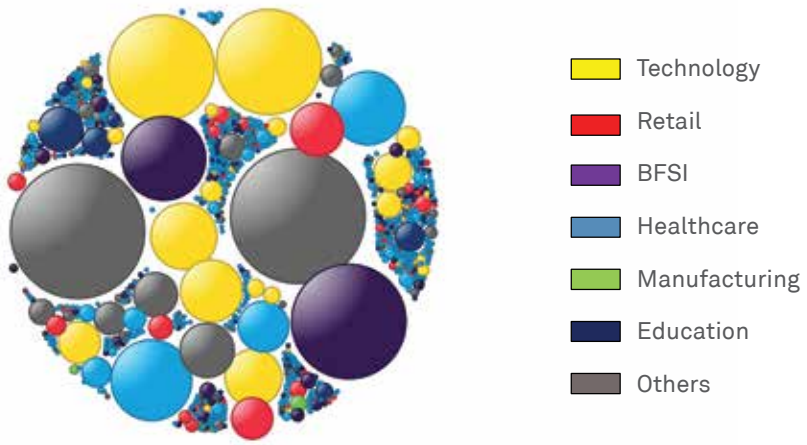


Figure 1: Relative number of the records lost/stolen across public breaches in 2017 (Larger the size of the bubble imply higher the records lost/stolen)

In the above bubble graph, the grouping of industry verticals has been done in the following manner:
BFSI – Banking + Financial Services + Insurance + Professional Services
Healthcare – Healthcare + Hospitality
Retail – Retail + Social media + Entertainment
Manufacturing – Manufacturing + Industrial
Technology – Technology
Education – Education
Others – Government + Non-profit + Others

The increasing frequency of personal data breaches in organizations has impacted customer faith. For example, in July 2017, personal data of more than 14 million customers of a leading communications provider were exposed from an Amazon S3 storage server. The data contained names, PINs and phone numbers that could be used to access a customer's account.

The data breaches of 2017, from the standpoint of the number of records breached on a quarterly basis, is presented in Figure 2 as compared to the same period in 2016. As is evident, 2017 has seen a clear increase in the volume of data records lost. In fact, the number of records hypothetically stolen per second for 2017 has gone up to 88 per second from 43 per second as reported in 2016.

88 records were lost or stolen every second in 2017

Quarterly distribution of stolen records

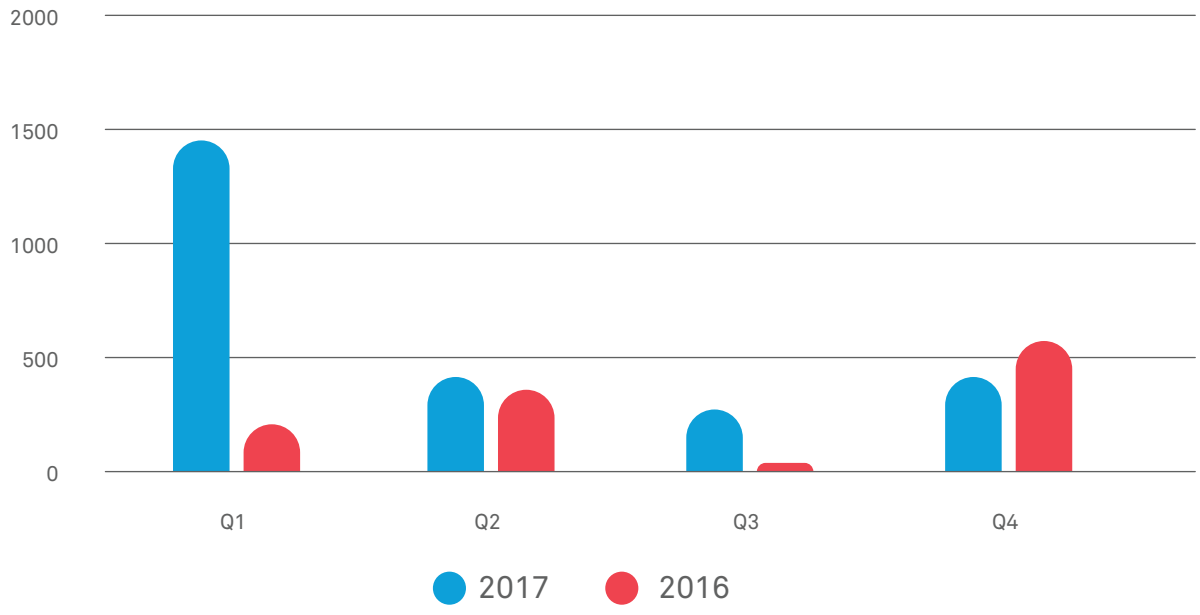


Figure 2: Number of stolen records (in million) in 2017 vs 2016 (quarter-wise)

Month-wise distribution of breaches

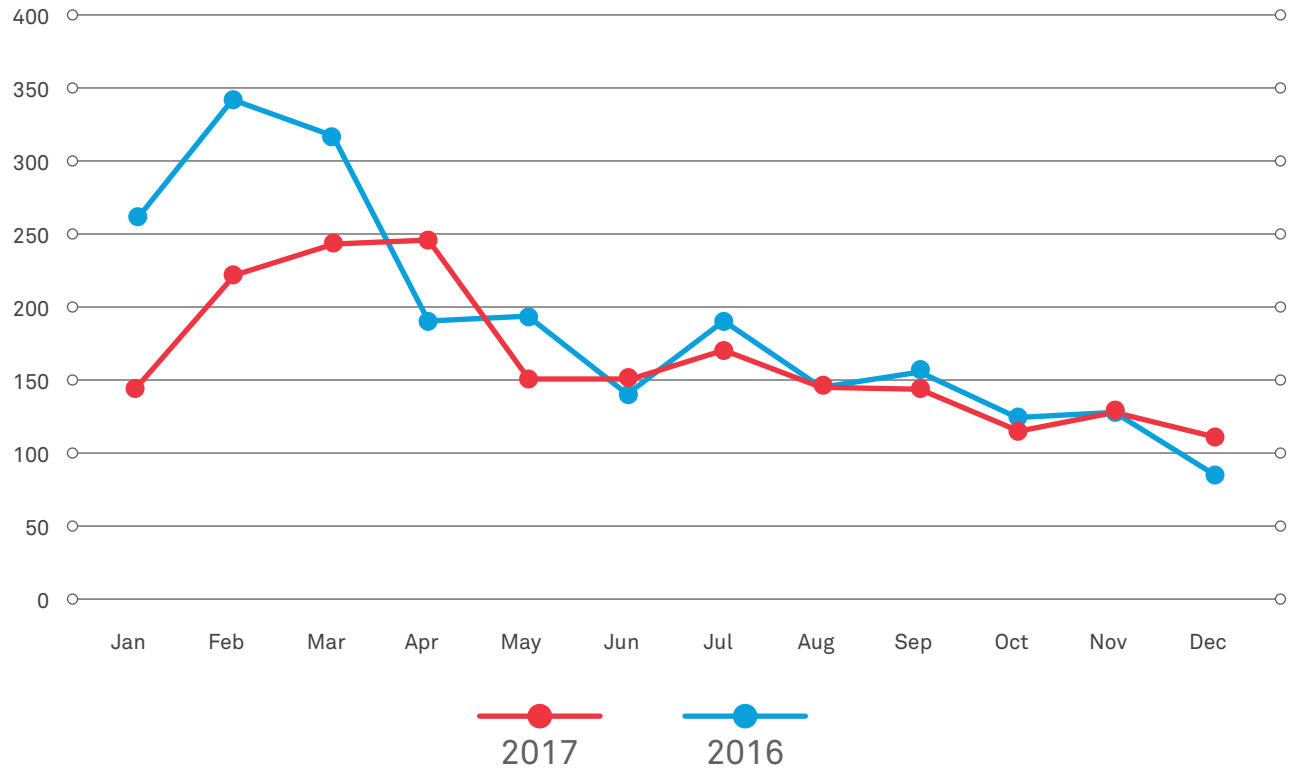


Figure 3: Number of breaches per month

When we compare the trends for the number of breaches per month in the last two years, a pattern can be observed in Figure 3. Both years saw escalating breaches occurring at the beginning of the year followed by a general reduction in the intensity of breaches. While Q1 witnessed the maximum volume of reported successful attacks, Q4 experienced the least in terms of distribution across the year. The percentage distribution across quarters was as follows: Q1:40%, Q2:23%, Q3:22%, Q4:15%. These statistics underscore the manifestation of cyber risks, historically. And with this increasing trend of attacks it is evident that enterprises across all verticals should invest more time and energy in safeguarding their information assets and the business processes they support.

Data breaches heat map

The research on the data breaches of 2017 also focused on the geographical intensity of attacks over the course of the year. The analysis was done taking into account the victim destination based on the geographical location of business.
Based on this analysis a global heat map was generated. As is evident from the heat map in Figure 4, the US has suffered the maximum volume of attacks. The evidence of geographical distribution, found over time, strongly suggests that cyber-attacks are emerging as a global phenomenon, whose intensity and scale threatens every organization, irrespective of the sector, nationality or size.

Worldwide data breaches heatmap

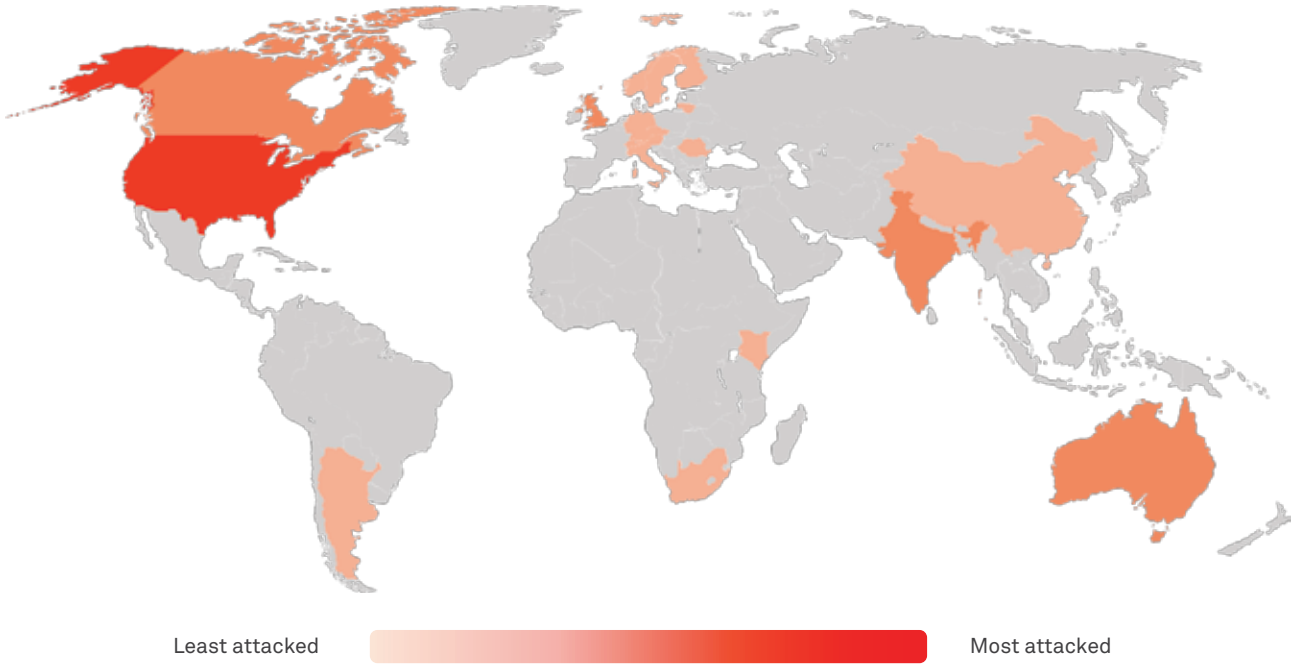


Figure 4 – Data breaches by geography - 2016

The data breaches heat map, as represented in Figure 4, hasn't changed much from 2016 in terms of the intensity of breaches experienced globally. The reasons behind this high concentration of attacks in certain countries can be attributed to different factors such as the presence of large corporations belonging to different industry verticals presenting attractive targets; geopolitical rivalries between countries leading to state-sponsored attacks; and strong breach notification law.

Industry analysis

The data breach analysis further looked at how the reported breaches fared against industry verticals. After analyzing over 2,700+ data breach incidents, which account for millions of records getting breached, the following was observed (Figure 5 illustrates the percentage of attacks across industry vertical):

Data breaches distribution across industry verticals

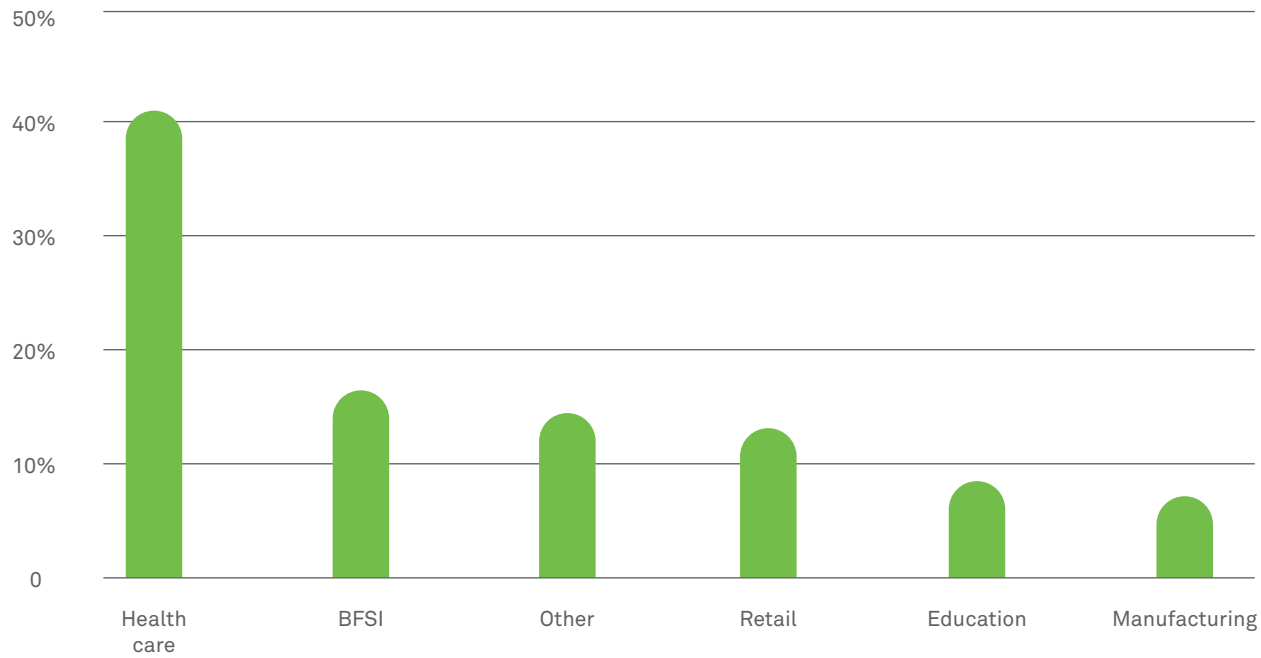


Figure 5: Data breaches spread across industry verticals - 2017

The healthcare industry has been an attractive target for hackers in 2017, as was also the case in 2016. Despite strong regulations prevailing in the healthcare sector across many countries, the propensity of attacks seems to be higher in this domain. With IOT enabling an increasing number of healthcare equipment and devices, the future in terms of addressing increasing cyber risks seems more challenging.

While in 2016, 30% of the attacks targeted the healthcare industry, in 2017 the number jumped to 41%

PII data analysis

To understand the impact of the breaches better, a detailed study of the type of data breached was carried out from available public sources for the top 40 breaches. Figure 6 helps to get a clear picture of the criticality of the data that was breached.

PII data analysis for top data breaches

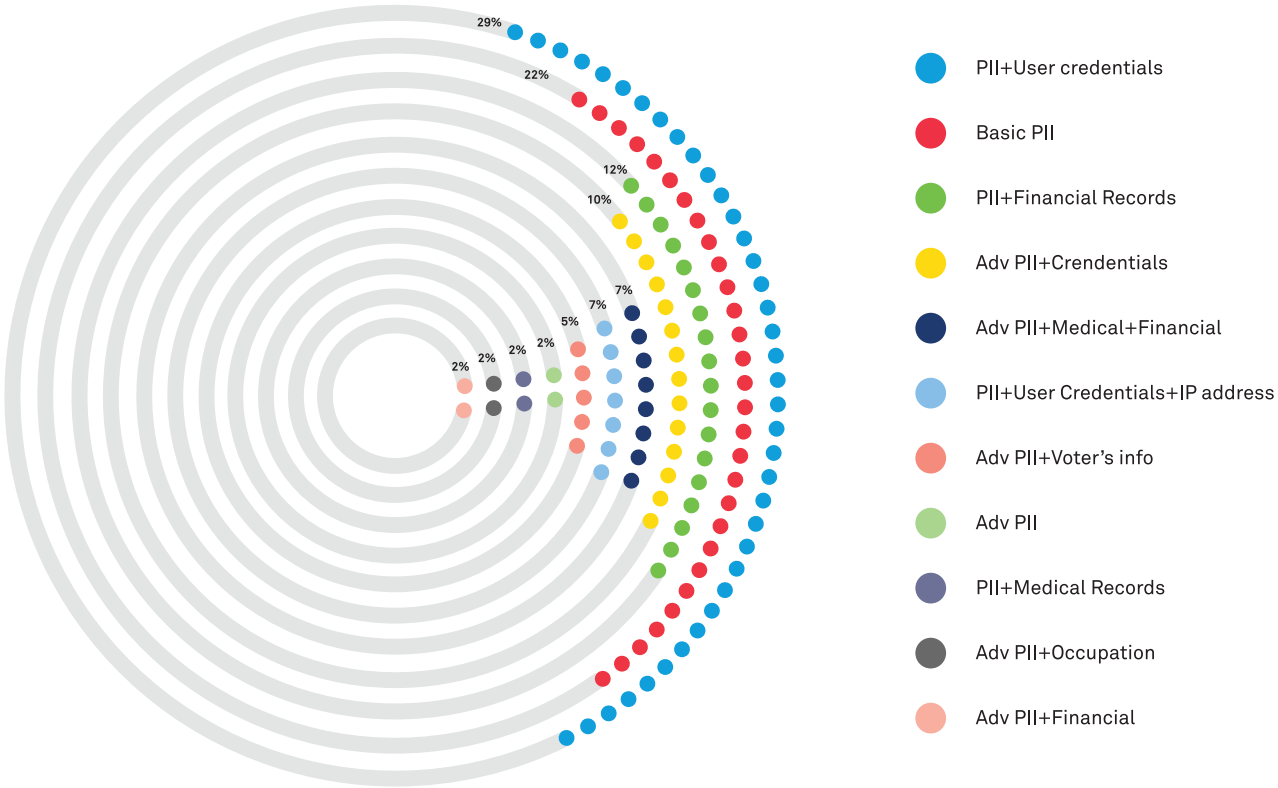


Figure 6: PII data analysis for top breaches - 2017

A combination of personally identifiable information can be utilized to stage identity theft/fraud actions post a breach. The PII analysis gives interesting insights on how top breaches are faring on this count. Identity fraud can lead to reputational and financial losses for the businesses and individuals affected. Our research shows that PII combined with user credentials tops the chart for 29% of the breaches. This is followed by Basic PII at second position and PII+Financial records at third place for most breached categories.

Share of PII+User credentials in 2017 jumped by 9% points to 29% as compared to 2016

Cyber weapons spread across 2017

This section of the report aims to highlight the malware attacks detected and thwarted by CDCs across a sample set of multi-geographic environments in 2017. The incidents were de-identified and then analyzed for the malware threat type, relative distribution and growth across the four quarters of 2017. The analysis was carried out by sampling 9,700+ incidents to generate the insights.

Malware by type

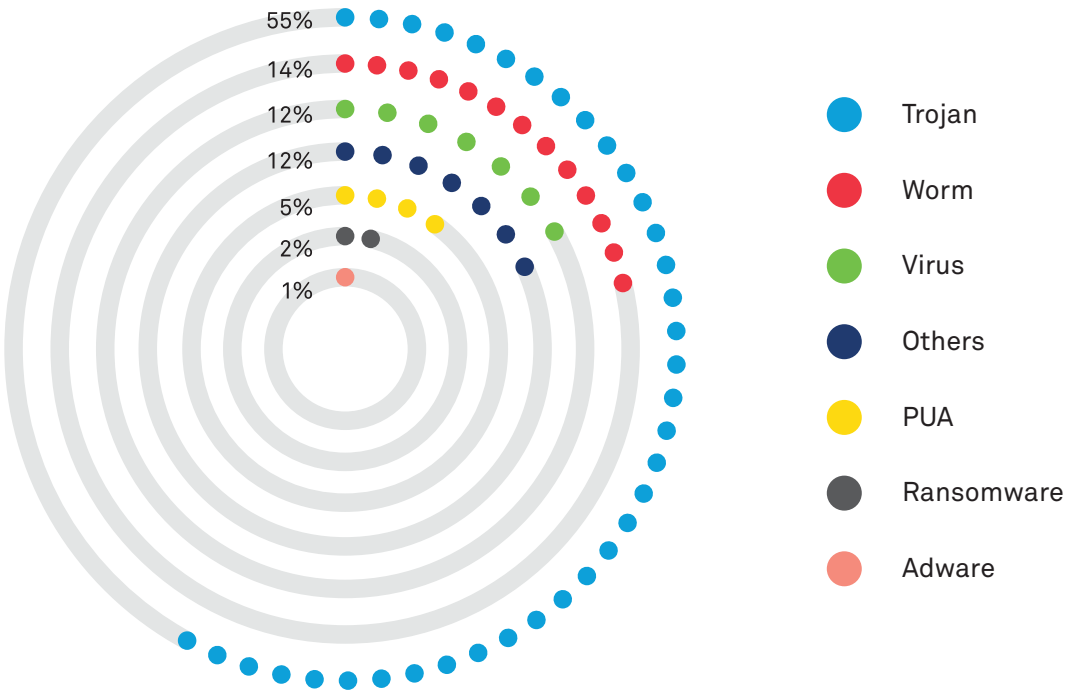


Figure 7: Overall malware distribution - 2017

Figure 7 illustrates the percentage of different types of malware that were detected in 2017 across the following categories: Trojan, Virus, Worm, PUA, Adware and Ransomware. Trojans followed by worms and viruses occupy the top three positions across the various types detected.

Quarterly distribution of malware types

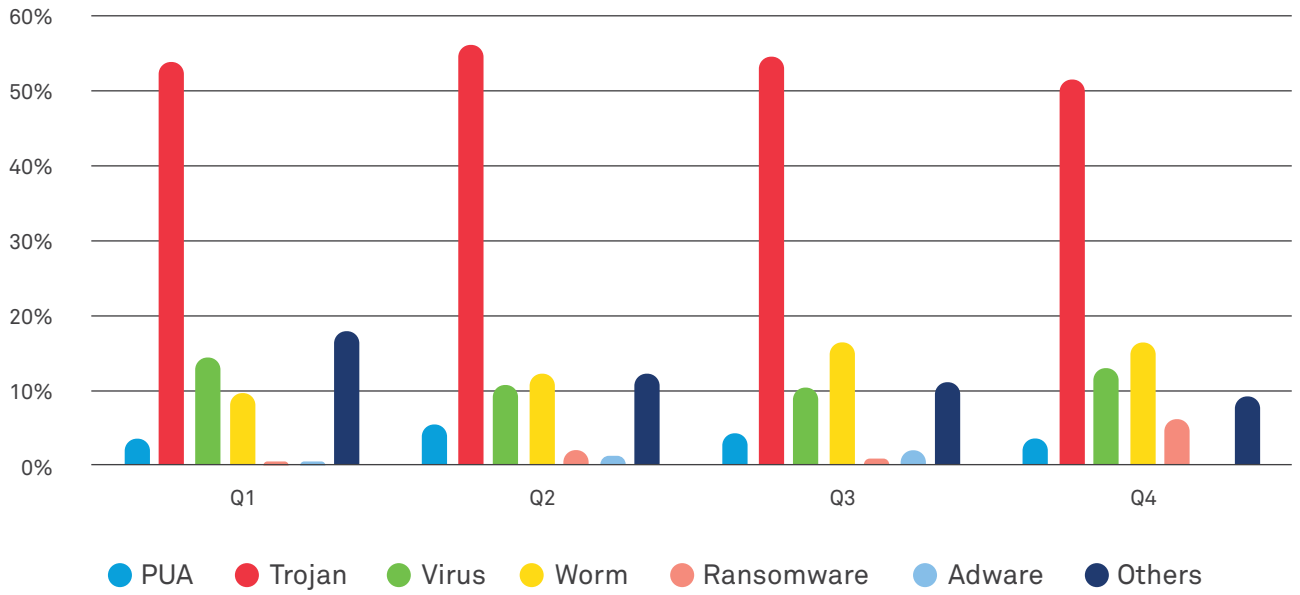


Figure 8: Quarter-wise analysis of major malware categories - 2017

Figure 8 shows the distribution of malware categories across the four quarters of 2018. As can be observed, spikes in the growth of ransomware are prominent from Q1 to Q2 and then Q3 to Q4. These gains can primarily be attributed to ransomware payloads distributed by malware like Ransom.Wannacry, Ransom.Kotver, JS/Nemucod, Bad Rabbit Ransomware, Mamba Ransomware etc.

43% increase in detected ransomware variants in 2017 from 2016

Detected top malware families

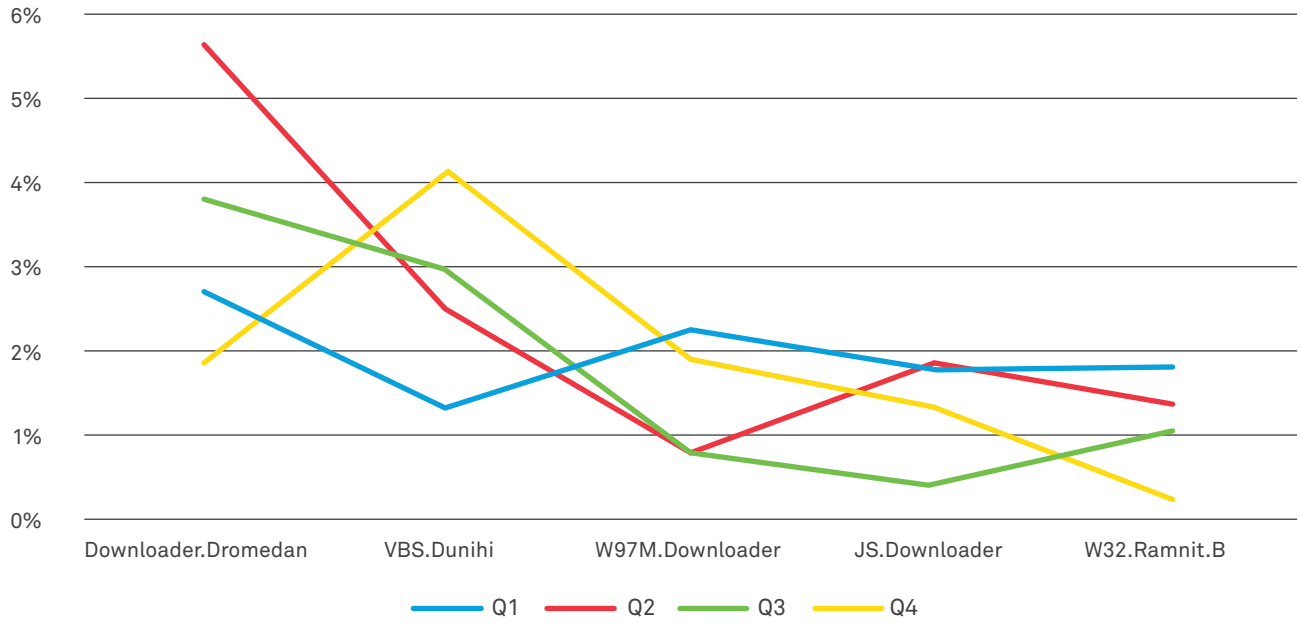


Figure 9: Quarter-wise distribution of detected top malware families - 2017

Figure 9 shows quarterly growth/fall in the incidence of top malware families detected and thwarted in the environments sampled. Apart from the mentioned families, also detected and thwarted were malware families like Trojan.Malscript, W32.Virut, W32.Sality, W32.Downadup, VBS.Downloader.Trojan, W32.IRCBot, Backdoor.Ratenjay, etc., amongst others.

High incidence threats

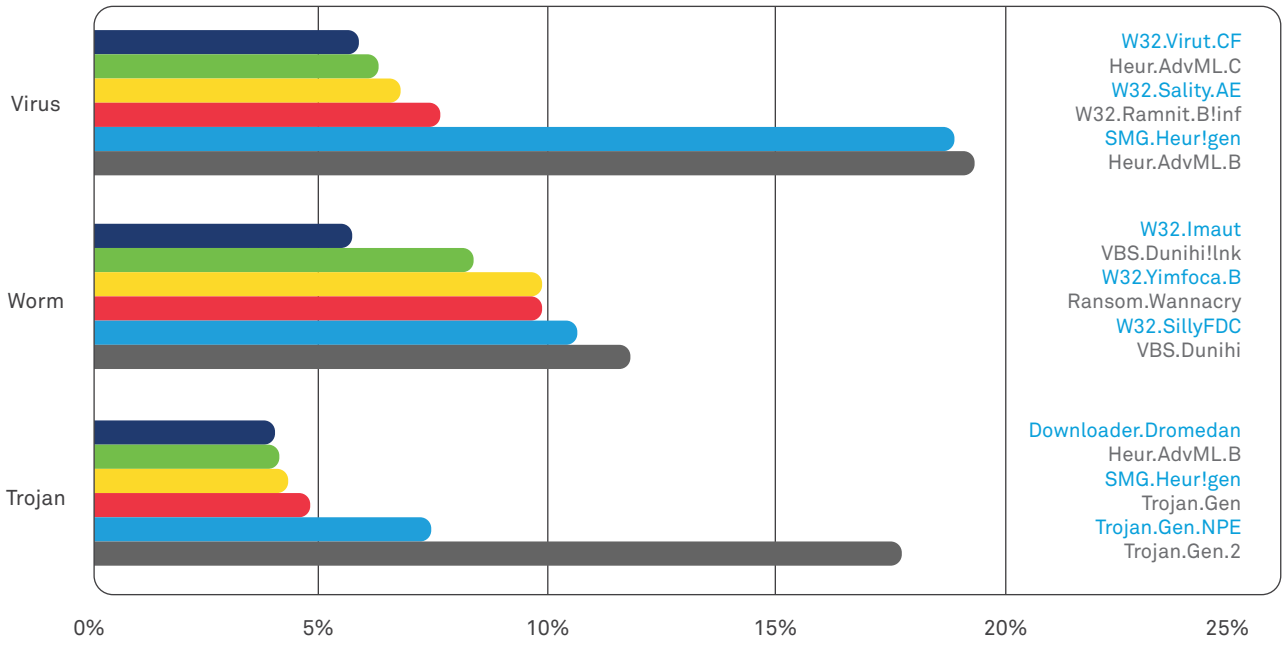


Figure 10: High incidence threats across Trojan, Worm, Virus categories - 2017

In the sample data subset analyzed, specific risks/threats were categories across the three malware categories–Trojan, Worm and Virus for 2017. The high incidence threats across these three categories are shown in Figure 10. Several instances of new malware risks/threats like Ransom.Wannacry, JS.Downloader!gen33, PUA.Jscoinminer and JS.Downloader.F released into the wild in 2017, were also identified in the analysis, although in smaller numbers.

Lastly, the data sampled was also analyzed for categories of exploits kits that were leveraged. Infrastructure and Cross-Site Scripting exploits showed the highest incidence (16%).

New malware risks/threats like Ransom.Wannacry, JS.Downloader!gen33, PUA.Jscoinminer and JS.Downloader.F released into the wild in 2017, were identified

Exploits distribution

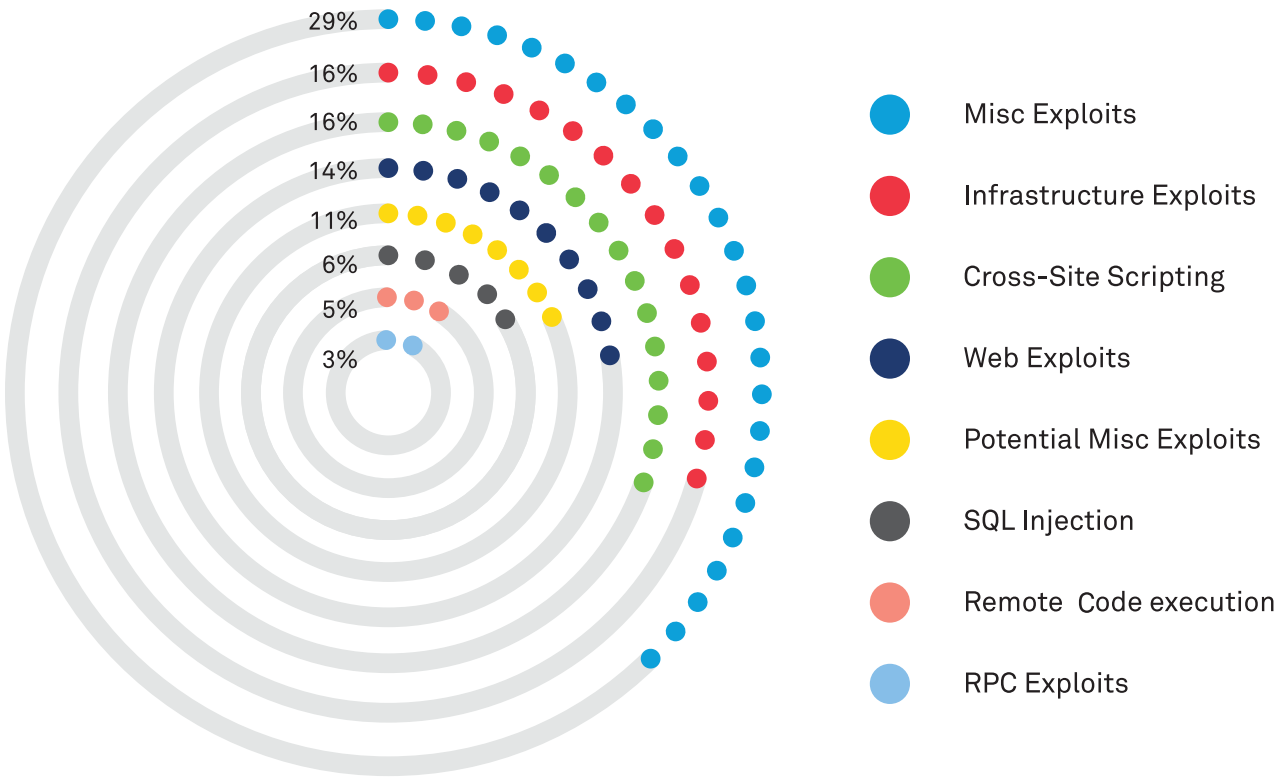


Figure 11: Distribution of exploits - 2017

Active APT groups of 2017

This section is contributed by a Wipro Ventures partner – IntSights, a Cyber Intelligence company that provides the most comprehensive and advanced tailor-made threat intelligence. IntSight's researchers track and monitor threat actors from all over the world, with special emphasis on APT groups.

Traditionally, APT groups receive orders, direction, support and funding from a nation-state according to their interests (political interests, military or intelligence needs). Whether their mission is to steal data, conduct industrial/business espionage, perform a denial of service or attack infrastructure - these threat actors obstinately pursue their targets using a wide and diverse range of TTPs (Tools, Techniques and Procedures).

Unlike cyber-criminal groups, APT groups pursue their targets for an unlimited period, running into months and even years. APT groups adapt to their targets' efforts to eradicate them, they frequently change their attack vectors or malware payloads and in extreme cases they develop dedicated TTPs in order to succeed in their missions.

As of January 2018, there were about 100 APT groups active around the globe. A sample of the most accomplished APT groups is summarized below:

Origin country	**Russia** 
Group name	APT29
A.K.A.	Cozy Bear, The Dukes, Iron Hemlock, Group 100 and CozyDuke
Overview	APT 29 is a cyber-espionage group that has been working for the Russian government since 2008, to collect intelligence related to foreign and security policy decision-making. According to reports, the group engaged in biannual large-scale campaigns against thousands of targets, most of whom belong to the governmental sector or are affiliated to governments.
Targeted sectors	Western European governments, foreign policy groups and other similar organizations

Origin country	China 
Group name	APT1
A.K.A.	Comment Panda, PLA Unit 61398, Group 3, BrownFox and Byzantine Candor
Overview	APT1 is a Chinese espionage group that conducted a cyber campaign against a wide range of targets starting in 2006. It is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department, which is most commonly known as Unit 61398. APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations and is able to steal from dozens of them simultaneously. It focuses on compromising organizations from over 20 industries, 87% of whom are in English-speaking countries. APT1 controls thousands of systems to support their computer intrusion activities. They established at least 937 Command and Control (C2) servers, hosted on 849 distinct IP addresses in 13 countries. The group targets organizations simultaneously. Once they establish access to a target's network, they continue to access it periodically over periods of time, ranging from months to years, stealing large volumes of intellectual property including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from the victim organization's leadership. Generally, APT1 uses IP addresses registered in Shanghai and systems set to use the Simplified Chinese language. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds, of human operators and a current attack infrastructure that includes over 1,000 servers.
Targeted sectors	Information Technology, Aerospace, Public Administration, Satellites and Telecommunications, Scientific Research and Consulting, Energy, Transportation, Construction and Manufacturing, Engineering Services, High-tech Electronics, International Organizations, Legal Services, Media, Advertising and Entertainment, Navigation, Chemicals, Financial Services, Food and Agriculture, Healthcare, Metals and Mining, Education

Origin country	North Korea 
Group name	Lazarus
A.K.A.	Hidden Cobra, Labyrinth Chollima, Group 77, Bureau 121 and NewRomanic
Overview	Lazarus Group is a North Korean espionage APT group. Their attacks were originally detected in 2009, during a cyber-espionage campaign against South Korea. They are considered to be the most dominant APT group in 2017, as they manage to execute several major cyber-attacks against the financial industry, especially via the secured transactions platform SWIFT. The group's TTPs are considered highly sophisticated and they reached their pinnacle in November 2014 when they released internal and confidential information from the Sony Pictures servers after being inside their network for over a year. This attack, known as Operation Blockbuster, is one of the biggest corporate breaches in recent history. Since then the group has been more focused on hacking banks including major attack on the SWIFT payment system of the Bank of Bangladesh, when they successfully stole about $80 million. The group is also said to be responsible for a campaign against worldwide financial institutions in February 2017. This was done by exploiting infected websites to redirect victims to a customized exploit kit. The group is also responsible for the WannaCry ransomware attack which managed to infect millions of computers all over the world.
Targeted sectors	Governments, Information Technology, Aerospace, Media, Advertising and Entertainment, Financial Services and Healthcare

Partner Content Credits: Contributed by Wipro Ventures partner IntSights (www.intsights.com).

Vulnerabilities in cyber defenders

Vulnerabilities in cyber defenders is a unique research contribution to Wipro's Report. Keeping critical systems and applications patched and free from known vulnerabilities is a catch-up game that organizations have been trying to perfect over time. Unfortunately, this has been an onerous task with varying time lags to accomplish patching, providing a window of opportunity to attackers. Security teams typically expect that the layered controls that are deployed in their environments have minimal or no security flaws. Last year, we researched the CVE(Common Vulnerabilities and Exposures) database to figure out how security tools across domains like AV, IDS/IPS, firewalls, DLP, Identity Management, Access Management, Database Activity Monitoring, Privileged Access, GRC, PKI, etc., fared. Surprisingly, the analysis last year pointed to a significant spread of vulnerabilities being reported on security tools. We extended that research this year and the outcome has been no different. The research identified and reported vulnerabilities present in CVE database for security tools.

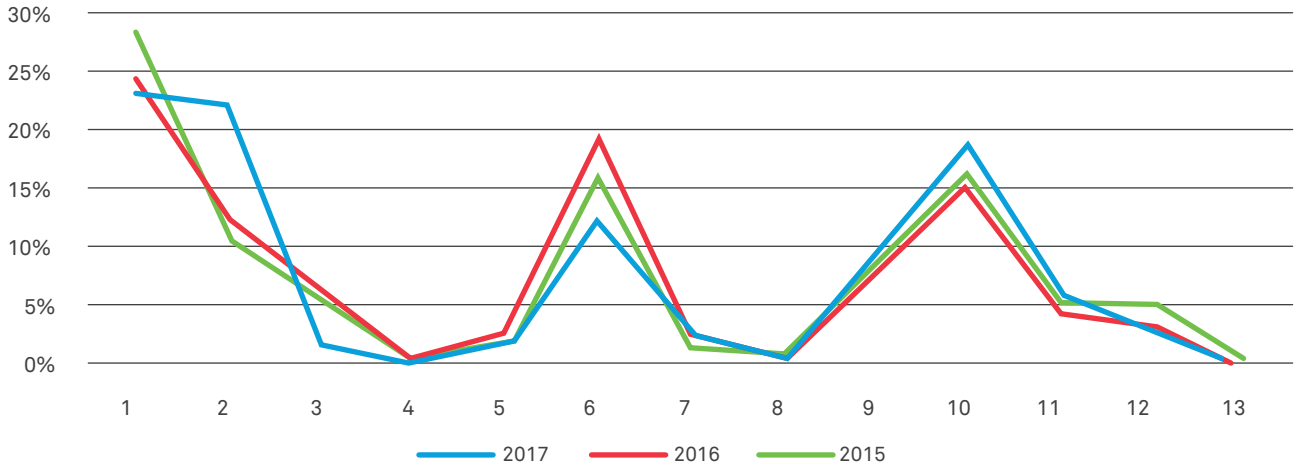
The following vulnerability categories were used to align the various reported product vulnerabilities:

- DoS
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Overflow
- Memory corruption
- SQL injection
- Directory traversal
- Cross-Site Request Forgery (CSRF)
- Gain information
- Gain privileges
- Bypass

On the basis of the above categories of vulnerabilities identified for each security product, a weighted average score was arrived at for the products, which indicated their risk profile individually. The scores of the products that have been grouped into the same domain area were then aggregated, using a weighted average method to arrive at the final domain scores.

Overall, across all domains, the vulnerability scores across the identified categories are reflected in Figure 12.

Product vulnerability trends



1 - Dos
2 - Code Execution
3 - Overflow
4 - Memory Corruption
5 - SQL Injection
6 - XSS
7 - Directory Traversal
8 - Http Response Splitting
9 - Bypass Something
10 - Gain Information
11 - Gain Privileges
12 - CSRF
13 - File Inclusion

Figure 12: Vulnerability trends in security products – 2017 vs 2016 vs 2015

- DoS, Code Execution and Gain Information are the most common vulnerabilities in security products. Code Execution type of vulnerabilities moved from fourth position in 2016 to second position in 2017
- Memory Corruption, Http Response Splitting, Directory Traversal, CSRF, File Inclusion and SQL Injection are the least common vulnerabilities in a security product.

Code Execution vulnerabilities have seen the highest jump among all-from 12% in 2016 to 22% in 2017

The security control domains analyzed this year include the following:

Security Intelligence & Analytics, Web Application Firewalls, Vulnerability Management, Secure Code Review, MDM, Firewall & VPN, File Integrity, SIEM, Access Management/Policy, etc. The scores for 2017 across identified security control domains are given in Figure 13.

Product domain-wise vulnerability scores

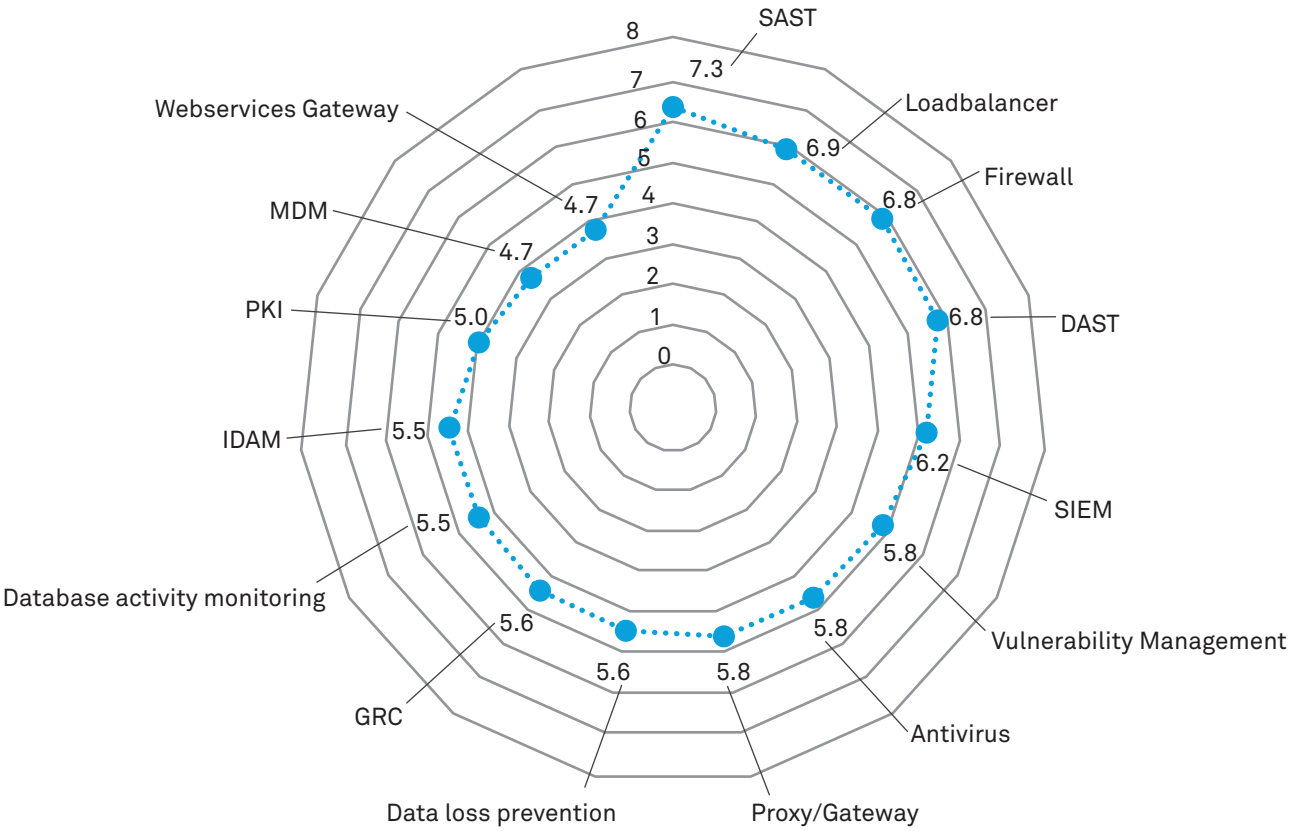


Figure 13: Security domain-wise vulnerability scores - 2017

Arriving at scores: To arrive at the final score, we calculated the weighted average of each vulnerability type for the last three years. After doing so, we could calculate the single average score for each of the products under the security layers.

DOS, Code Execution and Gain Information are the most common vulnerabilities in security products

On the basis of the scores mentioned in Figure 13 we can divide the vulnerabilities into high, moderate and least vulnerable.

Highly vulnerable domains = SAST, Load Balancer, Firewall, DAST, SIEM (vendors need to do more to reduce the vulnerabilities)

Moderately vulnerable domains = Vulnerability Management, Antivirus, Proxy/Gateway, Data Loss Prevention, GRC

Least vulnerable domains = Database Activity Monitoring, IDAM, PKI, MDM, Webservices Gateway (vendors need not put much effort into reducing their vulnerabilities)

Cybersecurity breach notification regulations

This section is the result of a detailed analysis carried out by the Wipro cybersecurity COE of laws relating to data breach notifications and restrictions on overseas transfer of data across 18 countries. The legal regimes that were covered are major data privacy regulations in each of the countries but are not exhaustive in nature. The 18 countries covered are Germany, UK, Sweden, Switzerland, France, Canada, Russia, South Africa, Singapore, Australia, China, Japan, India, Brazil, Mexico, USA, Norway and Dubai*. The key parameters that went into the two areas of analysis are shown in Table 1.

Focus Areas of Analysis	Parameters
Data breach notification requirements	• Mandatory notification of authority • Breach categorization • Mandatorily notify data subjects • Fine if not notified
Restriction on overseas transfer	• Consent of data subjects • If outside jurisdiction provides adequate protection • Binding Corporate Rules (BCRs) • Standard Contractual Clauses (SCCs) • Permission of Data Protection Authority

Table 1 - Analysed parameters for the different focus areas

The analysis based on these parameters was done across the 18 countries using a weighted average method. Weights were assigned to each of the parameters and each country was scored on a linear scale on the extent of meeting the parameter on a relative basis. The total weighted average scores were then used to represent the countries, as shown in the heat maps (Figure 14 and 15).

* Restricted only to a city based on available data

Heat map of breach notification laws

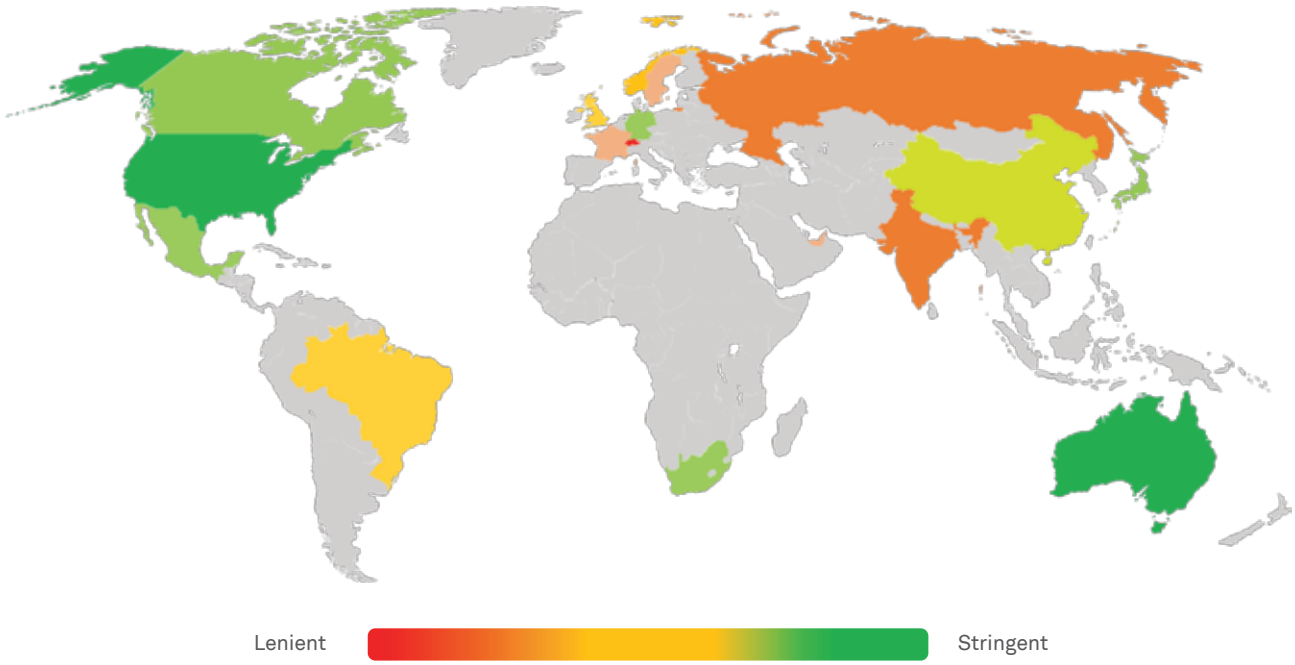


Figure 14: Heat map of country-specific regulations relating to breach notification - 2017

Heat map of cross-border data transfer laws

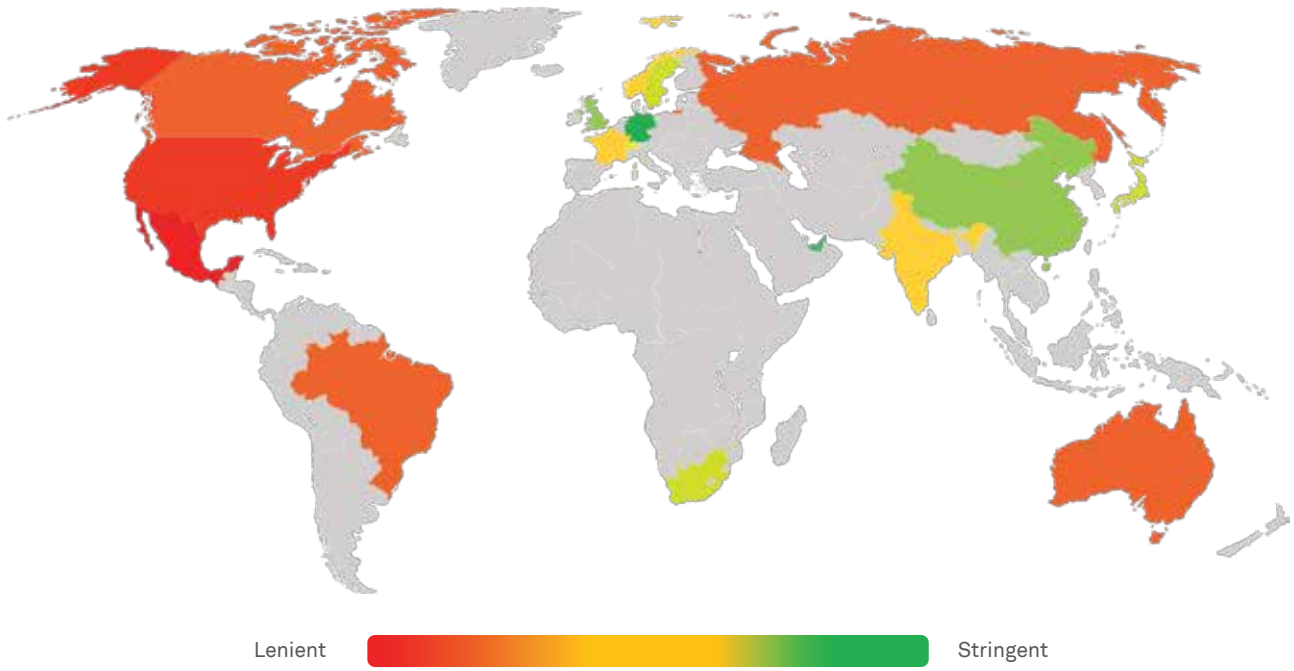


Figure 15: Heat map of country-specific regulations relating to overseas data transfer - 2017

As compared to the analysis done last year, the changes in regulations can be summarized below:

- Breach notification – Australia and China's scores have gone up
- Overseas transfer – China and Japan's scores have gone up

2017 roundup

The year 2017 can be considered a game changer for GDPR if we look back at it through the lens of privacy-related measures pursued by many countries. Out of these, we have analyzed the acts/legislations/efforts of 18 countries for breach notification and cross-border transfer laws. A look at the specific efforts made by these 18 countries helps us understand why we termed 2017 as a game changer.

Let us start with Australia's big leap forward when it passed the Privacy Amendment (Notifiable Data Breaches) Act in 2017 which amended the Privacy Act, 1988. The new act mandates prompt notification of eligible data breaches, as defined in the Act, by Australian Privacy Principles (APPs) covered entities to the Office of the Australian Information Commissioner (OAIC) and affected individuals. The other country in the Asia-Pacific region which made headlines for its privacy-related regulations was China. China's latest Cybersecurity Law, which came into effect in 2017, places tougher provisions on cross-border transfer restrictions and data localization requirements on personal information. However, the compliance window for the law is available till end of 2018. Both the laws we've discussed i.e. Australia's Privacy Act, 2017 and China's Cybersecurity Law have something in common: Both share similarities in one aspect i.e. they try to matchup with GDPR. Though the contrasting character of GDPR and China's Cybersecurity Law can be clearly pointed out, we can still draw a few parallels in terms of interpreting the parameters like PII, controllers and sanctions for non-compliance, amongst others.

One more interesting development, again in the Asia-Pacific region, was Japan's amended Personal Information Protection Act (PIPA) which came into effect in 2017. Some significant changes were incorporated in this amended Act regarding the definition of sensitive information, overseas transfer of personal information and record keeping obligations of personal information either received or transferred from/to third parties.

On the privacy front, India's top court ruled in favor of the 'right to privacy' as a fundamental right and stressed on the need for a data protection framework. This is a positive development for a country like India, where currently data controllers and data processors are loosely governed with respect to several privacy-related obligations, by the present IT Act, 2008. The framework is expected to have more clearly pronounced rules, in sync with the present privacy regulatory landscape.

Among other countries we've analyzed, Roskomnadzor, Russia's Data Protection Authority's (DPA) newly published privacy policy guidelines and Japan's amended Act on Protection of Personal Information (APPI) are to be seen as efforts to matchup with GDPR. The United Kingdom's new draft Data Protection Bill, 2017, talks about the 'right to be forgotten' apart from stressing on tougher sanctions for violation of present breach notification laws already existing in the UK. Also, the UK law aims to bring in measures for compliance with GDPR.

Germany's Bundesdatenschutzgesetz-new, its latest Federal Data Protection Act which aligns with GDPR, makes it the first EU member state to enact such an Act. Other countries, such as France, Norway, Sweden and Switzerland, have also started to make strides in the direction of GDPR through different methods -such as passing draft acts or through re-evaluating their existing laws for compliance with GDPR.

GDPR is no more esoteric in nature. We can see that much of the discussion that shaped privacy-related laws across the globe in 2017 revolved around compliance with GDPR. Businesses have already recognized the rapid pace at which the regulatory landscape is being constructed for a matchup with GDPR and are on the ball. Today, no business can afford to miss the boat and has to put measures in place for compliance with GDPR – and by that we mean measures with regard to their internal organizational policies, and externally with regard to their respective country's laws. In conclusion, the idea of this section is to help businesses understand the criticality of being compliant with GDPR.

50 % of the countries analyzed have clearly defined laws which mandate notifying concerned data subjects upon detection of a data breach (in 2016 it was 44%)

78 % of the countries analyzed have laws which mandate notifying the local authority post data breach (in 2016 it was 72%)

39% of the countries analyzed recognize BCRs (Binding Corporate Rules) as a means of providing adequate safeguards in case the external jurisdictions don't explicitly provide adequate protection (no change from 2016)

State of defense mechanisms

Organizations can be exposed to various kinds of cyber-attacks as illustrated in the previous section. The weapons of cyber destruction used in these attacks can wreak havoc on the enterprise's IT infrastructure if they are not prevented or otherwise detected and corrected. The CISO and his/her function is tasked with dealing with these risks through directed actions. These actions can be across multiple layers of the IT infrastructure, cutting across endpoints, servers, applications, network elements, cloud (IaaS, PaaS, SaaS or FaaS), mobile, emerging IOT and many others. This section lays out the findings from the primary research that was carried out across enterprises operating out of North America, Europe, Middle East, India and Asia-Pacific. The target group of the research were the CISO teams, and the areas of inquiry ranged across security funding, strategy, domain-wise current practices/metrics and future paths that may be taken in the respective enterprise contexts. The findings have been organized by sub-sections related to security governance (dealing with budgeting, metrics, roles) and technology domains. Where relevant, trends as compared to the previous year, have been charted with inferences.

Security management & governance

While the governance of information security involves multiple dimensions, for the purposes of this study, the focus areas were limited to budget, security metrics, accountability for data privacy and security competencies. Security budgets are a key signal indicating the empowerment of the IT organization, to deal with cyber risk and the same has been analyzed from different perspectives. The use of metrics to measure the effectiveness of the existing controls across preventive, detective and response control domains, helps the organization track the value in investing in security. The scrutiny of organizational practices relating to data privacy has increased in recent times due to many leaks of customer information, leading to lowering of customer confidence in the governance of privacy. Finally, right skill development is key to achieving the overall objective of realizing security best practices within organizations.

Security budget

The allocation of a security budget is influenced by various factors-such as risk assessments, regulatory and compliance drivers, actual spend on IT, contextual threat intelligence, value at risk, geographical practices, organizational culture, and so on. The aggregated view of our findings, from the primary research on security budget allocations, is shown in Figure 16.

Range of CISO budgets

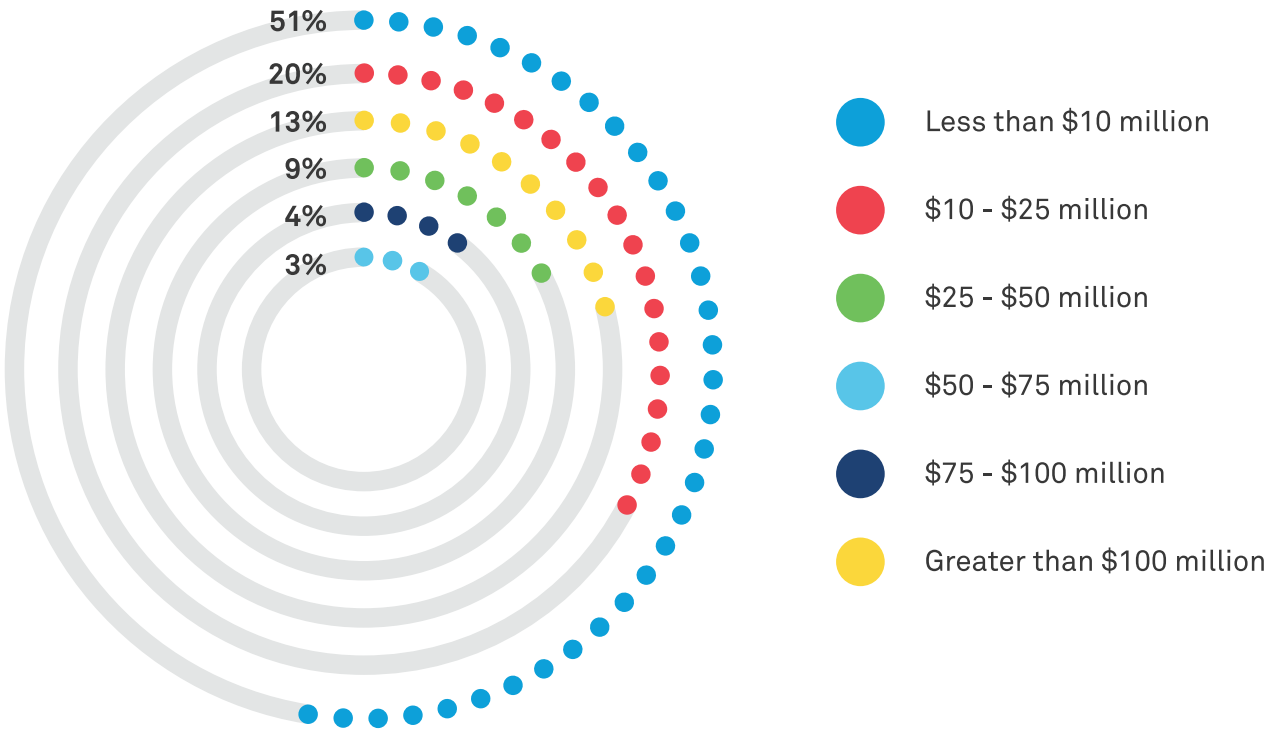


Figure 16: Range of cybersecurity budgets - 2017

About 51% of the respondents indicated that their annual IT security budgets were less than $10 million, with about 12% indicating that they had budgets greater than $100 million. We correlated the annual security budgets with the annual revenue of the organizations (where provided by the respondents) and found that there was no linearity. This lack of correlation can be potentially ascribed to the differential risks that enterprises face based on vertical and geographical location of operation and also differences in the sector-based regulatory regimes that are driving spending patterns.

13% of the respondents had IT security budgets greater than $100 million annually and 30% of the respondents belonging to BFSI verticals had greater than $100 million budget outlays annually

The second dimension of security budgets that the research focused on was the percentage of IT budget that is allocated to IT security. Figure 17 is a reflection of the relative importance given to security, at the planning stage of the year, by the custodians of organizational governance.

Percentage of IT budget allocated for security

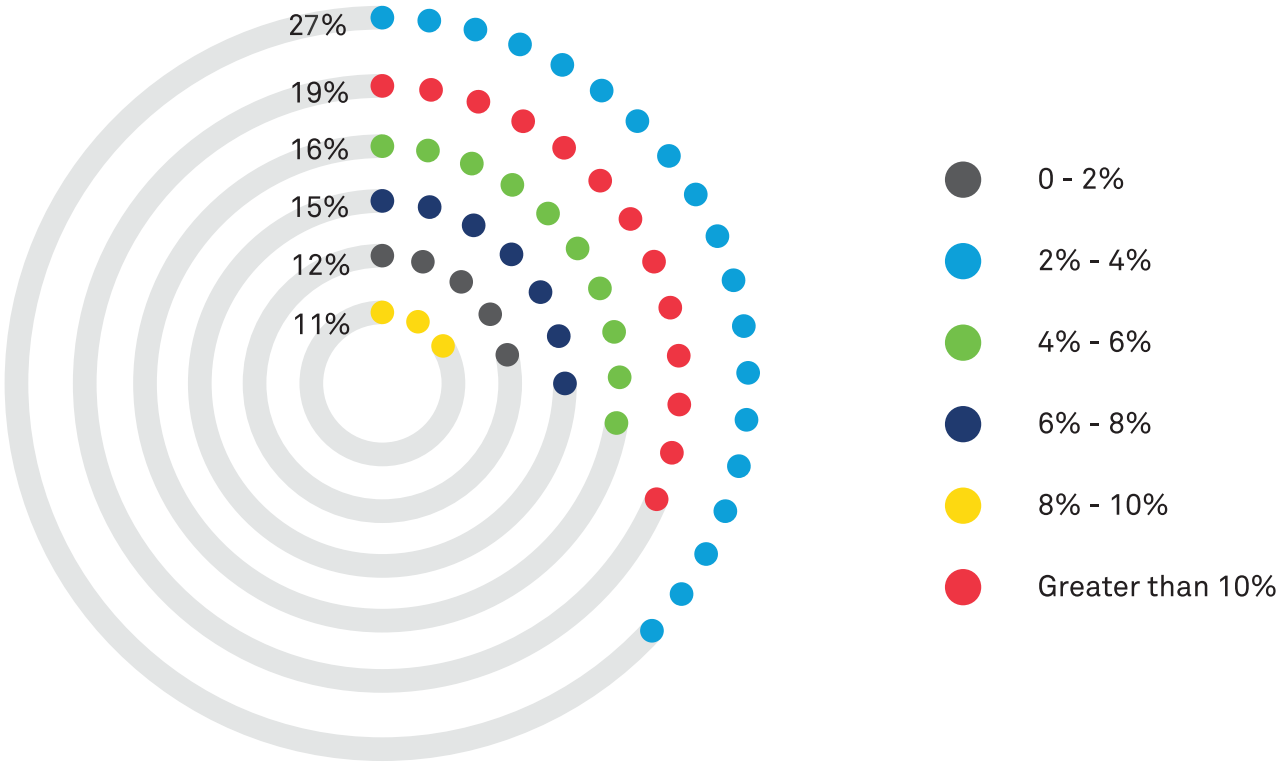


Figure 17: Percentage of overall IT budget allocated to security -2017

27% of the survey participants indicated that their security budget was in the 2-4% range and about 19% of the respondents indicated that they had allocations greater than 10% of the overall IT budget. Given the universal nature of cyber-attacks, companies that are spending proportionally less are possibly seeing a lower business risk or require their security teams to make a stronger case to obtain a higher proportion of the IT budget.

39% of the organizations polled had less than 4% of their IT budget allocated for security

Ownership of data privacy

The next aspect of governance that was explored was the ownership of data privacy within the enterprise. The question that was asked to survey respondents was on the ownership of data privacy within the organization, across roles such as CRO, CPO, DPO, CISO, Business Unit Heads, etc. Figure 18 shows how the ownership of governance of data privacy has changed over the last year.

Ownership of governance of data privacy

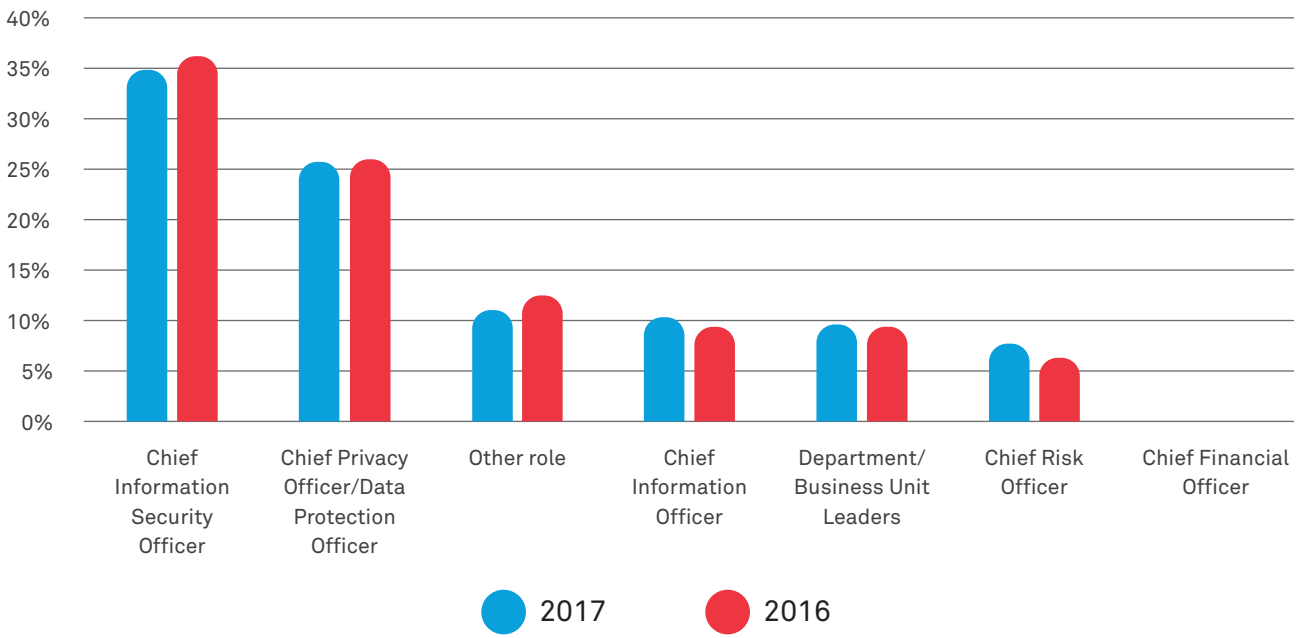


Figure 18: Organizational responsibility for governance of data privacy -2017 vs 2016

Between 2017 and 2016, there has not been much change in allocation of responsibility for governance of data privacy. While the CPO/DPO roles seem to poll high for ownership of data privacy governance in North American and European organizations, worldwide the CISO role seems to be still empowered by the management to track and preserve the privacy of customer data. The higher polling of CPO/DPO in Europe and America could be a direct result of regulations.

Worldwide 35% of the respondents said that the CISO is accountable for safeguarding data privacy. However, for US and Europe geographies CPO/DPO polled highest.

Security metrics

Performance review and measurement of the effectiveness of cybersecurity controls is a critical governance activity. This year, in our primary research survey, we asked CISO's and their direct reports about the types of metrics that they were collecting and getting visibility across preventive, detective and response related security functions.

Metrics usage across preventive, detective and response controls

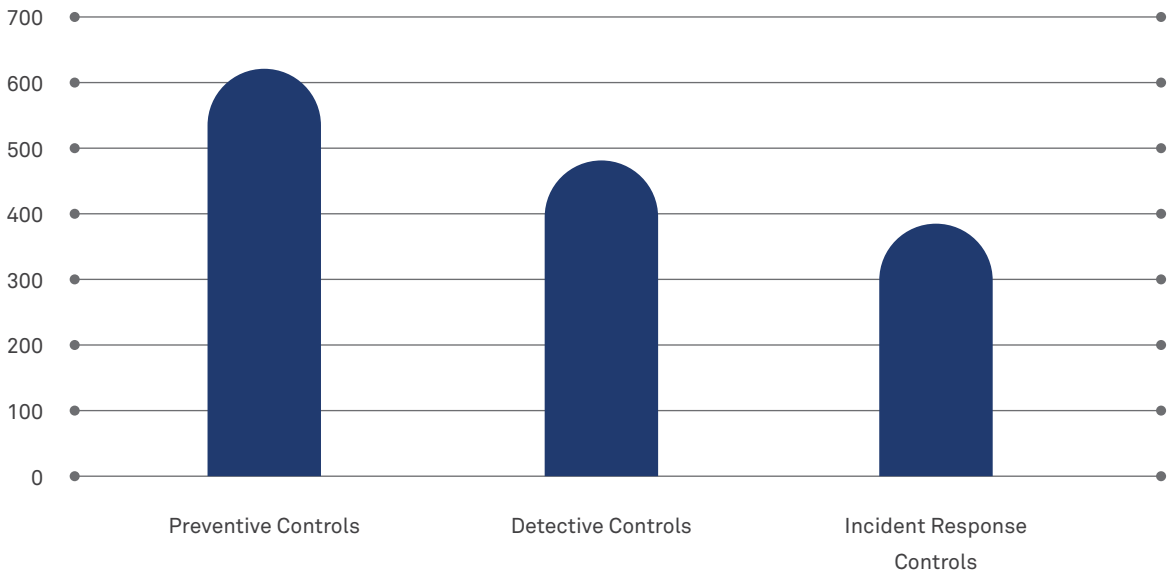


Figure 19: Security metrics tracked across Preventive, Detective, Response Controls - 2017

Most organizations have a higher focus on metrics around Preventive Controls followed by Detective and finally on Threat Response functions. The struggle in the latter segments (Detective and Response) has usually been in operationalizing these metrics, resource limitations and the lack of structured processes around these segments. It must be noted that organizations are stepping up coverage of Detective Controls with the growing realization that breaches are getting increasingly common.

Findings related to Preventive Controls Metrics (Figure 20) -

Relative usage of Preventive Controls

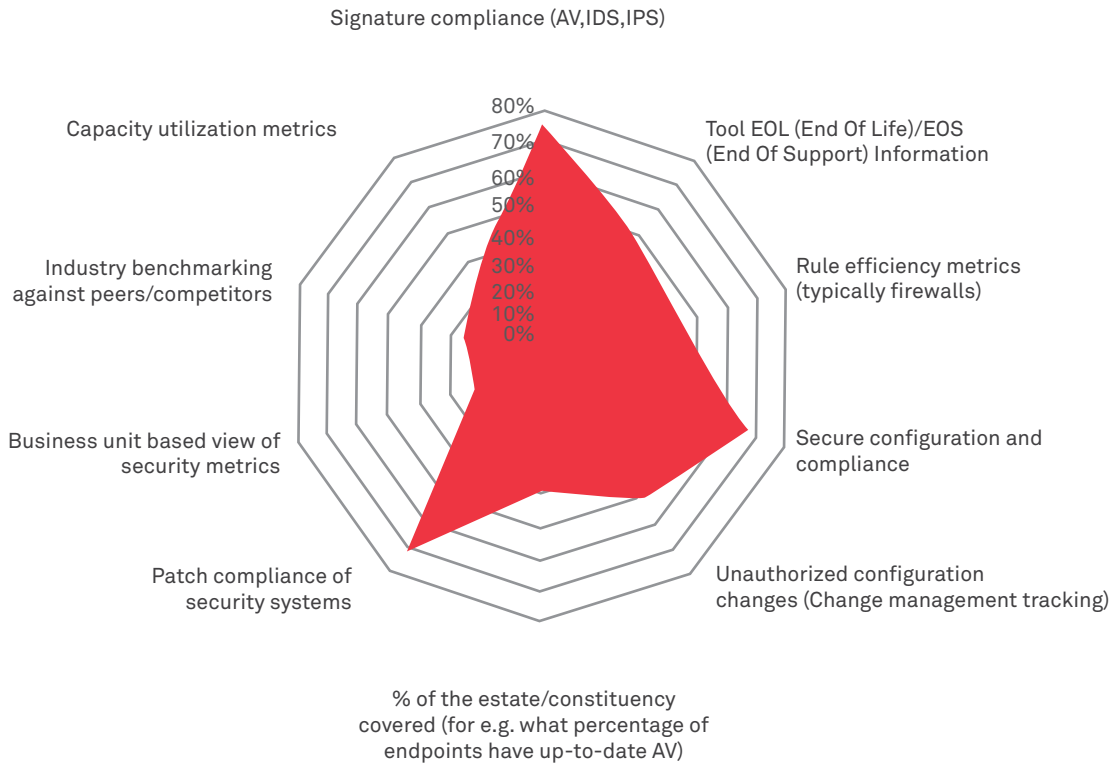


Figure 20: Metrics related to Preventive Controls used - 2017

- The BFSI (Banking, Financial Services and Insurance) sector was most focused on the metrics. More than 50% of the Banking and Financial sectors tracked almost all the metrics
- Financial Services sector respondents are the only ones to have industrial benchmarking in place, with around 63% indicating this. Outside the BFSI segments, only 21% have been able to achieve industry benchmarking
- One of the most desired metrics was to have a business-based view of the security controls. However, challenges in maintaining an optimal CMDB (Configuration Management Database) and business-based mappings greatly hinder this focus
- On an average, only 40% of the respondents had insights into the coverage their preventive tools provided

40% of the respondents had insight into coverage of preventive controls of their IT estate

63% of Financial Services sector had industry benchmarking of preventive security controls

Findings related to Detective Controls Metrics (Figure 21) -

Compliance with the latest signature/content/analytic packs, Threat coverage and Threat detection metrics were the top three detective controls across all correspondents

Relative usage of Detective Controls

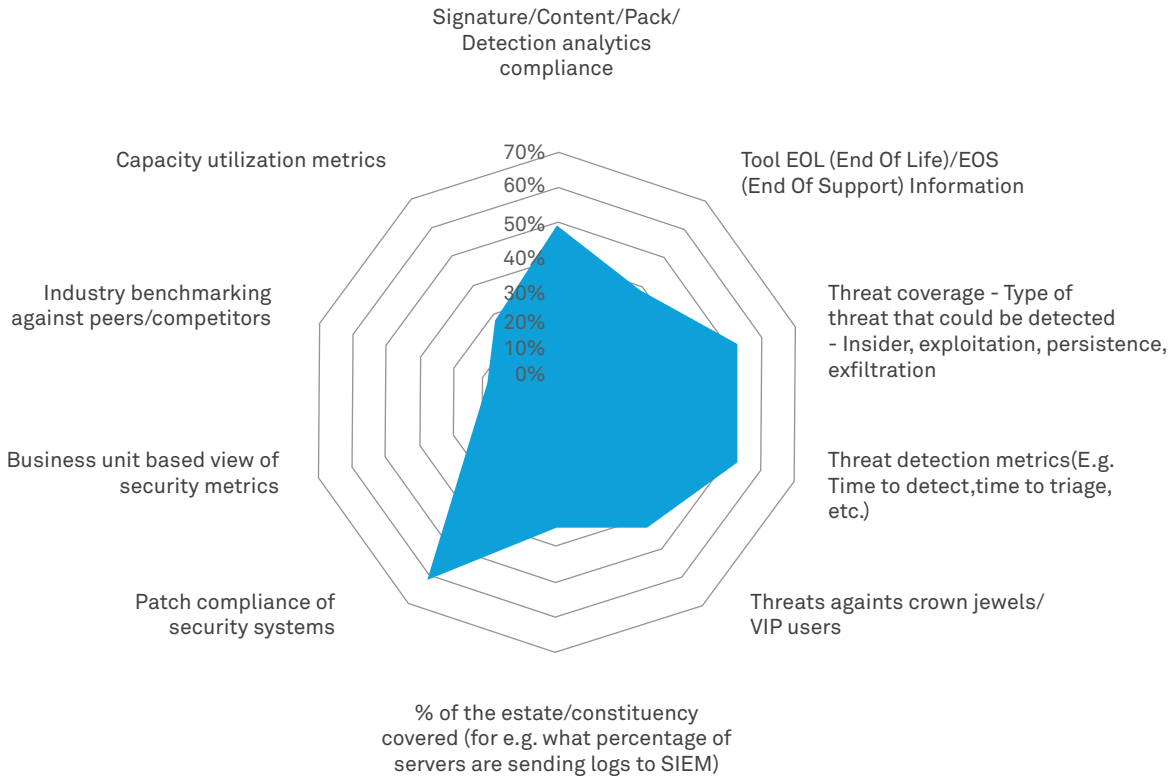


Figure 21: Metrics related to Detection Controls used - 2017

- Banking & Financial Services again show good governance in tracking detection metrics. Retail respondents also indicated a similar rigor in tracking metrics on the detection track
- From a Detection Coverage standpoint, our Retail, Banking, Financial Services and Energy & Utilities respondents have shown maturity in tracking the current detection capabilities across different attack categories. This usually helps SOC achive clarity regarding current gaps and make informed investments to enhance capabilities
- Visibility into current coverage inability to have a business-centric view and industry benchmarking still remaining the most challenging metrics to track

Banking & Financial Services, Retail enterprises have shown maturity in tracking detection metrics

Findings related to Response Control Metrics (Figure 22) -

Response metrics and ability to generate internal intelligence are the top tracked metrics across all correspondents

Relative usage of Incident Response Controls

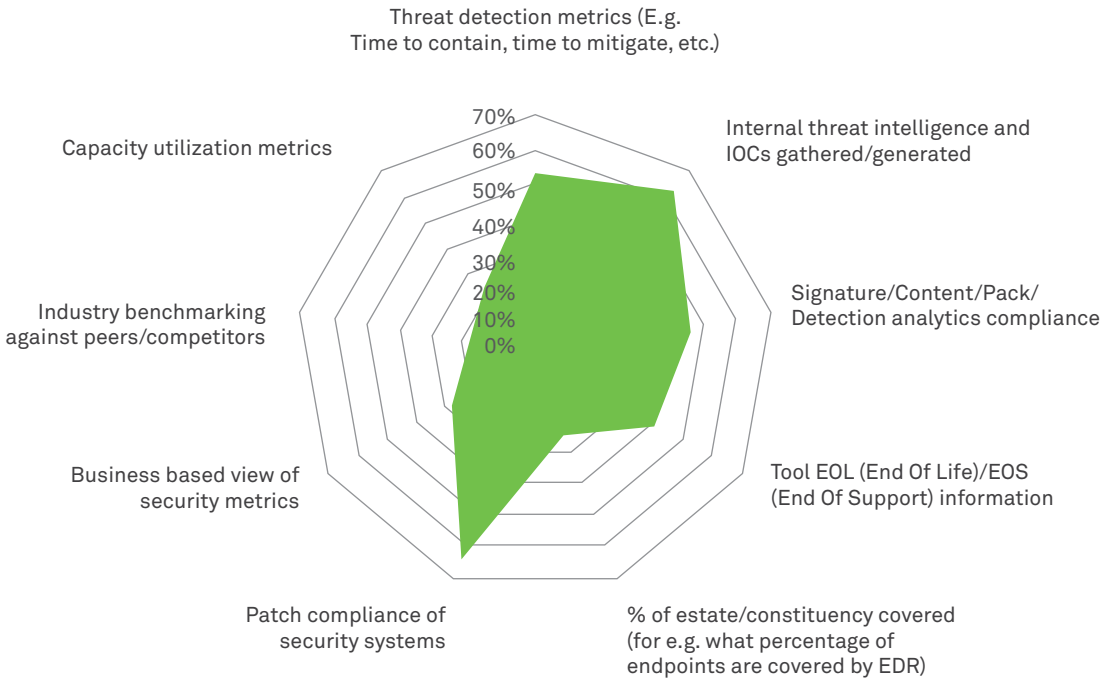


Figure 22: Metrics related to Incident Response Controls used - 2017

- Response metrics are scarcely tracked when compared to the other two controls. With the technology and focus on response readiness being more recent, most customers seem to have just embarked on the journey. Once fully operationalized these metrics would also follow the same adoption trend
- Interestingly, most Energy & Utilities, Retail, Banking & Financial Services respondents do track the value their response tools have added in generating internal threat intelligence. This could be indicative of a maturing Threat Analysis and Hunting focus amongst such enterprises

Incident Response Control metrics are scarcely tracked when compared to preventive and detective controls

A representation of the use of security metrics, defined across Preventive, Detective and Response Controls, categorized by industry verticals is shown below.

Preventive Controls	BFSI	Consumer & Media	ENU	Communications	Technology	Manufacturing
Signature compliance (AV, IDS, IPS)	71	77	100	83	50	88
Tool EOL (End Of Life)/EOS (End Of Support) information	61	69	14	42	33	13
Rule efficiency metrics (typically firewalls)	42	46	64	25	25	25
Secure configuration and compliance	63	77	86	75	75	25
Unauthorized configuration changes (Change management tracking)	58	42	57	75	8	63
% of the estate/constituency covered (for e.g. what percentage of endpoints have up-to-date AV)	47	31	29	42	33	63
Patch compliance of security systems	74	69	100	58	42	75
Business unit based view of security metrics	34	12	7	33	33	0
Industry benchmarking against peers/competitors	39	19	29	25	25	13
Capacity utilization metrics	42	27	29	33	22	25

Detective Controls	BFSI	Consumer & Media	ENU	Communications	Technology	Manufacturing
Signature/Content/Pack/Detection analytics compliance	56	48	46	45	33	38
Tool EOL (End Of Life)/ EOS (End Of Support) information	44	32	23	36	17	25
Threat coverage - Type of threat that could be detected - Insider, exploitation, persistence, exfiltration	61	52	54	36	17	25
Threat detection metrics (Ex. Time to detect, time to triage, etc.)	58	44	38	55	17	25
Threats against crown jewels/VIP users	53	28	31	45	8	38
% of the estate/constituency covered (for e.g. what percentage of servers are sending logs to SIEM)	36	40	38	27	25	50
Patch compliance of security systems	58	60	100	36	33	63
Business based view of security metrics	42	16	8	18	17	0
Industry benchmarking against peers/competitors	31	12	15	27	0	13
Capacity utilization metrics	31	24	15	27	8	38

Incident Response Controls	BFSI	Consumer & Media	ENU	Communications	Technology	Manufacturing
Threat detection metrics (Ex. Time to contain, time to mitigate, etc.)	66	33	42	50	55	57
Internal threat intelligence and IOCs gathered/ generated	69	67	67	50	36	57
Signature/Content/Pack/Detection analytics compliance	50	42	67	60	36	43
Tool EOL (End Of Life)/EOS (End Of Support) information	50	33	42	30	27	29
% of the estate/constituency covered (for e.g. what percentage of endpoints are covered by EDR)	28	25	17	10	18	43
Patch compliance of security systems	66	67	67	70	36	86
Business based view of security metrics	41	25	17	40	27	0
Industry benchmarking against peers/competitors	34	8	8	10	18	14
Capacity utilization metrics	34	13	8	30	18	29

(Please note – Blue colour implies relatively strong controls in place; White implies relatively medium controls; Red implies relatively weak controls or no controls at all. All numbers in the table are in percentage terms)

In the above representation, grouping of industry verticals has been done in the following manner:

BFSI – Banking + Financial Services + Securities + Insurance; Consumer & Media – Retail + Consumer Goods + Media + Transportation + Government; ENU – Energy and Utilities; Manufacturing – Manufacturing; Technology – Technology; Communications – Communications.

Human dimension

Despite innovative and strong technologies that can be deployed in enterprise networks and systems to prevent cyber-attacks, sometimes errant user behavior can be the weakest link in the security chain. Hence, many organizations invest time and money to educate their end users. In the survey, many respondents came back with e-learning being the top pick for security education followed by HR-based enforcement of policies. E-learning or computer-based learning was preferred by 78% of the respondents, followed by security policies and formal disciplinary processes that were polled by 70% (see Figure 23).

Approaches used to educate users against risky security behavior

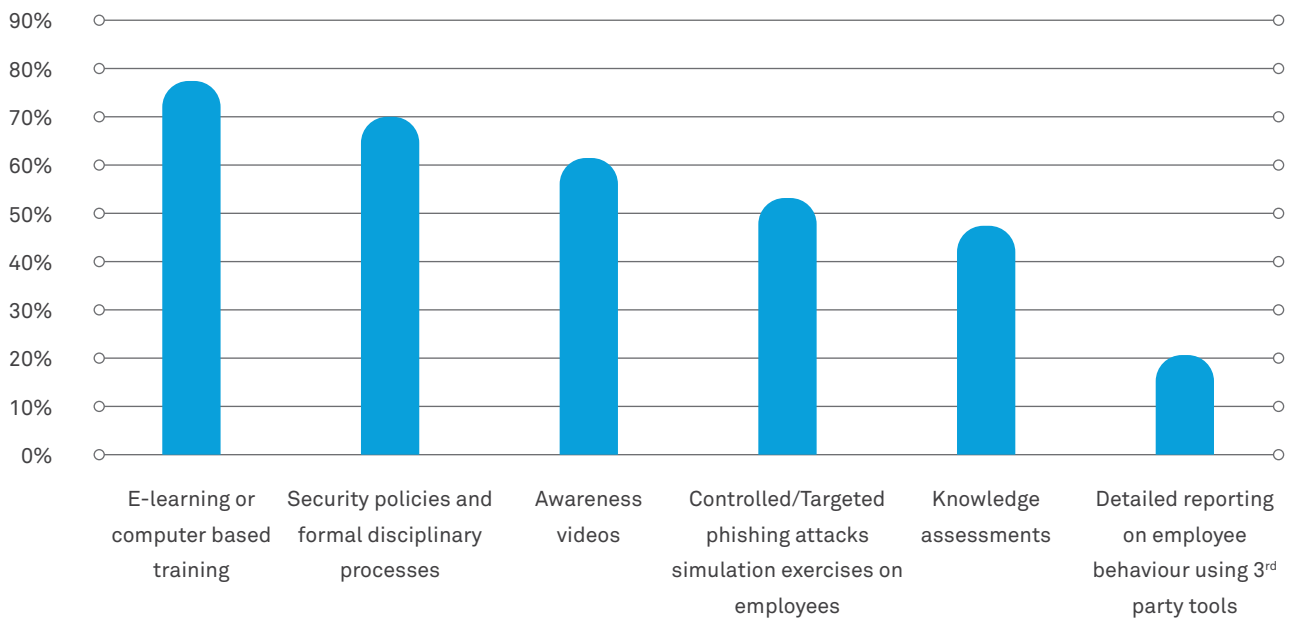


Figure 23: Approaches used to educate users against risky security behavior - 2017

Security competencies

In our 2017 Report we said that in the future, the battle is expected to be between the good and bad bots, with humans playing the role of orchestrators. This statement was made considering the overwhelming percentage of respondents who ranked ML/AI (Machine Learning and Artificial Intelligence) as their first preference when they were asked to rank critical security competencies for the future.

However, this time, when organizations were asked to rank the security competencies that they believe would help security practitioners excel in the cybersecurity domain, 31% ranked Security Architecture and Design as their first choice (see Figure 24). Both ML/AI and Risk Management and Compliance skills, which were ranked first by 19% each of the total respondents, mutually share the second spot.

Critical security competencies

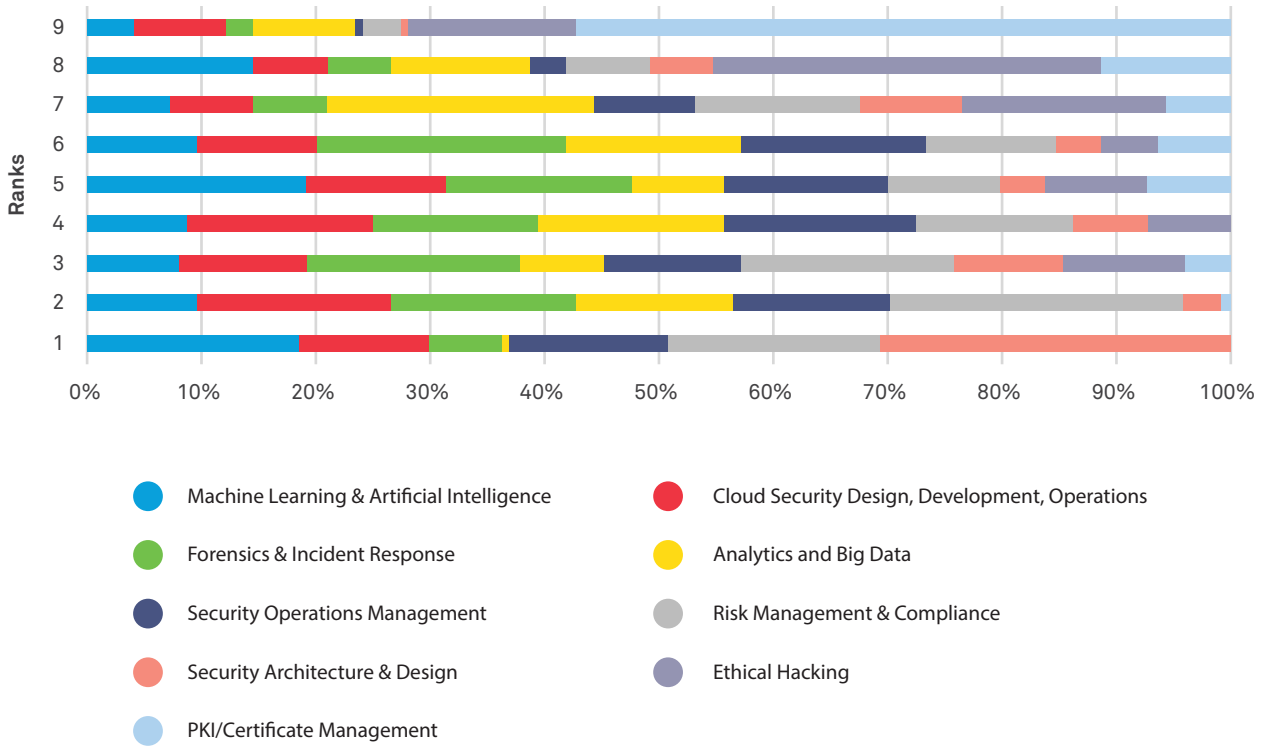


Figure 24: Ranking the most sought after critical security competencies - 2017

Data security

Investments in data security controls have grown steadily ever since the IT perimeter of the enterprise burst open and the free flow of data became essential. Various types of data security controls like Data Leak Prevention, Privileged Access Management (PAM), Data Obfuscation, etc. have been adopted for mainstream application. In the research, respondents were asked which data security controls gave them the most value. Figure 25 shows that 29% of the respondents ranked PAM (Privileged Access Management) as their first choice, which incidentally was also the first choice in 2016.

Effective data security controls

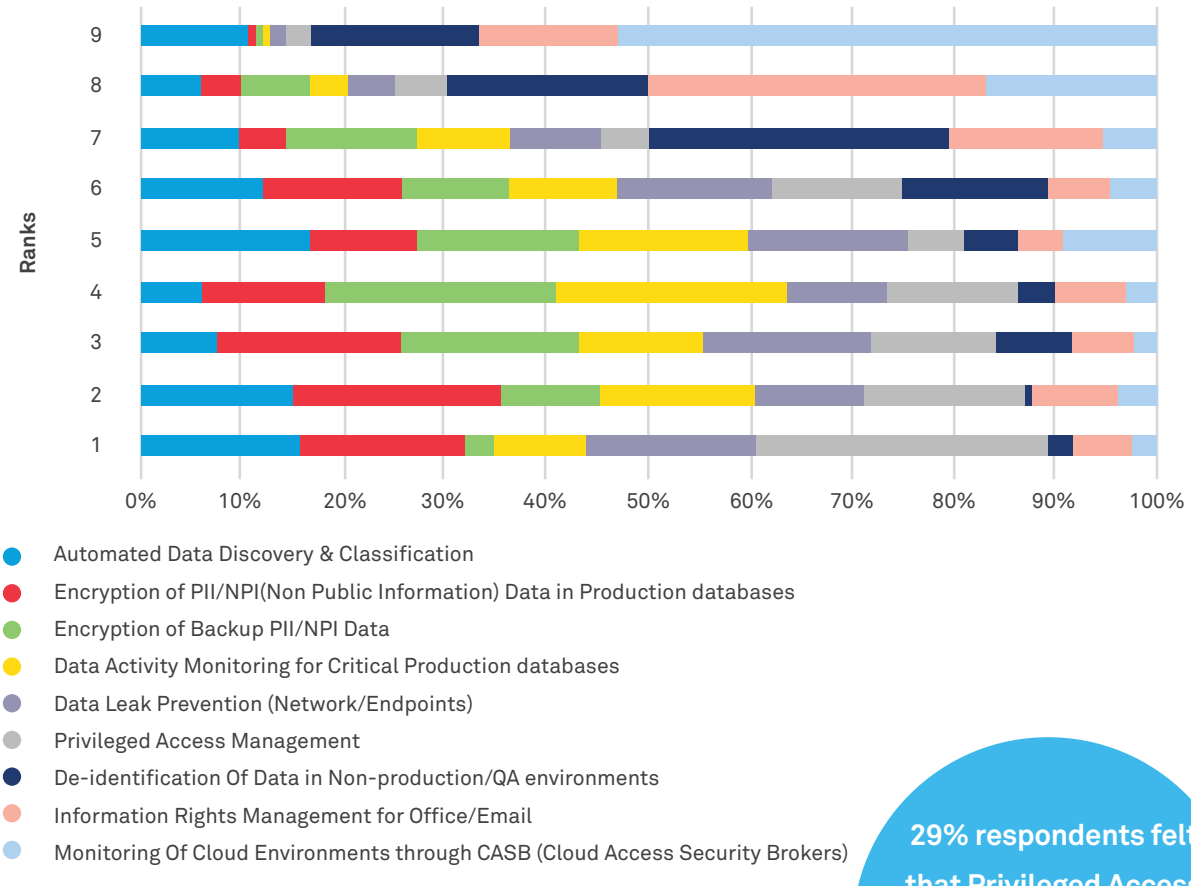


Figure 25: Data Security Controls ranked by effectiveness - 2017

29% respondents felt that Privileged Access Management (PAM) controls gave maximum value

Application security

Security vulnerabilities in sensitive applications of organizations are generally considered to be the hotcakes for hackers/attackers in today's business world. Throughout the lifecycle of an application, at different stages like design, development and operations, multiple processes are employed to mitigate the associated risks. Security assessments, which help organizations map their risks to business needs, hold special prominence.

When we asked a question on the frequency with which organizations were carrying out security assessments of business-critical applications, 22% said that they were doing it on an annual basis (see Figure 26). 21% said that they were doing it on a quarterly basis in 2017. This is an encouraging trend considering the fact that in 2016, quarterly was a preferred choice for only 12% of the respondents.

21% of the respondents said that they were testing their applications for vulnerabilities in every build, which remains unchanged from 2016. Organizations would be better off investing in testing for every build to minimize their application security risks.

Security assessments of business-critical applications

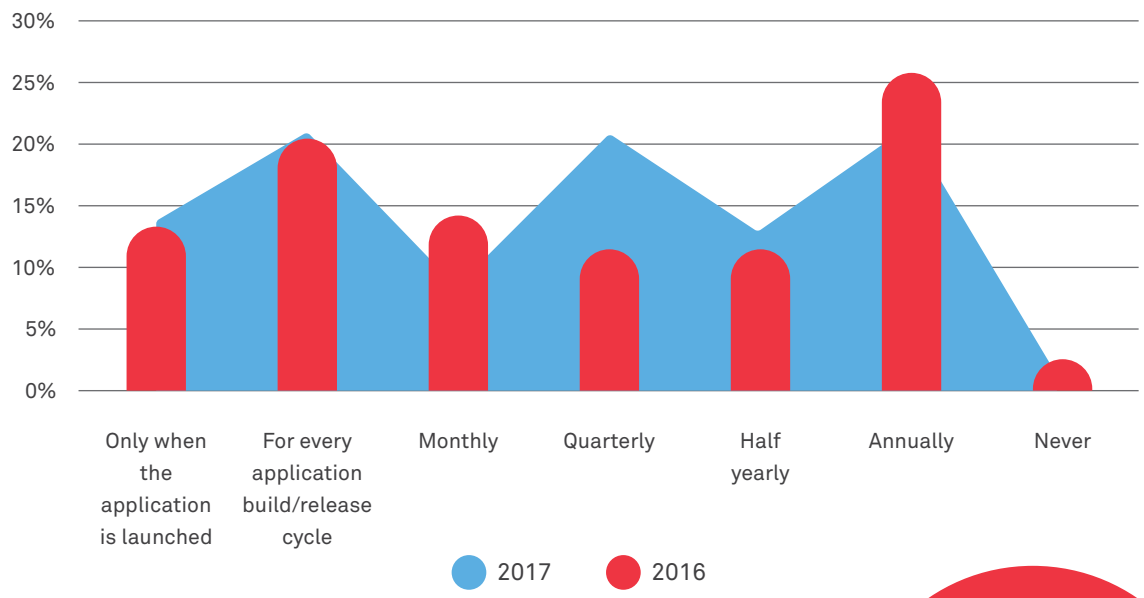


Figure 26: Frequency of security assessments of business-critical applications – 2017 Vs 2016

22% said that they were doing a security assessment of business-critical applications on an annual basis. In 2016 it was 26%

The survey also asked the respondents how much time was being taken to fix critical application security vulnerabilities. The finding that stands out in Figure 27 is that while 35% said that it took them at least one month to fix critical application security vulnerabilities in 2016, the percentage has significantly come down to 21% in 2017.

35% of the respondents in 2017 have said that they took a maximum of one week to fix critical application security vulnerabilities. In 2016 the same option garnered only 16%, which means a difference of nearly 20% points which is a clear indicator that organizations are waking up to the reality of application security attacks.

Time taken to fix critical application security vulnerabilities

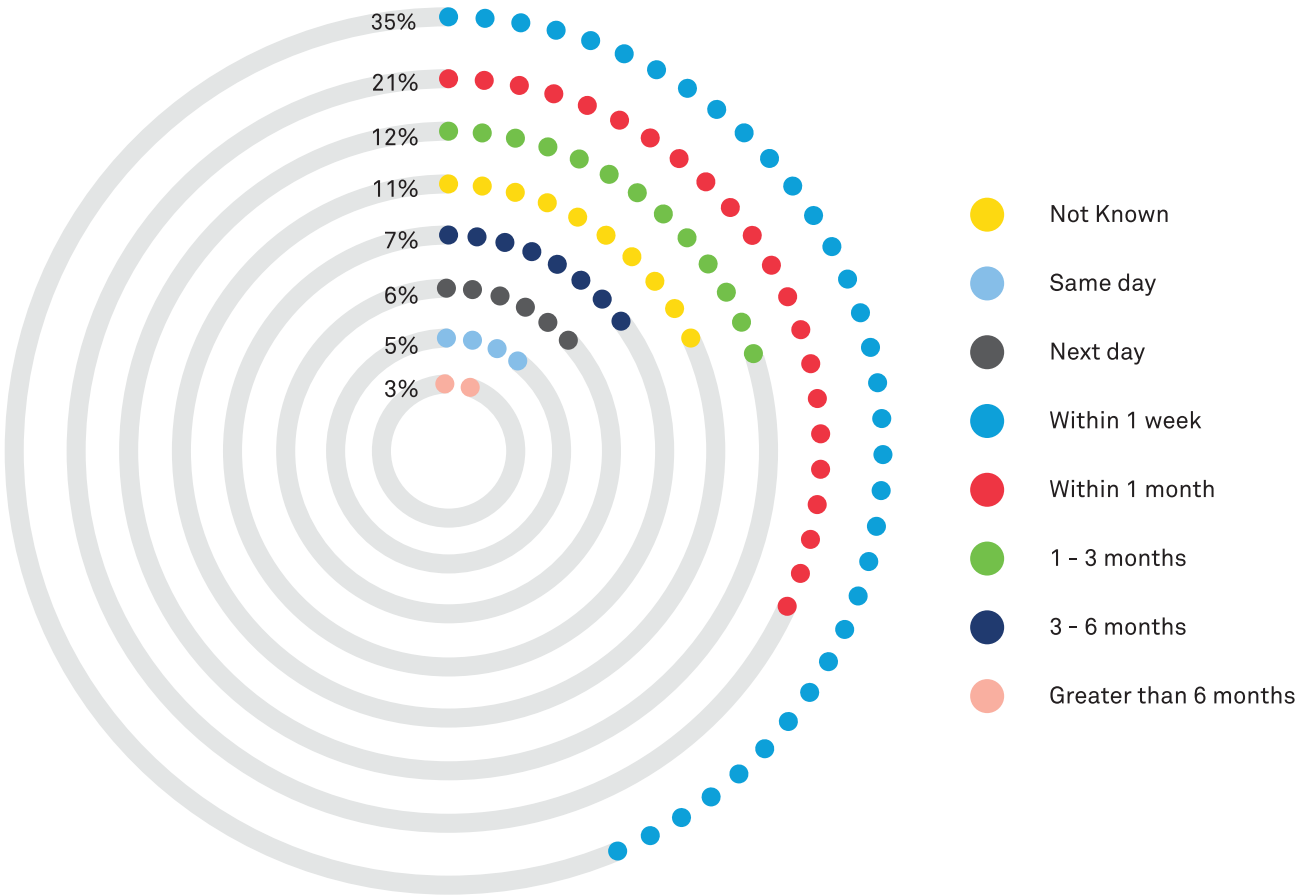


Figure 27: Time Taken to Fix Critical Application Security Vulnerabilities - 2017

35% of the respondents in 2017 have said that they took only 1 week to fix critical application security vulnerabilities compared to 16% in 2016

SecDevOps: Integrating application security testing into CI/CD pipelines

Organizations undergoing digital transformation feel pressure from several angles. First, they must go faster, driving innovation and bringing new products and services to market. In addition, they must address security. A failure to do so can have a tremendous negative brand impact and get organizations into trouble with regulators. Security needs to be embedded into any digital transformation, but the traditional approach is no longer viable. Addressing risk cannot be the last step in the process – a 'gate' to get through before a digital initiative can start providing value. This is a brittle approach that leaves organizations with security bolted on – at best – or simply ignored. In addition, it puts security into a position where they are anti-innovation, anti-progress, and anti- far too many positive things for the business. Instead, security needs to be integrated into the process and its risk management function needs to be a way for organizations to do more – both faster and safer.

DevOps

To go faster, organizations are starting to adopt new approaches to building the systems that support innovative products and services. The trend started out years ago as organizations moved from waterfall development methodologies to more agile approaches. This was a change in the way organizations organized their SDLC to do a better job of involving business stakeholders throughout the process. Involving these stakeholders allowed development teams to provide incremental wins and stay relevant to make sure what they were building was what the business needed in order to drive value.

Now we see organizations adopting DevOps principles to further accelerate innovation. DevOps is a cultural shift that aims to break down barriers between development teams and application operation teams. This casts off the practice of rare, monolithic application updates and ushers in the ability for organizations to rapidly update and quickly deploy applications. To be successful, it requires a culture of accountability and alignment.

Some DevOps practices can be alarming for security practitioners with a more traditional mindset. For example, if the line between development and operations is blurring, how do you enforce separation of duties? In addition, if you are releasing so frequently, how do you 'audit' the security of a build? However, forward-looking security practitioners should see the transition to DevOps as an opportunity to capitalize on rather than a trend to resist. At the end of the day they will lose that struggle – the business value of DevOps organization is too high to stymie the transition. Most importantly it represents an opportunity to use a time of change to better integrate security into business processes. DevOps transformations allow security to integrate their concerns and help transition the organization to SecDevOps.

Some key tools that organizations adopt as part of their DevOps transitions are Continuous Integration/Continuous Delivery (CI/CD) pipelines. These are upgrades to the traditional software build process that are crafted to quickly analyze the state of a new build and determine if it is suitable for delivery or deployment. These pipelines build software and run functional and non-functional tests on incremental updates to identify if recent changes have introduced any defects into the software that would preclude a release. The goal is to make both application development as well as application operations teams comfortable with their increased tempo of development and release.

Application security testing in CI/CD pipelines

How do leading organizations best integrate application security testing into DevOps and – specifically – into CI/CD pipelines? First, it is critical for security practitioners to understand their limitations. Before setting goals, security teams must endeavor to understand how DevOps teams are organizing their efforts, and the environment into which security must be integrated. As mentioned above, some practices in DevOps can seem foreign to security practitioners

and an understanding of the tools and practices of DevOps teams can help set reasonable expectations. One chief limitation is typically a requirement for speed. Organizations adopt CI/CD pipelines so that they can quickly 'bless' builds for further promotion and often deployment to production. The key concept here is 'quickly.' If an organization is trying to deploy new builds to production multiple times per day – or at least to determine that new builds of software are acceptable to promote to production – this places a constraint on how long the build and evaluation process can run. Given this goal, the time taken by security-specific tasks must be limited. If security teams assume that they will be able to complete full runs of a typical static analysis security testing (SAST) tool on a large codebase as part of their contribution to application security testing in CI/CD pipelines they are likely to be disappointed. Another limitation is a requirement for automation. Given the pace required to evaluate new builds, no part of the process can require manual intervention. This will significantly limit the types of security activities that can be integrated into CI/CD pipelines.

Based on an understanding of the challenges that security testing will face in a CI/CD pipeline, security teams can then work to set appropriate goals. Given the limitations outlined above, security teams need to determine what security evaluation tasks make sense to integrate into CI/CD pipelines. Activities that we have seen successfully integrated into CI/CD pipelines include:

- Differential SAST scanning with a limited ruleset focused on high-value results – serious vulnerabilities whose signatures are strong enough to limit the number of false positives
- Differential dynamic application security testing (DAST) scanning targeted at pages that are new or were modified since the last build
- Checks for open source components with known vulnerabilities that have been included in the build
- Basic checks for common application misconfigurations

Note that these tests have some things in common: they run quickly, they have little enough ambiguity that there should be few false positives, and they only cover a subset of what might be considered a 'complete' security analysis. It is critical to set expectations. The entirety of an application security testing program cannot be stuffed into a CI/CD testing pipeline. Thorough automated scanning takes too long to run and results in too many false positives, and comprehensive application security testing must also include a significant manual component. The goal here is to identify a subset of important issues with high confidence early in the process, and to provide quick feedback to developers so those issues can be resolved.

The value of SecDevOps for digital transformation

As outlined above, integrating application security testing into CI/CD pipelines benefits both security and development teams by identifying potentially serious vulnerabilities earlier in the development process so they can quickly be addressed. In addition to this obvious benefit, this integration helps to get the security team a seat at the table during this critical cultural transformation. Just as walls are coming down between application development and operations teams, security teams can also meaningfully involve themselves in the process, creating opportunities for them to act as a valuable risk-management resource. This sort of alignment between development, operations, and security teams, is crucial for organizations looking to innovate faster and bring new products and services to market while appropriately managing their risk exposure.

Partner Content Credits: Contributed by Wipro's partner Denim Group (www.denimgroup.com).

Network DDoS protection

In our 2017 Report we talked about how some of the biggest DDoS attacks of 2016 have managed to scale up their size to astonishing figures like 990 GBPS, for example, in the case of the OVH.com (French Web hosting company) DDoS attack. DDoS attacks continue to grow in size and frequency of attacks. Our research shows that this phenomenon is caused mainly because of two reasons. One reason is, as we observed last year as well, the growth of new technologies such as the Internet of Things being used by attackers as launch pads for carrying out DDoS attacks. The other reason is the easy access of DDoS attacks through DDoS for hire services which makes the job easy for beginners who lack sound IT or security knowledge to catapult threatening attacks.

In 2016, while 34% of the respondents had said that they experienced a DDoS attack which lasted more than 30 mins, in 2017 the percentage dropped down to 29% (see Figure 28). However, in 2017, 8% of respondents have said that the attack lasted more than a day when compared to only 4% in 2016. In 2017, the longest DDoS attack that was observed was on a Chinese telecom company which lasted for almost 11 days. Also, the percentage of respondents who said that they didn't experience any DDoS attack went up from 42% in 2016 to 56% in 2017.

Peak DDoS attack duration

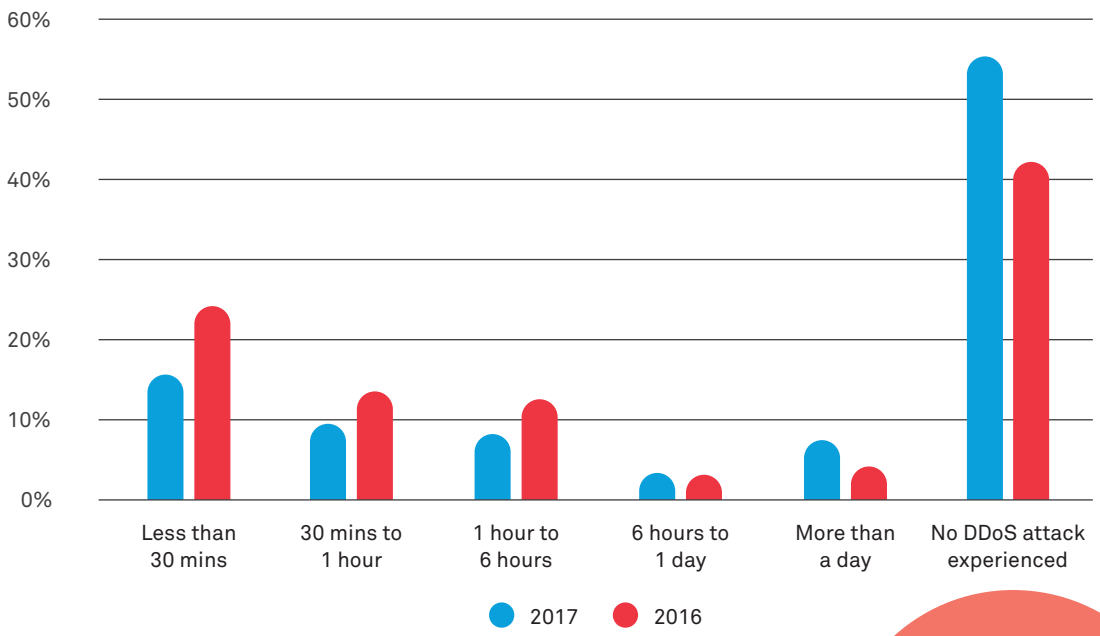


Figure 28: Peak DDoS attack duration – 2017 Vs 2016

29% of the respondents said they experienced a DDoS attack, which lasted more than 30 mins

8% of respondents in 2017 have said that the attack lasted more than a day when compared to only 4% in 2016

The survey also explored the type of defense mechanisms that were popular against DDoS attacks. Figure 29 shows that 67% of the respondents were reliant on intelligent DDoS prevention systems to contain DDoS attacks when compared to 51% in 2017.

DDoS mitigation techniques

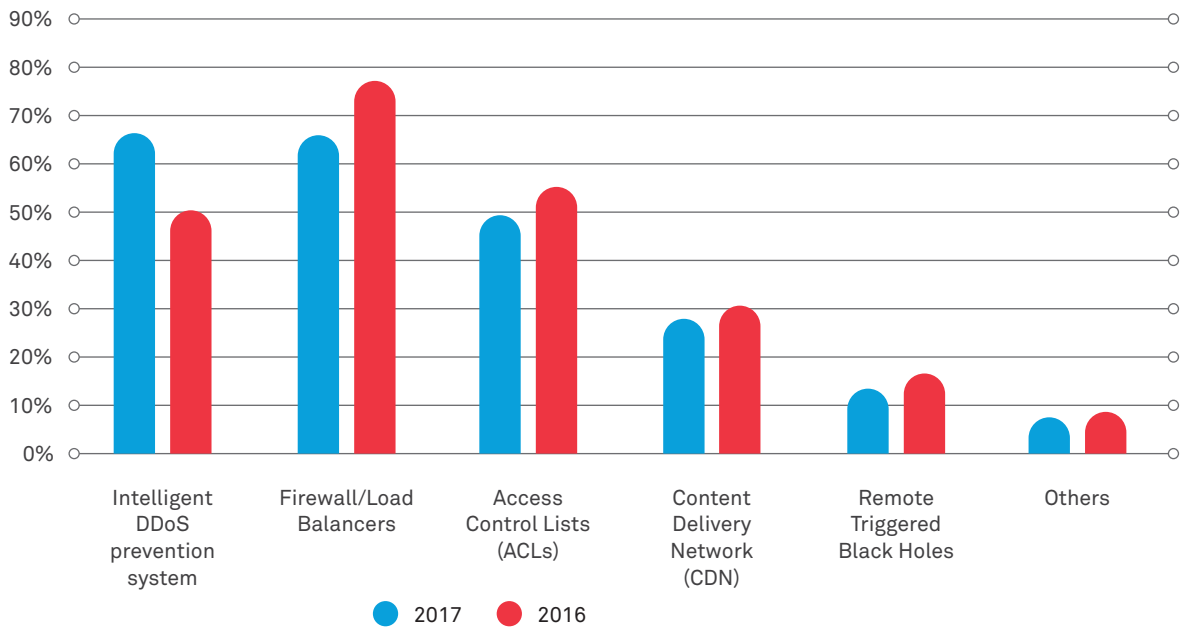


Figure 29: DDoS mitigation techniques leveraged by organizations – 2017 vs 2016

Traditional techniques like Firewall/Load Balancers are still popular with the respondents, as 66% of the respondents have opted for them to contain DDoS attacks.

67% of the respondents preferred techniques like intelligent DDoS prevention systems to contain DDoS attacks (an increase of nearly 16% points from 2016)

Endpoint security

Relentless security attacks routed through the end user/endpoint have resulted in the placement of endpoint security as a foundational/strategic focus area of cybersecurity.

Endpoint attack vectors

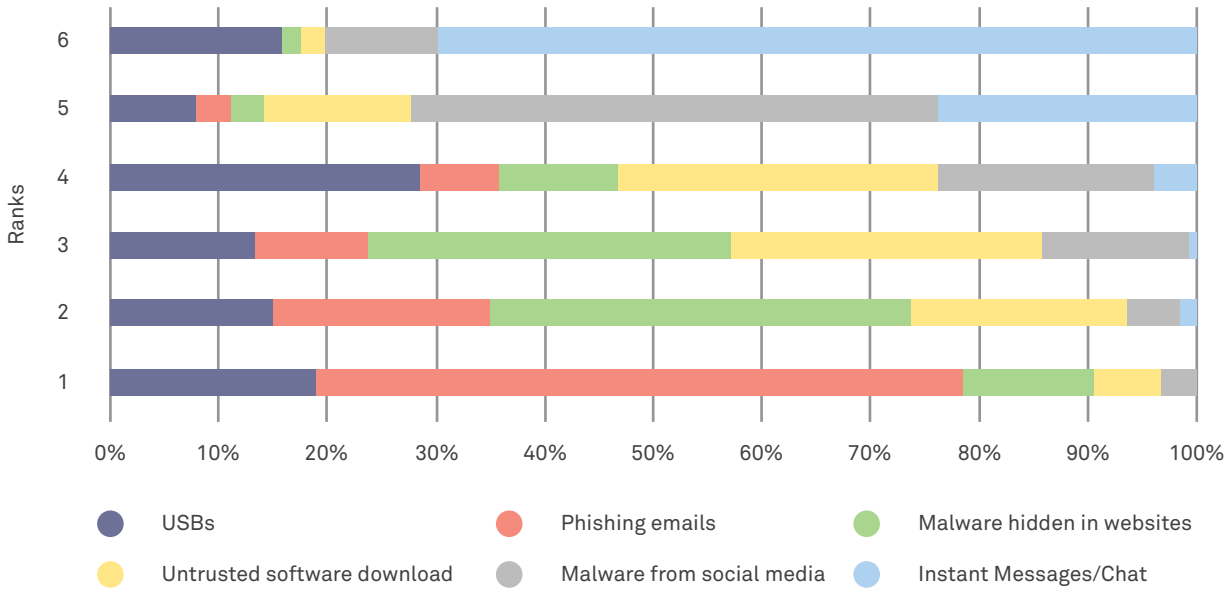


Figure 30: Endpoint attack vectors ranked by frequency - 2017

In 2016, when we asked about the most common vectors that lead to compromise of endpoints, 59% of the respondents ranked phishing emails as the first option among others such as USBs, malware hidden in websites, untrusted software download, malware from social media and instant messages/chat.

Surprisingly, as Figure 30 shows, findings from 2017 only reinforced the results of 2016. In 2017, 60% of the respondents have ranked phishing emails as the primary vector. 39% of the respondents have ranked malware hidden in websites at the second position.

60% of the respondents have ranked phishing emails as the primary vector of endpoint attack

Endpoint mitigation techniques

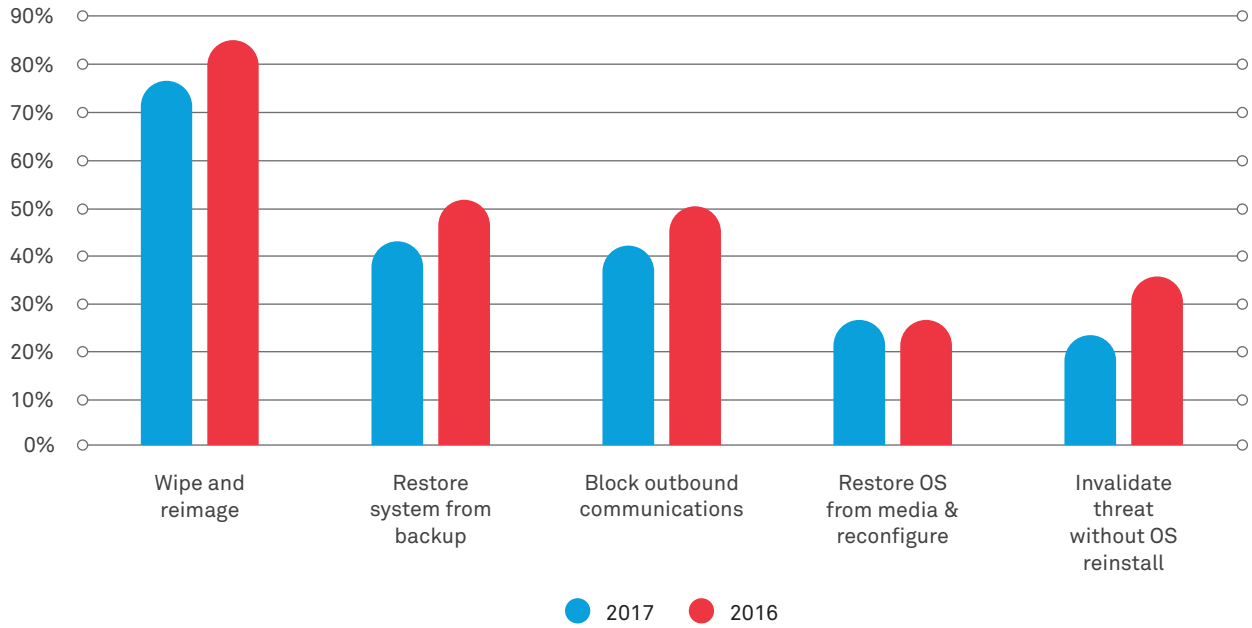


Figure 31: Endpoint mitigation techniques leveraged – 2017 Vs 2016

Wipe & reimage still ranks the first with 77% of the respondents opting for it as a technique to remediate/restore compromised endpoints

In terms of the techniques employed by organizations to remediate/restore compromised endpoints, wipe and reimage still ranks the first with 77% of the respondents choosing it among other options like restore system from backup, block outbound communications, restore OS from media & misconfigure and invalidate threat without OS reinstall (see Figure 31).

Restore system from backup and block outbound communications mutually share the second place as nearly 43% each have chosen them.

Security monitoring and analytics

As highlighted in Section 1, data breaches are on the rise and with the kind of advanced techniques employed by the attackers, threat detection assumes the highest priority for organizations to thwart future attacks. The security monitoring and analytics discipline plays a very important and distinct role in terms of threat detection mechanisms.

In 2016, 83% of the respondents said that they were able to contain and recover from cyber-attacks within a week. In 2017 the figure went up to 87% which is a welcome sign (see Figure 32).

Time to contain attacks

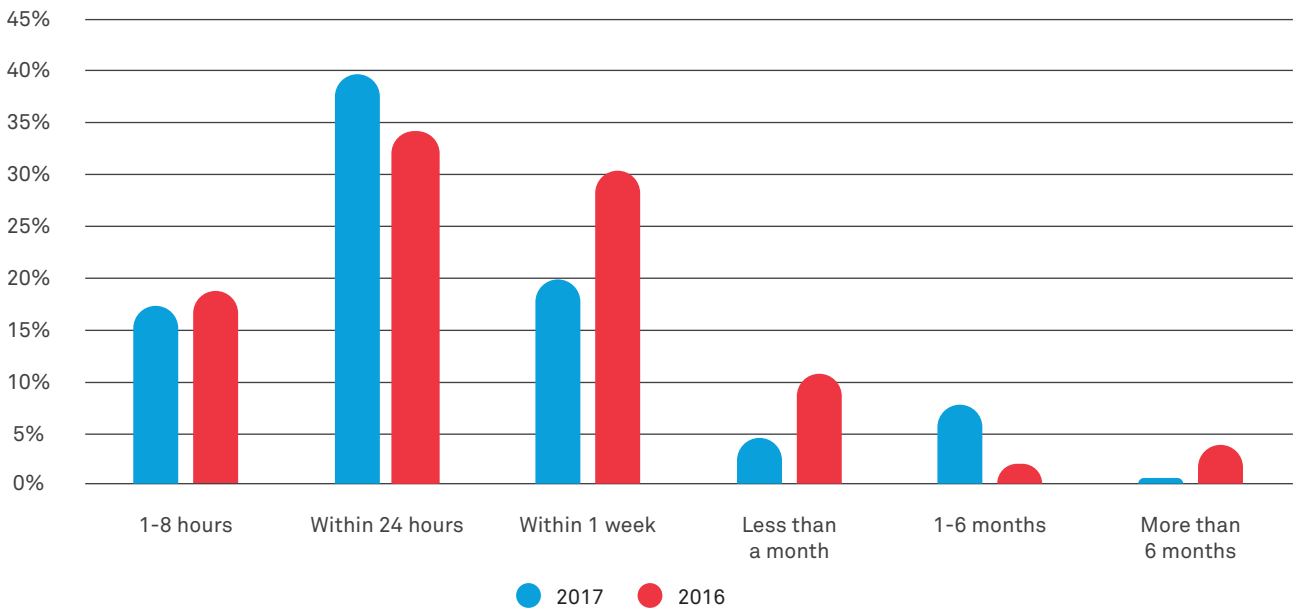


Figure 32: Time taken to contain and recover from attacks 2017 Vs 2016

87% of the respondents said that they could contain and recover from cyber-attacks within a week

When asked about the toolsets contributing to security event notifications, SIEM was still the preferred choice for 85% of the respondents in 2017 (see Figure 33). In 2016, SIEM was preferred by 82% of the respondents. The second most effective control chosen by respondents were perimeter defenses like firewall, IDS/IPS by 77% of the respondents when compared to 79% in 2016.

Tools contributing to most security event notifications

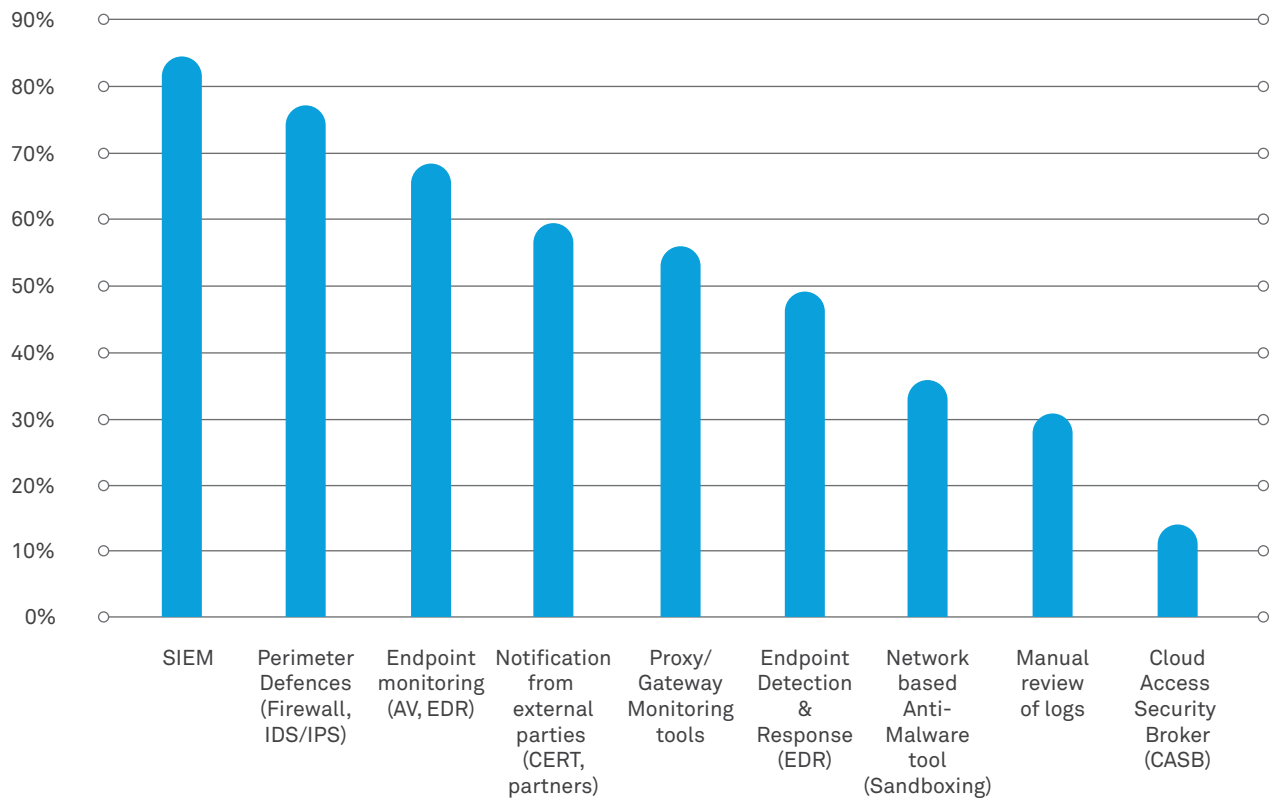


Figure 33: Tools contributing to most security event notifications - 2017

In 2017, SIEM was still the most preferred choice for 85% of the respondents – an increase of nearly 5% points from 2016

With respect to the opportunities that businesses saw in helping them to improve their threat detection capabilities, Figure 34 shows that 68% preferred implementation of automation tools. Only 56% of the respondents chose this option in 2016. Compared to 2016, the threat intelligence option witnessed a downfall of 14% points. 67% of the respondents still see threat intelligence integration as something that can help them to improve their threat detection capabilities when compared to 81% in 2016.

One of the influential reasons behind security automation taking the first place in 2017 could be because SOC teams are increasingly relying on automation to reduce their dwell times.

Opportunities to improve threat detection

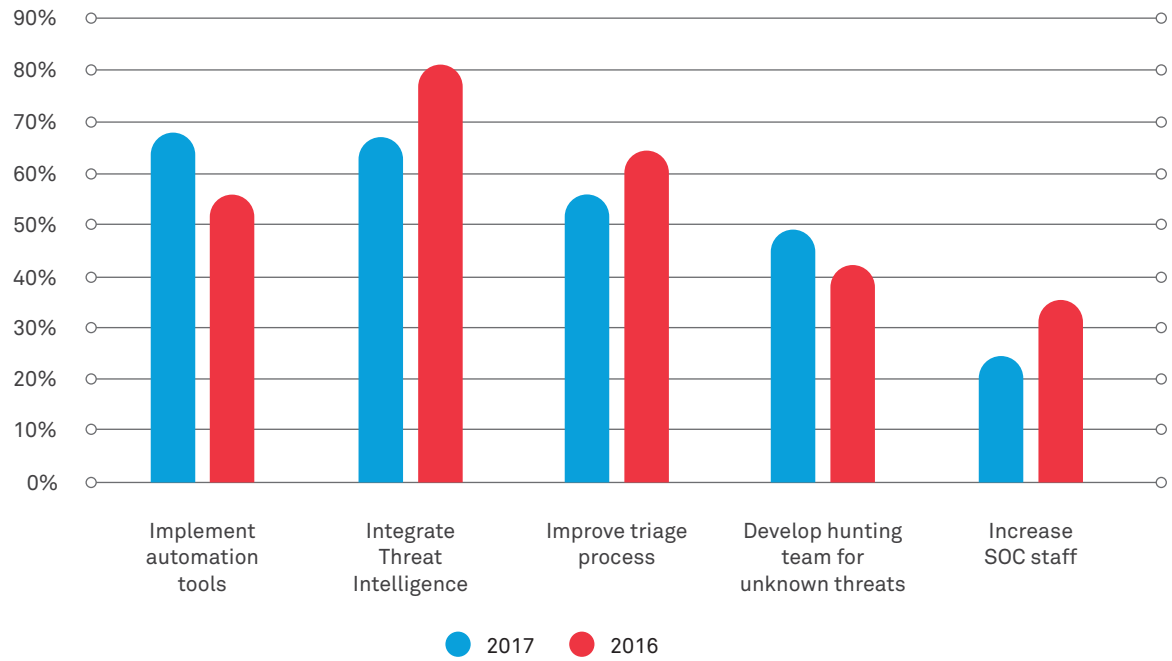


Figure 34: Opportunities to improve threat detection capabilities – 2017 vs 2016

68% of organizations preferred the implementation of automation tools to help them improve threat detection and containment time

Cloud security

As the adoption of cloud services has increased rapidly over the last few years, from Infrastructure as a Service (IaaS) to Platform as a Service (PaaS) and to Software as a Service (SaaS), there is a very visible shift in the areas where the efforts are focused: From the traditional model, where the execution environment is managed by a dedicated operations team within the environment, to the newer models where managing the execution environment is left to the experts (Cloud Security Providers), the focus has shifted towards the development/configuring of applications. In the primary research survey, the question of preferred choice of cloud model was posed to the respondents keeping the security constraints in mind. The finding from the survey, shown in Figure 35, indicated an increased preference for adoption of Platform as a Service (PaaS) and Software as a Service (SaaS), at 40% and 55% respectively.

Usage of cloud deployment models

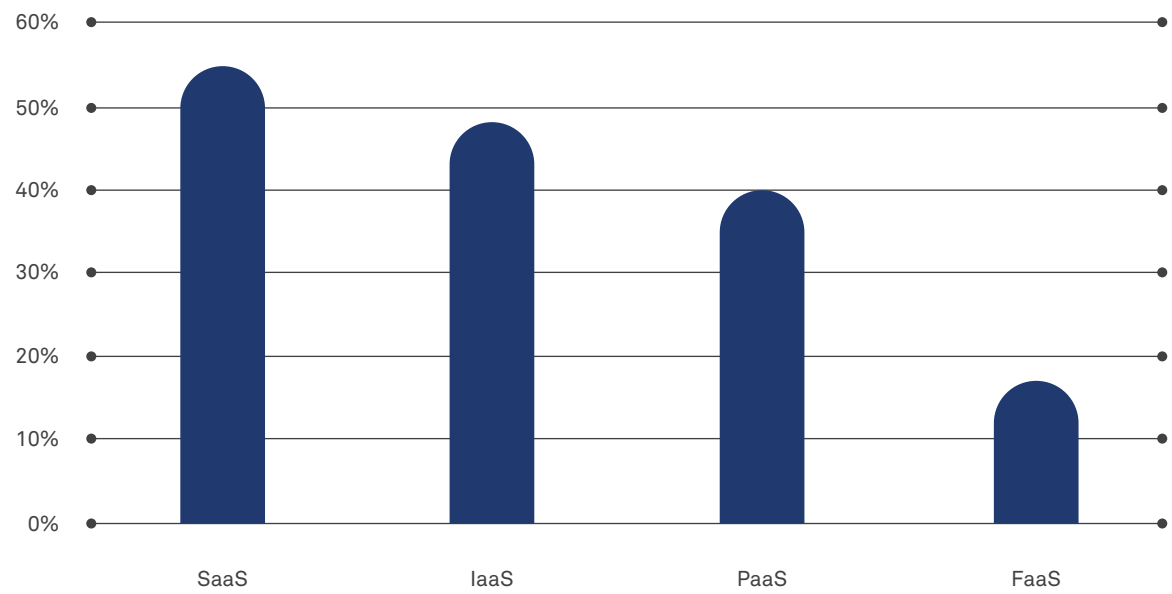


Figure 35: Preferred cloud deployment model within security constraints - 2017

Two interesting facts have emerged from the survey:

- There is still a high usage (48%) of Infrastructure as a Service. This can be attributed to the fact that it is not easy to migrate traditionally built monolithic applications to a newer model
- Function as a service (Serverless computing), a next step to the theme of 'reduced management of the execution environment' is slowly gaining wider acceptance (17%).

Serverless computing/FaaS

Serverless computing can be defined as, "a cloud computing model of design and deployment, in which, the resources to run applications or services are dynamically allocated by the cloud service provider and scaled up and down as per the current load, without the need to pre-set any upper or lower thresholds. The cost associated in this model is purely based on the actual usage of resources and there is no cost for idle time of the resources."

Serverless computing/FaaS is slowly gaining popularity with 17% of the respondents already having adopted it

In Serverless computing, are servers not used at all? The name is a misnomer as Serverless computing does involve servers. To avoid the confusion, the new term "Functions as a Service" is used instead, which is a more accurate description for this model of deployment.

How is Function as a Service different from Platform as a Service?

In the PaaS model of deployment, typically one single monolithic application is deployed and there is a perpetual process running on the server to execute requests as and when they arrive. Whereas in a FaaS model of deployment the application is broken down into smaller functions and each function is deployed independently. Each function is run on demand when some event is triggered.

In the PaaS model of deployment one still needs to give some thought to the servers, like the minimum and maximum number of servers (VMs) required to manage the load, the criteria (%CPU usage, %RAM) on which servers should be ramped up or down, etc. Whereas in the FaaS model of deployment one does not need to think of the servers or the capacity. The cloud service provider dynamically allocates resources to execute the required function and scales as per the current load.

FaaS is made available by various providers, the most popular being AWS Lambda. Others include Microsoft Azure Functions, Google Cloud Functions, IBM/Apache's OpenWhisk, hook.io, Oracle Cloud Fn, etc.

Pros and Cons of Functions as a Service

There are various advantages to move towards the FaaS architecture. In addition to all the advantages that come with migrating to the cloud, there are additional advantages of moving towards a FaaS architecture model:

- Focus on functionality – developers can focus on the actual development of the code, logic and the functional requirements and not worry about some of the non-functional requirements like Infrastructure management, scalability, capacity, application resilience, etc
- Reduced cost –IaaS and PaaS reduce CapEx for an enterprise. The FaaS model takes this to the next level by bringing down not only CapEx but also the OpEx of an enterprise. With FaaS, resources are dynamically allocated when there is a trigger for a function and the cost is calculated only for the duration of execution of the function. In a nutshell, cost of idle resources is avoided, and we literally get close to the often-used cloud phrase – "pay for what you use"
- Highly scalable and resilient – with FaaS, requests are served by dynamically allocated resources without a need to specify the minimum and maximum capacity. The cloud service provider owns the responsibility to scale up and ensures sufficient computing resources are made available as per the load, making the overall application code more resilient under heavy load

Though there are advantages that come with FaaS, there are some disadvantages as well:

- Increased complexity – breaking a large monolithic application down into smaller deployable functions makes the architecture complex. The functions by themselves become simple but the system becomes complex due to the various inter-dependencies. Managing multiple functions, however small they are, is more complex than managing one large monolithic application
- Potential redesign - a very basic need of a FaaS architecture is to make the functions stateless and hence an existing stateful application will have to be completely re-designed
- Relatively higher latency – when compared to other 'as a service' models, where there is a perpetual process always running to execute an incoming request, FaaS resources are dynamically allocated as and when a new request arrives. This requires some initialization and warm-up time, especially where functions are accessed infrequently, leading to higher latency
- Difficult to debug – because of the ephemeral nature of the environment where the code is executed, debugging and identifying root-cause of issues becomes difficult

Security considerations of Functions as a Service

- As the underlying infrastructure is managed by the cloud service providers and managing servers being their core competency, one can be assured that the servers will be patched regularly and in a timely manner. This reduces the major risk of exploiting known OS-level vulnerabilities and preventing WannaCry type of attacks
- Because the servers in FaaS are ephemeral, long-lasting attacks based on compromised servers become redundant
- Because the resources are dynamically allocated on demand, DOS attacks to overload the servers might not be successful but could really stretch the bills
- The application code is still written by the same developers - so the application level vulnerabilities remain the same and hence OWASP top 10 is still relevant. Along with the application code, third party application dependencies are equally vulnerable and remain a threat if not updated in a timely manner. These threats become more relevant with FaaS because of the reduced attack vectors available for attackers
- Access privileges under FaaS need to be managed at individual function level rather than at an application level. If neglected, this could become a bigger attack vector in FaaS
- Concerns related to Data-in-Transit and Data-at-Rest remain. The functions which previously used to run on a single server will run on different servers in the FaaS model and hence there will be more data in transit. If appropriate controls are not put in place, it could lead to bigger security concerns
- And finally, security monitoring becomes extremely difficult. The current monitoring solutions do not necessarily work with the FaaS model given that most of the solutions require an agent to run on the server and in the FaaS model the servers are ephemeral. The agents could still run on these ephemeral servers but the overhead these would create further deteriorate performance, which is already a drawback of FaaS. Over time, monitoring solutions will evolve and this concern could be alleviated

Challenges to migrate to the FaaS model

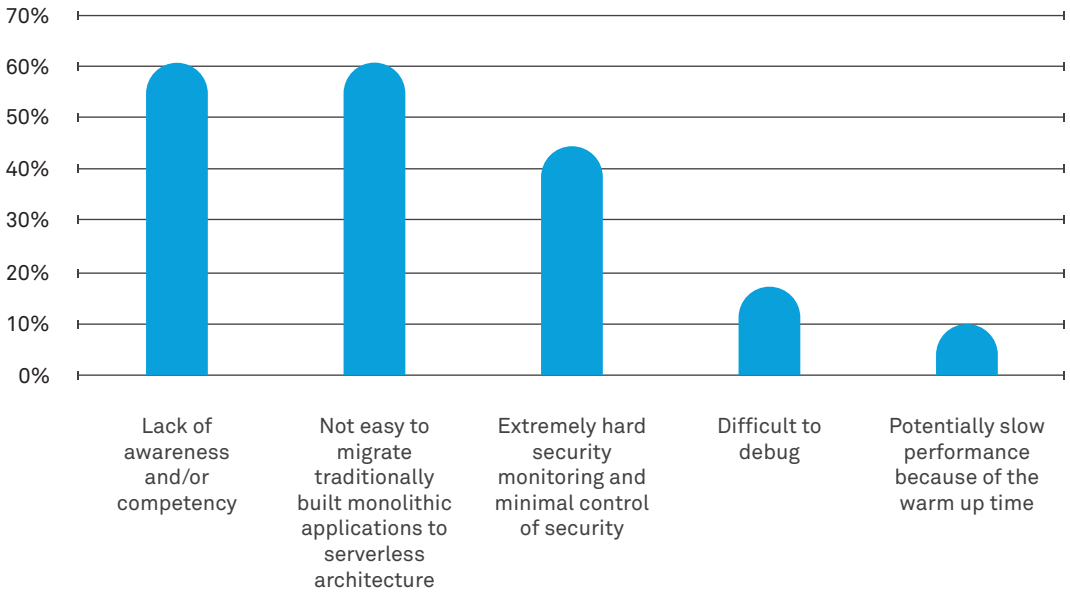


Figure 36: Challenges to migrate to the FaaS model - 2017

Security monitoring in FaaS environments is a challenge for enterprises

As the survey tells us, with increased awareness and competency and better monitoring solutions in place (see Figure 36), more and more applications would move towards the FaaS model. With that, application security would be a bigger focus than what it is at present and developers would be held more responsible to write secure code.

IOT security

IOT adoption in enterprises is clearly still in its infancy. With the ubiquitous availability of sensor-based devices, enterprises are able to collect data, process them in the cloud and using insights, to take timely action. Health systems are being IOT enabled, factories are having their assembly lines enabled with connected robotic devices and energy and utilities industries are also beginning to use sensors and data to better streamline their delivery mechanisms. In all of this, the use of IOT is plagued by one common challenge – that of an inferior level of security. The lack of strong built-in security functions is the result of low compute capability, minimum security functionality being factored in design, minimal instances that support over the air patching, etc. What makes the security problem more complex is the presence of a multitude of hardware devices and software platforms - unlike the PC world where variety was limited.

As part of the primary research, one of the questions asked to respondents was the percentage of their IT assets that were IOT based currently and what that would look like, a year from now. A majority of the respondents indicated that they had less than 5% of their asset base recognized and tagged as IOT but expected it to double and grow to 5-10% in the next one year (see Figure 37 for details). This influx of IOT devices could be in specific business units or could be due to common administrative functions such as facilities management.

IOT assets share among IT assets

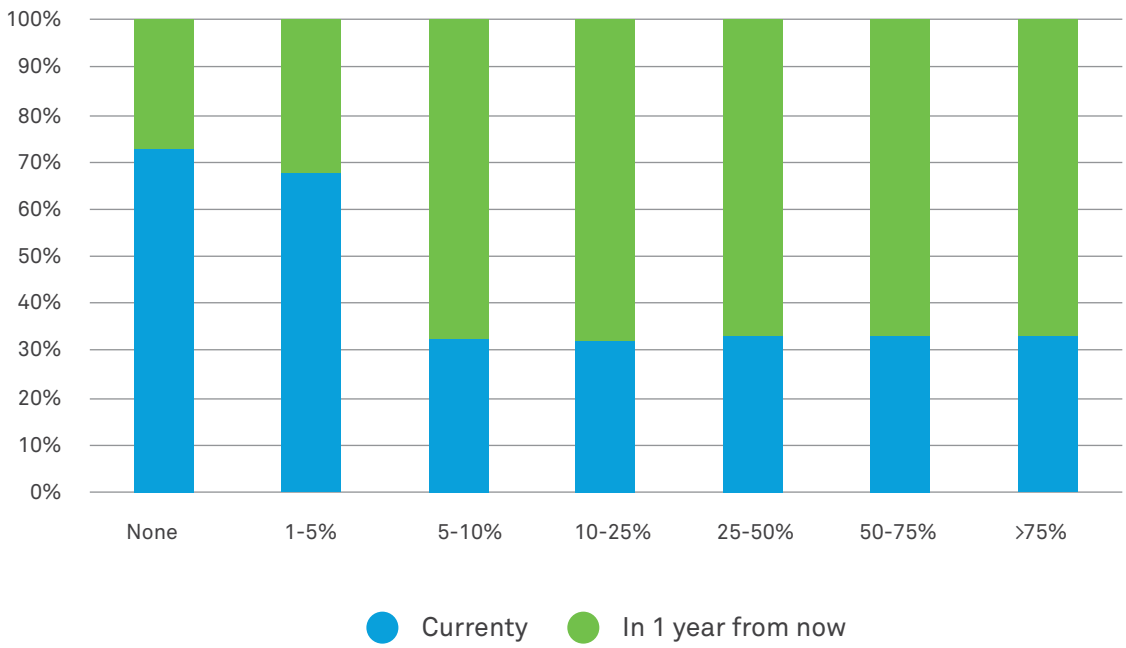


Figure 37: Percentage of IT assets that were classified as IOT - 2017

We also asked the respondents, what kind of IT controls were deployed or were planned to be deployed in the next 2 years related to mitigating IOT threats. Many respondents indicated that security log monitoring was the route they took to monitor presence and activity of IOT devices. But as Figure 38 shows, most respondents indicated that in two years they would be exploring agentless network threat detection solutions that could identify threats emanating from new IOT devices using machine learning and such techniques.

A significant percentage of the organizations are planning to have agentless network threat detection and network segmentation IOT controls in the next 2 years

74% of the organizations have currently IOT security assessment controls in place already

IOT risks mitigation controls

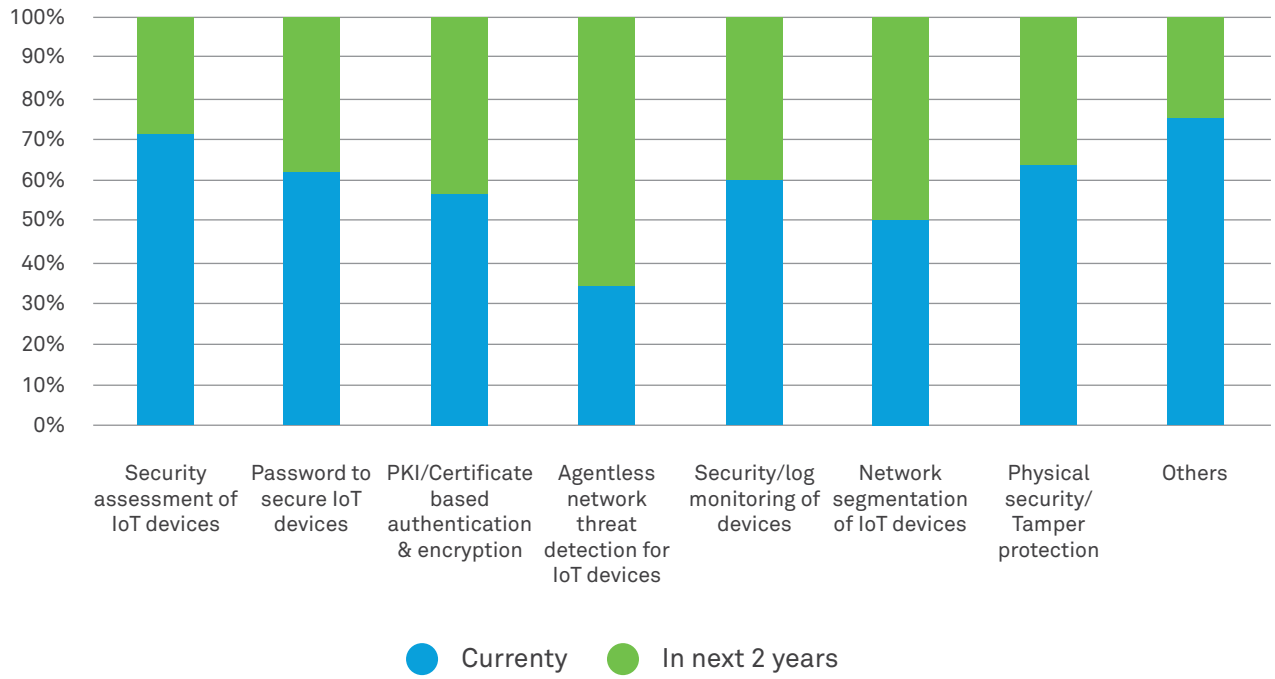


Figure 38: Controls planned to be deployed to mitigate IOT risks - 2017

State of collaboration

The old adage that three strands are stronger than one is extremely relevant to strengthening the cyber response capability. The 2017 edition of the Report covered how organizations gathered and reviewed threat intelligence, how businesses collaborated in cyber-attack simulation exercises and what threat data companies were willing to share with their peers. Some fascinating insights were generated based on the research last year. This year too, we revisited the area as part of the primary research.

Threat intelligence

Sources of threat intelligence for organizations

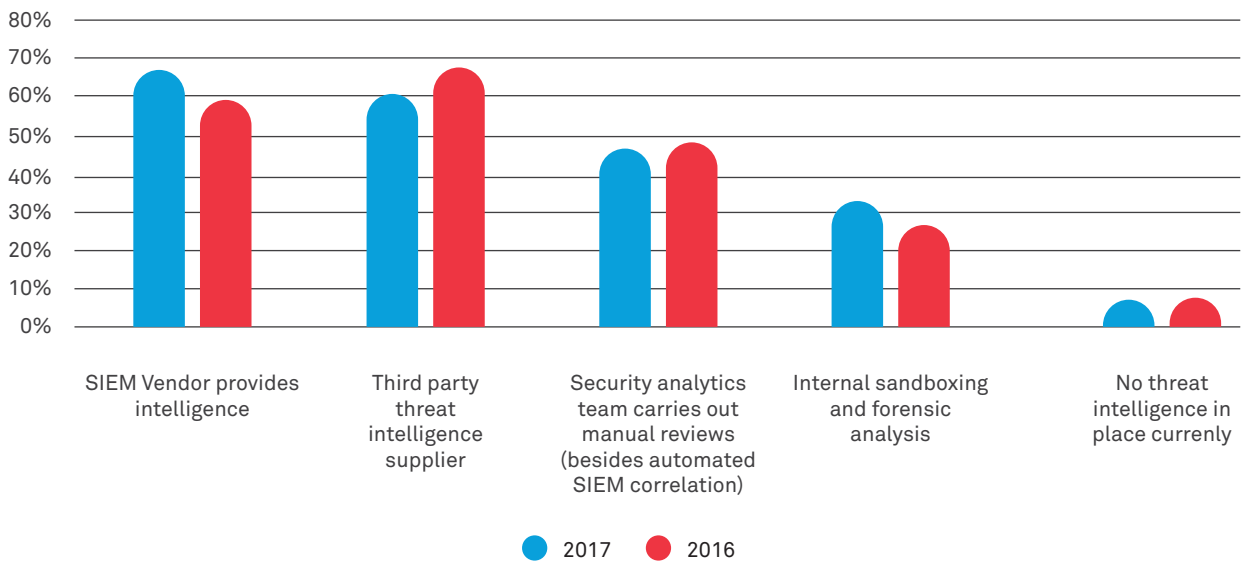


Figure 39: Sources of threat intelligence for organizations – 2017 Vs 2016

In today's digital age, new vulnerabilities are discovered every day and zero-day exploits make organizations highly susceptible to cyber-attacks. The trend is only getting worse with each passing day. Timely threat intelligence provides the ability for any organization to reduce the window of opportunity that an attacker has. In 2016, 68% of the respondents indicated that they were reliant on an external TI partner for intelligence feeds with the SIEM vendor coming a close second. However, in 2017, interestingly, many organizations have indicated that they are reliant on the SIEM vendor for TI (see Figure 39). The implication from the survey results for 2016 and 2017 is that customers are still using alternate sources of TI to be well informed of threats emerging from the wild.

68% of the respondents in 2017, compared to 60% in 2016, have opted for SIEM vendor providing TI

Cyber-attack simulations

Organizational participation in cyber-attack simulation exercises

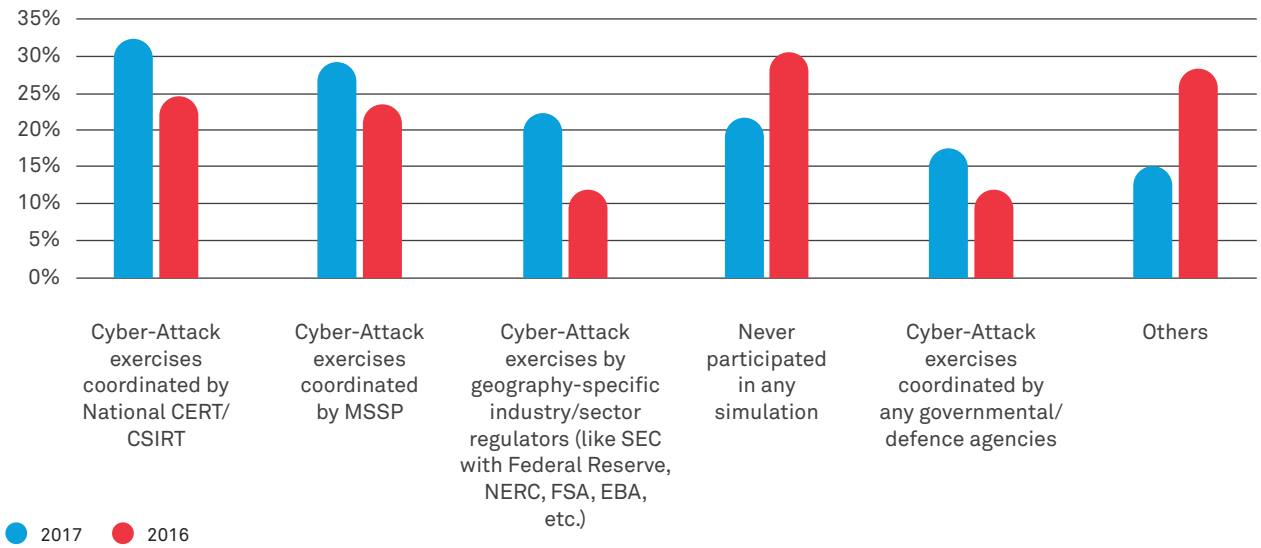


Figure 40: Organizational participation in cyber-attack simulation exercises – 2017 Vs 2016

Simulating cyber-attacks and testing for preparedness is highly essential for critical infrastructure providers whose services, if disrupted, can impact an entire nation's economic activity. All surveyed organizations have existing practices around penetration testing of their critical application and infrastructure layers. However, for many organizations cyber resilience is still a theoretical, tabletop concept that is untested because of their lack of participation in any simulation exercises. Recognizing the high importance of such simulation exercises, national regulatory agencies across the world have now started to conduct simulated attacks and joint response exercises.

Last year, when we asked this question on participation in cyber-attack simulation exercises, 31% said that they have never participated in any simulation exercise. This year, the percentage has come down to 22%, implying that more organizations are being pushed by regulators to partake of joint exercises. At the same time, 33% and 23% of the total respondents said that they had already participated in such exercises coordinated by national CERT/CSIRT and by geographic-specific industry/sector regulators respectively. This is clearly a forward movement, since the same parameters had recorded 25% and 12% respectively in 2016 (see Figure 40).

Respondents who selected the option as 'others' said that they went for methods like custom assessments to ascertain SOC preparedness, internal table tops, cyber-attack exercises coordinated by a third party - non MSSP, and cyber drills conducted internally etc.

Participation in cyber-attack exercises organized by geography-specific industry/sector regulators (like SEC. Federal Reserve, NERC, FSA, EBA, etc.) recorded the highest jump from 2016 by nearly 11 % points

Information sharing

Threat information sharing challenges

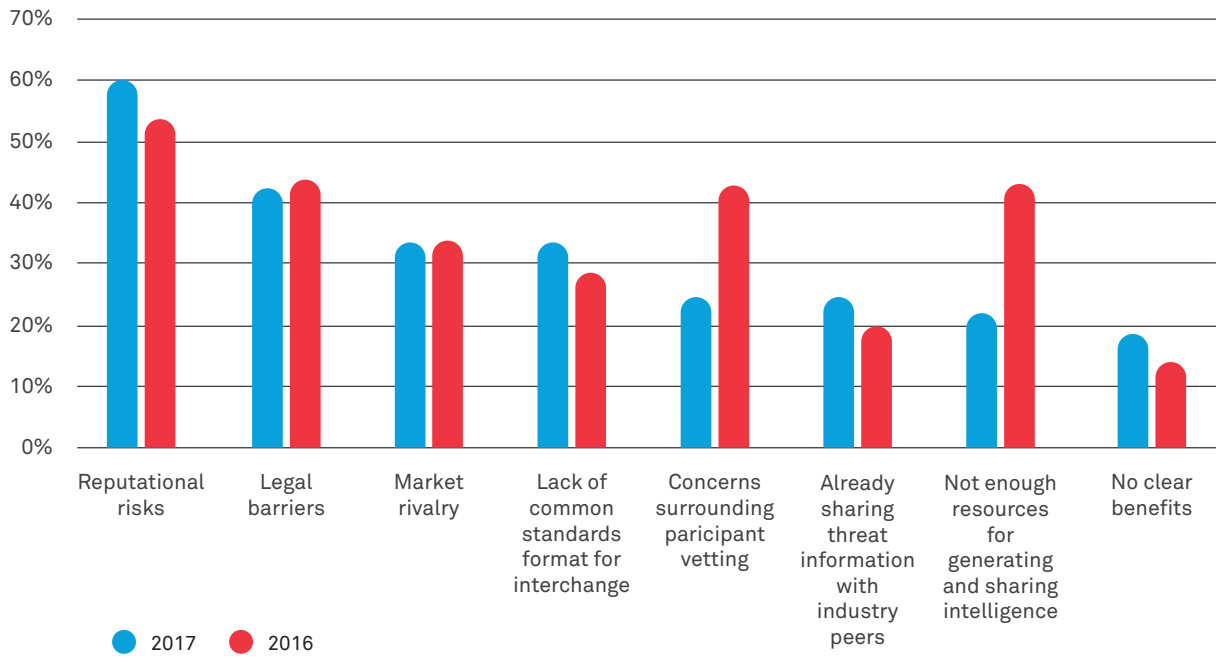


Figure 41: Challenges towards sharing threat information in peer networks – 2017 Vs 2016

One of the long-standing issues in the cybersecurity community has been the challenges around sharing of actionable information between organizations. Sharing of threat intelligence information between industry peers can help companies respond quicker to potential attacks. Researchers have been highlighting this elephant in the room for years, and regulators and government agencies have tried to set up frameworks for information sharing. Unfortunately, organizations are reluctant to share threats/attack information in peer groups. 54% of the respondents in the 2016 research were reluctant to share intelligence with sharing groups mainly due to reputational risks. However, the number went up to 60% in 2017 (see Figure 41). Among many others, one pragmatic reason could be the growing scrutiny of media and immediate after-effects like losing customer faith and erosion of brand value which can negatively impact a business.

60% of the respondents were reluctant to share intelligence with sharing groups mainly due to reputational risks

At the same time, concerns around participant vetting and resources needed to share intelligence have come down considerably in terms of percentage from 2016 to 2017. Interestingly, the proportion of respondents already sharing information with industry peers went up in 2017 when compared to 2016 i.e. 20% to 25%, which is a welcome sign.

Threat information types that organizations are willing to share

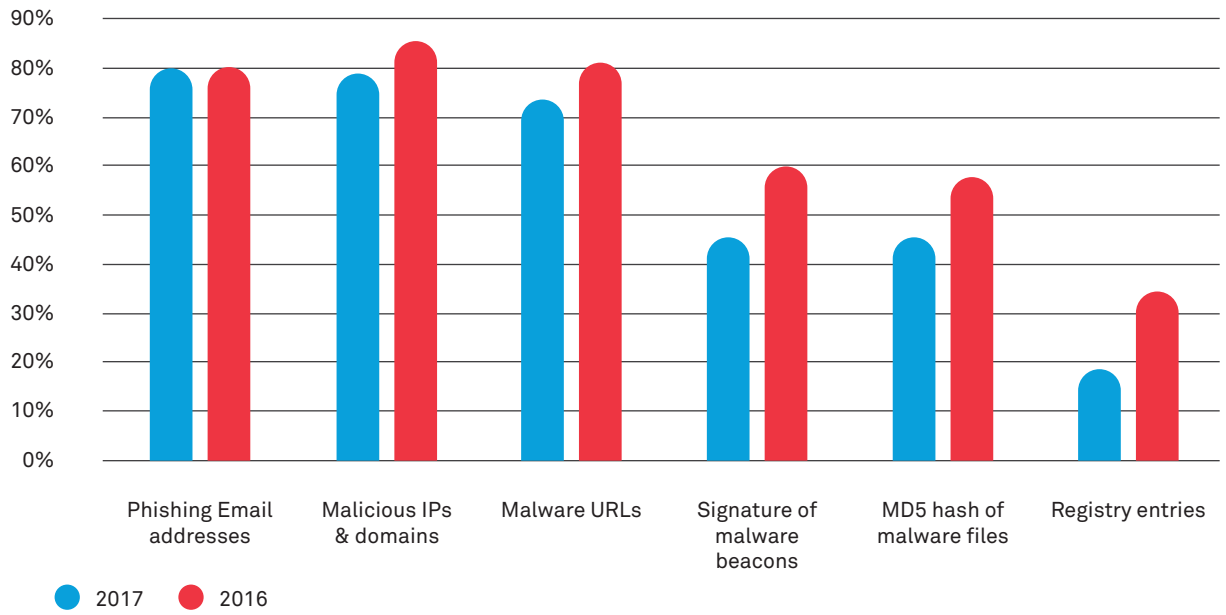


Figure 42: Threat information types that organizations are willing to share – 2017 Vs 2016

So which way did the wind blow?

Of the threat information that organizations are already sharing, we were curious to understand the information categories they were willing to share with industry peers through common forums. As Figure 42 shows, 80% of the respondents were willing to share phishing email addresses with their peers, immediately followed by malicious IPs and domains at 79%.

The top three threat information types have remained the same in 2017 from 2016 except for the slight change in positions. All types of threat information have dropped down in terms of percentage levels when compared to 2016. Overall, the community has not been able to find common ground to make information sharing actionable and ubiquitous.

70% of the respondents were willing to share malware URLs, blacklisted IPs and phishing email addresses with their peers, with an organizational mandate in place

Cyber insurance

Cyber insurance as a partial risk transfer mechanism is quickly finding ground as a supplementary risk management strategy for many organizations. The primary research findings clearly show a trend between 2016 and 2017. As Figure 43 shows, about 52% of the respondents last year had indicated that their firms did not have cyber insurance coverage. This year the number has dropped to 46%, underscoring the strides that the cyber insurance industry is making in filling up white spaces in the enterprise risk management domain.

Cyber insurance policy adoption

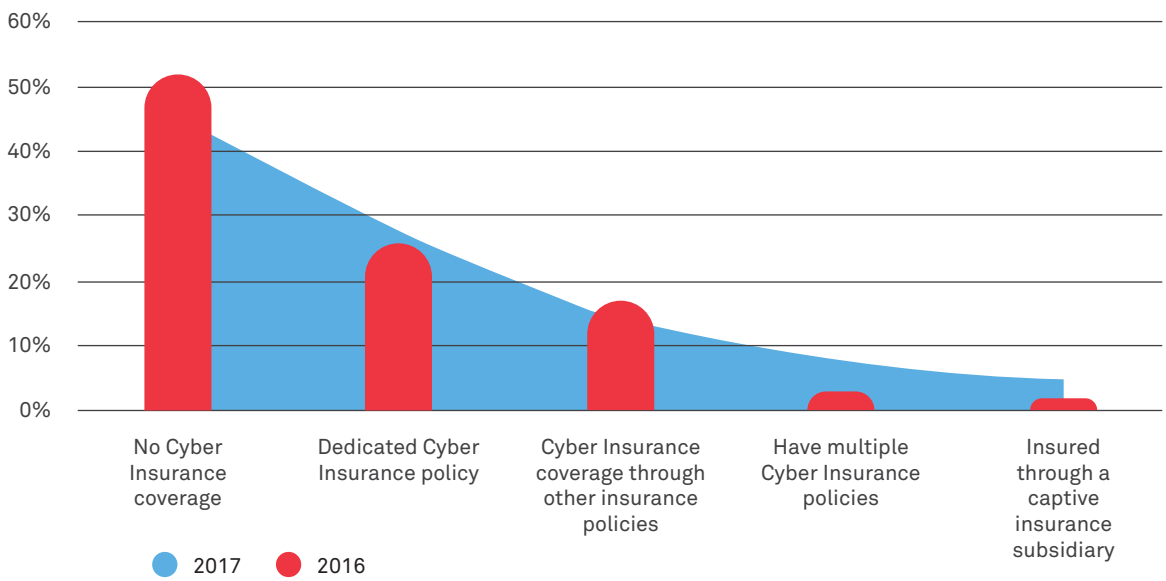


Figure 43: Cyber insurance policy adoption – 2017 Vs 2016

28% of the respondents in 2017, when compared to 26% in 2016, said that they have a dedicated cyber insurance policy in place. Also, an important observation is that options like having multiple cyber insurance policies and insurance through a captive insurance subsidiary have seen their numbers go up in 2017 from 2016.

46% of the respondents have no cyber insurance

Future of cybersecurity

This section examines a select few emerging trends that can impact the field of cybersecurity in the coming years. The section starts off by making a broad sweep of the strides that the industry is making in quantum computing and the repercussions of the same for the future of encryption technologies. A bird's eye view of the domain of blockchain is also covered as it relates to the field of security. Lastly, the section also examines the potential of automation in various process domains of incident detection and response mechanisms that can be orchestrated in the near future.

Strides in quantum computing

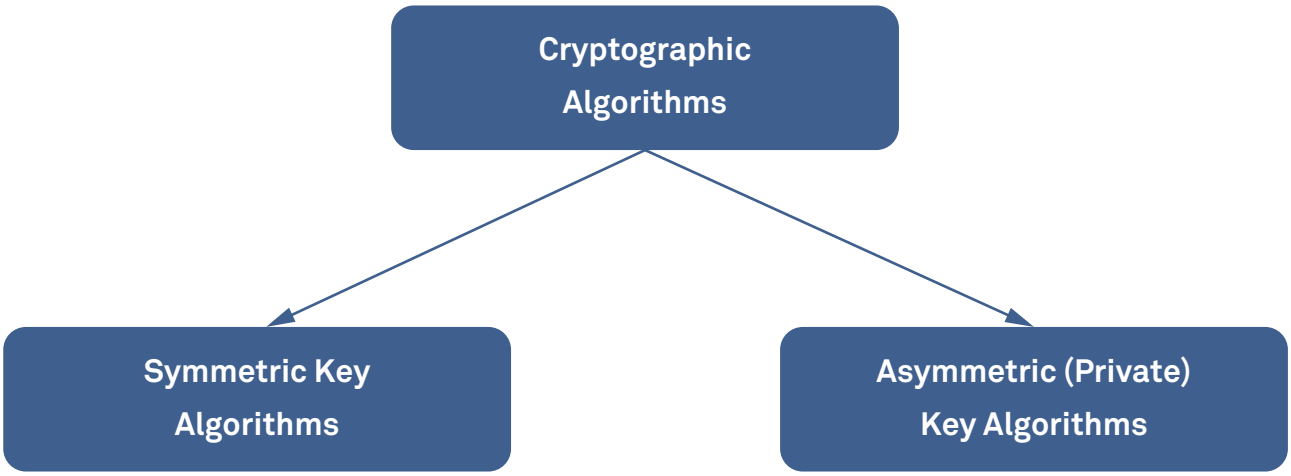
Data is the new currency for most organizations and data volumes are continuing to grow at an explosive rate. While the advantage of collecting such large volumes of data is obvious, protecting it from cybercriminals and malicious actors is becoming increasingly difficult. Conventional security mechanisms are failing and large-scale security breaches, despite increasing security spends, are becoming commonplace. This, along with growing regulatory requirements and privacy laws have brought 'Data Security' – protection of the data itself whether in motion, in use or in transit – into strong focus.

Encryption has been one of the pillars which enterprises and governments have traditionally relied upon to secure sensitive data. This field has evolved over centuries to its current robust state where it is considered practically unbreakable. Several standards have evolved and modern encryption technologies have withstood the test of time to scale and protect our most sensitive data – from banking transactions to the sensitive governmental secrets.

What if this 'status-quo" is flipped on its head and there is a new development that dents the very assumptions that modern cryptographic algorithms derive their strength from? This has been a topic of intense discussion amongst the academia and research community and 'quantum computing' has been identified as a potential candidate for triggering this disruption. This section examines the basis of modern cryptography, the challenges that quantum computing poses, the current state of quantum computing and what enterprises need to do, if at all, to ensure that their most critical assets continue to be protected.

How traditional cryptography works, and what exactly are the challenges posed by Quantum computers?

Modern cryptography can be classified as Symmetric/Asymmetric as shown below, with their secrecy essentially being based on certain mathematical or trap-door functions that these algorithms are based on.



The strength of these algorithms is derived from a set of hard problems and the inability to solve these hard problems using currently available technology. Quantum computing, through the use of special algorithms, can potentially offer the means to solve these hard problems in much shorter time frames and therefore compromise the security of these encryption systems. As indicated in a paper from Entrust, "Certain problems, whose difficulty increases exponentially with the problem size in the classical model, scale polynomially (or even linearly) in the quantum model, thereby making a solution possible even for large systems." In plain English this means that Quantum computers are good at solving certain problems and have a substantial advantage over conventional ones. Some of these problems happen to map to current cryptographic algorithms and therein lies the challenge! For example, the impact on popular and extensively used Public key algorithms is listed below:

Algorithm	Impacted (Yes/No)
RSA-1024, RSA-2048, RSA-4096	Yes
ECC-256, ECC-521	Yes
Diffie Hellman	Yes

Quantum Computing Basics

The basic unit of information in classical computing is a 'bit' which can take on one of the two states - either a '0' or a '1'. This concept is extended using gates which take as input one or many of such states and produce an output which is dependent on the inputs. This fundamental concept is extended using various techniques and acts as the basic building block for a modern computer. On the other hand, quantum computers rely on a concept of 'qbits' or Quantum bits which can be a combination of '0' and '1' at the same time. While this is counter-intuitive, there are several physical entities that can be used as a qbit - for example a photon or even an electron, with 'spin up' or 'spin down' representing the two states. This can be best illustrated by the following table. In classical computing, two bits can be in any of the following four states. We get exactly two bits of information when we are presented with any of the four states below.

A	B
0	0
0	1
1	0
1	1

In the quantum world the output in the following table - '00' or '10' (used for illustration purpose only) can be viewed as the sum of the products of the Coeff and the States across each of the rows (α * State-1 + β* State-2 + Ω* State-3 + π*State-2)

#	A	B	Coeff	Output
State-1	0	0	A	00
State-2	0	1	B	
State-3	1	0	Ω	01
State-4	1	1	Π	

By measuring the output state we would be able to get 4 bits of information (the values of α, β, Ω and π) as against the 2 bits in the case of the classical computer. This is deterministic and there are circuits that can be built to measure these values. The number of bits of information increases with each additional bit of output measured and for an 'N' bit output we would be able to get 2^N bits of information – an exponential increase.

While this is a significant performance boost, it does not imply that quantum computers would be able to replace classical computers universally. It turns out that quantum computers are not generic computers that can solve any algorithmically solvable problem. However, they provide a super-efficient way to solve a certain category/type of problems; some of the classical cryptographic algorithms like RSA fall under this category.

Current state of quantum computers and cryptography

There is a race amongst technology giants like Google and IBM to build a practical Quantum computer. IBM in November 2017 had announced that it had built a 50-qbit quantum computer and Google has recently indicated that it has achieved a significant breakthrough in achieving the stability required for a 72-qbit computer. However, this is currently far from stable, and is capable of holding its state for only about 90 microseconds. While it is estimated that it would take at least 15 years before practical quantum computers can break current crypto algorithms like RSA, there is a large body of work which is working on developing algorithms that are 'quantum resistant'. NIST has recently called for proposals for submission of quantum-resistant crypto algorithms for evolving new public key standards. The stated aim of this exercise is to evolve 'a process of achieving community consensus in a transparent and timely manner'. The Round 1 submissions for this exercise concluded on 30th November 2017 and submissions are available for evaluation.

Quantum computing has the potential to upset the current state of cryptography, significantly diminishing the security of many currently used public key algorithms. Although it is estimated that we are still some way away from building practical quantum computers of scale, it is a problem that CISOs as well as CIOs need to be aware of. This is a rapidly evolving field with new breakthroughs being announced frequently. The fact that NIST is in the process of evaluating possible candidates for achieving quantum-resistant algorithms itself signifies that developments in this area need careful monitoring and could impact future spend decisions. One thing that is certain, however, is that there is going to be a significant impact on current applications and products which rely on existing algorithms as swapping them with new standards is going to be expensive and messy. We recommend that enterprises keep a close eye on these developments and give careful consideration to these aspects to make sure that they continue to be prepared and 'future ready.'

Cybersecurity in the era of blockchain

Distributed Ledger System (DLS) or Blockchain technologies (as they are commonly known) have arrived and are here to stay. DLS has greater potential to revolutionize the way governments, institutions and enterprises work than ever before. It can help governments in collecting the tax, issuance of documents, licenses and disbursement of social security benefits as well as voting procedures. The technology has disrupted industries such as finance, media, precious assets, supply chains of various commodities and much more.

Blockchain for security

As many security practitioners observe, there is a tremendous potential for blockchain for security use cases in the future. Organizations are exploring the use of permissioned blockchain environments for management of identity assertions within an industry consortium or group of companies, leveraging the loose coupling of a distributed ledger and yet having required boundaries of trust.

Another interesting use case to be explored is the notification of validated platform vulnerabilities in the public domain. A platform vulnerability reporting blockchain can make the known vulnerabilities data transparently validated and accessible as and when they are detected and reported. Fixes can be validated on various platforms and reported by users, making the entire process of rolling out security patches a lot more transparent and reliable.

Blockchain security

Blockchain as a technology is still in a Catch 22 situation. We say this because, though there are excellent opportunities and well-defined use cases, security concerns continue to foreshadow gloom around blockchain.

The distributed ledger technology is running in production mode as it is still in its early stages for many of the blockchain frameworks that are available today. Blockchain security is an area that needs to keep pace with the introduction of faster consensus protocols and highly scalable blockchain frameworks.

While blockchain could potentially change how we operate, the technology is accessible to both consumers and malicious attackers. It is important to factor in the need to do real-time blockchain network analytics and implement built-in validation checks to safeguard blockchain networks.

When asked about the risks that concern organizations the most regarding blockchain, 42% of the respondents chose criminal activity to be the risk they were most concerned about. Transaction privacy leakage and private key security were the next two causes for concern with 34% share each of the total responses (see Figure 44).

A few of the respondents who chose the option ‘others’ mentioned that complexity and ownership of risk and compliance are concerns as well.

Blockchain adoption concerns

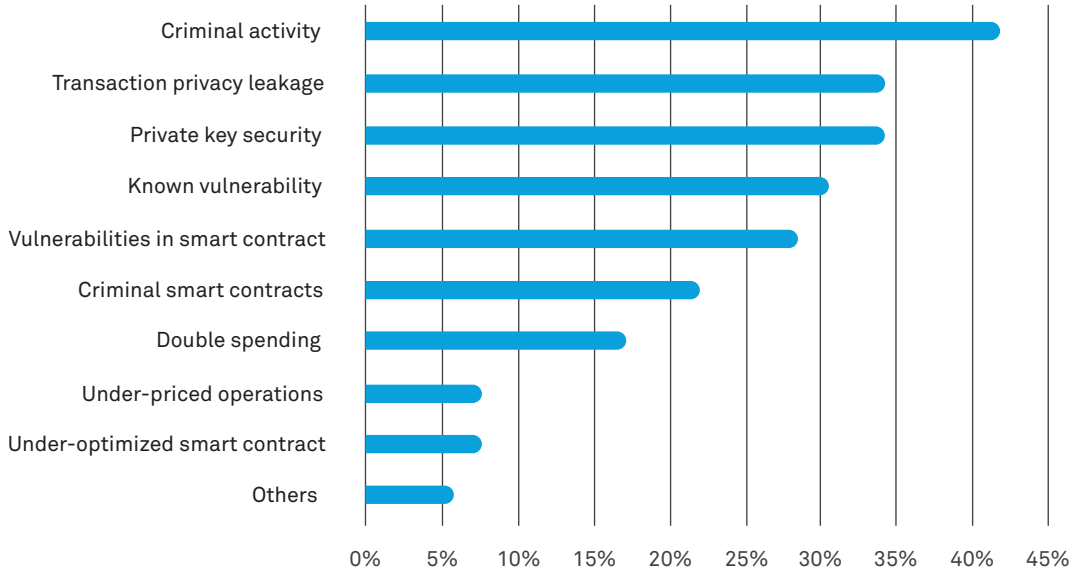


Fig 44 – Concerns associated with blockchain adoption - 2017

Way forward

Having discussed much about the present scenario of blockchain, we need to build techniques and processes that will secure the network from hacking, manipulation and vulnerability breaches. To prevent such breaches, the pointers mentioned here will help shape blockchain ecosystems in a secure way:

- Information security standards will evolve to ensure data confidentiality and to govern what is kept and how data deletion from the ledger will happen
- Most blockchain frameworks will lean towards incorporating the principle of privacy by design into their architecture
- Better, faster and efficient consensus methods using more plug-and-play components around consensus and membership services will be implemented
- Interoperability between different distributed ledger protocols will become a necessity and a requirement to enable globally verifiable identity and authentication
- Privacy-preserving smart contracts will become the order of the day
- Wallet Management will change. Wallet application will have to become more secure without giving any private information to the wallet providing services
- Consortia and foundations like Hyperledger and Enterprise Ethereum Alliance (EEA) will focus on tooling for security and not just managing vulnerabilities
- As a side effect of technologies like quantum computing, advanced components like Quantum Resistant Ledgers with methodologies to do real-time migration of data between ledgers will start making their presence felt
- Governance controls to ensure that we do not have any run-away contracts or AI bot wars using blockchain networks

The above-presented pointers, when mainstreamed, will resolve many of the existing concerns of organizations discussed in this Report. At the same time, looking from an overall security landscape, blockchain will help in escalating the resilience of existing threat response mechanisms which is needed for the ever-expanding threat landscape. In conclusion, we can confidently say that cybersecurity and blockchain are so tightly connected that it is easy to foresee their partnership in their technology evolution journey in the near future.

Security automation

2017 stayed true to the adage, "The more things change, the more they remain the same". The threat landscape continued to evolve with expanded attack surfaces heralded by BYOD and IOT, new entry vectors and attack combinations, and more sophisticated masking techniques that made attack detection that much trickier. This change led to the persistence – and in some cases, escalation – of the same cyber-defense pain points: a paucity of skilled security analysts, a proliferation of alerts, and a sub-optimal return on security product investment due to increased dwell times and analysis paralysis.

In this scenario, the value of automation has never seemed more enduring. As security automation and orchestration products gained a strong foothold in CyberDefense Centers, repeated patterns arose that were usually the first candidates for automation. The major observed patterns were:

Phishing enrichment and response

For combatting phishing attacks, playbooks trigger whenever a suspected phishing email is forwarded to the company mailbox. The playbook extracts indicators like URLs, IPs, and hashes from the mail, and checks their reputation by orchestrating across threat feeds the SA&O (Security Automation and Orchestration) product integrates with.

If malice is found, the end user is informed about it through an automated email, tickets are opened, the incident's severity is increased, and all instances of the phishing mail are deleted. In more advanced playbooks, email attachments are investigated further and correlations with other incidents are studied to detect any potential lateral movement in the attacks.

IOC enrichment

For IOC (Indicator of Compromise) enrichment, playbooks orchestrate across a range of products to automate actions that would otherwise have taken analysts over an hour to perform. These playbooks parse indicators from the incident, check threat feeds for their reputation, query DNS information for URLs, and update the endpoint database in case malicious indicators are found.

If any malicious indicators are found, the playbooks raise incident severity, send the analyst a mail, and stop at a manual task for the analyst to review playbook results.

VPN checks

Automation patterns are being noticed for both proactive and reactive processes. VPN checks are one of the most common proactive processes that are scheduled to run via playbooks at predetermined intervals. Sophisticated playbooks cross-reference user locations from VPN and CASB networks, send an automated mail to the end user in case of any discrepancy, and act on the discrepancy if it's confirmed by the end user.

Endpoint analysis and diagnostics

Automated endpoint-focused workflows are also both proactive and reactive in nature. On the proactive front are playbooks that regularly check for unmanaged and uncommunicative endpoints, ping them to verify responsiveness, and open tickets if the endpoints remain unresponsive before adding comments for further investigation.

On the reactive front, playbooks orchestrate across EDR (Endpoint Detection & Response) tools to query all endpoints on the system for malicious files, extract the malicious files, and study them before marking for deletion.

Malware analysis and sandboxing

CyberDefense Centers often have standardized playbooks that run automatically when certain alerts are ingested from malware analysis and sandboxing tools. These playbooks perform checks to initiate triage, run detonation actions, and return the reports to the analysts for subsequent investigation.

Analysts save time and redundant effort by automating triage and detonation tasks, and instead use their energies for more cerebral and sophisticated investigation tasks. This also ensures a standardized response, reduced error rate, and no alerts slipping through the cracks.

Policy and compliance checks

The automation use cases for policy and compliance are manifold. One popular workflow checks all systems for SSL certificates that have either expired or are nearing expiry, pulls account details of the user and manager for targeted endpoints, and sends a mail advising them to redress this potential expiry.

With international, federal, and state regulations of prime importance, another oft-used workflow triggers whenever a data breach is detected and walks the analyst through all steps to comply with relevant breach notification laws. This workflow includes tasks to check whether any PII was breached, authorities to inform, filling in notification templates, and taking corrective action for breached accounts.

System health checks

Novel attacks such as coin jacking have gained momentum this year, prompting the rise of automated workflows that regularly check granular system health metrics such as CPU and memory usage. These workflows report back any discrepancy with respect to sudden usage spikes, time anomalies, and application anomalies, notifying the analysts to study those endpoints or servers further before taking corrective action.

The future of security automation

While workflows that are currently prime automation targets tend to focus on repeatable, menial tasks, there are nascent signs of automation having much farther-reaching consequences on the cybersecurity space.

Unifying disaster and security recovery: There is currently a disconnect between security and I&O (Infrastructure and Operations) teams during cases that require a combined incident response. Playbooks that coordinate across teams, codify tasks to be done by each team, and enforce those tasks through automation wherever possible, will lead to greater synergy between hitherto disparate teams. Automation will also make it easier to infer and measure business risks, helping bring teams together towards a common goal.

Regulation and compliance: With governments and regulatory agencies cracking down on the importance of data privacy, integrity, and breach notification, semi-automated playbooks can aid organizations in complying with these requirements. For example, a 'Right to be Forgotten' request from an end user (as part of GDPR requirements) can trigger an automated playbook that implements the request with some analyst-driven checks and balances.

Self-learning workflows: As the same workflows are used more often, the underlying data can be mined and used as a source of learning. Tools that learn from existing workflows to suggest leaner task-branches, more efficient operating procedures, and ideal analyst-playbook matches will be the future.

Combatting expanded threat surface: With smart devices expected to permeate society in the coming years, the next level of security automation will not only orchestrate across security products, processes, and personnel, but also 'speak' to IOT devices, CCTV outlets, and biometric sensors. One immediately foreseeable use for this evolved automation will be the melding of digital and physical security measures.

Partner Content Credits: Contributed by Wipro Ventures partner Demisto (www.demisto.com).

Conclusion

2017 was a tumultuous year when looked through the lens of cybersecurity considering the large-scale data breaches, worldwide ransomware attacks and huge GBPS volume DDoS attacks that lit up the year. Through this report, as you can find in the first section, we made a concerted effort to bring to the notice of organizations across the globe, the state of attacks and regulations the world of cybersecurity witnessed in 2017. Based on the current trends, 2018 may be no different or maybe even worse. However, to deal with this ever-evolving threat landscape, organizations need to keep on improving the maturity of their defense mechanisms. In the second section of the Report we analyzed and presented the current state of defense mechanisms of organizations by examining various dimensions such as security management and governance, security metrics, security practices from the point of view of applications, network, endpoint, data, cloud, IOT, etc. The rapid rate at which technology evolution is happening requires us to also examine trends around areas like Serverless computing, IOT, etc., that are knocking disruptively at the doors of IT. Not to our surprise, we clearly saw trends where organizations are still lacking visibility into threats in these emerging areas and security best practices to mitigate those threats.

Today to ward off cyber-attacks, timeliness in detection and response to emerging threats is becoming critical. A mature security posture is only good at a given point in time and organizations need to constantly adapt their environments to identify new vulnerabilities, patch their systems, deploy new detection rules for new vectors, etc. For all of this to happen faster than the attackers can get to you, collaboration becomes key for organizations to protect themselves from future cyber-attacks. Hence to understand the state of collaboration as it was in 2017, we posed a few questions in the primary research relating to collaboration. Our analysis generated mixed results - which is something to cheer about. For example, we observed an increase in the number of organizations which participated in state-sponsored cyber-attack simulation exercises, as was presented in the third section. Finally, in the fourth section we tried to examine through different dimensions how quantum encryption, security automation and blockchain technologies will impact the future state of cybersecurity.

A summary of the key observations and inferences that can be made from the Report are provided here:

Macro environment:

1. The annual breach rate almost doubled to 88 records/sec. Organizations need to be prepared with a holistic breach response plan taking into account operational, regulatory/legal and moral considerations, if the unthinkable happens.
2. Breach notification laws are stringent in about 78% of the countries analyzed and more countries will follow suit. For global companies, developing a unified control framework to address breach notification laws across states will simplify the compliance process.

3. State actors are active, taking on big corporations across borders. Actively participating in local regulator or agency-led attack simulation exercises can help preparedness for D-day.
4. Security products are made by mortals. The research data indicates a propensity to have residual vulnerabilities. Test your security stack also regularly for weaknesses and keep the vendors accountable.

Micro environment:

1. Security budgets still form a meager portion of IT budget allocations despite the high visibility brought by cyber-attacks. Boards need to have expertise and knowledge of cyber risks and make informed choices to enable the IT executive leadership with necessary resources.
2. Metric tracking across preventive, detective and response controls in organizations seem to be minimal except for verticals like Banking which are more mature.
3. Industrial benchmarking seems distant and mostly based on personal relationships, where happening in pockets. Benchmarking can be enabled through sharing networks or vendor relationships.
4. Applications continue to be the soft underbelly for hackers to target. Organizations still struggle with imbibing security in the DevOps processes and this will have to be an area of focus.
5. Serverless Computing is fast catching up as a means to onboard business functionality on the cloud, but the security challenges related to the same are not well understood. Organizations need to find compensatory controls while onboarding business functions into FaaS/Serverless models.
6. Organizations are just beginning to categorize IOT assets in the enterprise environments. We are expecting organizations to find the quick path to detect and address IOT threats which are not device-dependent but can work in other layers like the network or edge.

Meso environment:

1. Organizations need to move from generic TI consumption to more actionable and targeted intelligence.
2. Information sharing within the same industry remains elusive due to legal challenges. Organizations need to enable more resources towards threat hunting internally to be able to contribute back to the community.
3. Cyber insurance still has not seen mainstream adoption and organizations can explore it as a secondary risk transfer tool.

Future:

1. Investment in security automation needs to be strategic to reduce the threat detection and response cycles.
2. Permissioned blockchain which clearly has some utility for specific use cases related to security, identity management and compliance should be on the radar of security teams

About Wipro CRS

Cybersecurity & Risk Services (CRS)

Wipro's Cybersecurity & Risk Services (CRS) enables next-generation global enterprises to enhance their business resilience through intelligent and integrated risk and security management programs. CRS uses the business resilience levers of standardization at the core and differentiation at the edge to enable enterprises to embrace future technology with agility while keeping their processes efficient, secure and robust. Leveraging a large pool of 7500+ experienced security professionals and a Global Delivery Model, CRS assists more than 500+ customers in defining their risk and security needs, make best practice recommendations, technology evaluations, implementations, and delivering managed and hosted security services.

Global

Sheetal Mehta sheetal.mehta@wipro.com

CRS Marketing crs.marketing@wipro.com

Americas

Siva VRS siva.vrs@wipro.com

Europe

Shivam Arora shivam.arora@wipro.com

Rajesh Pillai pillai.rajesh@wipro.com

Middle-East

Bharat Raigangar bharat.raigangar@wipro.com

India

Jayesh Kumar jayeshkumar.warier@wipro.com

APAC

Karthikeyan V karthikeyan.veerappan@wipro.com

Credits & key contributors

We are indebted to our customers across the globe, who helped us through the CISO survey response as part of the primary research. Many analysts from the CyberDefense Centers have also contributed indirectly through insights and valuable suggestions on the threat research. We are also grateful to our partners who have shared valuable inputs in this edition of the report. Lastly, we want to also thank Bhanumurthy B M, President & COO and Hiral Chandrana, SVP & Global Business Head - Modern Application Services (MAS), for their executive support and sponsorship from the Wipro Leadership.

Wipro Contributors:

Josey V George – Editor & Distinguished Member of Technical Staff, Wipro | 2016 Chevening Fellow for Cyber Security

Venkatesh M – Sub-Editor, Security Analyst, CRS, Wipro

Mohona Mukhopadhyay – Marketing, CRS, Wipro

Group Captain (Retd) Anand Kanuri – Practice Head, Data Security, CRS, Wipro

Vinod Panicker – Senior Member of Technical Staff, Wipro

Deepak Kothari – Lead Architect, CyberDefense Platform, CRS, Wipro

Kalpesh Rajendra Wani – Security Analyst, CRS, Wipro

Lalit Dilip Desale – Security Analyst, CRS, Wipro

Cheshta Batra – Security Analyst, CRS, Wipro

Ajish John – Lead Consultant, CRS, Wipro

Dhanashekhar Devaraj – Consulting Manager, CyberDefense Center, CRS, Wipro

Tanya Khanna – Business Analyst, CRS, Wipro

Manish Rathour – Head, Strategic Marketing, Wipro

Ushnish Paul – Brand and Marcom, Wipro

Saksham Sunil Khandelwal – Thought Leadership, Wipro

Kevin Abraham – Strategic Marketing, CRS, Wipro

Gaurav Kwatra – Strategic Marketing, CRS, Wipro

Partner Contributors

Itay Kozuch – Director of Threat Research, IntSights (www.intsights.com)

Abhishek Iyer – Technical Marketing Manager, Demisto (www.demisto.com)

Dan Cornell – CTO, Denim Group (www.denimgroup.com)

References

1. https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies
2. https://www.eveningexpress.co.uk/fp/news/local/laptop-and-files-with-confidential-information-about-children-stolen/
3. https://www.sbs.com.au/news/top-secret-information-about-fighter-jets-navy-ships-stolen-after-defence-contractor-hacked
4. http://www.marinemec.com/news/view,tanker-group-says-it-faced-cyber-attack-in-july_49564.htm
5. www.khmertimeskh.com/5089533/ministries-hacked-by-vietnam-group/
6. https://motherboard.vice.com/en_us/article/3daywj/hacker-steals-900-gb-of-cellebrite-data
7. https://www.oag.ca.gov/system/files/DBM%20Global%20Data%20Breach%20Notice%20Letter_0.pdf?
8. http://citizen.co.za/news/news-national/1479032/eff-treasurer-generals-car-broken-sensitive-files-stolen/
9. https://www.doj.nh.gov/consumer/security-breaches/documents/forest-city-trading-20170403.pdf
10. https://timesofindia.indiatimes.com/city/goa/for-data-leak-9-coastal-body-staff-sacked/articleshow/60977986.cms
11. https://www.zimeye.net/shocking-theft-of-secure-criminal-records-at-gutu-magistrates-court/
12. https://www.privacyrights.org/data-breaches
13. https://www.symantec.com/security-center/threats
14. http://cve.mitre.org
15. https://www.cvedetails.com/index.php
16. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
17. http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20(ALRC%20Report%20108)%20/51-data-br'
18. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/
19. https://www.cnil.fr/en/home
20. https://www.cnil.fr/en/rights-and-obligations
21. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
22. http://www.cert-in.org.in/
23. http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/act2000.pdf
24. http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
25. http://eng.rkn.gov.ru/personal_data/
26. http://www.ppc.go.jp/en/
27. http://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Infomration.pdf
28. https://www.pdpc.gov.sg/legislation-and-guidelines/overview
29. http://www.gesetze-im-internet.de/englisch_bdsg/
30. http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf
31. https://www.datatilsynet.no/english/
32. https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/
33. http://www.datainspektionen.se/
34. http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/forberedelser-for-personuppgiftsansvariga/
35. https://www.edoeb.admin.ch/datenschutz/index.html?lang=en
36. https://www.admin.ch/opc/en/classified-compilation/19920153/index.html
37. http://www.gov.za/documents/protection-personal-information-act

38. http://www.gov.za/sites/www.gov.za/files/37067_2611_Act4of2013ProtectionOfPersonalInfor_correct.pdf
39. http://inicio.ifai.org.mx/SitePages/English_Section.aspx
40. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
41. https://www.difc.ae/files/7814/5517/4119/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf
42. http://www.npc.gov.cn/englishnpc/Law/Frameset-page2.html
43. https://snyk.io/blog/serverless-security-implications-from-infra-to-owasp/
44. https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf
45. https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/
46. https://research.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html
47. https://www.youtube.com/watch?v=wWHAs--HA1c (2014 PQCrypto conference in October, 2014)
48. https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf
49. https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions
50. https://www.sciencedaily.com/releases/2018/03/180301144140.htm
51. https://blockchainhub.net/blockchain-intro
52. https://www.antuit.com/blog/future-blockchain-cyber-security-challenges/
53. https://www.nspe.org/sites/default/files/resources/pdfs/NSPE-Whitepaper-Blockchain-Technology-2016-final.pdf
54. https://techcrunch.com/2016/12/05/how-blockchain-can-help-fight-cyberattacks/
55. https://letstalkpayments.com/21-areas-of-blockchain-application-beyond-financial-services/
56. http://www.information-age.com/how-blockchains-are-redefining-cyber-security-123460713/

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/BRD/MAY 2018-APR 2019