State of cybersecurity report 2017

Demystifying cyber risks in the global context

Contents

Foreword

Sheetal Sharad Mehta

VP and Global Head – Cybersecurity & Risk Services, Wipro Limited

Wipro's Cybersecurity & Risk Services (CRS) practice has evolved over the last two decades into a market challenging position for end to end security. Hundreds of Wipro customers across North America, EMEA, APAC, Middle East and India markets with varying levels of risk, leverage us globally for Consulting, System Integration and Managed Security Services. The insights generated from our research, work in helping customers deal with their cybersecurity threats through our regional Cyber Defense Centers (CDCs). Wipro's CRS CoE (Center of Excellence) team works with the broader cybersecurity ecosystem consisting of emerging technology players, cybersecurity venture startups, regulatory bodies, government agencies dealing with critical infrastructure protection and academic institutions to keep a constant vigil of technology disruptions and related threat perceptions. This operational and strategic knowledge, that is derived through our services, is being brought out and presented for the first time through this State of Cybersecurity Report 2017. This report will henceforth be an annual contribution from Wipro's CRS practice to the cybersecurity industry and our current and future client base. This report differentiates itself from other reports in the market by combining knowledge from our aggregated operational data, our primary research (the customer voice) and interleaves these two with secondary research (the industry perspective) to provide the reader with practice insights that can be acted upon. The report also provides aggregated insights on operational capability across different information security domains which can be used by the reader to benchmark themselves as they make strategies and operational plans. I am confident this report will provide useful takeaways for readers across different functional teams within security organizations and for executive management teams with global companies that are operating in today's cyber threat context.

Editor's note

Josey V George
Practice Head, Solutions Engineering
Cybersecurity & Risk Services, Wipro Limited

We conceived the State of Cybersecurity Report 2017 with the intention of providing insights that are useful to two distinct constituencies a) operational teams that are battling the daily threats from the trenches b) IT management executives across cybersecurity strategy, operations and risk management who are tasked by the board to be driven more strategically in order to identify and contain cyber threats to the enterprise. We have endeavored to address these distinct needs across different sections of the State of Cybersecurity Report.

The core of the report has been structured into four distinct sections. Section 1 is the ice breaker section and it sets the context for the novice and the experienced by laying out the battleground across the industry during the year that has gone by. The major cyber breaches across the globe have been compiled and chronicled chronologically giving perspectives on the scale of the data loss and the type of data that cyber criminals and state and non-state actors have been after. This section also captures the output of the research from our CDCs on the 'Weapons of Cyber Destruction' that have been largely used by various hacktivists, hackers and others in perpetrating these breaches and attacks. Section 1 also captures our research around the top vulnerabilities in security products and platforms that have left many enterprises grappling with challenges to contain the attackers. This perspective is quite unique and has not been addressed in any security report from large service providers so far. I am sure it will provide food for thought for Security Operations Center (SOC) teams to 'fortify the defenders' themselves. The global view of changing breach notification regulations will, I am sure, awaken compliance teams as global companies need to adhere to regulatory requirements that are being imposed on MNCs due to pervasive / cross continental data flows.

Section 2 of the report will be a delight for the SOC teams and their management. It deals with the various layered defensive mechanisms used by the industry and their effectiveness. This section covers our primary research across endpoints, network, applications, cloud, mobility, security monitoring and the user as various realms of threats.

Section 3 will be useful to CISOs (Chief Information Security Officers) to understand trends in collaboration for better cybersecurity. Collaboration here covers patterns that are being applied for data flow integration with Managed Security Service Providers (MSSPs), Computer Emergence Response Teams (CERTs), government agencies, etc., which can better equip an enterprise to face future threats.

Last but not the least, Section 4 looks at the future and how trends around Cyber Insurance, IoT, Drones and Persistent Identities can change the game. We hope the first edition of the report has insights that will keep the reader engaged and wanting for more in the future!

Methodology & demographics

The State of Cybersecurity Report 2017 from Wipro was developed over a period of five months. The methodology that was followed to develop the report has been three-fold:

1) Primary research (external)

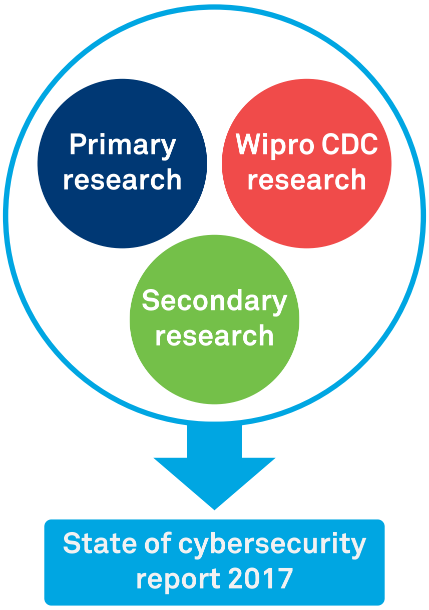
2) CDC research (primary research through our CDC)

3) Secondary research

The primary research (external) was driven through questionnaire filled out by security leadership, operational analysts and architects. The survey was conducted through online surveys with a detailed questionnaire that respondents were required to fill in 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 2016.

The CDC research is borne out of the analysis of the live and historical data, that has been generated in the CDCs and dissected by the analysts over a period of time. Lastly, 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.

Various views of the demographics of the organizations that we engaged with as part of the primary research are presented below. 64% of the companies whose cybersecurity personnel we engaged in interviews had employees in the range of 5,000 to 500,000. We covered 15 different industry sub-verticals in our survey with Banking and Manufacturing topping the list. 77.2% of the companies surveyed had revenues greater than 1 Billion USD.



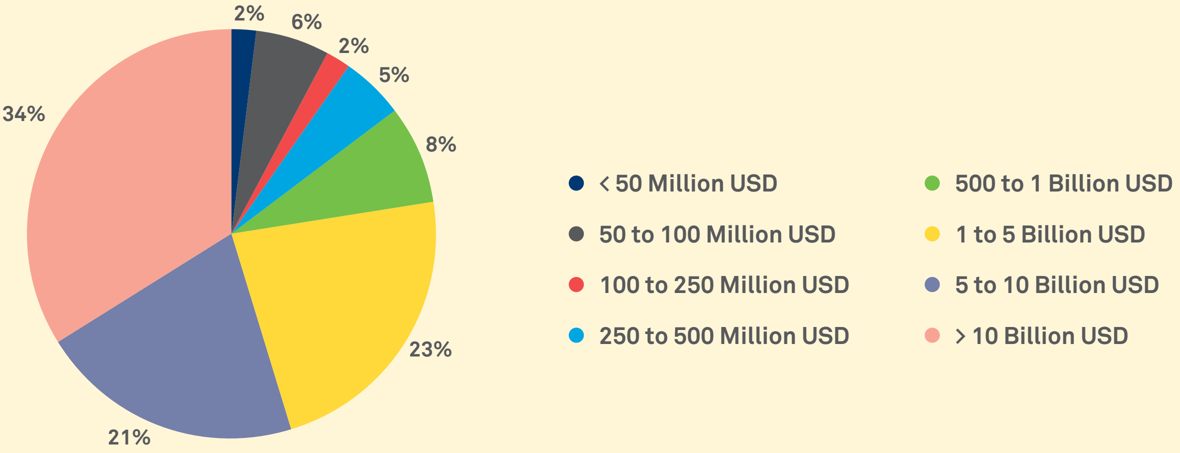
Primary research

Wipro CDC research

Secondary research

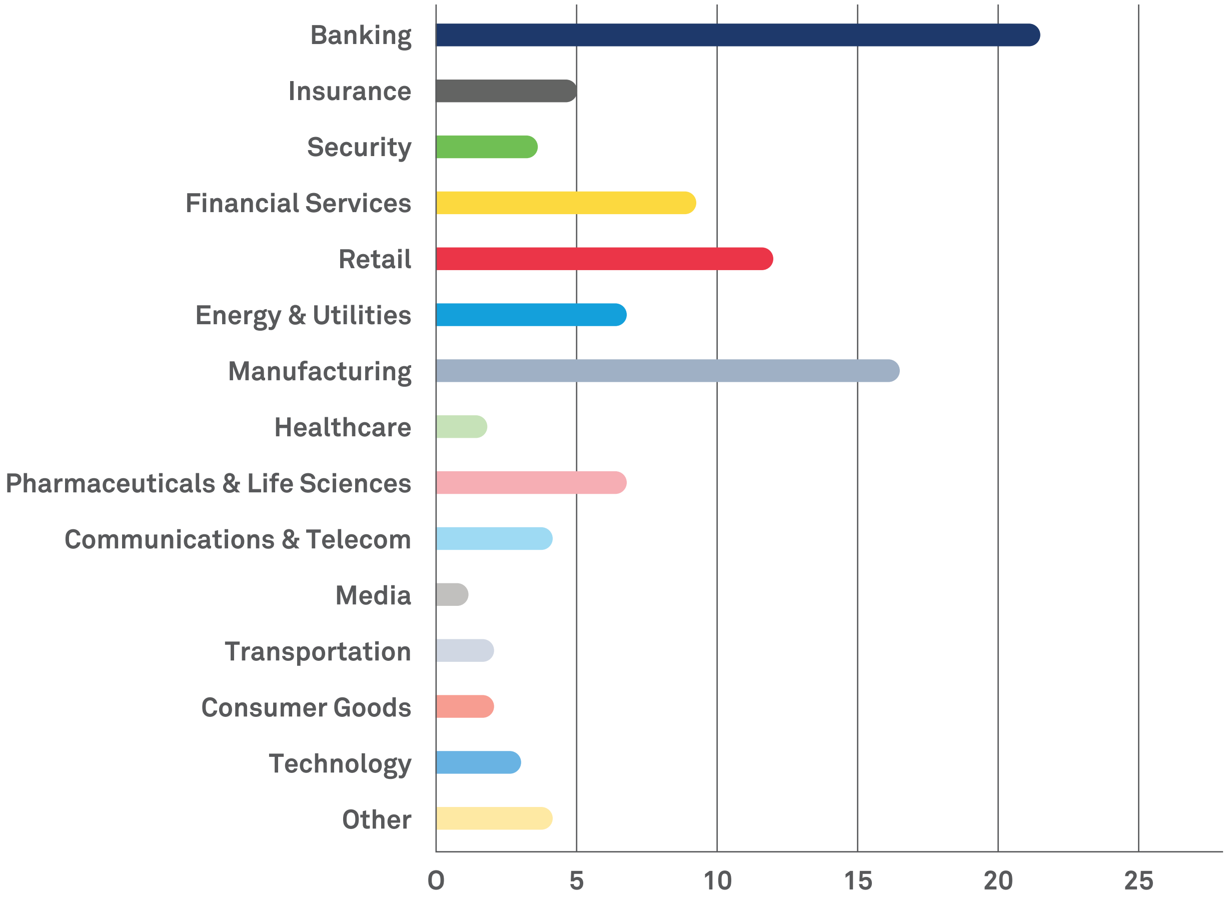
State of cybersecurity report 2017

Organizations surveyed by revenue



139	Organizations surveyed
11	Countries covered
3,304	CDC incidents analyzed
189	Malware families analyzed
111	Security products analyzed for vulnerabilities
18	Countries breach notification laws analyzed

Organizations surveyed by vertical



Structure

DNA of the report

In this edition of the 'State of Cybersecurity Report', we laid out four key objectives that we wanted to achieve. Through this edition, we wanted to cover and provide a perspective of **1) the macro environment** around the globe in relation to cybersecurity – an outside-in perspective, 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 Micro and Macro Environments and **4) Disruptions that can affect the macro, micro and meso environments,** and upset the temporary equilibrium.

With these objectives in mind, Section 1: State of attacks, breaches and laws 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 lastly culminating in Section 4: Future of cybersecurity that takes a view on possible disruptions of the future. Further details on each of the sections are given as follows.

Section 1: State of attacks, breaches and law

This section illustrates the research around the major breaches that happened during 2016. It analyzes the profile of data elements that hackers were after, and takes a background look at how social media and sentiments on that were reflected for the companies and institutions that were breached. Section 1 follows up with the attack analysis and with the research findings on the Weapons of Cyber Destruction from our CDCs around the globe. This section also analyzes the vulnerability trends of security products and how breach notification regulations are changing across the globe.

Section 2: State of defense mechanisms

This section is borne out of the primary research that Wipro carried out with 139 organizations across North America, Europe, APAC, Middle East and South Asia. 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 users (social engineering), endpoints, network, applications, cloud and mobile environments.

Section 3: State of collaboration

This section is based on the primary research carried out with the CISO organization. It focuses on the readiness of the security organizations to collaborate with the external cybersecurity ecosystem to better manage the risk. The collaboration here would typically be with regulatory bodies and in several instances 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 evolved from within the CRS CoE. The topics covered range from Cyber Insurance and its play in risk management, IoT security, Drones and cybersecurity and the changing face of the future cybersecurity analyst.

Executive summary

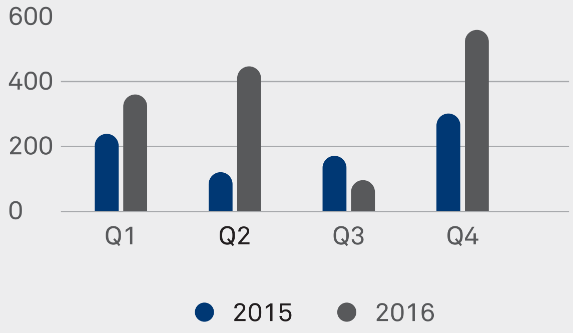
The year 2016 has seen some unprecedented cyber-attacks across different commercial sectors and geographical locations. However, what probably catapulted cybersecurity to the limelight for the first time in the political arena was the recently concluded US presidential election. The year has seen it all: 53.6% increase in data records stolen across the globe for reported breaches, unprecedented DDoS attacks peaking at a phenomenal 990 GBPS, newer versions of highly evolved malware families and evolving regulations that enterprises need to be bound by. The defensive tactics employed haven't kept pace with the sophistication of the attacks. However, the future doesn't look all that gloomy – there is hope. The State of Cybersecurity Report 2017 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 around the globe.

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

This section illustrates the research around the major breaches that happened during 2016. It analyzes the profile of data elements that hackers were after, and takes a background look at how the social media and sentiments on that were reflected for the companies and institutions that were breached. Section 1 follows up with the attack analysis, with the research findings on the Weapons of Cyber Destruction from our Cyber Defense Centers (CDC) around the globe. This section also analyses the vulnerability trends of security products and how breach notification regulations are changing and the implications of the same.

The leaky faucet just got worse

The instances of data breaches have increased more than ever and 2016 was no different. With the momentum building up on cloud, mobile and IOT, potential attack platforms have increased. Organizations like Time Warner Cable, Yahoo & FriendFinder became victims of data breaches. Cyber-attacks are affecting all possible industries. We carried out a historical sentiment analysis on breached companies and the same depicted a negative perception among their end customers in the aftermath of the breaches which can lead to brand reputation loss and ultimately impact the bottom-line.



Millions of Records Stolen

There has been 53.6% increase in stolen records in 2016 over the previous year.

Weapons of cyber destruction

Malware variants have been continuously on the rise since the last few years. Our CDC data analysis point out that 56% of all the malware attacks that have taken place in 2016 were a result of Trojans. Likewise, viruses and worms accounted for 19% and 20% respectively. Other types of malware threat categories like PUA, adware and ransomware together though accounted for only 4% attacks, often can lead to significant damages. The incident data analysis from our CDC points to exploits distribution in 2016 as follows: nearly 41% is a result of web exploits followed by 29% of Infrastructure exploits. Angler, RIG, Nuclear were some of the most commonly found types of exploit kits that were used by attackers to

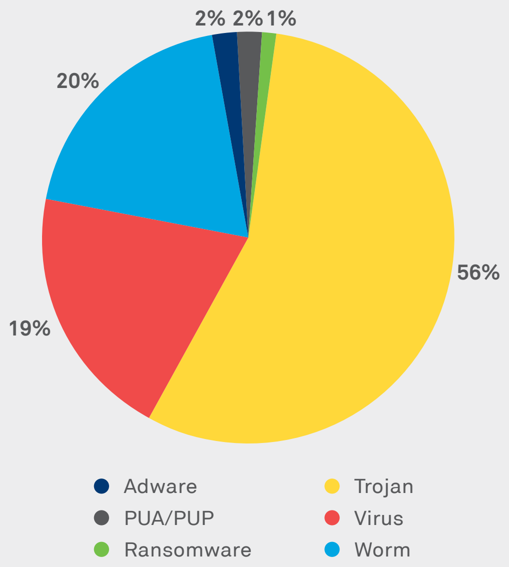


Figure 1 - Overall Malware Distribution

land ransomware, spyware, etc., which target by exploiting the software vulnerabilities in devices.

Defenders need fortification

Organizations have been using controls like Antivirus, DLP, Firewalls, SIEMs and many more tools to protect themselves from attacks. With new vectors of attack emerging, can security tools themselves become susceptible to vulnerabilities and attacks. After analyzing similar tools of different control domains, we have concluded that serious vulnerabilities exist in security tools too and vendors need to constantly improve their products to instill confidence amongst customers.

SAST, SIEM and NAP security controls were the ones with highest critical vulnerabilities.

Spreading tentacles of breach law

Breach notification laws along with privacy laws have been evolving every year. 2016 has not been an exception. Restrictions on cross-border data flows are also evolving with regulations like GDPR. Wipro has developed a standard decision framework using multiple weighted parameters to assess the extent of breach notification requirements and level of restriction on overseas transfer of information.

88.9% of the countries analyzed have defined sensitive personal information at some level of granularity.

44.4% of the countries analyzed have laws which mandate notifying concerned data subjects about breaches.

GDPR mandates data owners to notify within 72 hours.

Based on the primary research/survey findings, Wipro recommends that the enterprises incorporate the following guidelines in their cybersecurity strategy.

DATA BREACHES

In the event of a breach, have processes in place for communications with end users and force them to change their credentials.

CYBER DEFENDERS

Cybersecurity products need to be regularly tested for vulnerabilities to assess and act on their inherent risks.

This section is borne out of the primary research that Wipro carried out with 139 organizations across North America, Europe, APAC, Middle East and South Asia. The primary research was carried out by direct interviews and an online survey with key stakeholders across the CISO organization. The research focused on the current state of defense mechanisms around users, endpoints, network, applications, data, cloud and mobile environments which are simple layers that are the target of attacks. Understanding the trends and changes happening in these layers is key to defining future cyber strategies.

User is still the real enemy

Human dimension

Teaching the lay user to not fall prey to social engineering or deceptive technical attacks has provided only incremental benefits in reducing cybersecurity incidents. Organizations might need to supplement security education of users with technological solutions such as UBA (user behavioral analytics) that can profile, detect and alert behavioral anomalies.

The user is still the real enemy (59% rank phishing as number 1 threat vector), with a high reliance on e-learning to change the user behavior (84% still use e-learning as one of the methods).

The crown jewels have left the fortress

Data privacy

Shadow IT consumption from the cloud through SaaS applications is increasing at a phenomenal rate. While SaaS adoption has made businesses nimble in the way they exploit and leverage IT, it has left the IT security teams chasing the data that has left the organizational shores. The centralized IT risk and security functions have been left considerably weakened and their ability to maintain control over sensitive data has been eroded.

Responsibility for governance of data privacy is still highly centralized, lying either with the CIO, CISO or CPO for 71% of organizations. Managing privileged access to data was ranked as the number 1 control amongst data security controls.

Smart applications have become the soft underbelly

Application security

The 'app store' culture is now very contemporary and businesses are enabling their ecosystem, including partners and consumers, to develop custom applications to solve common problems. Cognitive and analytical enablement of applications is the new norm to automate processes, increase velocity and reduce costs of operations. In this fast-changing pace of application development and evolution, the challenge in managing application security is to simplify the lifecycle, and detect and address security vulnerabilities early on. With even infrastructure becoming code, processes have not evolved to review security weakness in the infra-as-a-code.

20% of the respondents said that they test their apps for vulnerabilities and eliminate them in every build. Application security lifecycle management standards have seen low adoption (Microsoft SDL at 15% was the highest).

Internet of Things will become the new cyber weapon

Network security

Emergence of new Internet of Everything 'surfaces' like connected cameras, cars, health and industrial automation devices are proving to be a great launch pad for the "hacking for hire" industry. The emerging IoT devices come with a low memory and processing footprint and usually accommodate very little security capabilities including patching. Such devices, once they are 'online' with an IP address, are easy prey for sophisticated hacking syndicates. These syndicates can develop custom malware to take control of IoT devices en masse and use them as a launchpad for cyber-attacks. Cyber Insurance might turn out to be an alternative risk transfer mechanism for IoT providers if they cannot address the security vulnerabilities/ risk which are inherent in these platforms.

The size of DDoS attacks has reached a whopping 990 GBPS using 150,000 compromised public IoT-enabled CCTV cameras.

58% of the respondents experienced some form of DDoS attacks last year.

Bring your own key (BYOK) will be a game changer for cloud data protection

One of the biggest challenges for enterprises to adopt cloud-based platforms has been loss of control over data and compliance with regulatory processes. Once the data moves out of the enterprise periphery to the cloud environment, there is a loss of control particularly over what the privileged users of the cloud services provider can do with the data. This challenge has existed despite the native encryption capabilities provided by the cloud platform provider – because key storage locally with the cloud provider would defeat the purpose of the encryption. BYOK might be a game changer for cloud adoption by giving compliance and control to enterprises over their data wherein the enterprises could hold on to their keys and an agent housed with the cloud provider could provide the real-time encryption and decryption capability.

Cloud encryption

64% of respondents said meeting compliance and legal obligations were a hurdle towards moving data to cloud.

Future battles will be fought between bad bots and good bots

The battlefield in the cyber domain has been asymmetric as the weaponry in many instances of attacks have been deceptive command and control bots that can be operated from the other end of the globe. The detection apparatus in the enterprise SOC have been a combination of people, processes and technology. The technology layer has been helpful only to raise alerts or to provide indicators while response and recovery still involve a lot of human intervention. Use of cognitive technologies to automate a significant percentage of the incident response procedural stages will be the future given that organizations are facing challenges to minimize mean time to detect, mean time to respond and attract/ retain good security analysts.

Security monitoring

46.8% of the organizations felt they lack skilled security analysts who can help improve both detection and containment lifecycles.

81% of the respondents said they needed contextual threat intelligence within security monitoring processes for improving their mean time to detect and respond.

Based on the primary research/survey findings, Wipro recommends that the enterprises incorporate the following guidelines in their cybersecurity strategy.

Data privacy

Define Executable RACI for Data Governance Processes across CIO, CISO, CPO, CRO and CXO hierarchies

Cloud encryption

Remote Key Management & Encryption is getting mainstream. Cautiously adopt for core Data and Apps

Application security

Infra-As-Code needs immediate attention for vulnerabilities. Adopt standards (SAMM/SDL etc.) based security maturity improvement across Enterprise Apps

Human dimension

Complement security education drives with periodic simulation based targeted attack exercises

Network security

Prevent your IoT infrastructure from becoming a DDoS launchpad. Patch and refresh your device ecosystem

Security monitoring

Reduce dwell time for persistent threats supplementing SIEM with security analytics using machine learning driven use cases

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

Compete in the market and collaborate on cybersecurity – clash of interests?

Many enterprise customers are reliant on an external threat intelligence provider for third party inputs. However, the direct peer-to-peer or exchange-based sharing of contextual threat intelligence is still in its infancy. This can be attributed to the challenges faced by competing firms to embrace each other for cybersecurity benefits.

67.6% of the respondents said they use a third-party threat intelligence supplier for their intelligence feeds.

War gaming for cyber preparedness

Most organizations are dependent on penetration testing for validating the strength of an application to withstand cyber-attacks. However, coordinated attacks, particularly from formidable attackers such as nation state agencies, may be multifold and aimed at taking down related critical infrastructure and causing systemic failures. Cyber-attack simulation exercises or war gaming exercises can test the combined effect of people, processes and technologies to reduce risk and also explore larger systemic issues that can be caused.

30.6% of the respondents said they haven't participated in any kind of cyber-attack simulation exercise.

Reputational risks prevent sharing

If details about a hack or attack come out in the public domain, it can have a direct bearing on information sharing process.

53.9% of the respondents said they are reluctant to share intelligence with sharing groups due to reputational risks.

Give with one hand and take with the other

Security teams understand the value of real time information on attack vectors, actors and indicators of compromise. Any such timely information can be used to calibrate existing monitoring systems to detect new threats. In order for enterprises to contribute effectively to such sharing networks, it is necessary to invest in forensic capabilities that can generate shareable intelligence from attacks that are manifested on a daily basis.

80% of the respondents said they are willing to share either blacklisted IPs, domains or malware IOCs and phishing addresses.

Based on the primary research/survey findings, Wipro recommends that the enterprises incorporate the following guidelines in their cybersecurity strategy.

In-house forensic capability

For enterprises to effectively participate in threat information sharing networks run by regulators and agencies; they need to invest in in-house forensic analysis capabilities that can generate inputs.

The last section focuses on the future and is largely based on secondary research and viewpoints evolved from within the CRS Center of Excellence (CoE). The topics covered were chosen based on their perceived impact on people, process and technology in the context of cybersecurity. The topics range from the changing face of the future cybersecurity analyst (people) to Cyber Insurance and its play in risk management (process) to IOT security and drones (technology).

Emergence of the good bots

People

With cybersecurity skills getting more specialized and hard to find and an increasing volume of attacks perpetuated by bots orchestrated by their human masters, the cyber battleground is witnessing an asymmetric power distribution. This asymmetry is never going to be balanced by additional skilled human capacity. The future of cyber battles seems to be shifting to one where protagonist and antagonists are going to be bots, with the strings being pulled by their human owners. Machine learning and artificial intelligence are playing a significant role in this tectonic shift and it is in the best interests of organizations and their cybersecurity analysts to embrace them fervently for solving the emerging challenges.

32.8% of respondents indicated that knowledge and experience on ML and AI technology is going to be a key driver.

CISOs need to evolve to embrace insurance as a supplementary risk transfer mechanism

Process

Risk transfer through Cyber Insurance may have been frowned upon a decade or so back, but it is an avenue that is emerging as a serious supplement to strategies that are employed by enterprises. The approaches employed for underwriting and quantification are evolving and maturing.
There is better confidence emerging amongst insurance companies to calibrate an enterprise's cyber risk exposure.

47% of the responding organizations had some form of Cyber Insurance policy coverage. 58% of the respondents who had coverage had insurance for recovery from business interruption and data loss.

Hacking of commercial drones - Sky is the limit

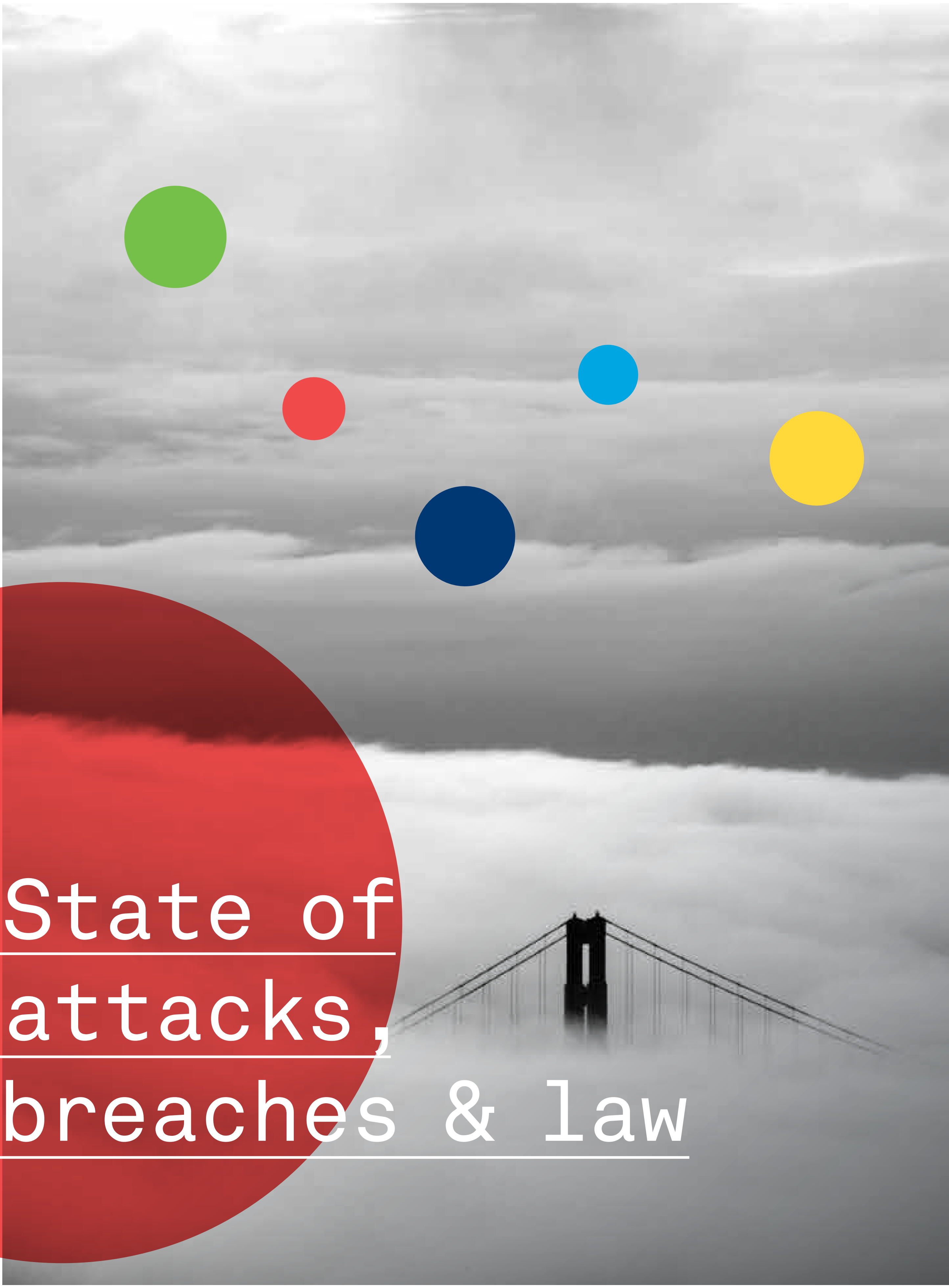
After the FAA released the rules for UAS (Unmanned Aircraft Systems) on August 31, 2016, there has been a significant increase in the use of drones in different industrial scenarios. Drone operators could be exposed to legal action in the event that their drone causes injury to people or property in the normal course of operations.

Skyjacking of drones has become the number one threat for cyber attacks on commercial drones across verticals.

Technology

Persistent identity for smart environments

A unique, consistent and seamless identity will be a pre-requisite for every user across different environments in the smart digital world. The notion of such Persistent Identity will be a critical enabler for security in smart enterprises, avatar environments and IoT devices. With evolution of technologies in the IoT space, the use of smart devices for simplification of security processes is going to be a natural evolution. Standardization will help speed up adoption and interoperability of persistent identities.



State of attacks, breaches & law

The 'State of attacks, breaches & law' section lays out the broad environment that defined cybersecurity around the globe in 2016. In this section, we will re-visit the key data breaches of 2016, the type of data that was stolen and how the online world reacted to cybersecurity attacks on specific enterprises. This section also analyzes the 'Weapons of Cyber Destruction' that were developed by hostile elements in the digital underworld and how they were used to perpetuate various attacks on commercial IT infrastructure. Further, the section weaves its way into troublesome territory, and analyzes the security weaknesses in commercial security products and what that holds out for CISOs and their teams as they leverage these products to fortify their defenses. Last but not the least, the 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 overseas cross-border flow of information.

Dissecting the data breaches of 2016

2016 has seen enterprises across multiple verticals experiencing increased number of data breaches. The frequency of attacks increased in 2016 (Figure 2) and their impact has also been magnified to a great extent. At the minimum 1.38 billion records of data were reported stolen in 2016. It is not just the sheer quantity of information assets that have been lost or disclosed publicly, but in the aftermath of the attacks, customer faith has been severely dented for many enterprises. The social media sentiment analysis that we have carried out in this context for top attacks supports this assertion. Our research indicates that even though 2015 has seen some of the most successful breaches of high-value targets, in 2016 the story has only gotten worse. There has been a significant growth of 53.6% for stolen records in the year 2016, when compared to 2015.

53.6% increase in number of stolen records in 2016

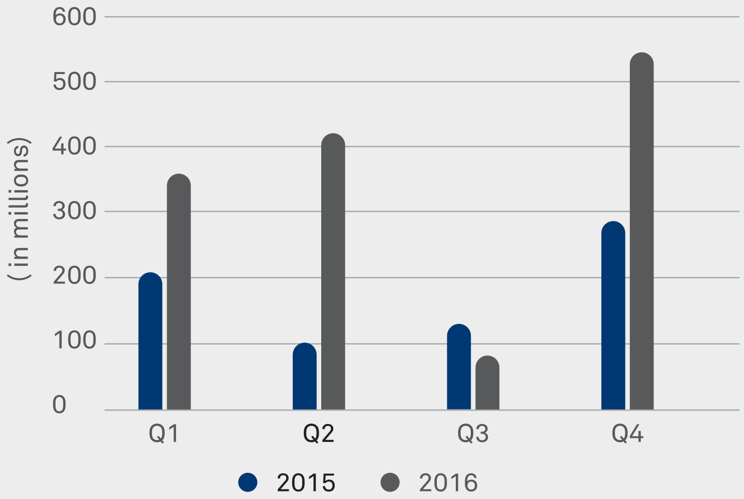
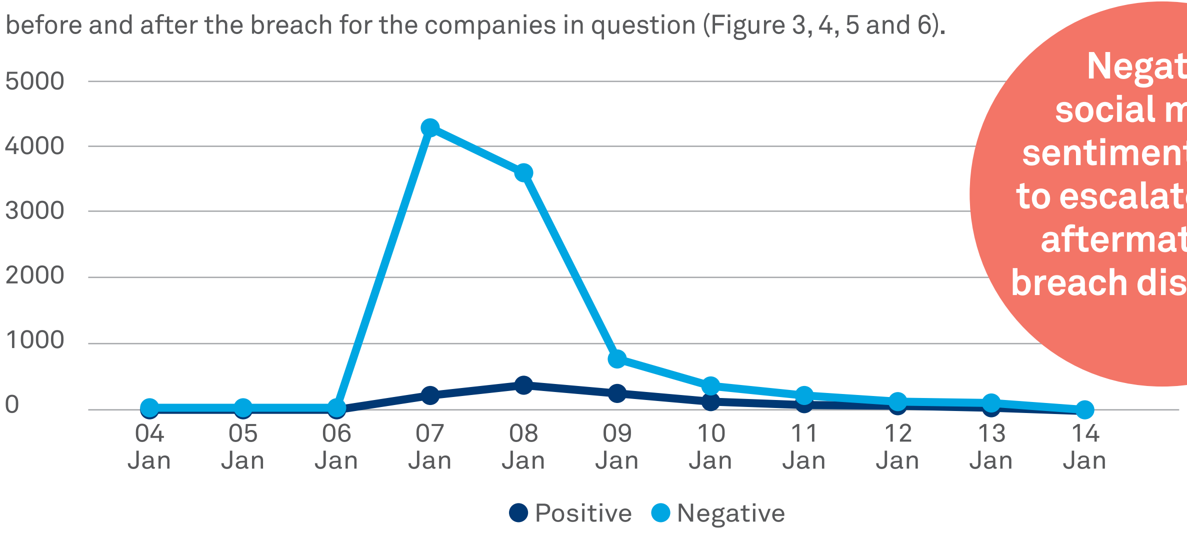


Figure 2 - Number of Stolen Records in 2015 vs 2016 (quarter-wise)

43 records were stolen every second in the year 2016

Sentiment analysis post leading breaches

Following on from our analysis of the top breaches in 2016, we picked up specific instances of companies that had data breaches and investigated how the social media sentiments of the general public varied before and after the breach for the companies in question (Figure 3, 4, 5 and 6).



Negative social media sentiments tend to escalate in the aftermath of a breach disclosure

Figure 3 - Time Warner Cable 2016 Breach Sentiment Analysis

The sentiment analysis was done for some of the major breaches of 2016. We have collected the sentiments from tweet mentions a week before and after the breaches were made public. Subsequently, we plotted it on graphs which depict both positive and negative sentiments.

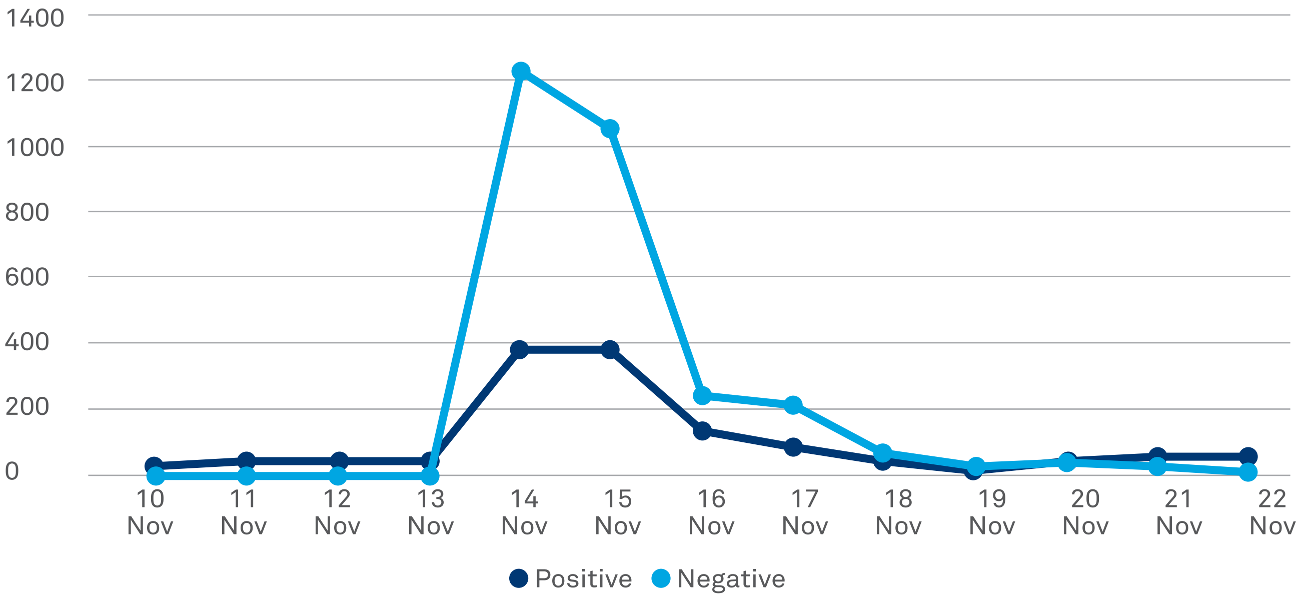


Figure 4 – FriendFinder 2016 Breach Sentiment Analysis

From the sentiment analysis graphs, one can clearly infer that public sentiment was very negative for a period after the breaches were notified. This negativity usually tends to translate into stock price dips and/ or lower business online, ultimately hitting the bottom line.

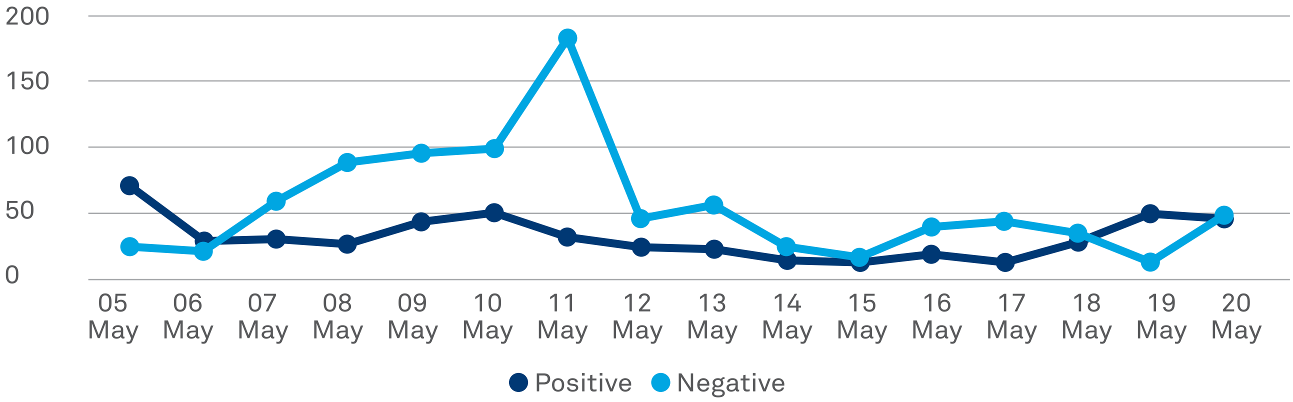


Figure 5 – Equifax 2016 Breach Sentiment Analysis

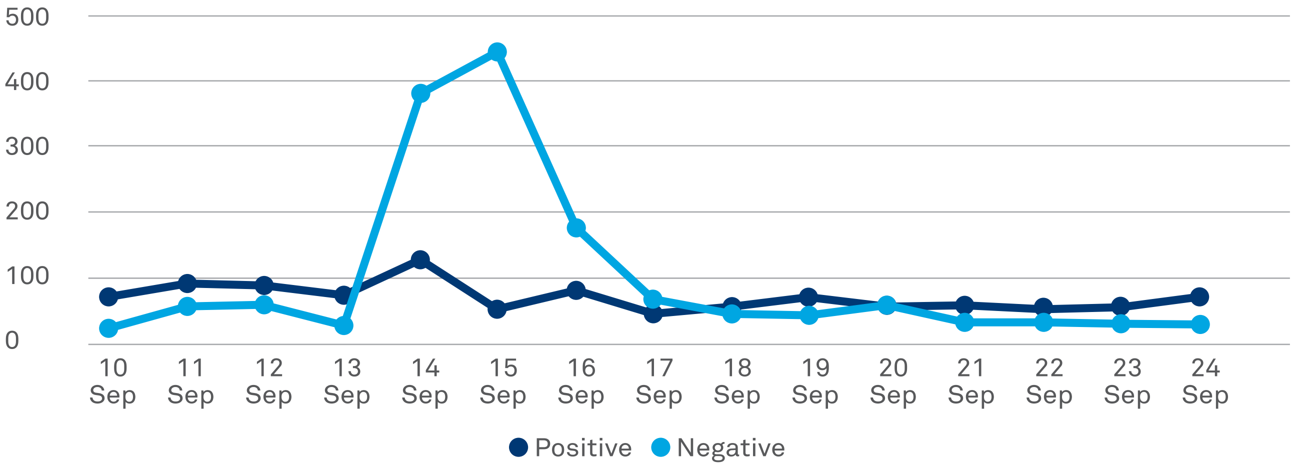


Figure 6 – ClixSense 2016 Breach Sentiment Analysis

PII Analysis of the major data breaches

From the major data breaches of 2016, we carried out an analysis of the type of data elements (PII - Personally Identifiable Information) that were breached. The PII analysis gives a clearer picture of the criticality of the data that was breached. For the sake of the analysis, Basic PII was classified as First Name, Last Name, Email, Gender and Address. Advanced PII is Basic PII + SSN (or any other

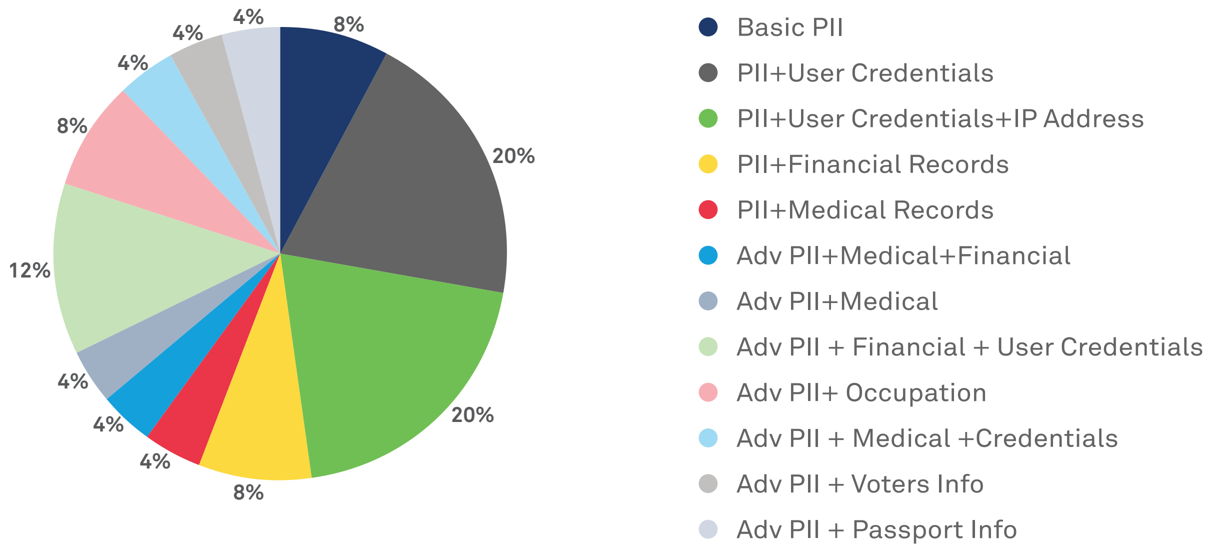


Figure 7 - PII Split Analysis - 2016

regional tax identifier). The PII data types were classified into 12 categories for this analysis as depicted in Figure 7. The analysis revealed that 56% of the breaches analyzed involved a combination of user credentials (i.e., username and password), which can be leveraged for further malicious acts. Hence, for breaches that involve user credentials, organizations need to have processes to quickly communicate with users and reset their credentials / passwords.
A combination of such PII data can lead to further extraction of additional confidential data related to a person through social engineering. Research indicates that hackers are primarily after a combination of Basic PII with security credentials followed by data that is domain specific.

56% of the stolen data had 'User Credentials' as one of the major data elements

Data breaches by geography

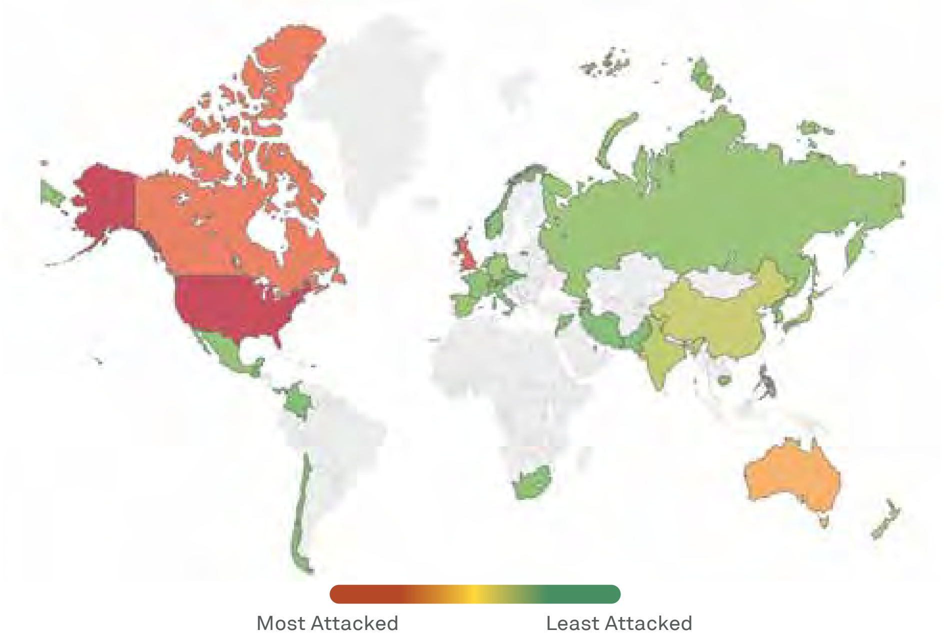
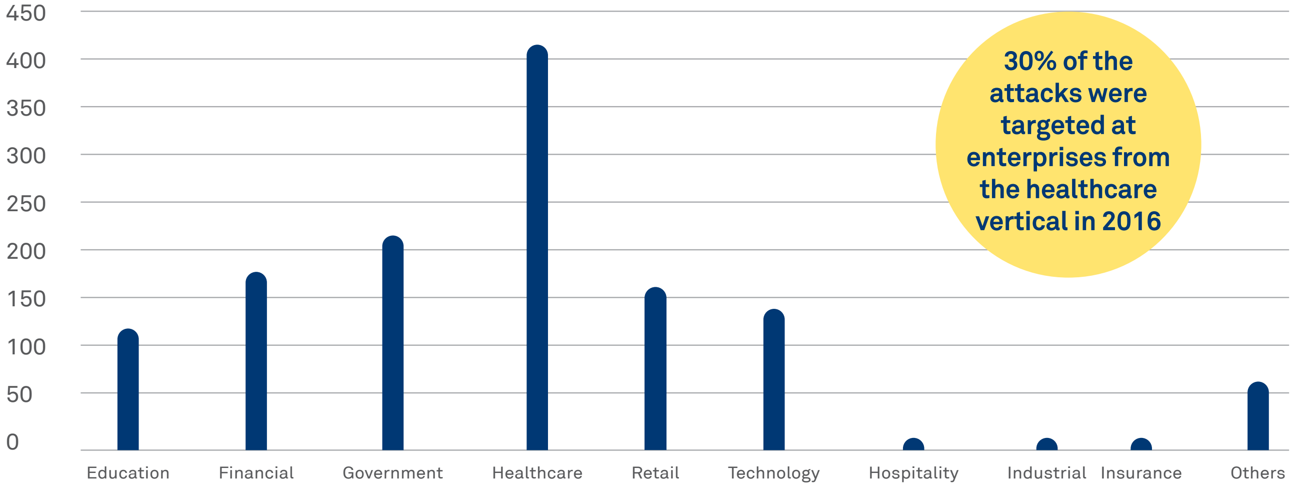


Figure 8 – Data Breaches by Geography - 2016

The heat map (Figure 8) indicates that over time cyber-attacks are expanding into a global phenomenon, whose intensity and scale threatens every organization, irrespective of the nationality.

Industry wise analysis

To further drill down the analysis, we also studied industries which were targeted the most in the last one year. After researching publicly disclosed attacks, we see that the healthcare vertical was the most impacted in 2016. 30% of the attacks were targeted at the healthcare vertical (Figure 9).

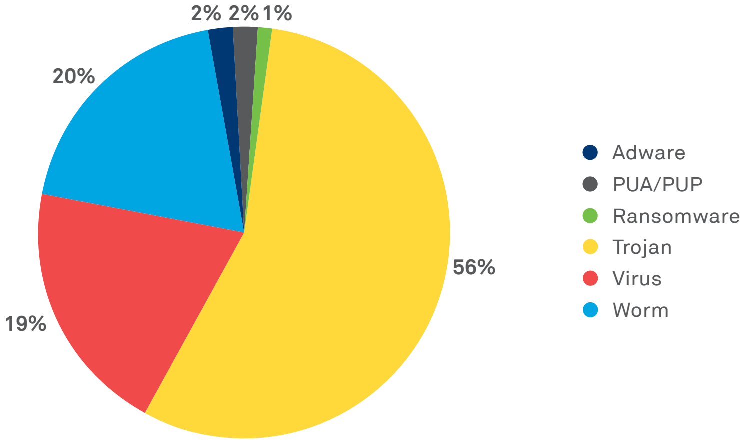


30% of the attacks were targeted at enterprises from the healthcare vertical in 2016

Figure 9 – Data Breaches by Industry Verticals - 2016

Weapons of cyber destruction abound in 2016

This section of the report aims to highlight the major malware detected by the Wipro CDC across a sample set of environments in year 2016. The detections were de-identified and then analyzed for the malware threat type, relative distribution, and growth across all the four quarters in 2016.



Trojans accounted for 56% of the attacks

Figure 10 - Overall Malware Distribution - 2016

Figure 10 illustrates the major different types of malware that were detected in 2016 across the following categories: Trojan, Virus, Worm, PUA, Adware and Ransomware. Trojans, however, followed by worms and viruses occupy the top three positions of the various types of malware that were detected in 2016. And as you can observe in Figure 11, there was a growth in proportion of detected viruses and worms, from Q1 to Q2, Q3 and Q4.

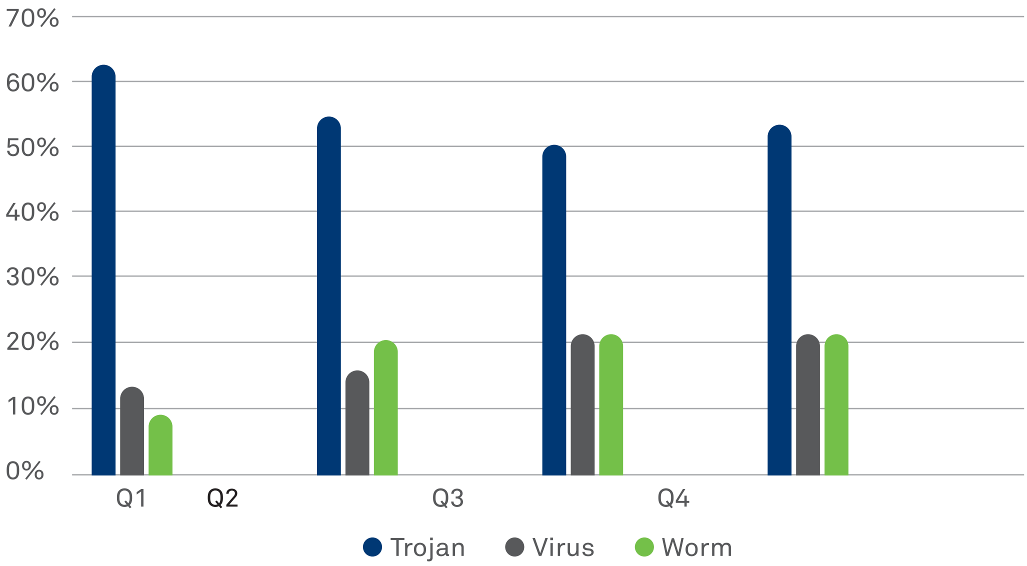


Figure 11 - Quarter-wise Analysis of Malware - 2016

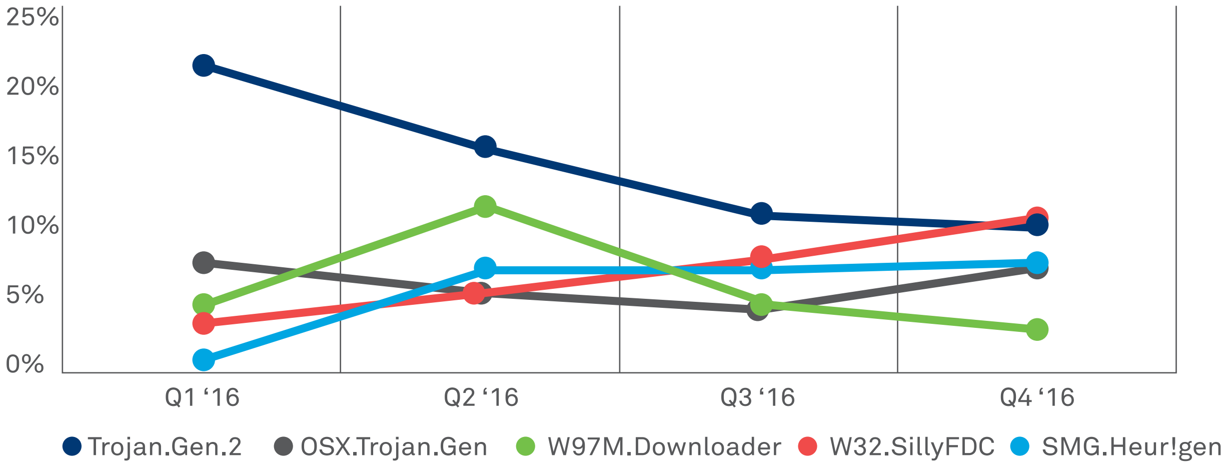


Figure 12 - Quarter-wise Growth of Top 5 Malware Families in 2016

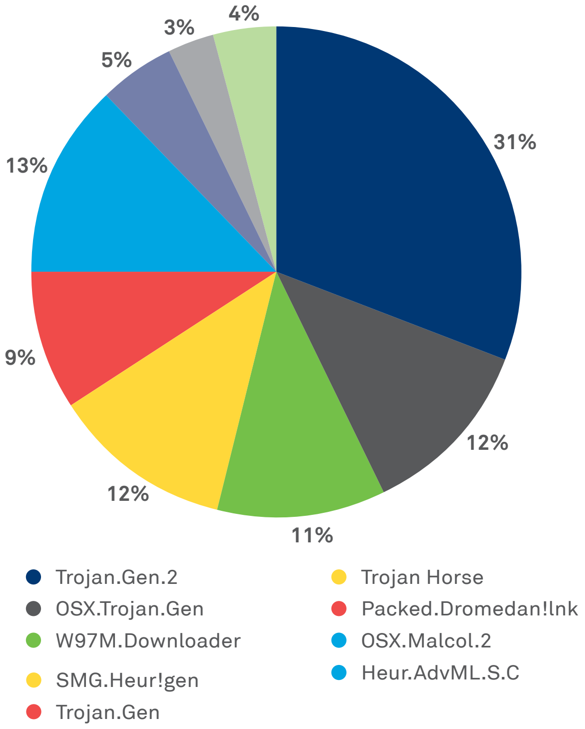


Figure 13 - High Incidence Trojan Malware Families in 2016

Trojan.Gen.2 was the most popular Trojan of 2016

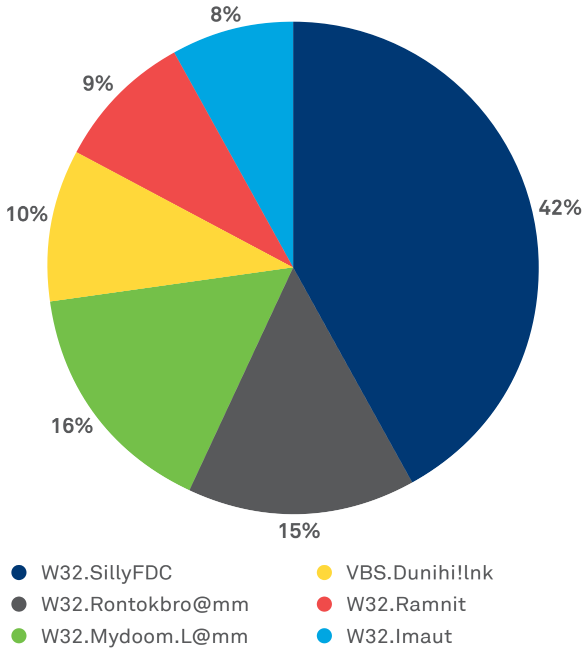


Figure 14 – High Incidence Worm Malware Families in 2016

W32.SillyFDC recorded the highest incidence in worm threat category

Of the malware families discovered in 2016, Packed.Dromedan!gen23 recurred the most

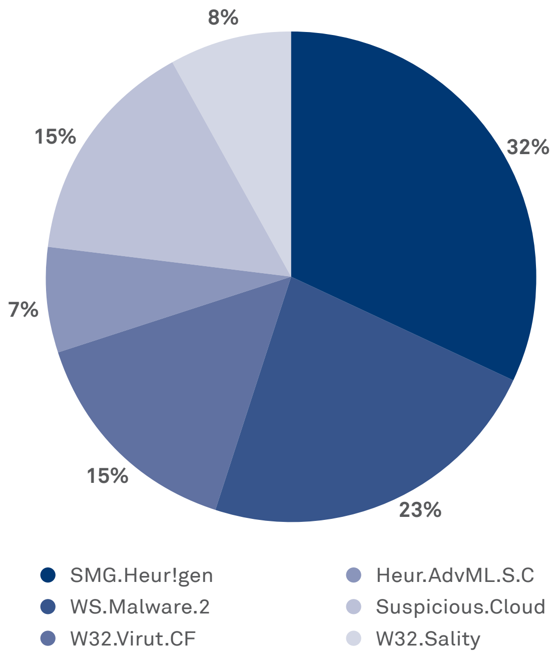


Figure 15 – High Incidence Viruses in 2016

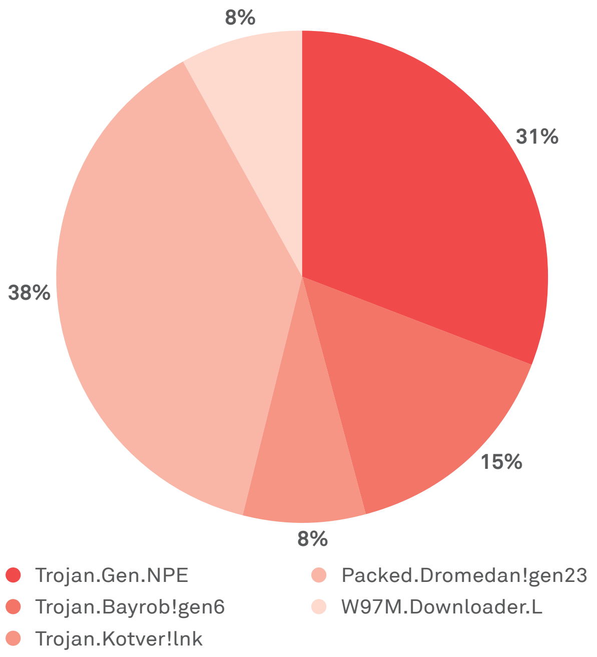


Figure 16 – Top 5 Malware Families Discovered in 2016

In the sample subset of CDC environments analyzed, 189 unique malware families were detected across three threat categories–Trojan, worm and virus–in 2016. Using this data, we have captured the top five malware families in terms of high incidence and also generated a graph on quarter wise growth of the same (Figure 12). We also captured the top Trojan, Worm and Virus (Figure 13, 14 and 15) malware-families detected using the data across different environments that we have taken into consideration.

We also analyzed the malware that were reported newly by different AV security vendors in 2016 and examined their split across the events that were reported in the last year. By cross checking this data with our findings, the top 5 malware and their normalized percentage distribution was found out.

Exploits

An exploit is a piece of code that can be used to attack (in the form of accessing information or installing malware) by taking advantage of software vulnerabilities existing in operating systems, web browsers, applications, or software components the targeted system has.

In 2016, we observed a large variety of exploits that manifested through different types of exploit kits available in the public domain. Exploit kits are basically collections of exploits bundled together and sold or rented in cybercriminal circles as commercial software or as a service. In general, an exploit kit is a collection of webpages containing exploits, that can be installed by the attacker on a malicious web server and the device can be then compromised through drive-by download attacks.

In the exploits that were detected across the first three quarters of 2016, five types of exploit kits were predominantly discovered: Angler at 33.3% was followed by RIG at 23.8% and Nuclear at 19%.

At 33.3% Angler was the most observed exploit kit

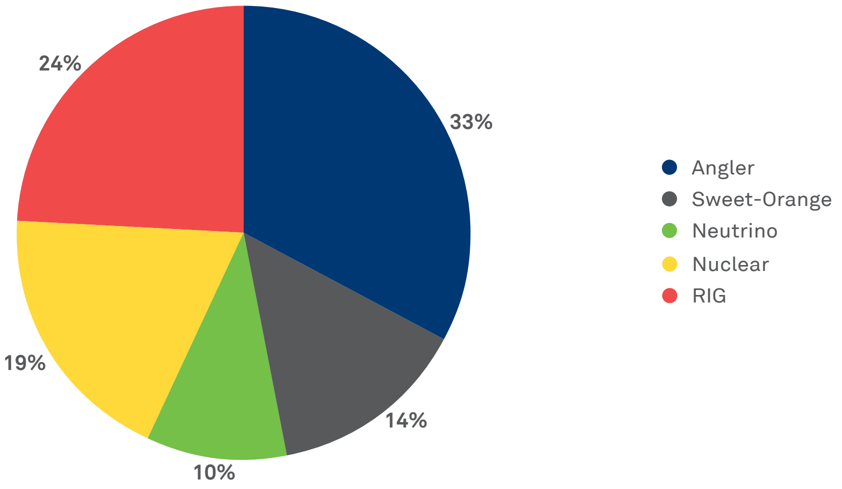


Figure 17 - Top 5 Exploit Kits of 2016

Vulnerabilities in cyber defenders

Vulnerability management has been an Achilles heel for many organizations in the race to keep systems and applications up to date with the latest fixes. In spite of implementing the best detection technologies, organizations continue to get compromised. While attacks are getting more sophisticated with the passage of time, it is also the inability of the organizations to keep a tight control on their vulnerabilities that is a defining factor for increasing compromises.

The focus on vulnerability management in most organizations has remained on general IT applications and infrastructure. Security teams take for granted in good faith that their protective and detective controls/tools are not insecure by themselves. But is that true? Do vulnerabilities exist in security tools that operate in domains such as firewalls, IDS/IPS, AV, DLP, Identity Management, Access Management, Database Activity Monitoring, Privileged Access, GRC, PKI, etc.?

As part of this report the CRS CoE carried out a historical analysis of vulnerabilities listed against security tools in the CVE (Common Vulnerability & Exposures) database between 2014 and 2016. When we analyzed the CVE listing for security products across different domains, the alarming data that emerged was that a vast majority of security products had some form of security vulnerabilities. We deepened our study in this area to further get a clear picture and the findings from that study are presented here.

Vulnerabilities in security product domains

As part of the study, we first listed down several leading cybersecurity products which can be mapped back to domains and which can be further mapped back to layers where they operate such as network, endpoint, identity, data and more. For each of such products occurrence of vulnerabilities and CVE scores over the last three years were captured.

In the last three years, the most frequent types of vulnerabilities found in various security products reported in the CVE database (accessed through source: www.cvedetails.com) were DoS (28.4%), Code Execution (18.4%) and Information (Gain) Leakage (16.5%) out of 13 categories listed (Figure 18).

Domain Security Score Rating: To arrive at the final score for each control domain (that had similar products mapped into) the weighted average of each of the vulnerability types for the last three years was calculated. Once the weighted average score was arrived upon, the single average score per domain was arrived upon.

Based on the domain score ranging from one to ten (with 10 indicating a higher prevalence of vulnerabilities) a RAG (Red, Amber, Green) status map was drawn out per domain. The key takeaway for the reader from this RAG status is that most of the domains (and indirectly the products associated with them) have had vulnerabilities being reported in the last three years. The security teams responsible for vulnerability identification across the organization thus need to also focus on the security products which are meant to defend the organization and not take for granted that they themselves are secure.

DoS, XSS and Gain Information are the most common vulnerabilities in security products

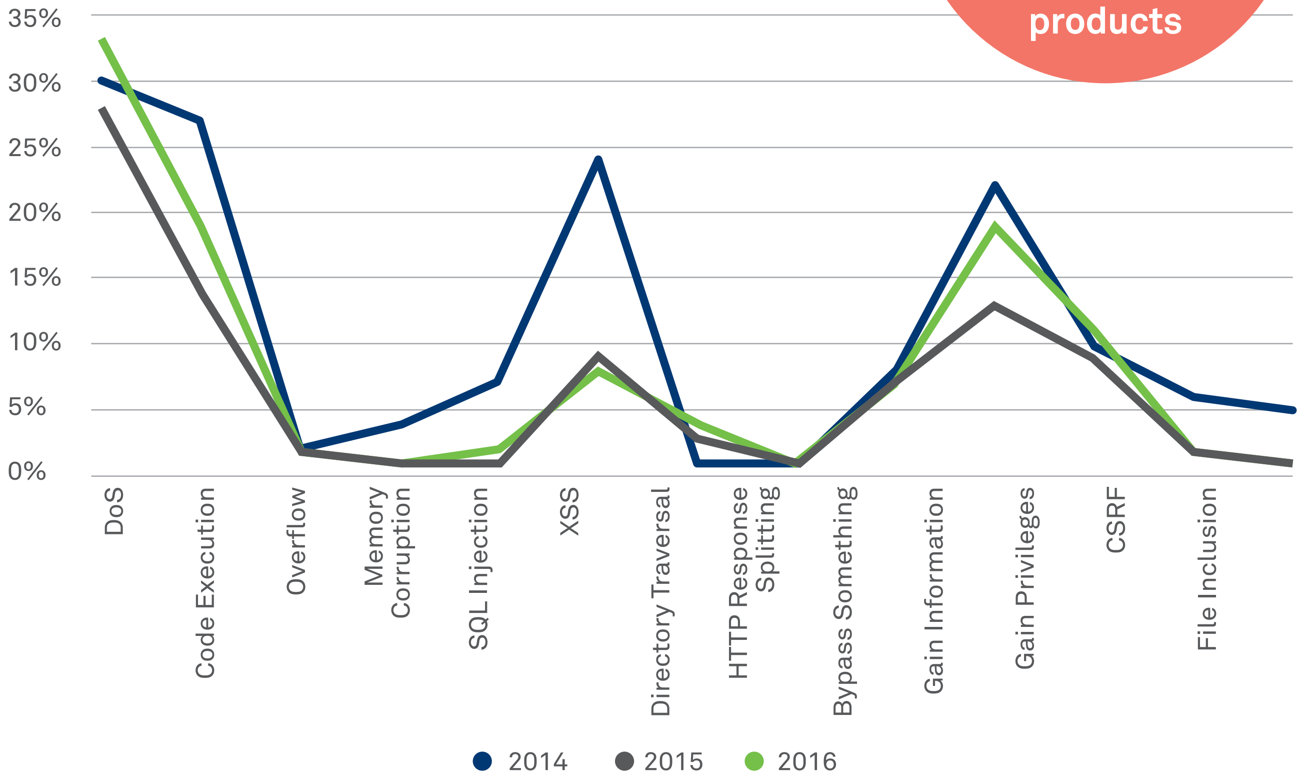


Figure 18 - Vulnerability Trends in Security Products

HIGHLY VULNERABLE

- SAST (7.7)
- SIEM (7.2)
- Network Access Policy (7)
- Firewall (6.5)
- Load Balancer (6.4)

MODERATELY VULNERABLE

- Proxy/Gateway (6.2)
- Web Services/ API Gateway (6.1)
- Antivirus (5.9)
- Database Activity Monitoring (5.9)
- VM (5.7)

LEAST VULNERABLE

- IDAM (5.6)
- DLP (5.6)
- GRC (5)
- PKI (4.1)
- MDM (4)

Note: The weighted vulnerabilities score is dynamic and is illustrative at the time of publication as there are new vulnerabilities that get added every day.

The average product category score was 5.8, indicating that vulnerabilities exist across the board

SIEM, SAST and NAP product categories had scores greater than seven - an indication that vendors need to do more to minimize security vulnerabilities during release cycles

Regulatory landscape: breach notification and overseas transfer

This section is the output of a detailed analysis that was carried out by the CRS CoE of laws relating to data breach notification 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, US, Norway and Dubai*. The key parameters that went into the two areas of analysis are illustrated in the table below.

Focus Areas of Analysis	Parameters
Data breach notification requirements	1. Mandatory notification of authority 2. Breach categorization 3. Mandatorily notify data subjects 4. Fine if not notified
Restriction on overseas transfer	1. Consent of data subjects 2. If outside jurisdiction provides adequate protection 3. Binding Corporate Rules (BCRs) 4. Standard Contractual Clauses (SCCs) 5. 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 classify the countries across a heat map that was represented on a world map (Figure 19).

Data breach notification requirements

Ever since the State of California enacted the first data security breach notification law that became effective on July 1, 2003, the world has seen a rapid development in breach notification laws across several countries.

44.4% of the countries analyzed have laws which mandate notifying concerned data subjects upon detection of a data breach

GDPR requires data owners to notify consumers and the DPA within 72 hours of a breach

* *Restricted only to a city based on available data*

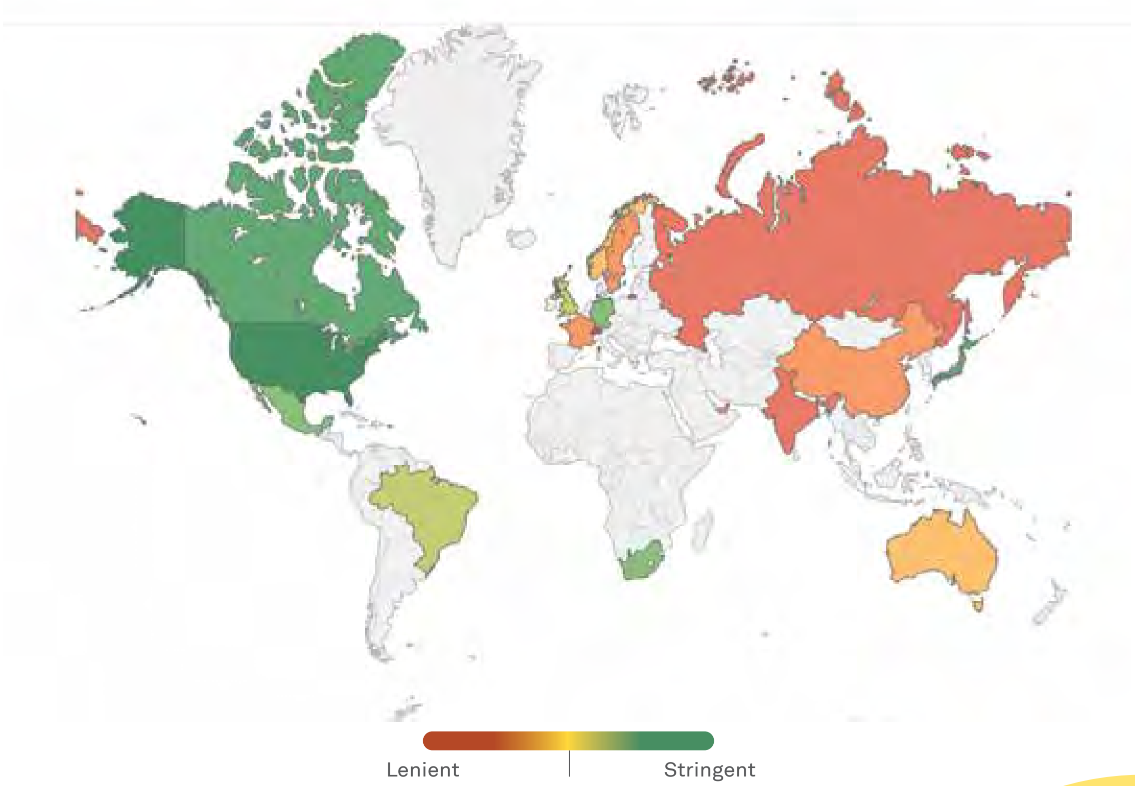


Figure 19 – Global Breach Notification Requirements -2016

Breach notification laws around the globe have some foundational elements that have been time tested. These key elements include: who must comply with the law, what defines personal information, what constitutes a breach and how notice must be given to data subjects.

Significantly, the European Commissions voted to approve the EU-US Privacy Shield on July 12, 2016 which will replace the Safe Harbor regime under which US companies certified compliance with EU-standard data privacy practices. The General Data Protection Regulation (GDPR), the set of rules which will replace the EU Data Protection Directive, will come into force by May 2018. One cloud that will hover over the minds of many is how the post-Brexit privacy regime in UK would evolve. We expect the English Data Protection Act 1998 and privacy directives from Brussels to be upheld as the law of the land in the near future.

As discussed, in effect from May 2018 (expected), the EU GDPR will mandate data controllers a 72-hour data breach notification requirement for all businesses operating within EU in case of a personal data breach. Data controllers in the notification must show the numbers and categories of data subjects and files affected, likely fallout and mitigation response.

In addition, the new GDPR also places some direct obligations on even data processors who should from now on notify the data controllers without undue delay after discovering a breach.

Also the data controllers must inform the affected data subjects without undue delay if breach is of high risk to the rights and freedoms of the concerned parties.

72.2% of the countries analyzed have clearly defined laws which mandate notifying the local authority post data breach

Our research indicates that countries like US, Canada, Japan, Germany, Mexico, and South Africa currently have the most stringent breach notification requirements.

Some of the countries analyzed had provisions for breach notification in the local regulatory regimes, yet there was ambiguity or no explicit statutory requirements on breach categorization or statutory fines. Considering all such criteria, countries like Singapore, Switzerland, France, Sweden, Russia, China and India were rated as lenient.

At the same time, it is encouraging to see countries such as Australia stepping up to introduce the Privacy Amendment (Notifiable Data Breaches). This instrument that was recently passed has amended the Privacy Act 1988 to introduce a mandatory data breach notification scheme. One more example is the Dutch Data Protection Act (Wet Bescherming Persoonsgegevens or WBP) which sets the precedent in Netherlands to general data breach notification obligation and higher sanctions. Brazil has plans to enact the data protection bill known as the Bill of Law (No. 5.2726/16) for establishment of a data protection framework (which was considered in this research with the presumption of passage).

From a data breach notification law point of view, 2016 can certainly be rated as a positive year with more countries implementing strong data breach notification laws, and the ripple effect of the same being visible across the globe.

Restriction on overseas transfer

Cross-border data transfers have been a key outcome of globalization and the mushrooming digital economy. Right to Privacy has been a fundamental driver for securing sensitive data of citizens or consumers that are collected, processed, stored by enterprise in the ordinary course of their business. Due to outsourcing and movement of data across borders, the concern around security of such data has been further heightened.

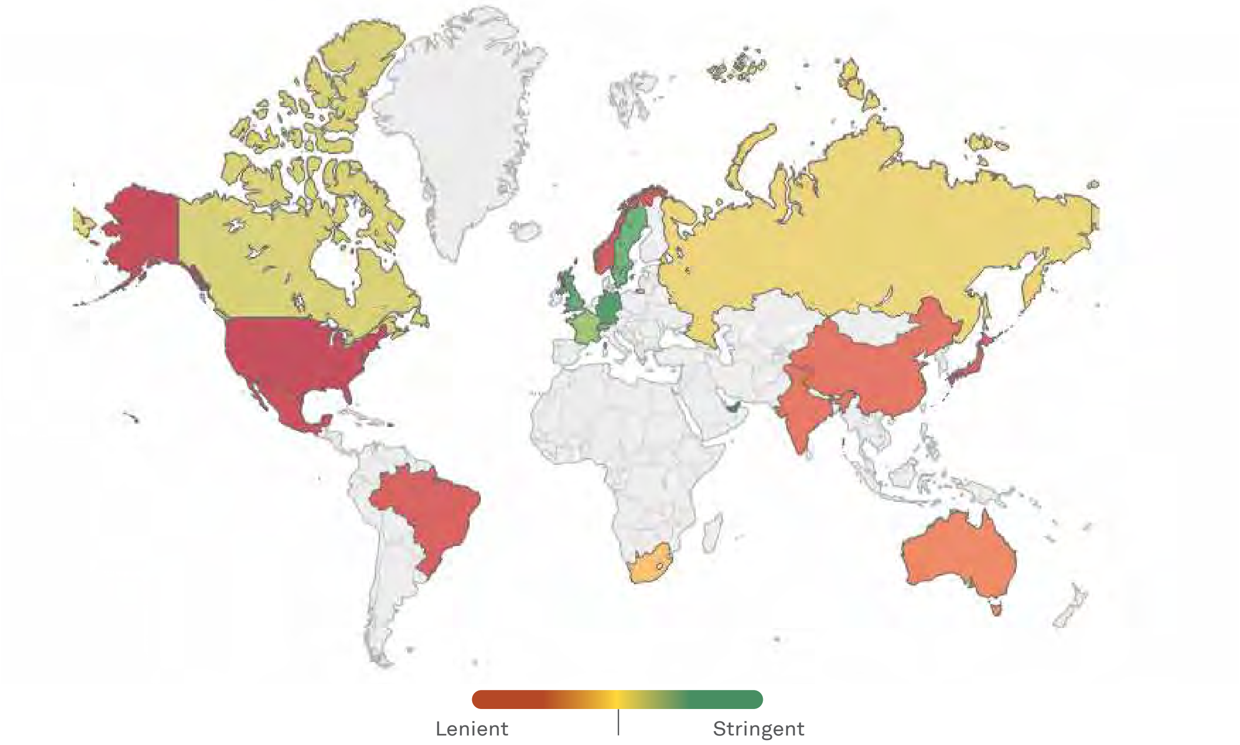


Figure 20 – Restriction on Overseas Transfer of Sensitive Data- 2016

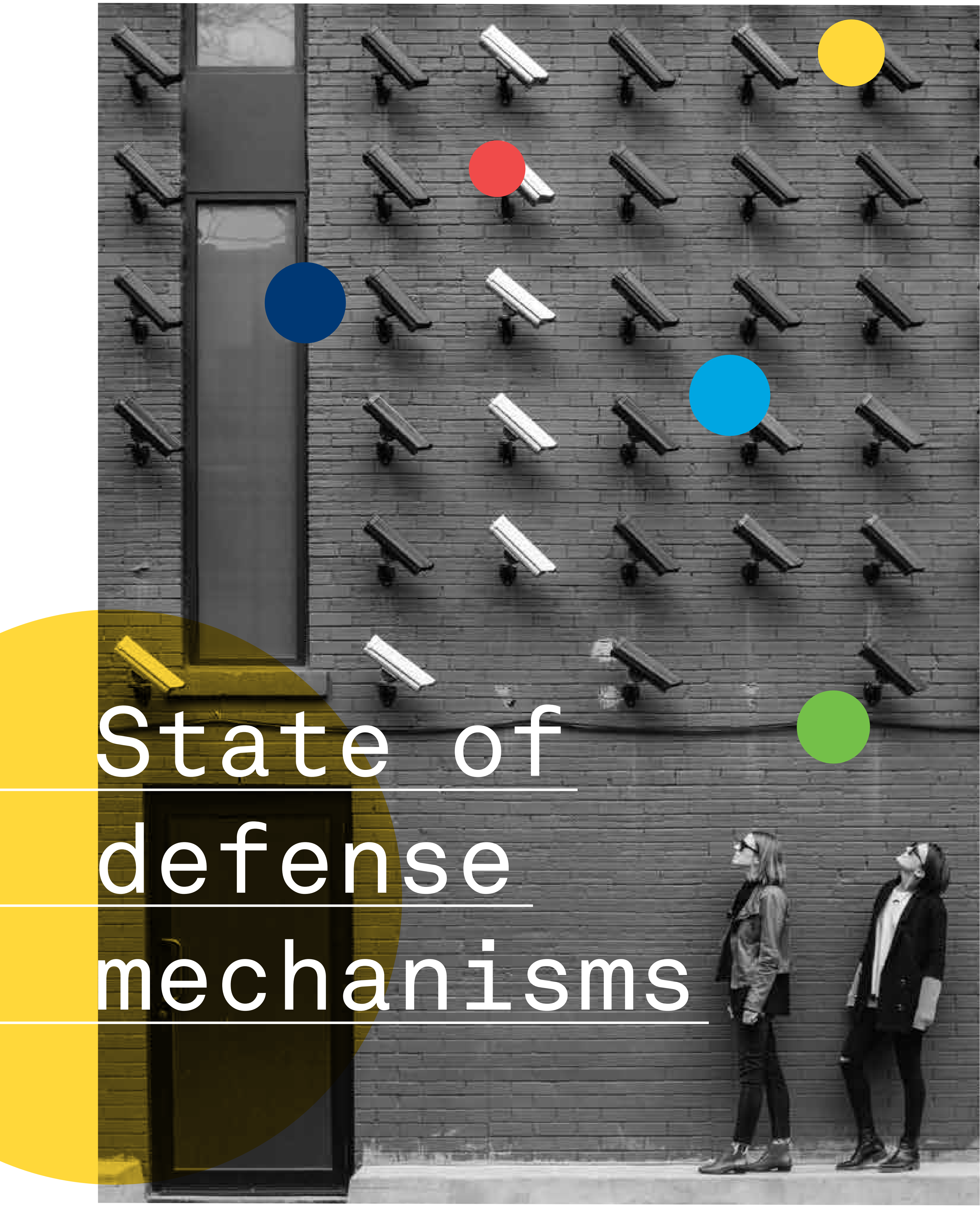
Several parameters were considered to build the heat map related to restrictions on overseas transfer of data as listed in table 1. They include: consent of data subjects, adequate overseas protection, binding corporate rules, standard contractual clauses and permission of data protection authority.

Using the weighted average methodology applied across these five parameters, the heat map was generated (Figure 20) and the same indicated that Dubai, Germany, UK, Sweden and Switzerland stand in the league of countries that have relatively high restrictions on overseas transfers. US, Mexico, Norway and Brazil scored low on restrictions imposed on overseas data transfers. A few countries like Dubai, Germany, China, Japan, and South Africa had regulatory requirements to notify their local regulators about overseas transfer of data.

38.8% of the countries analyzed recognize BCRs (Binding Corporate Rules) as a means of adequate safeguard in case the outside jurisdiction doesn't explicitly provide adequate protection.

94.4% of the countries analyzed recognize SCCs (Standard Contractual Clauses) as a means of adequate safeguard in case the outside jurisdiction doesn't explicitly provide adequate protection.

38.8% of the countries analyzed recognize BCRs (Binding Corporate Rules) as an adequate safeguard in case the outside jurisdiction doesn't explicitly provide adequate protection



State of defense mechanisms

The previous section analyzed attacks, vulnerabilities, cyber weapons and regulations that helped shape the public perception around cybersecurity in 2016. This section moves from attacks to the defense mechanisms that are privately employed by organizations to protect themselves from various forms of cyber-attacks. These defense mechanisms have been classified into control domain areas around data, application, network, endpoint, cloud, mobile and the end user. This section also reports on the current state of security monitoring as a discipline in organizations and explores its effectiveness in detecting and combating cyber-attacks in a timely manner. The findings related to these control domains have been arrived upon through our primary research with 139 practicing respondents across 11 countries and 16 industry verticals.

Human dimension

The amount of publicly available data should be restricted to contain social engineering attacks

Social engineering has been a tool in the arsenal of the hacking community for many years. It has been used to manipulate people to get them to share information or perform acts that can help in the process of subverting the security controls in place. The methods used through social engineering to manipulate the victims can be categorized into technical and non-technical. Non-technical methods include ones such as dumpster diving, tailgating, shoulder surfing. Technical attacks would include pre-texting, whaling, spear phishing, water hole attack, etc.

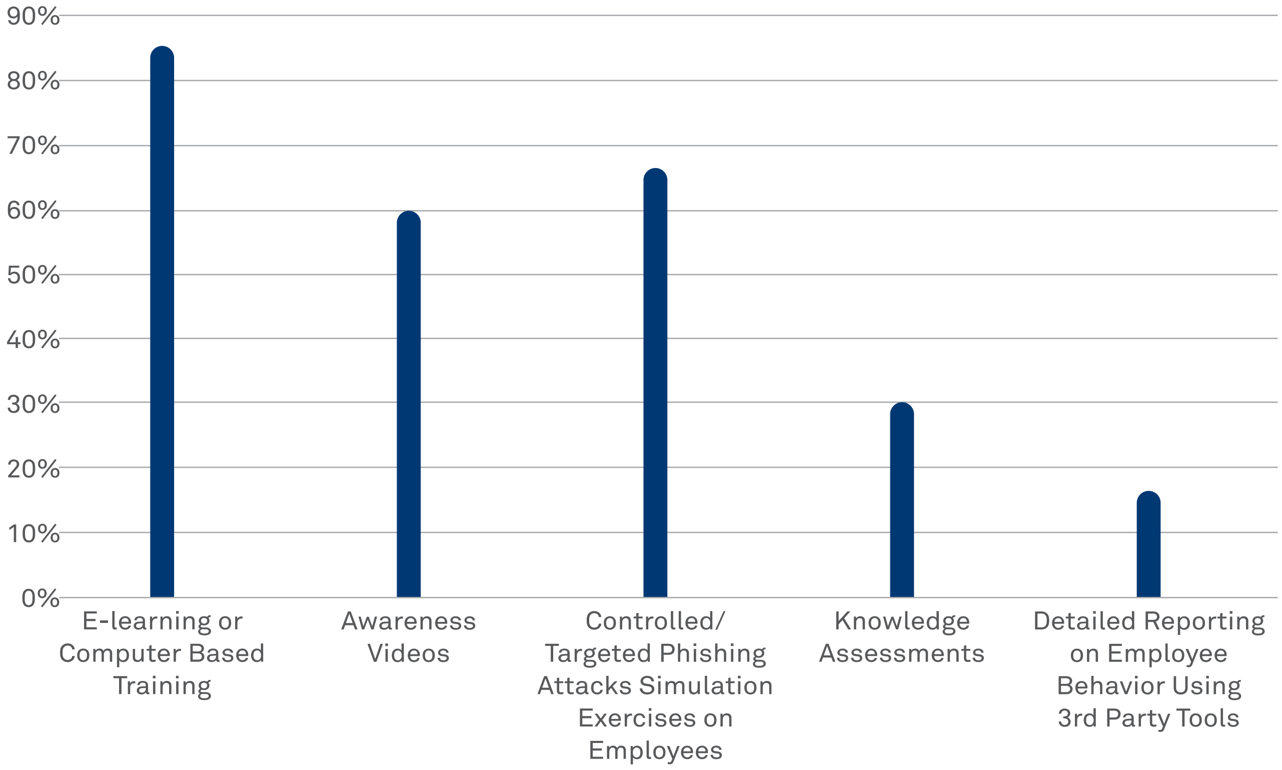


Figure 21 - Steps Taken to Educate End Users to Minimize Accidental Behaviors - 2016

Lack of employee training and awareness has been considered one of the main reasons why incidents related to inadvertent user action or social engineering have been on the rise. Security organizations have been increasingly investing in security education to curtail this trend and minimize the risk related to social engineering attacks. In our primary research, we asked the respondents what approach is preferred to educate and change the behavior of users to not fall prey to social engineering. The responses indicate that most of them prefer e-learning or computer-based training as the primary medium to educate users. Computer-based training is the simplest way to improve awareness about the possible liabilities from an employee's standpoint. Assessments and attack simulation exercises are on the rise as they give the end user a practical exposure as compared to e-learning which is more a theoretical exercise.

Supplementary strategies to e-learning that can be applied include:

- Minimizing publicly available information through social media policies
- Simulated attacks and follow up action
- Adopt smart security tools at the gateway and endpoint layers

Data security

We asked our respondents as to who is primarily responsible for the governance of data privacy within their respective organizations. 36.6 % of the respondents said that the CISO was still accountable for enforcing data privacy safeguards followed by the CPO (Chief Privacy Officer) at 26% (Figure 22). We also asked our respondents what they considered to be the most critical data security control that provided them the maximum returns. The unanimous choice for 34% of the respondents was Privileged Access Management (PAM) (Figure 23).

36.6% of the respondents say CISO is still responsible for safeguarding data privacy

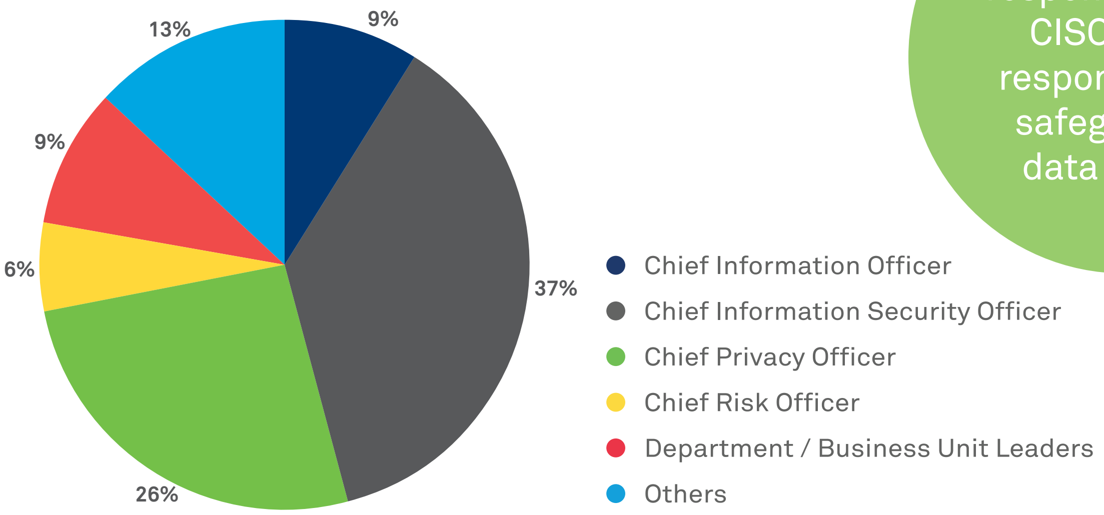


Figure 22 - Organizational Responsibility for Governance of Data Privacy - 2016

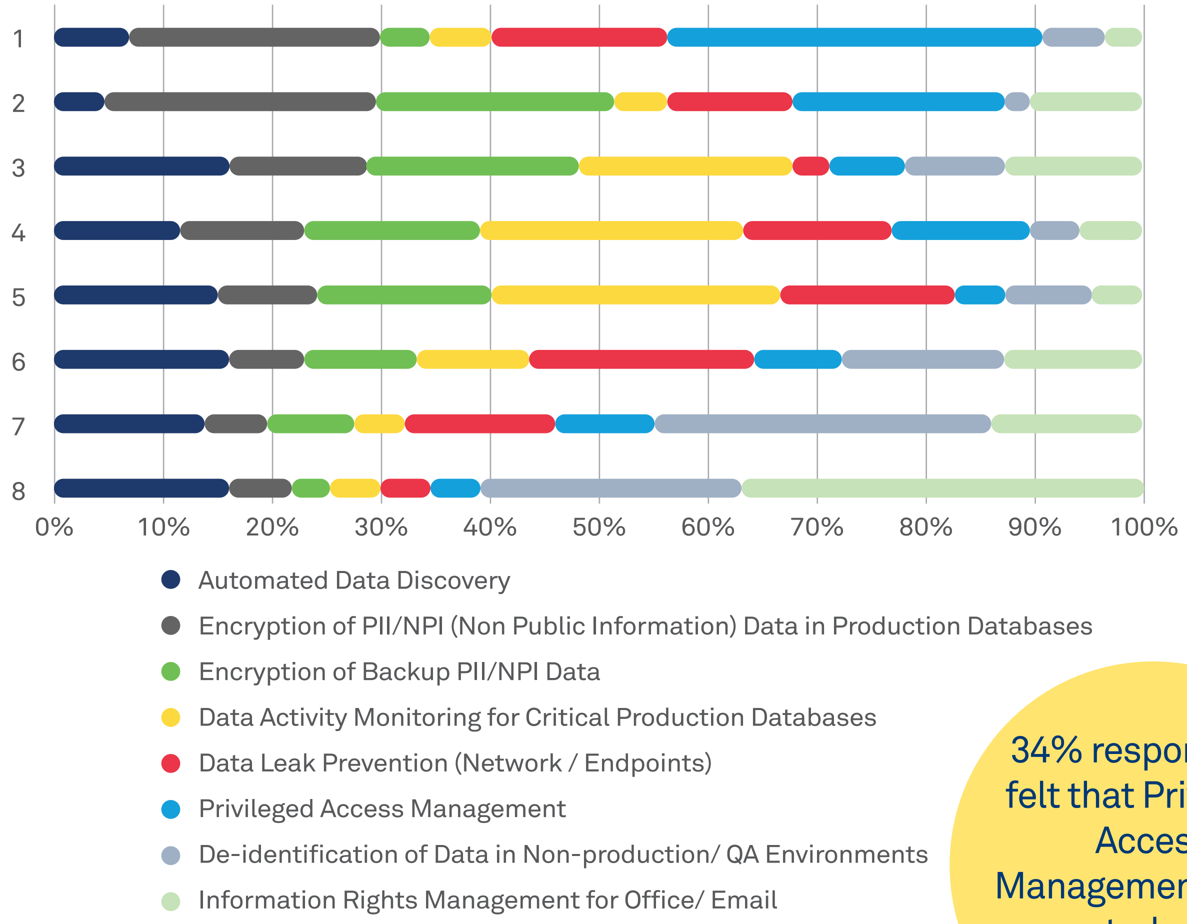


Figure 23 - Data Security Controls Ranked by Effectiveness - 2016

34% respondents felt that Privileged Access Management (PAM) controls gave maximum value

Application security

Application vulnerabilities have overshadowed network vulnerabilities in recent times due to the custom nature of application development. With the rapid expansion of the app store economy, most enterprises are under pressure to develop more applications and launch them quickly to meet specific business needs. The maturity of the processes employed by the enterprise to manage the application security lifecycle, will impact the key metrics around time to detect and fix vulnerabilities which in turn contribute to reduction in risk.

We asked our respondents on standards that are followed by them in the application security domain and an overwhelming 81.3% of them confirmed that they followed OWASP (Figure 24). However, what stood out was the low adoption rate of standards like SAMM and BSIMM that can help improve the maturity of processes related to application security in the software development lifecycles.

81.3% of respondents asserted that they were following the OWASP Standard for Web Application Security

Application security lifecycle management standards have seen low adoption (Microsoft SDL at 15% was the highest) indicating a lower maturity in application risk management

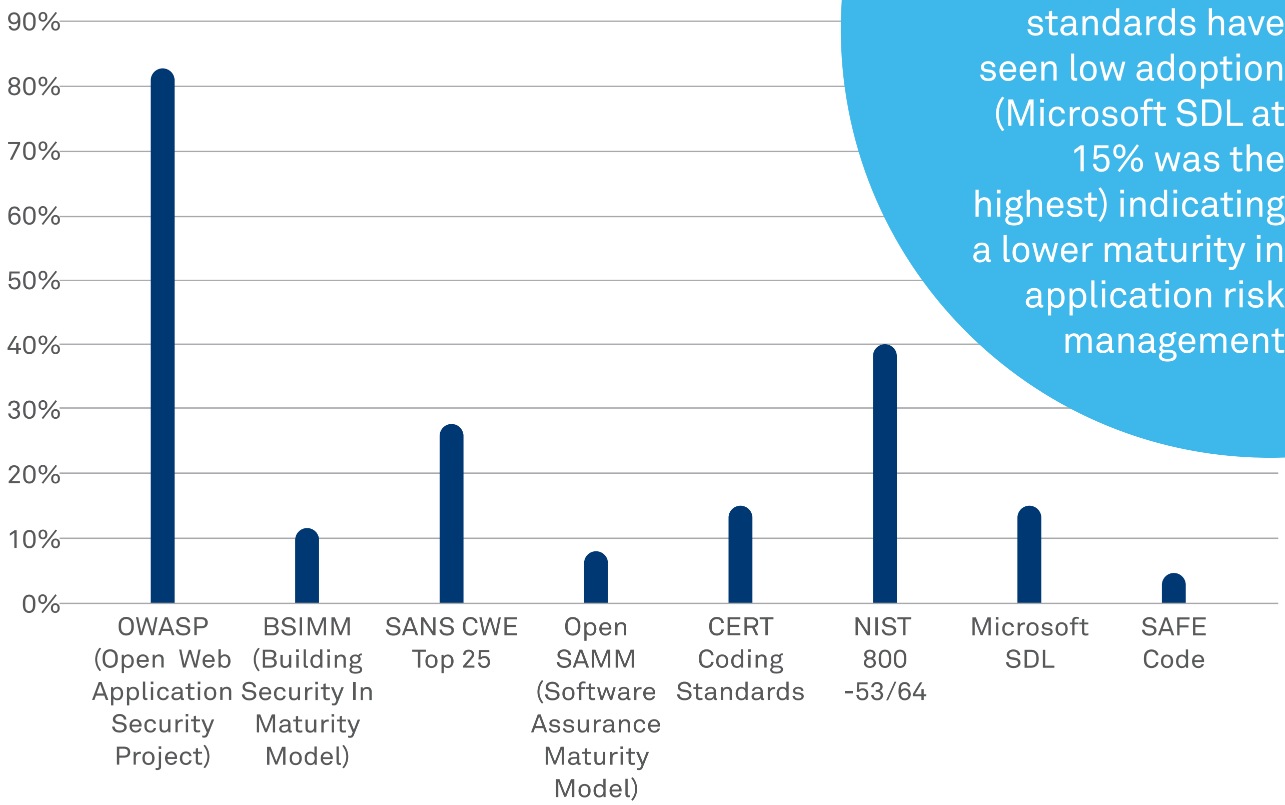


Figure 24 - Application Security Standards Leveraged by Organizations - 2016

When we queried our respondents on the frequency with which they were carrying out application security assessments, 26% said that they were doing it on an annual basis (Figure 25). However, only 20% of the respondents said that they were testing their applications for vulnerabilities in every build.

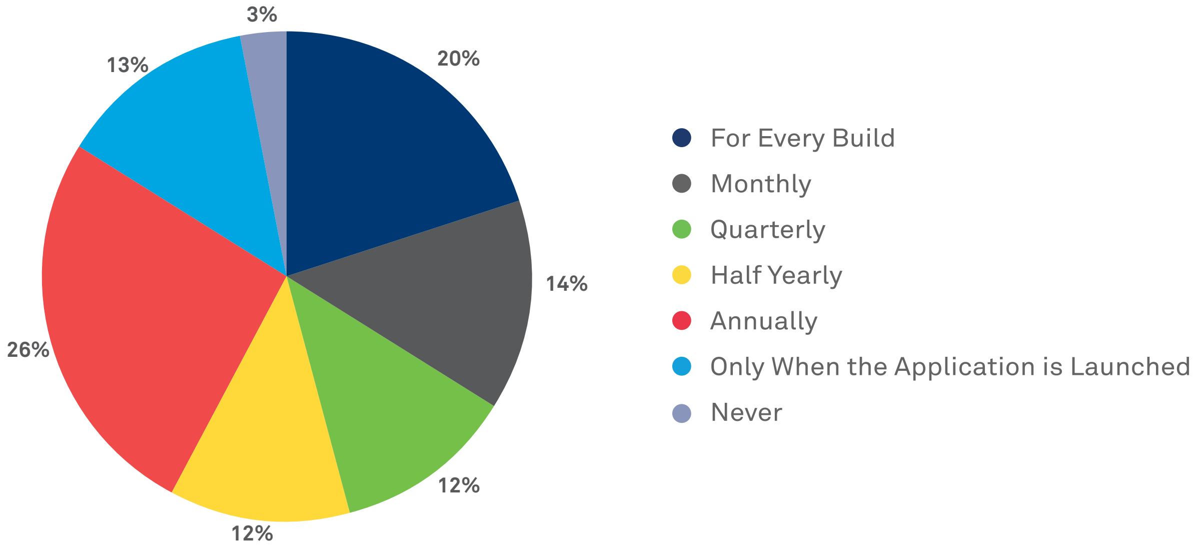


Figure 25 - Frequency of Security Assessments of Business-Critical Applications - 2016

Around 22.6% of the respondents stated that it took them one to three months to fix critical application security vulnerabilities once reported and 21.7% of the respondents said it took them a month (Figure 26). The delay in addressing these vulnerabilities might result in applications going out to production with the business owners accepting the residual risk. The time to fix can only be reduced by inclusion of application security check points early on in the SDLC and making the review and remediation process a part of the organization's IT DNA. Secondly, automation of security reviews in DevOps can lead to faster builds and deployments. But many IT environments continue to use heritage tools and processes to manage configuration management, resulting in error prone and slower deployments.

With increasing migration into virtual private cloud environments and public IaaS providers, organizations have started automating the processes of build and deployment by converting infrastructure into code. Infrastructure-as-code facilitates automated build, configuration and provisioning of infrastructure through scripting to reduce manual effort.

However, this poses a new threat. This new Infrastructure-as-code by itself could contain software vulnerabilities and will need to become an additional focal point for security reviews. The next section shares some insights on this emerging paradigm of infrastructure-as-code and how organizations can minimize vulnerabilities related to them.

Codification of infrastructure – new attack surface

Web application vulnerabilities have continued to dominate the discourse around application security for a decade and will continue to receive paramount attention as long as custom applications are deployed. However, this section attempts to throw some light on application code vulnerabilities that have emerged as a new attack surface due to the codification of infrastructure, particularly in the cloud. Infrastructure-as-code integrates orchestration and provisioning tools, configuration management tools, testing frameworks, etc., to automate almost everything. Orchestration and management tools help build the underlying components to provide support for server instances, on which the configuration management tools like Puppet or Chef manage the configurations, applications, dependencies, etc. With the help of these solutions, one can install

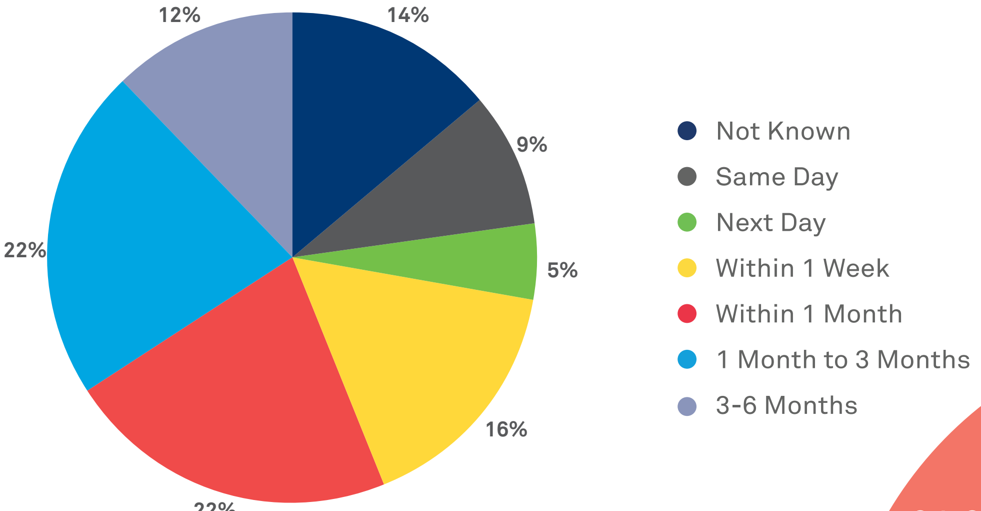


Figure 26 - Time Taken to Fix Critical Application Security Vulnerabilities - 2016

34.8% of respondents said they took at least one month to fix critical application security vulnerabilities scalable server instances, set up databases, define user groups all through custom scripts or code.

Security review of codified infrastructure

Security related testing remains a significant challenge in validation of infrastructure-as-code modules and scripts. Testing can be absurdly slow given that the actual environments will have to be brought up for real time validation. Alternatively, emerging tools can be applied to help review cloud configuration templates codified for different platforms and identify potential misconfigurations and vulnerabilities in them. Such tools can be used to check for rules in the template for security misconfigurations.

Codified infrastructure needs to be viewed like applications and reviewed for vulnerabilities

Network DDoS protection

The year 2016 saw a stepped-up series of Distributed Denial of Service (DDoS) attacks that left many enterprises crippled on the Internet. With new technologies coming to the forefront, it looks like DDoS attacks will become more sophisticated and malicious in the future. A downtime of even a few minutes, as a result of a DDoS attack, can have ripple effects on the enterprise or organization.

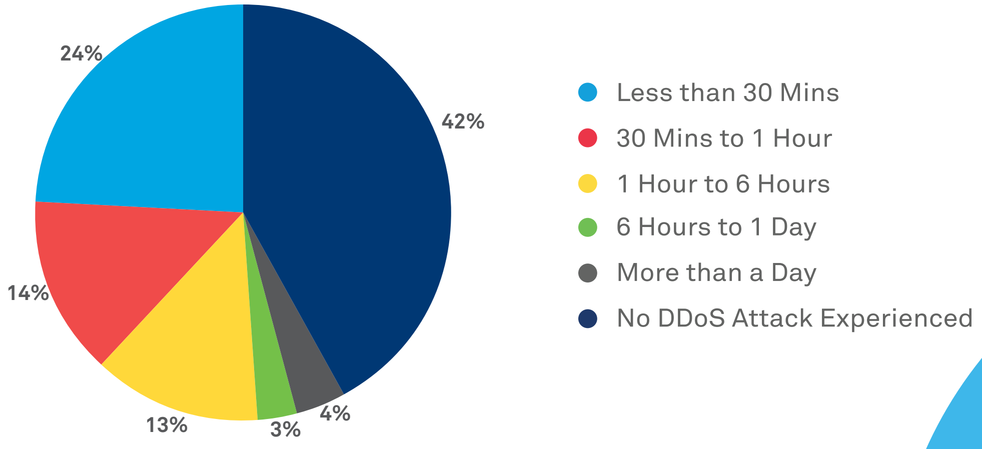


Figure 27 - Peak DDoS Attack Duration Experienced by Enterprises - 2016

While 42.1% of the respondents had not faced a DDoS attack, however, 33.7% of the respondents said they experienced a DDoS attack which lasted more than 30 minutes (Figure 27).

33.7% of the respondents said they experienced a DDoS attack, which lasted more than 30 mins

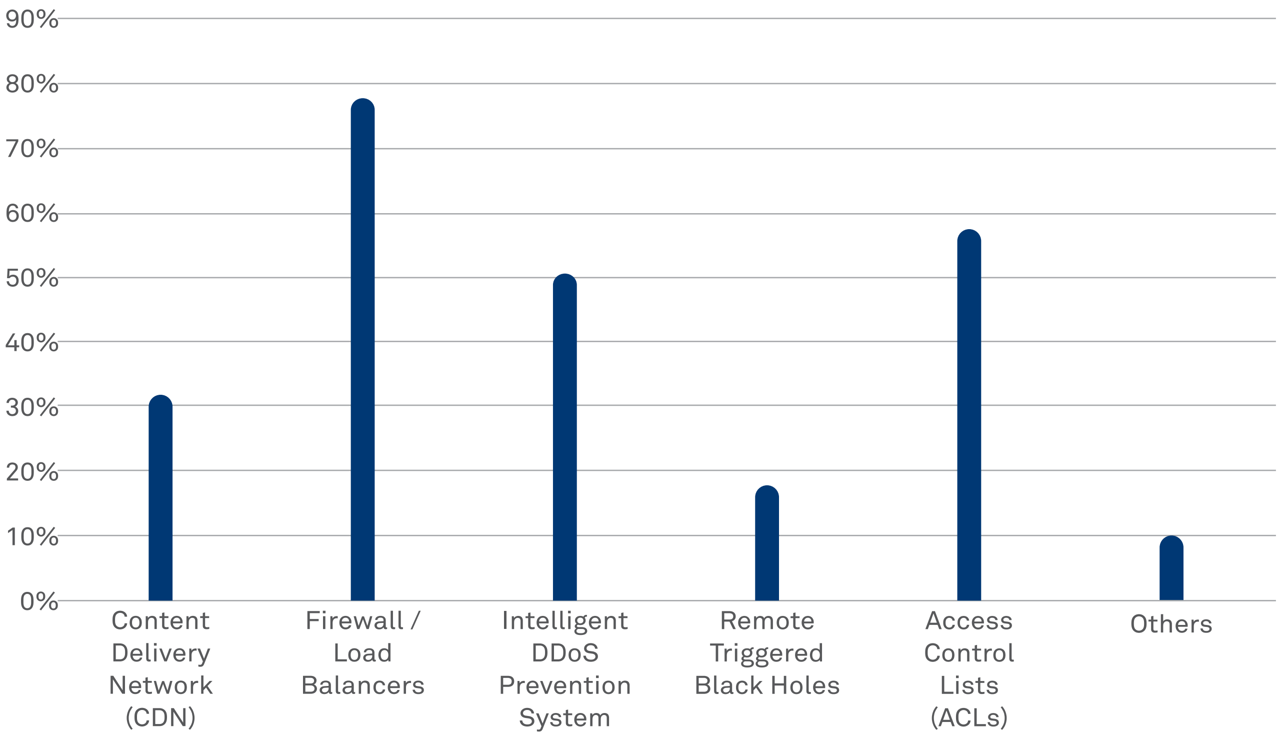


Figure 28 - DDoS Threat Mitigation Techniques Used by Enterprises - 2016

77.2% of the respondents were reliant on traditional network controls like firewalls and load balancers to contain DDoS attacks at a foundational level supplemented by other mechanisms. Intelligent DDoS prevention techniques were used by 50.5% of the respondents (Figure 28).

A couple of years back attacks of the size of 100 GBPS were considered huge, but now have become common-place. The size of DDoS attacks have now reached an enormous 990 GBPS. Some of the biggest DDoS attacks in 2016 were:

Date	Victim	Industry	Attack size (in GBPS)	Duration	Attack type
Jun 7, 2016	MIT	Education	295	1 day	Combination of DNS reflection, SYN flood, UDP fragment, PUSH flood, TCP flood, and UDP flood
Jun 14, 2016	Chinese Gambling Company	Entertainment	470	4 hours	Complex nine vector. SYN payloads, generic TCP and UDP data packets

Attackers identify weak IoT devices in the network and infect them with malwares to take control of other devices in the network

Date	Victim	Industry	Attack Size (in GBPS)	Duration	Attack Type
Jul 18-23, 2016	ISPs in Mumbai	IT	200	4-5 days	Millions of virus-hit IP addresses
Aug, 2016	Rio Olympics	Entertainment	540	1 day	The targeted takedown included DNS chargen, SSDP, flooding attacks like SYN, UDP and also attacks in the application layer
Sept 25, 2016	OVH.com- French web hosting company	IT	990	48 hours	Targeted by various types of traffic like TCP data packets, SYN flood, including Generic Routing Encapsulation (GRE) traffic
Sept 25, 2016	KrebsOn Security.com	Web Content	620	NA	No amplification or reflection techniques but garbage SYN, GET and POST floods
Nov 3, 2016	Telecom operators in Liberia	Telecom	500+	Very short duration	DNS flood

Use of IoT devices as launch pads in DDoS attacks

Year 2016 saw the use of IoT devices in DDoS attacks for the first time on a large scale. In October 2015, surveillance cameras in shopping malls were targeted to form a large botnet, to cripple large websites, by launching DDoS attacks. With connected devices, attackers can have complete access to the Internet without any bandwidth limits. Without even using any amplification technique, the wide range of such devices can generate large amounts of network traffic. IoT devices like routers, modems, NAS devices, CCTV systems, ICS systems, typically run on Linux based operating systems. IoT devices are mainly vulnerable because of improper patching, insecure exploitable codes, weak or default passwords, insecure SSH and telnet support with which to install malware and unencrypted traffic between the device and its control service. Smart devices such as home routers, CCTV cameras etc. have default user name and passwords, which were widely available on the Internet. Only a few customers change them after installation and such devices are hardly ever patched during their lifetime.

Endpoint security

The previous section explored the culpability of the accidental user in social engineering attacks. This section explores the endpoint systems as the vector that hackers target to gain entry into enterprise networks. Most acts of the users succumbing to technical social engineering attacks are perpetuated on the endpoint systems. When we asked our respondents what they thought were the most common vectors leading to compromise of endpoints, phishing emails topped the list with 59.2% (Figure 29).

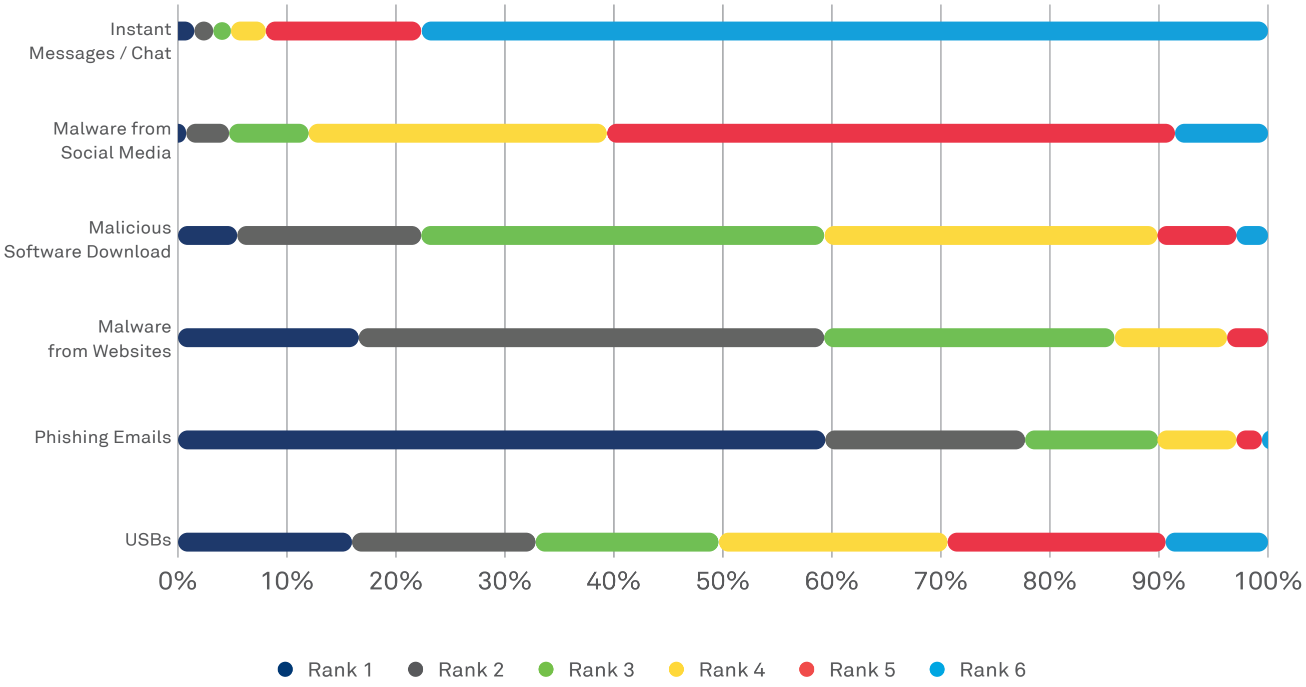


Figure 29 - Ranking Vectors Leading to Compromise of Endpoints - 2016

Phishing emails still remain the primary vector leading to endpoint compromise

When we asked the respondents on techniques they applied to restore compromised endpoints, 84.9% confirmed that wipe and reimage was the most popular approach (Figure 30). Endpoints continue to be a source of concern for enterprises. But with the emergence of newer advanced threat detection tools of malware detection, there is hope for one of the weakest links in the chain.

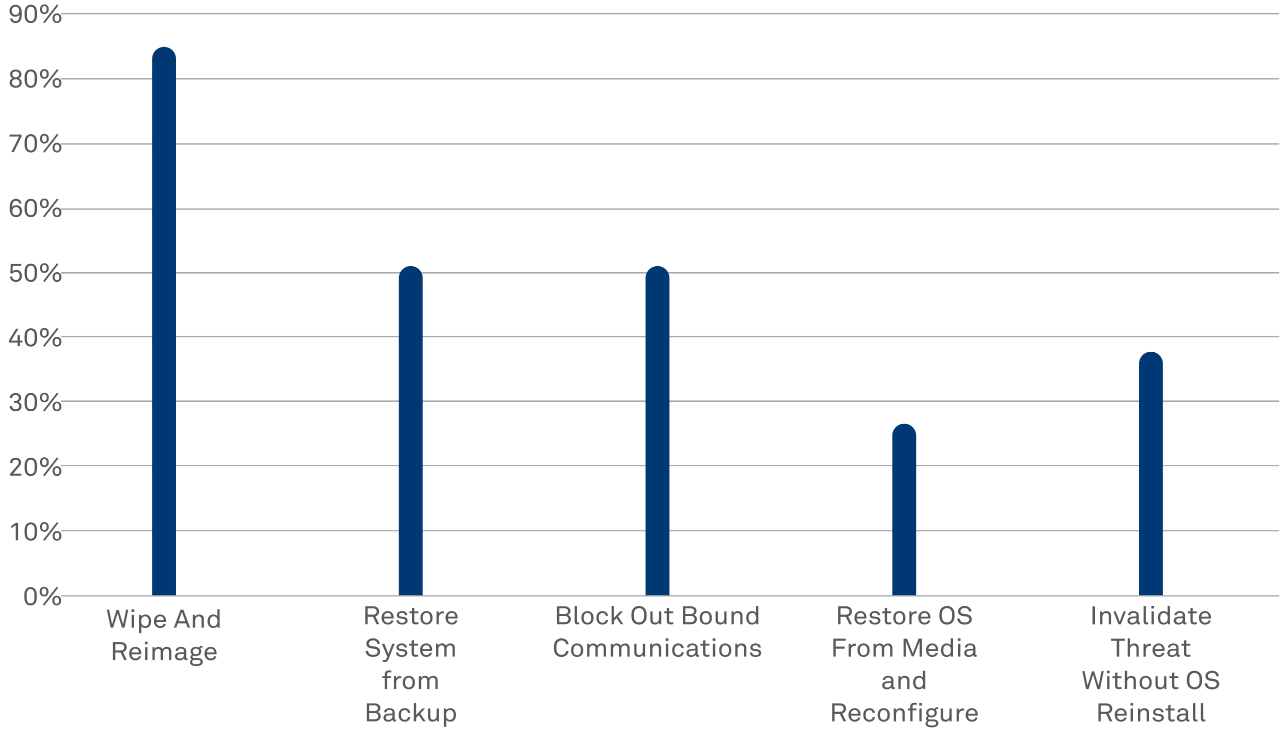
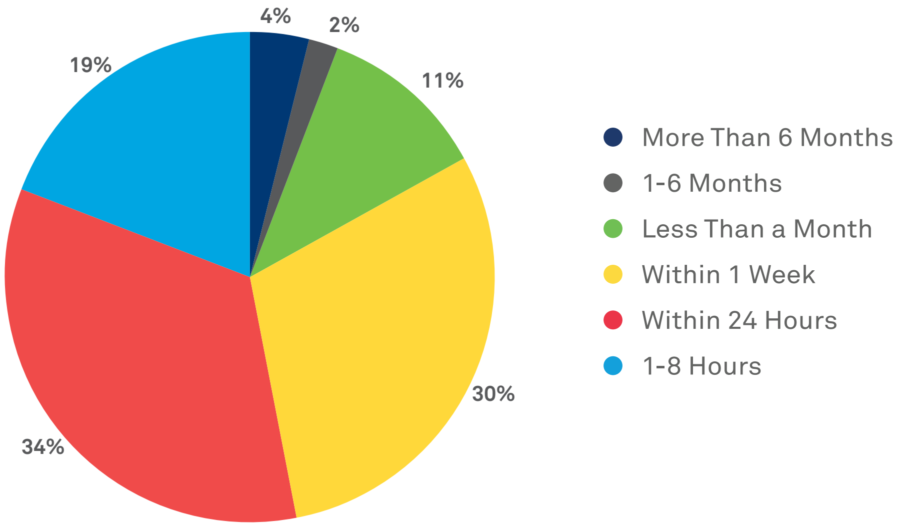


Figure 30 - Techniques Applied by Enterprises to Remediate or Restore Compromised Endpoints - 2016

Security monitoring and analytics

We have consistently seen that businesses aren't just quick enough in identifying threats and mitigating the danger in time, particularly when the attacker has compromised the network and has been hiding tracks for an extended period. Security analytics as a discipline aspires to reduce the dwell time as much as possible. We asked companies how long it took them to contain and recover from an attack and 83% responded that they were able to contain most attacks within a week (Figure 31). More than half of them were getting it under control within a day. 'Threat response' isn't the main problem for an organization, but 'threat detection' is and will be for a long time to come.



81% of the respondents say that security events are notified through SIEM

Figure 31 - Time Taken to Contain and Recover from Cyber-attacks - 2016

We took a look at the spectrum of toolsets that are usually available at the disposal of the SOC team and asked our respondents on their effectiveness in notification of attacks. We see that most of them have their security events notified through basic perimeter defense tools like Firewall, IDS and IPS and also the SIEM. 81% of the respondents said that they got their security event notifications through the SIEM (Figure 32).

We asked the companies what capabilities could help them improve their threat detection capability. At 81.3% improving threat intelligence was the most popular response (Figure 33). As the risk of the unknown-unknowns keeps on increasing, threat intelligence will play an even more important role to track changing landscapes and the associated risks. Collaborating with peer and public groups, and using the in-house data along with them, one can construct in-depth threat profiles. Improving triage process was the next most popular choice for 64.5% of the respondents. The amount of security event data being analyzed these days has seen an exponential rise. Thus, the need for sifting through real time raw data and finding the most important events to focus on has become even more critical for successful outcomes.

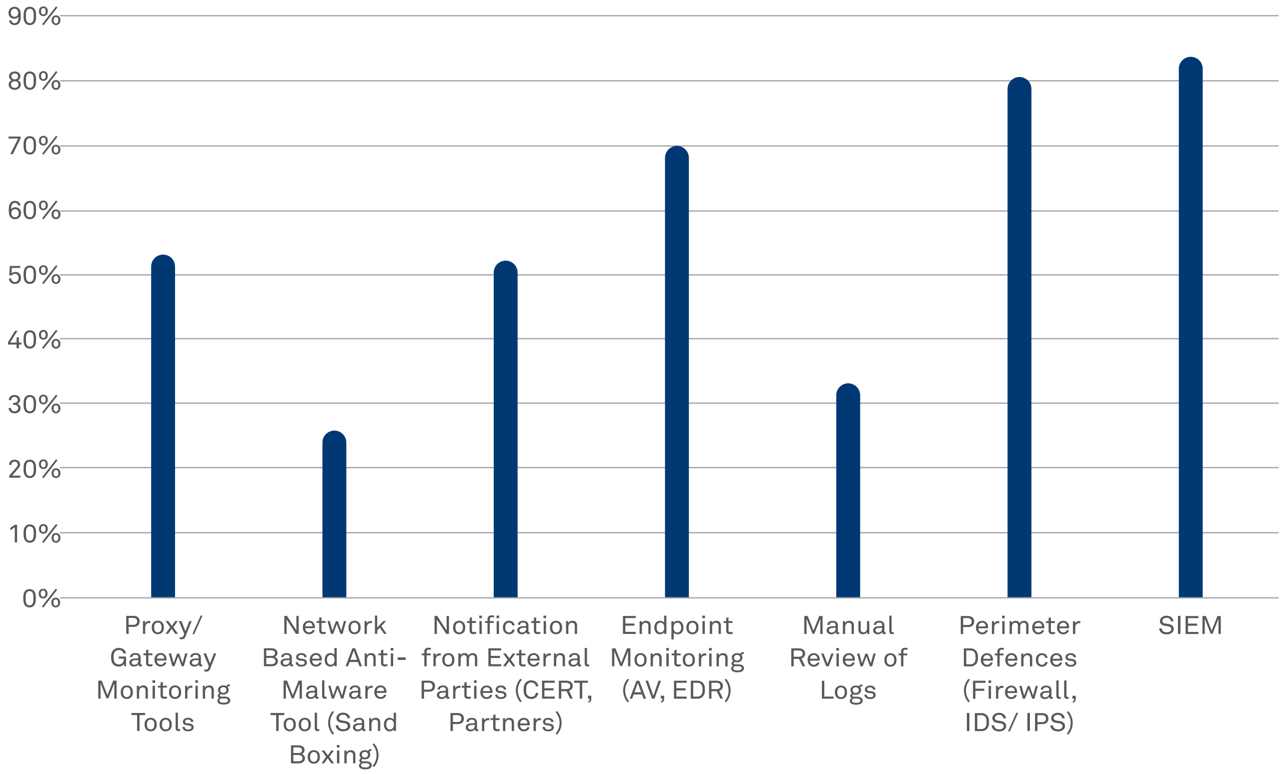


Figure 32 - Toolsets Contributing to Security Event Notifications - 2016

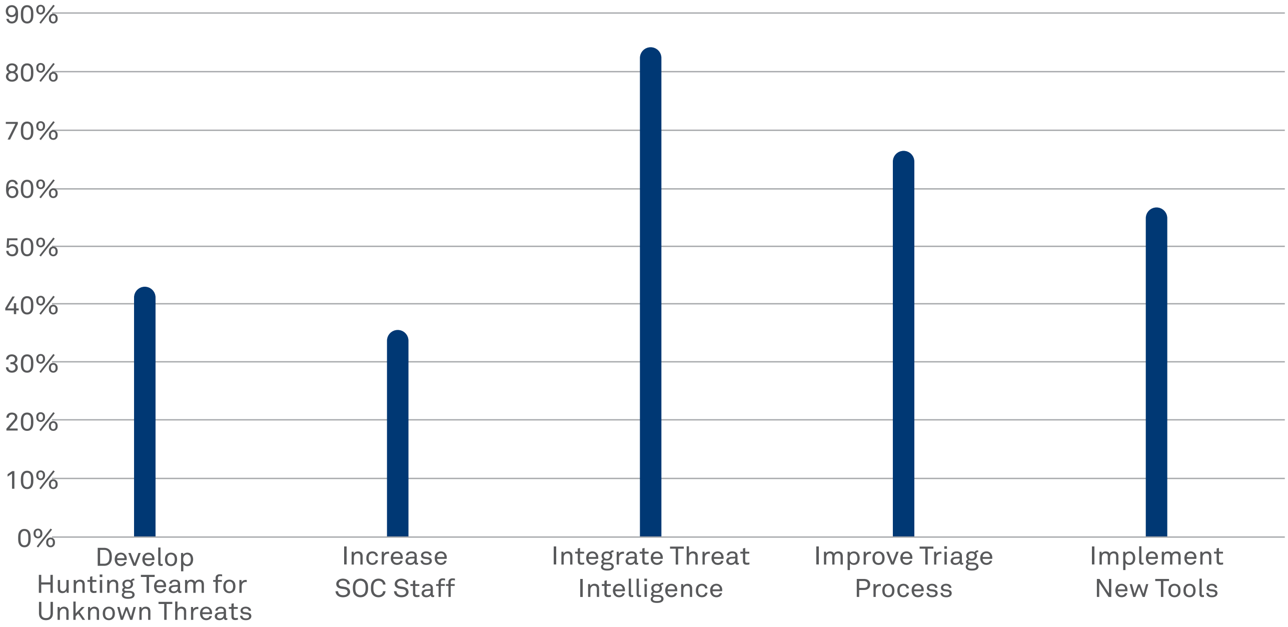


Figure 33 - Opportunities Organizations see in Improving Threat Detection and Containment Time - 2016

A big question looming over the CISOs is whether they have the best security controls in place. With the attackers getting stronger with each passing day and the attacks getting sophisticated, traditional systems find it hard to contain them. Enterprises are deploying new tools to stay up-to-date with the most complex of attacks. With the changes that cybersecurity landscape is experiencing, SIEMs appear to be one step behind in the race. Traditional SIEMs are now being steadily supplemented by the use and reliance on independent SOC driven security analytics in this fast-paced environment.

We asked our respondents on the most useful security analytics use-cases that they are building or have built. Most enterprises are using security analytics capabilities to help detect insider threats and external malware threats. It is also playing a major role in finding unknown threats (Figure 34).

64.5% respondents believe triage processes can be improved to detect threats

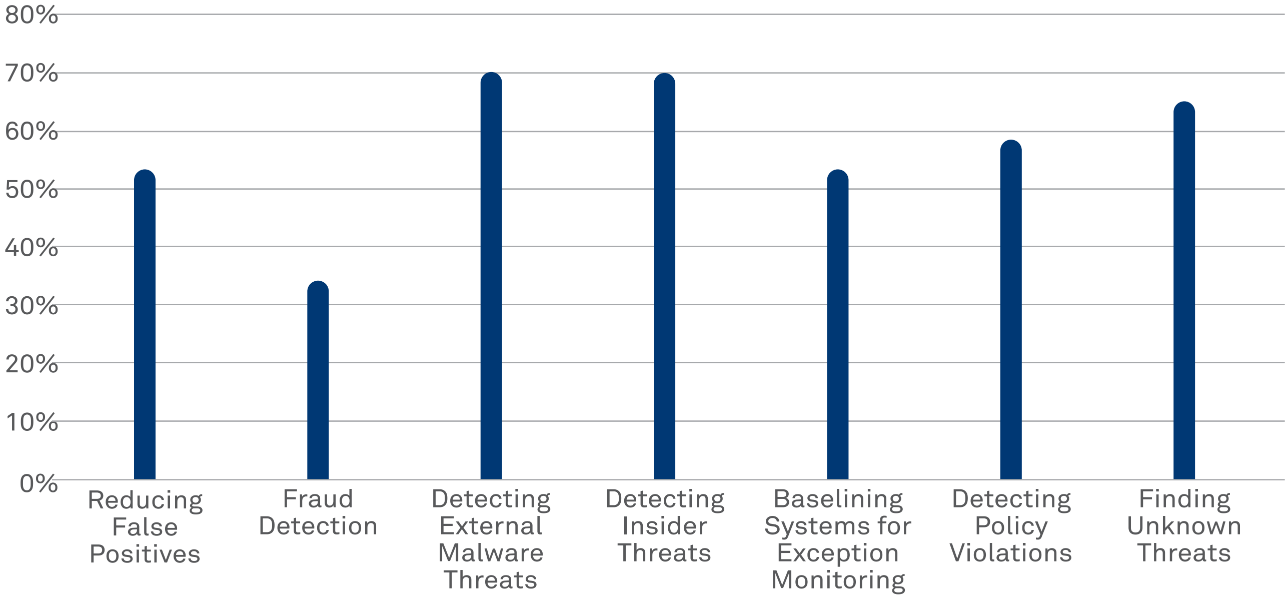


Figure 34 - Most Useful Security Analytics Use Cases - 2016

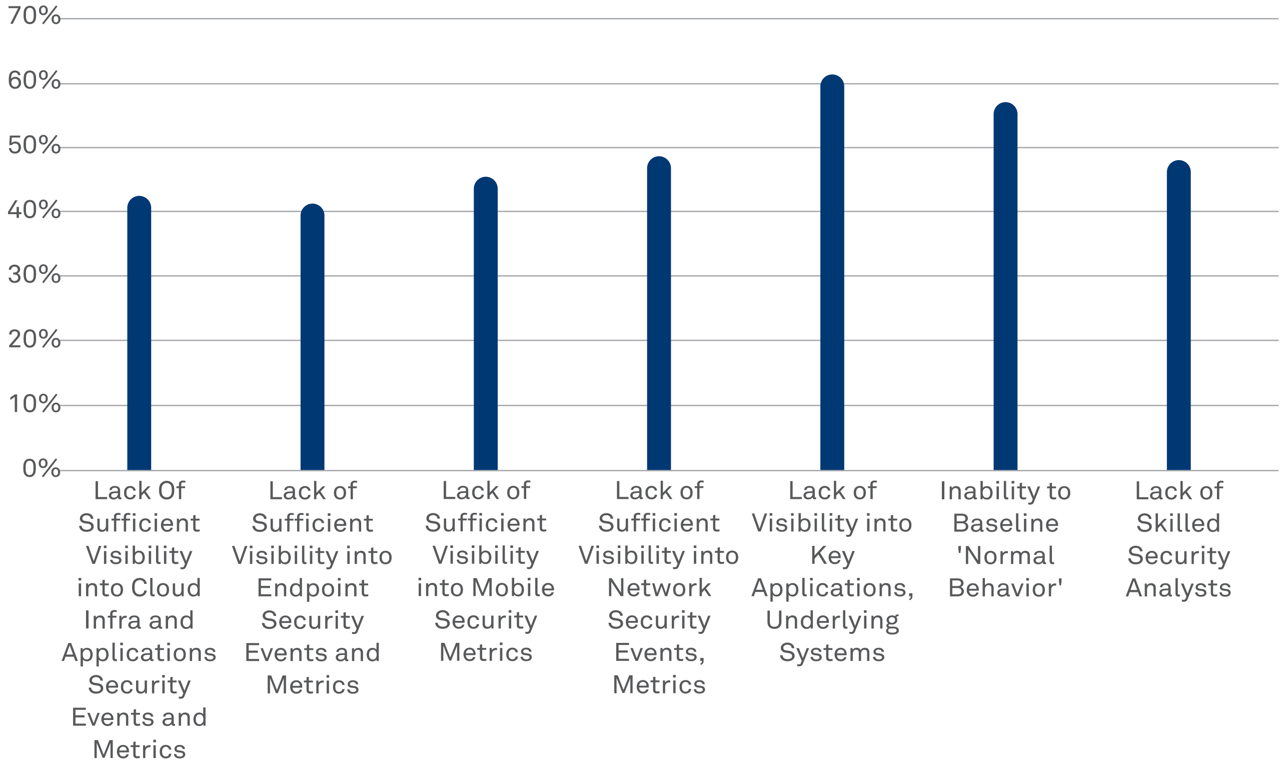


Figure 35 - Key Impediments to Attack Detection - 2016

Effective use of security analytics to reduce the dwell time for persistent threats can help detect attacks faster and reduce the risk and consequential damage to an enterprise's cyber infrastructure.

Cloud security

Cloud migration programs have grabbed the multi-functional attention of the CIO, CISO and Risk & Compliance teams across enterprise IT in recent times due to regulatory, business continuity and cyber

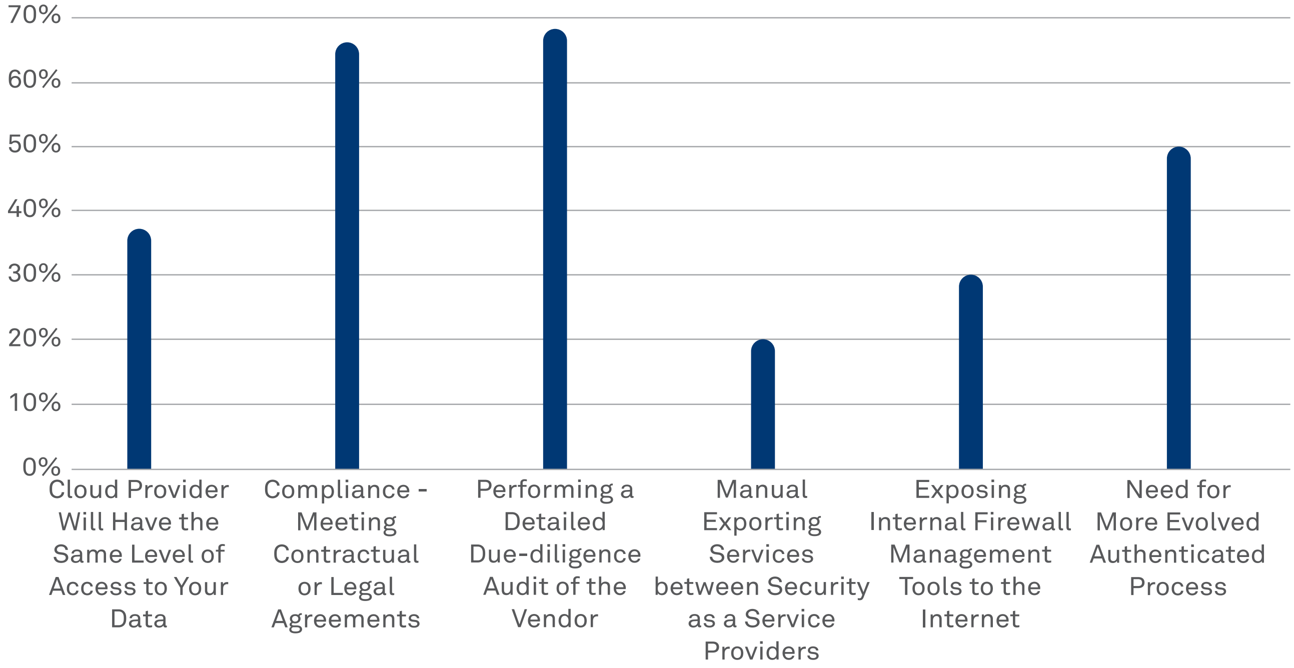


Figure 36 - Major Challenges/ Risks of Deploying Cloud-Based Services - 2016

risks that are involved. Cloud adoption across both infrastructure (IaaS) and applications (SaaS) has been on the rise. When we asked our respondents what they thought were the major risks of deploying cloud-based services, 64.1% felt that meeting contractual and legal obligations was a major challenge. 66.3% responded that performing a detailed due-diligence audit of the vendor was a challenge as well (Figure 36).

64% of respondents said meeting compliance and legal obligations were hurdles towards moving data to cloud

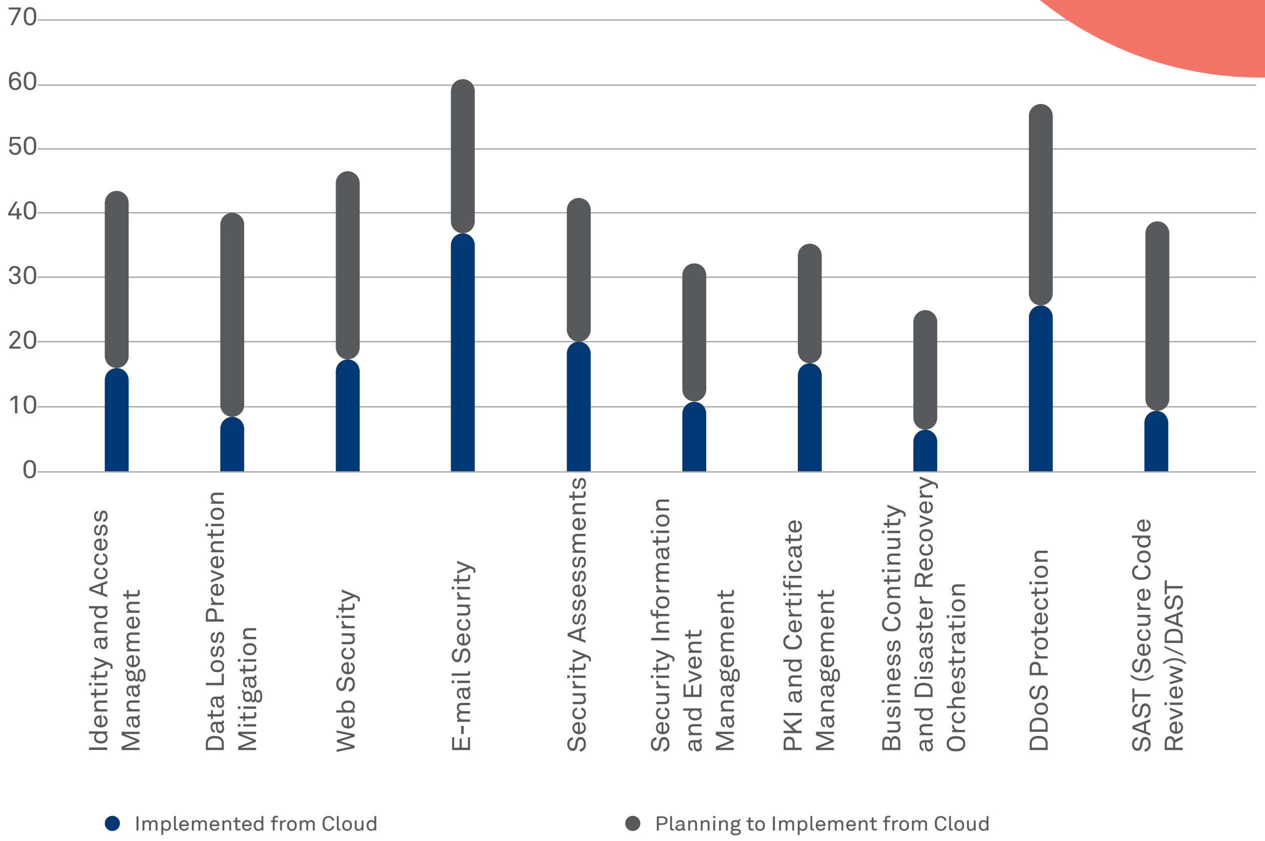


Figure 37 - Security Controls that Enterprises are Implementing / Planning to Implement from Cloud - 2016

When the respondents were asked about what types of security services they were planning to consume using SaaS-based cloud service, Data Leakage Prevention seemed the most obvious choice. For organizations that have security-from-the-cloud, most respondents had embraced Email security.

The biggest challenge about meeting compliance requirements on the cloud was around the loss of control of data once it was moved to the cloud. While encryption has been touted as the panacea for protecting data on the cloud, the dilemma facing many organizations has been the storage and management of encryption keys. Keeping the encryption keys in the cloud defeats the purpose particularly when the system admins of the cloud environment could get access to the key. However, the cloud IaaS providers have been inching forward to offer capability to the enterprise to encrypt the data in the cloud but maintain local control of the keys. Some of the solutions doing the rounds in this context include:

1. BYOK (Bring Your Own key)
2. CASB (Cloud Access Security Broker)
3. HYOK (Hold Your Own Key)

We have listed only three solutions considering various factors like adoption rate, potential, buzz generated, etc.

BYOK (Bring Your Own Key)

BYOK is appropriate for businesses that are regulated and need complying with HIPPA, PCI DSS, and other regulations. With the regulations preventing unauthorized data disclosure and compliance with data residency and privacy mandates, this provides a way in which the data provided to the Cloud Service Provider (CSP) is controlled tightly.

Under this security model, the owner/manager of the encryption keys is the customer/enterprise, and not the Cloud Service Provider (CSP). It limits access to the keys from the cloud service provider. The enterprise in combination with the cloud service provider is responsible for key management, encryption, vaulting or other software and hardware to allow encryption functionality. In other words, when any data leaves an enterprise's virtual machine and is written to storage in cloud, the data is encrypted and administrators in the cloud have no visibility to the data.

BYOK is also of great advantage when CSPs are legally forced to share the customers' data without the customers' consent. Furthermore, it helps an enterprise to enforce spoliation, in case it wants to change the cloud service provider. Now-a-days many CSPs and third party vendors are offering access management (helps organizations enforce geographic restrictions on data) and logging tools or other key brokering capabilities as a part of their offering while supporting BYOK. Even the enterprise tenant key can be replicated across a controlled set of Hardware Security Modules (HSM), for scale and disaster recovery (within region or instance), without the pain of exporting it via CSPs.

CASB (Cloud Access Security Broker)

When it comes to migrating to the cloud, one key concern for the CISO is regarding the visibility part of the scenario. Visibility is a major challenge once the data moves to the cloud. Hence, this concern directs a CISO to further questions on security and compliance. The CASB not only answers the questions regarding visibility, it also helps in compliance, data security and threat prevention.

Of these four factors, a CASB using encryption/tokenization controls helps in enforcing data-centric security policies at both the field level and file level. Primarily, there are two modes in which a CASB can be operated when it comes to encryption/tokenization: Proxy vs API. The proxy approach can be further classified into two types: forward proxy and reverse proxy. Though these two approaches have their own share of benefits, there are a few limitations as well. The limitation for reverse proxy approach is that it does not support all endpoint applications. In forward proxy, the limitation is that it invades user privacy. A common limitation is the impact on network performance. An API approach however moves the encryption engine to the CSP but with end users having control over the keys.

Apart from the encryption capabilities explained above, a CASB helps in application discovery (to counter shadow IT problems), data control (on sanctioned apps via API based integration) and threat protection (through behavioral analytics, etc.).

HYOK (Hold Your Own Key)

HYOK allows an organization to keep its own encryption keys. The encryption and decryption work is done on premise. Microsoft Azure provides HYOK service, which enables its customers to own keys for SharePoint Online, and is soon planning to roll out the service for Exchange Online as well.

The downside of this is the huge maintenance cost of handling the encryption infrastructure on premise. The data is inaccessible once the key is lost. Presently, the offerings that could complement HYOK to make it a wholesome solution are still not very clear. However, HYOK can be seen as disruptive in the way it handles keys and provides an

HYOK can be seen as disruptive to handle keys in cloud deployments innovative way for businesses to take ownership of the data.

In short, the secure export and encrypted storage of data to the cloud with enterprise control of the keys is beginning to be enabled by different CSPs.

Customers should look at movement of core apps and data using this underlying encryption capability with utmost caution.

Mobile security

Enterprises have been trying to minimize risks related to data loss from smart devices. With the advent of BYOD (Bring Your Own Device) as a policy imperative in organizations, keeping track of the flow of critical data has been challenging. We asked respondents about the measures they have adopted to prevent loss of data from mobile devices and we got the following response from them - 84% of the respondents said they use remote wipe to protect data in case of a loss. This is basically deleting data remotely from lost or stolen devices. While it can be effective in taking immediate action, remote wipe can cause privacy concerns by putting the user's personal data at risk.

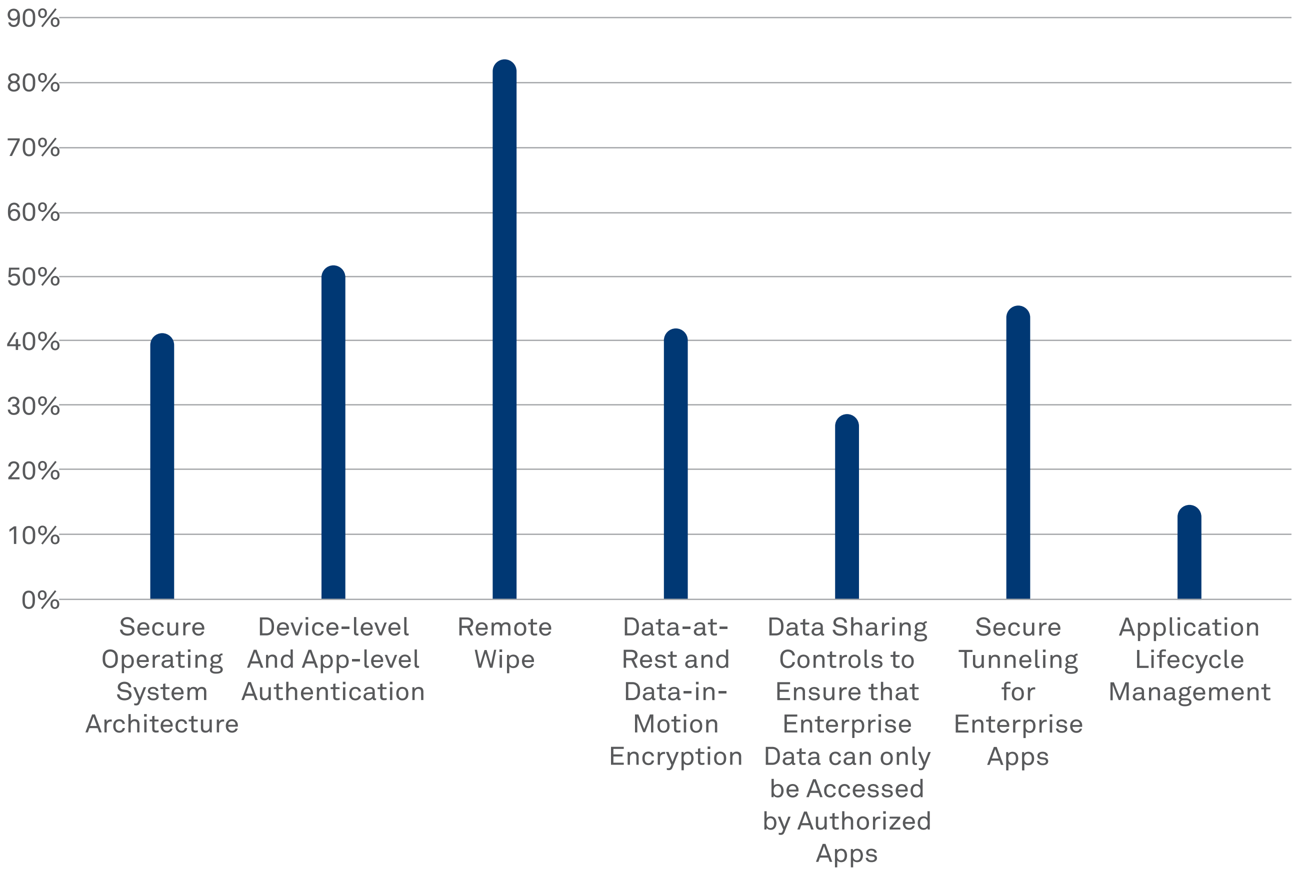


Figure 38 - Measures to Prevent Loss of Data Through Mobile - 2016

52% of the respondents believe in effectiveness of device and app level authentication to protect data from unauthorized access (Figure 38). Data encryption needs to complement this measure. Encrypting data at rest and in motion is the best safeguard against unauthorized access and man-in-the-middle attacks while allowing users easy access to their data.

45% of the respondents indicated that secure tunneling is a viable option for protecting data. Application tunneling is being leveraged using data containerization and Mobile Content Management to separate the enterprise data flowing through a secure channel and personal data flowing through some unsecured network.

Data sharing controls which restrict opening, forwarding, copying, pasting and printing certain types of content are an important complementary control. Other measures include secure operating infrastructure which isolates application data into separate containers to limit the damage of data and application life cycle management that helps prevent rogue apps from being downloaded and blacklists/whitelists unauthorized apps on a device.

83.5% of the respondents say that they use remote wipe to prevent loss of data through mobile

In conclusion when it comes to mobile security, enterprises need to strengthen their internal controls around content protection over external controls like remote wipe, etc.

State of collaboration

In today's world, advanced knowledge of threats can be a force multiplier for organizations trying to deal with impending attacks. The type of threats faced by enterprises in the same vertical or geography often tend to have commonalities associated with them. Sharing of such threat information or actual attack and forensic information with industry peers can help organizations learn from each other and improve their preparedness to face new cyber-attacks. This section explores enterprise thinking related to collaboration with the industry ecosystem such as peers, regulators, CERTs and how to make the most of the information that can be obtained through this network.

Threat intelligence

Gathering of threat intelligence is a complex exercise and organizations often rely on external sources for this. However, many organizations with a mature cyber capability build their own threat intelligence as well. We asked the respondents on how they were gathering intelligence and 67.7% said they were dependent on partner threat intelligence feeds (Figure 39).

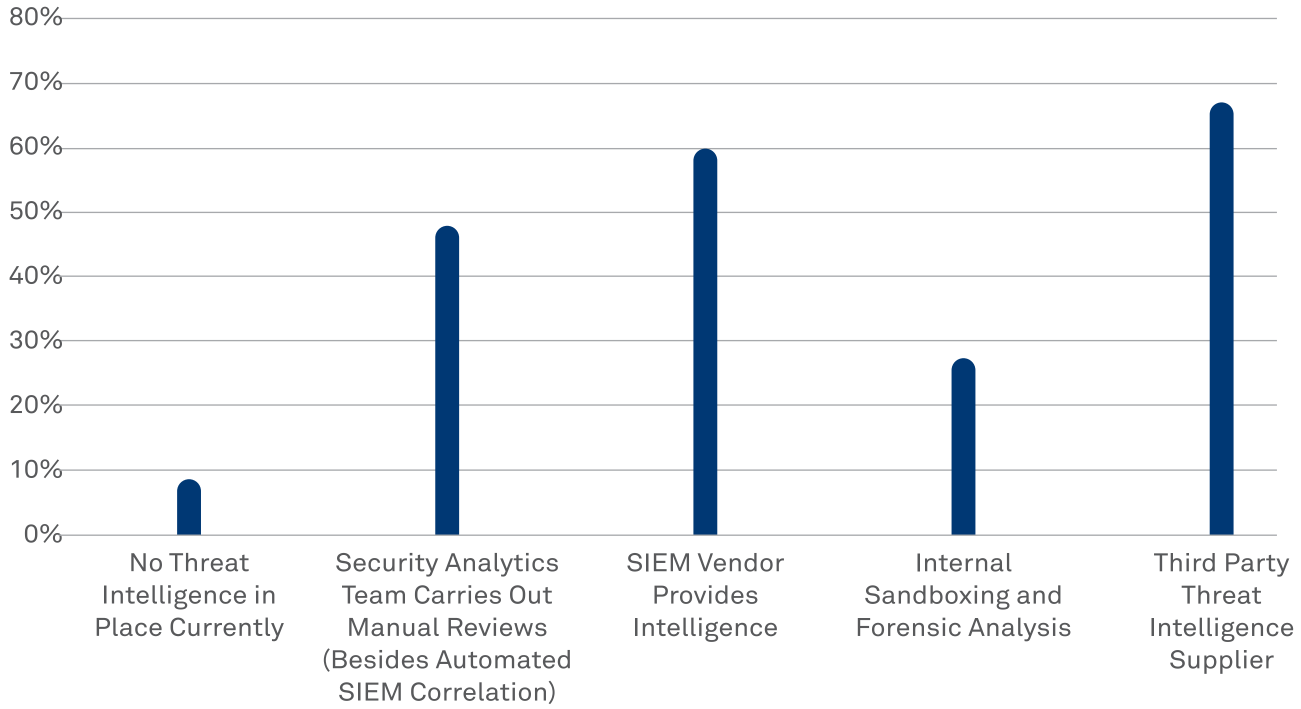


Figure 39 - How Threat Intelligence is Gathered and Reviewed - 2016

67.7% of the respondents said that they were dependent on an external TI partner for intelligence feeds

Cyber attack simulations

Many organizations have been carrying out periodic vulnerability assessments or penetration testing of the infrastructure and applications to identify weaknesses that they need to address. However, cyber-attacks are often multi-faceted. When coordinated by a well-equipped and informed adversary, they can involve social engineering followed by attacks on dependent infrastructure (such as telecom providers etc.). Nowadays, many national agencies are chartered to work with such providers to simulate coordinated large scale cyber-attacks. Participating in such simulations can help enhance the preparedness of organizations. We asked our respondents on their participation in cyber-attack simulation exercises and 30.6% said that they have never participated in external simulation exercises conducted by the regulatory or CERT bodies within their national or geographical context. 24.7% of the respondents had participated in exercises conducted by national CERT or CSIRT organizations (Figure 40).

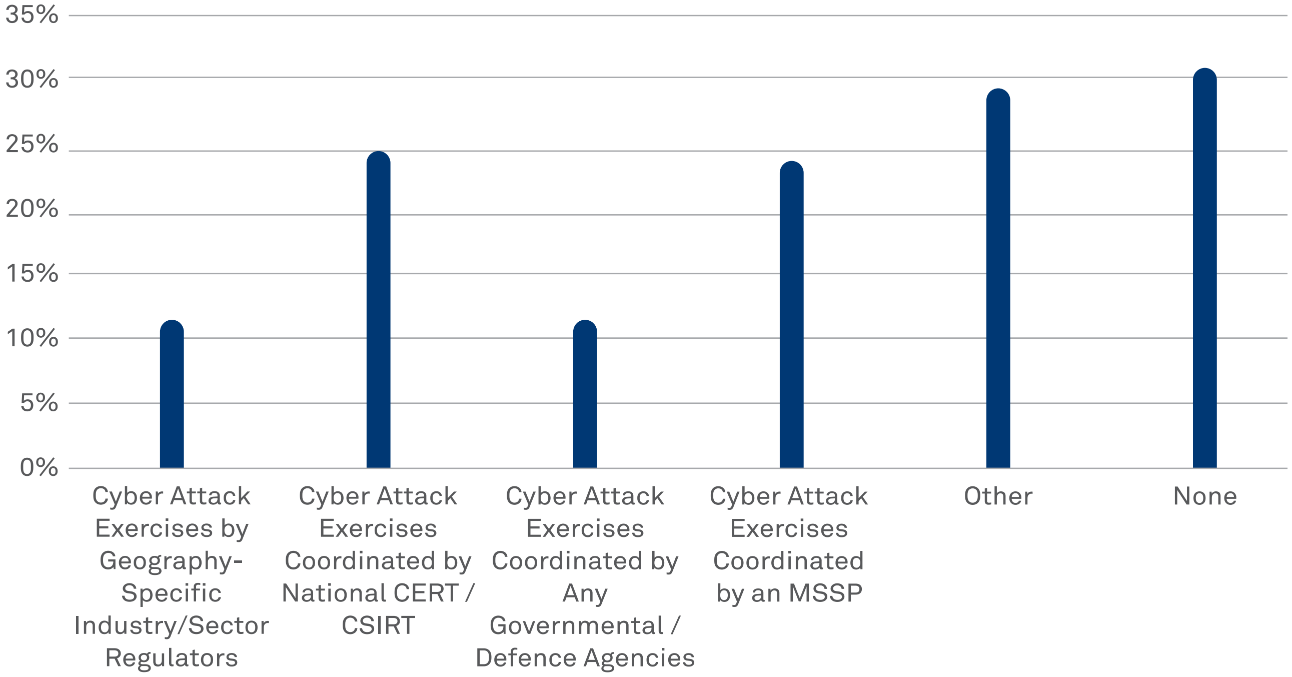


Figure 40 - Types of Coordinated Cyber-Attack Preparedness Simulation Exercises Participation in-2016

30.6% of organizations had never participated in any cyber-attack simulation exercises by external bodies

Information sharing

The more we share, the more we have

In the market place businesses compete fiercely but in so far as cybersecurity is concerned, they inherently face the same kind of risks that their peers face. While collaborating with a competitor is mostly a taboo subject, over the years with prodding from governments, organizations who provide services and have national critical infrastructure have begun to realize the value of sharing intelligence between peer groups. We asked our respondents about the biggest barrier they faced towards information sharing and 53.8% of them affirmed that perceived fear of reputational risks kept them away from sharing information (Figure 41).

53.8% of the respondents said they are reluctant to share intelligence with sharing groups due to reputational risks

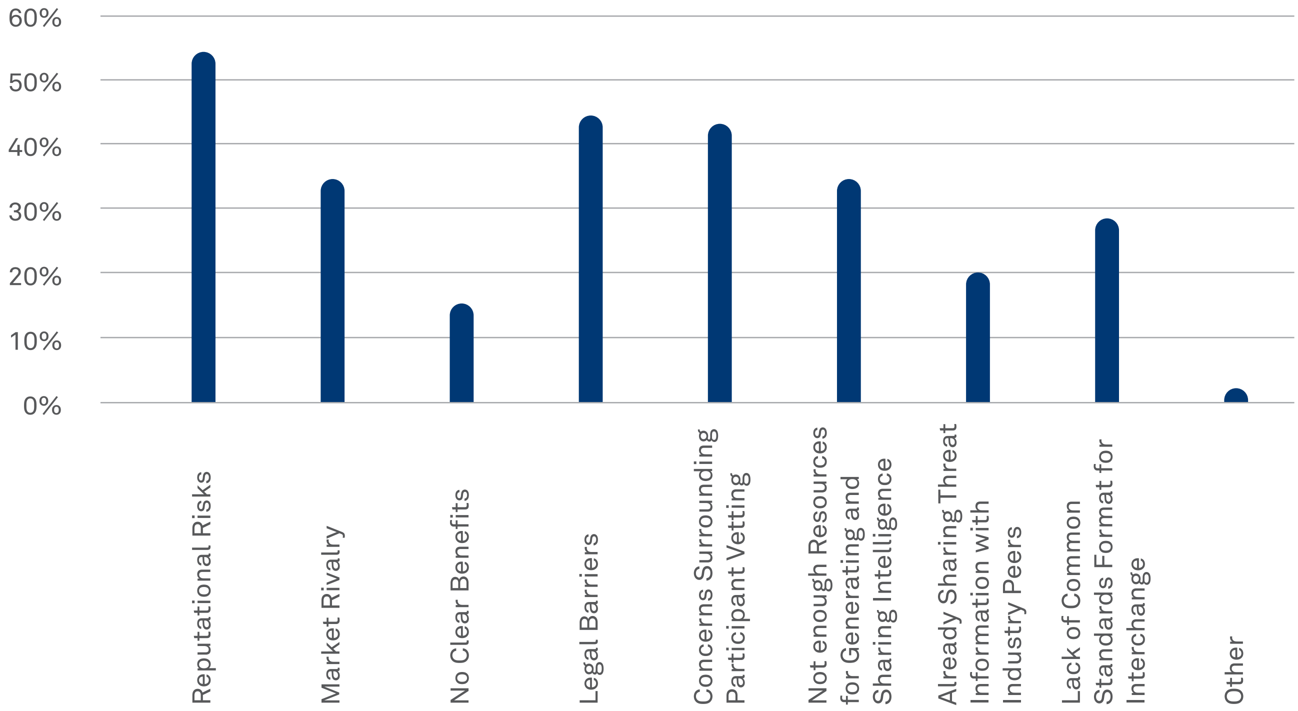


Figure 41 - Reasons Organizations are Reluctant to Participate in Information Sharing Groups - 2016

What are you willing to share?

We asked our respondents on the type of threat information they are willing to share with industry peers through common forums and more than 80% of them were willing to share Malware URLs, Blacklisted IPs and Phishing email addresses with their peers, provided they had the organizational mandate for the same (Figure 42).

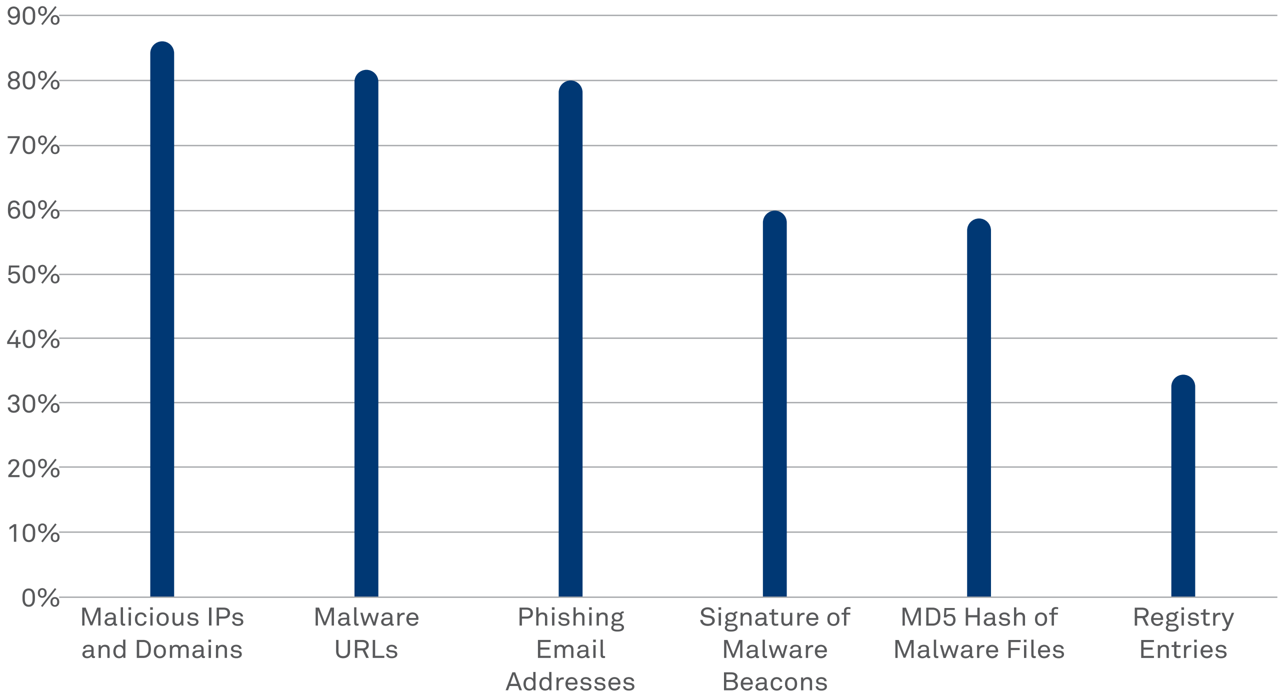


Figure 42 - Threat Information Companies are Willing to Share with Peers - 2016

80% of the respondents were willing to share Malware URLs, Blacklisted IPs and Phishing email addresses with their peers, with an organizational mandate in place

Future of cybersecurity

The previous sections of the report have explored the breaches of 2016, changes in the regulatory landscape, state of defenses that organizations are putting up and how enterprises are moving towards collaboration in cybersecurity. This section looks at the future of cybersecurity and analyzes some trends that our CoE identified as interesting trends to follow. The section examines the role of Cyber Insurance as a risk transfer mechanism, the emergence of drones and their cybersecurity risks, IoT and the need for security in emerging use cases and Persistent Identity as a unifying layer that will potentially bring all these things together. Finally, this section also analyzes the shortage of skills in the cybersecurity industry and how the future analyst will need to evolve to meet the needs of the industry.

Cyber insurance

Cyber Insurance is emerging as a viable supplement to traditional risk mitigation measures adopted by the enterprise for self-protection and decreasing risk. Issues like the lack of actuarial data, short history of claims, lack of common framework for pricing, less coverage etc. have impeded the growth and large scale adoption of Cyber Insurance. Apart from low awareness among organizations, many are skeptical about the extent of coverage that Cyber Insurance provides.

52.3% of the respondents have no Cyber Insurance

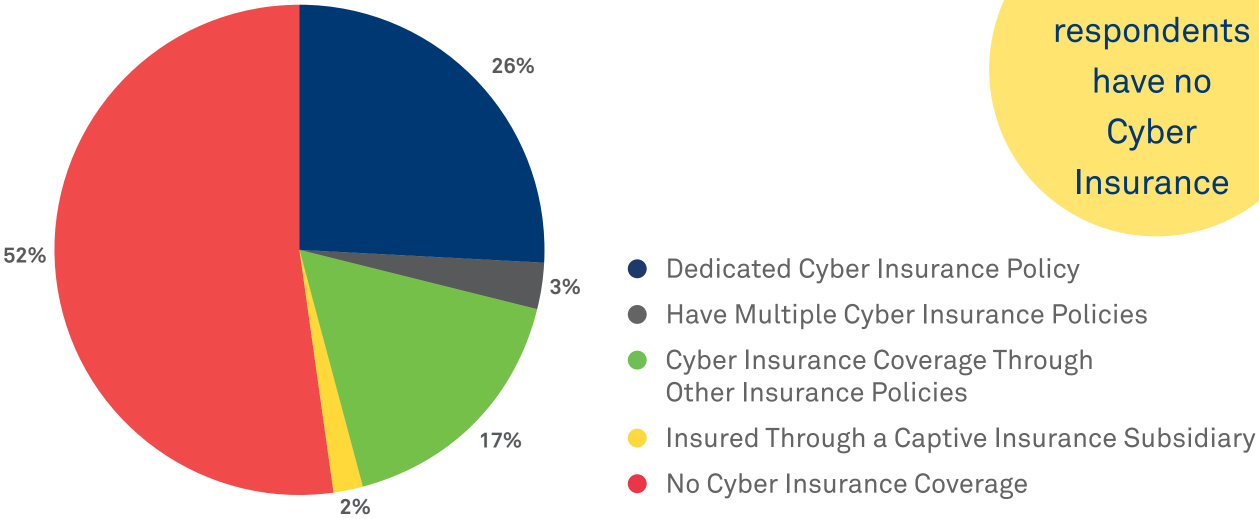


Figure 43 - Cyber Insurance Policy Types Subscribed to by Enterprises - 2016

Different types of policies that provide varying coverage in the market include:

- Standalone Cyber Insurance policies- Specialized cyber risk coverage tailored to a company, depending on the technology being used and the level of risk involved (e.g., specific to data breach and privacy related liabilities)
- Coverage under multiple specialized Cyber Insurance policies (e.g., errors and omissions insurance, media liability, network security and privacy liabilities)
- Covered as top-up to traditional insurance policies (e.g., to cover cyber losses)

We asked our respondents about the types of Cyber Insurance that they have subscribed to. 52.3% said they didn't have Cyber Insurance coverage (Figure 43). 26.2% of the respondents said they have a dedicated Cyber Insurance policy in place. This clearly indicates that Cyber Insurance, which has been in the market for more than a decade now, is not prevalent in many industries, countries and businesses. Organizations are probably not aligned to the perceived advantages of Cyber Insurance protection and the expenses that it can save in the event of a catastrophe.

The basic first and third party coverages that Cyber Insurance provides are:

- Data breach/privacy crisis management cover: First party damages like expenses related to investigation, notification, credit checking, legal costs, regulatory fines, etc.
- Multimedia/media liability cover: Damages arising out of website defacing and similar incidents
- Extortion liability cover: Losses due to a threat of extortion like DDoS attacks
- Network security liability: Costs related to theft of data on third-party suppliers and systems

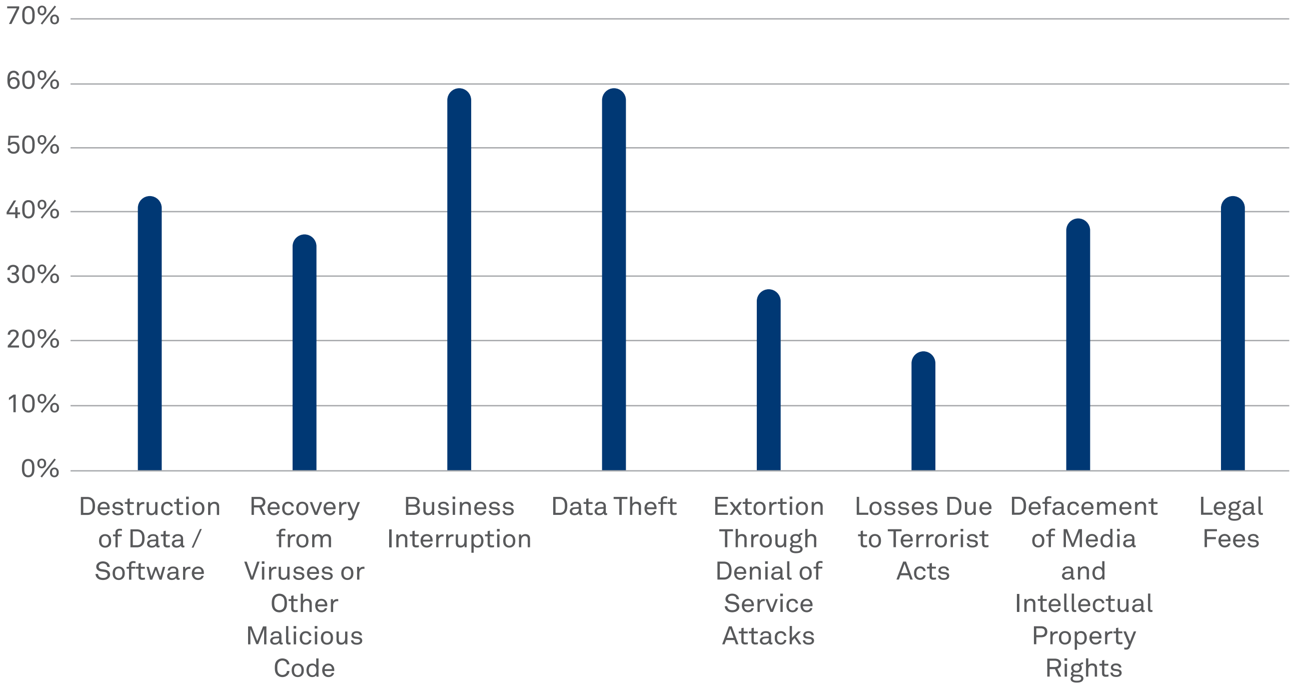


Figure 44 - Cyber Insurance Policy Coverage of Enterprises - 2016

We also asked our respondents what their current Cyber Insurance policy covers and 58.8% indicated data theft and business interruption were the most covered areas (Figure 44). 41.2% indicated that their coverage included destruction of data and legal fees. Not many respondents were covered against extortion and cyber terrorism.

58.8% of the respondents indicated that their Cyber Insurance coverage included protection against data theft and business interruption

Drones: hackers' new favorite

Drones or Unmanned Aerial Vehicles (UAV) are still relatively new in the consumer space, but the industry in the civilian domain has begun picking up momentum as more and more industries are defining use cases. In the US, the FAA (Federal Aviation Authority) released the rules for small UAS (Unmanned Aircraft Systems) in 2016. Similarly, different countries are stepping up and defining airspace controls for UAS. Drones are emerging as another set of platforms that cyber criminals are investing their efforts to explore various vulnerabilities that are present, and how they can capitalize on them as their adoption increases.

Drones use cases

Insurance Claim Validation: Insurers in the US have started receiving FAA permission to test drones for commercial use. Drones will be used to assess potential roof damage during the insurance claims process and to respond to natural disasters.

Security: Security companies have created drones that will automatically self-launch when an intruder is detected and follow them. These drones are targeted for organizations with large areas to cover, such as shopping malls and parking lots.

Organ Transplant Delivery: Different companies are developing drones for the delivery of human organs for transplant.

Cargo Delivery: Drones are being explored for delivery of medicines and essential goods to remote places and settlements.

There are various types of UAVs in the market. Each one of these drones can perform different tasks according to the technology that it is using.

Unmanned Aircraft Systems technology is still maturing and is at an early stage where it can be easily exploited by cyber criminals

UAVs and cybersecurity: drones an emerging threat

Cyber criminals have devised different ways to infiltrate these UAVs using various attack vectors as mentioned below:

GPS Spoofing Attack- Sending fake geographic coordinates to the control system of the UAVs/drones, which misleads the onboard GPS thus hijacking the vehicle.

A physical manipulation of the UAVs/drones and infecting it with malware to corrupt its software can help hijack the drone.

An attack carried out via a radio connection, over a compromised control channel, can lead to a hijack of the UAV/drone and the data being streamed by the drone can be compromised.

GPS Signal Jamming - It is easy to interrupt the GPS signal transmitted to the UAVs/drones using GPS signal jamming techniques against the device.

Drones are dependent on GPS technology for navigation. The technology allows them to be easily maneuvered from a ground control station. There are possibilities that vulnerabilities in the navigation systems could allow cyber criminals to hack into a drone's system and even spoof the connection to the ground station.

Sending spoofed geographic coordinates to the control system of the drones can lead to hijacking of drones

Future of drones

New technology comes with new vulnerabilities and threats, that can sometimes cause damage to life and property. UAS/UAV/drone technology is still maturing and is at an early stage where it can be easily exploited by people with malicious intent. Drones in the military sector are better protected and secured from infiltration but nevertheless there have been incidents of drones being hijacked. Encryption of the data streamed from the drone and the signals sent from the authenticated ground stations play a vital role in this technology. Without this encryption, hijacking of drones can cause havoc in any industry.

Persistent identity

Persistent Identity is a concept which can be leveraged for creating a unique and consistent identity for every user to communicate with the digital world. This interaction with digital systems has to take place in a secure and convenient manner. In simple terms, persistent identity makes our lives easier in the present world where we are inundated with multiple usernames and passwords and where owning our identity matters the most.

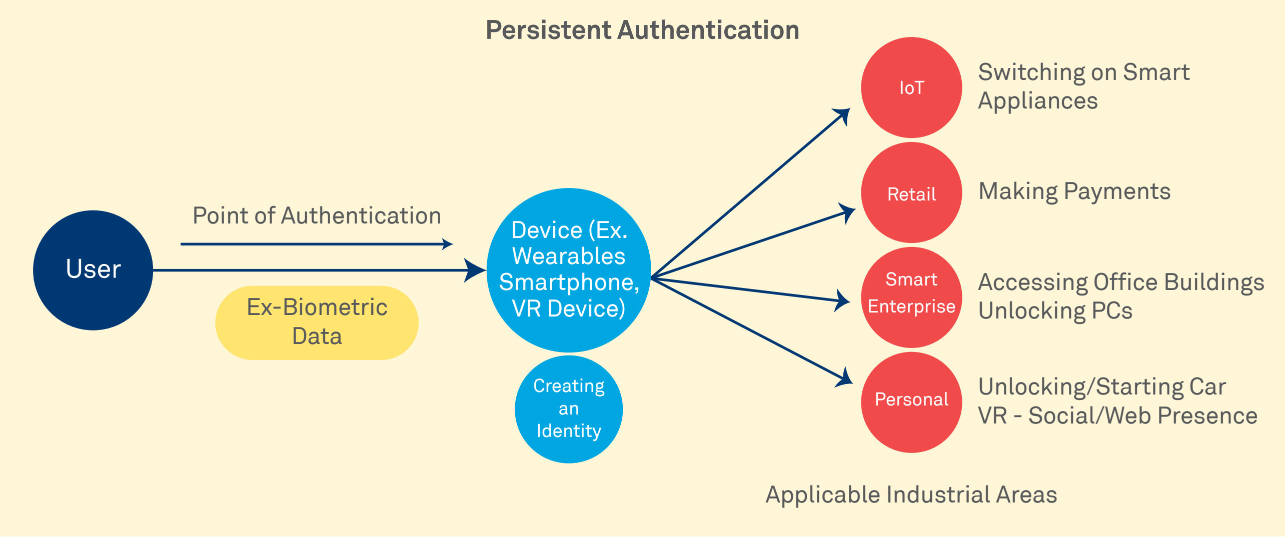

Persistent Authentication
User
Point of Authentication
Ex-Biometric Data
Device (Ex. Wearables Smartphone, VR Device)
Creating an Identity
IoT
Switching on Smart Appliances
Retail
Making Payments
Smart Enterprise
Accessing Office Buildings Unlocking PCs
Personal
Unlocking/Starting Car VR - Social/Web Presence
Applicable Industrial Areas

Figure 45 - How Persistent Identity Works

As shown in Figure 45, persistent identity is driven primarily by three important factors: 1. Point of Authentication, 2. Device that enables persistent authentication and 3. Endpoints that are compatible with the authentication environment. The first factor refers to the unique biometric data of users designed by the respective technology provider to authenticate a user. Post that, this biometric data is fed into the device to be authenticated by the user. Many technologies are emerging in this regard and it is worth mentioning that wearables are one category that we expect to see making a big leap in the near future. Persistent Identity can be applied in multiple environments such as retail payments, smart enterprise, Virtual Reality (VR) environment (where avatars are created for users to represent themselves in social interactions). The Nymi wearable band, which uses the Electrocardiogram (ECG) of a user as a biometric identifier, enables a secure, persistent biometric solution and is a very good example to note.

Apart from the aforementioned three driving factors, this transformational shift requires authentication technology to have standards that ensure interoperability. The security standard Fast IDentity Online (FIDO) launched by the FIDO alliance is a significant step in this regard. Problems related to the lack of interoperability among authentication devices and users having to keep track of multiple usernames and passwords can be addressed through standardization. So, working in this direction, specifically in order to lessen the dependency on passwords to authenticate users, FIDO has come up with two sets of technical specifications-namely U2F and UAF that define an open, scalable, interoperable set of mechanisms.

IoT security and emerging concerns

IoT has connected everyday objects to the Internet and has brought about a host of benefits and risks. As more devices are becoming a part of the network infrastructure, the attack surface for hackers is increasing exponentially. All the smart devices have an IP address and have the ability to transfer data over a network. IoT has advanced from just being the conjunction of various wireless technologies, microservices and the Internet. Connected devices having self-configuring capabilities based on standard interoperable programs can communicate with each other. In the physical and virtual world, these ‘things’ have identities as well as personalities and with the help of advanced platforms they can seamlessly communicate with each other in a network.

Securing the future IoT

As the technologies enabling IoT advance, the complexities and associated risks will also increase and so will the vulnerabilities. The challenge for organizations would be to ensure that their IoT ecosystem does not provide cyber criminals with opportunities to exploit the vulnerabilities and create havoc.

IoT ecosystem vendors need to, at the minimum, ensure that security practices are followed through the development of devices and associated services. Some recommended practices include:

Security features and policies: The device manufactures who are developing IoT devices should keep in mind the importance of security, and at least focus on the basic security controls that need to be present in the devices. Security controls like data protection and encryption should be in-built in the connected devices of the future, where privacy and security of data is of concern.

Security features need to be designed into IoT devices from the outset

Provisioning and configuration: Connected devices need initial set up and provisioning as well as standardized authentication and identification processes for the device and the user. Enterprises should make sure that regular patching and updating of the connected devices is practiced and is factored into the design through over the air type of connectivity.

Domain-wise IoT threat vectors

Domain	Types of Devices	Threats
Automobiles	In Car Wi-Fi Infotainment System	• Hack the car's head end systems and take controls of the brakes, etc. • Attacker can spoof a car, connect to servers and access customers PII
Health	Mobile Medical Devices (Infusion pumps, pacemakers, smart pill boxes)	• Medical records disclosure • Unreliable diagnosis due to failure of the device • Indicating incorrect information and in turn making harmful decisions
Consumer Products	Wearables	• Location information vulnerabilities may give access to stalkers • Third party information disclosure
	Smart Homes	• Cyber criminals trying to access by compromising the security system
Retail	Retail Inventory Monitoring	• Usage of IoT enabled transmitters that will connect to the internet makes them vulnerable to Internet based attacks
Industrial IoT Devices	SCADA Systems (Water, gas plants PLCs)	• Cyber terrorist trying to cause physical harm to the energy & utility plant
	Mining (Autonomous drilling, pressure sensors, gyroscopes)	• Hacktivist attempting to disrupt the operations
	Manufacturing (Robotics)	• Hacktivist attempting to disrupt the operations
Smart Cities	Infrastructure & Services (Traffic lights, billboards, smart cameras)	• Hacktivist attempting to disrupt the operations • Launch DDoS attacks from compromised IoT devices
	Smart Transportation (Connected vehicles, autonomous vehicles, pedestrian warning devices)	• Hacktivist attempting to disrupt the operations

Outsourcing to cyber bots

CISO organizations all over the globe generally acknowledge that they are understaffed in so far as qualified cybersecurity analysts are concerned. Enterprises are reporting a shortage in information security professionals, mainly because there aren't enough specialists.

Mitigating the cybersecurity skill gap

Scarcity of cybersecurity resources that aren't highly qualified, presents a huge problem to the cybersecurity industry. With new threats emerging continuously and the IT landscape changing frequently, skills are getting obsolete. Professionals need to have the foresight in changing times to be relevant in the industry. Against this milieu, we look at what businesses can do to counter the huge cybersecurity skill gap.

Respondents believe machine learning will help security practitioners innovate the most

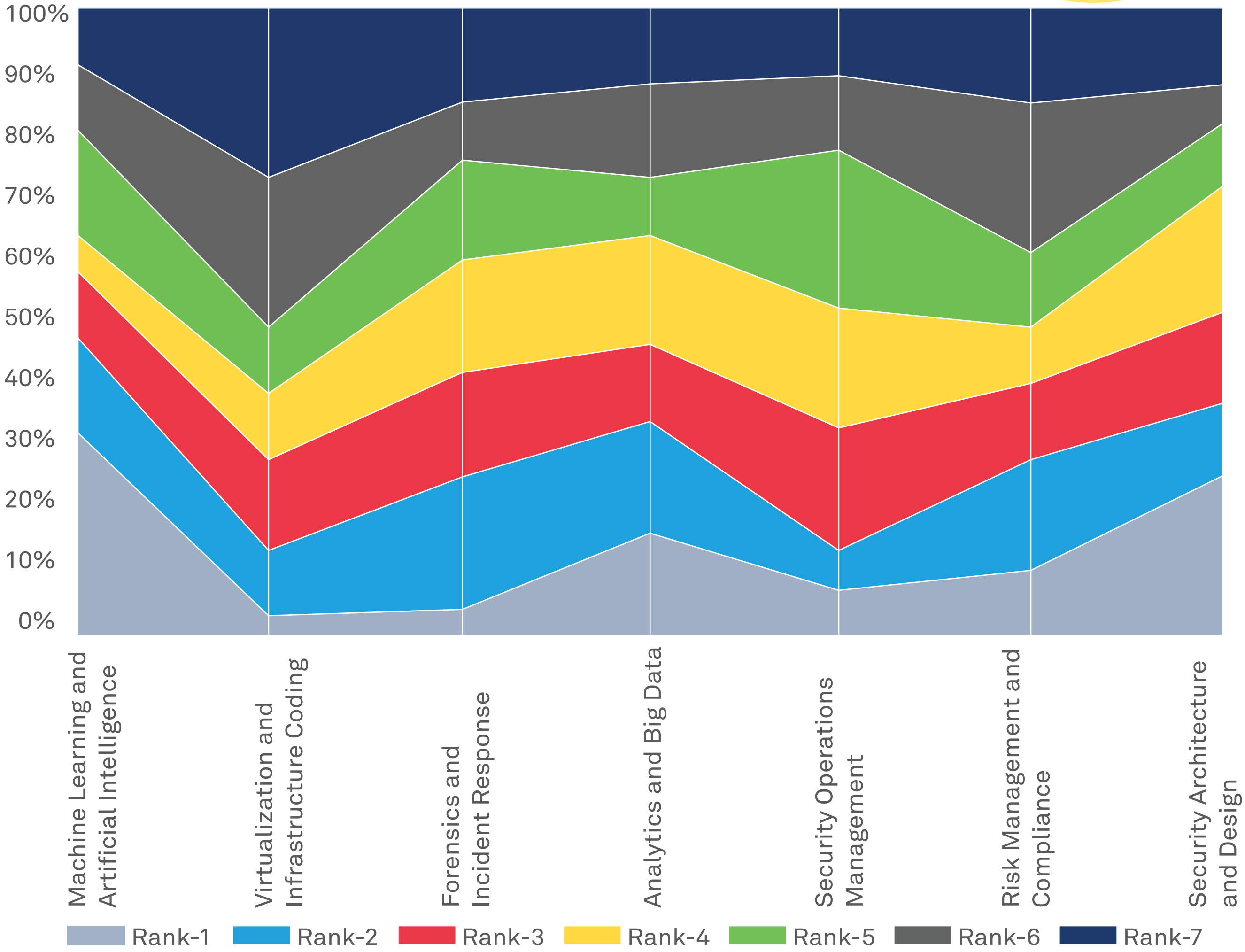


Figure 46 - Ranking Critical Security Competencies for The Future

When we asked our respondents to rank the key security competencies that will help cybersecurity practitioners to innovate and reinvent themselves for the market, 32.8% indicated that knowledge and experience on machine learning technology is going to be a key skill. Additionally, 25.4% of the respondents highlighted that security design and architecture skills will play the foremost role in stitching together cybersecurity management solutions across disparate environments, geographies and technology layers (Figure 46).

With the onset of ML/AI in cybersecurity, the role of an L1 security analyst becomes almost obsolete. In the future, complex algorithms will automate the role of the L1 analyst and minimize manual interactions. With the arrival of Big Data, the amount of data to be analyzed by the security team keeps increasing. It becomes humanly impossible to analyze the data in such large volumes and derive timely and actionable output from it. Machine learning is already emerging as a handy approach to solve this problem. Taking into account the lack of expertise in professionals in the system, ML/AI is the solution that can improve the effectiveness of analysis of cyber-attacks.

In the future, the battle is expected to be between the good and bad bots, with humans playing the role of orchestrators.

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 & hosted security services.

Contact: crs.marketing@wipro.com

Disclaimer:

This document is an informatory report on cybersecurity and cyber risk, and should not be misconstrued as professional consultancy. No warranty or representation, expressed or implied, is made by Wipro on the content and information shared in this report. In no event shall Wipro or any of its employees, officers, directors, consultants or agents become liable to users of this report for the use of the data contained herein, or for any loss or damage, consequential or otherwise. Some of the content and data have been collected from third party sources with professional care and diligence, and have been reported herein; nonetheless, Wipro doesn't warrant or represent the accuracy and fitness for purpose of the content and data.

Credits & key contributors

We thank our valuable customers across many CISO organizations who extended their support, time and shared practical and current insights that helped make this report both authentic and relevant.

We also thank the CRS practice leadership and the account leadership across different geographies who invoked the customer connections and blocked the time on the calendars for the primary research to happen.

We are also grateful to the many CDC analysts who shared their time and insights on the analytics we derived from live operational data of ongoing and past attacks that were visualized and acted upon.

Without the executive support and sponsorship from the Wipro Leadership, especially Bhanumurthy BM, President & COO and Hiral Chandrana, SVP & Head of Business, Application Services (BAS), this report would not have been possible. We thank them for their extensive support and valuable insights through the entire journey.

We would also like to thank the following key consultants who contributed to the report:

Mitan Das – Security Analyst, CRS CoE

Venkatesh M – Security Analyst, CRS CoE

Monalisa Sarkar – Security Analyst, CRS CoE

Himanshu Chandra – Security Analyst, CRS CoE

Mohona Mukhopadhyay – Security Analyst, CRS CoE

Dhanashekhar Devaraj – Lead Consultant, CRS CDC

Akash Jain – Lead Consultant, CRS

Ramesh Shetty – Lead Consultant, CRS

Kevin Abraham – Strategic Marketing, CRS

Gaurav Kwatra – Marketing, CRS

References

1. http://news.softpedia.com/news/mit-faced-35-ddos-attacks-in-the-first-six-months-of-2016-506542.shtml
2. http://news.softpedia.com/news/chinese-gambling-company-was-target-of-a-nine-vector-470-gbps-ddos-attack-505850.shtml
3. http://tech.firstpost.com/news-analysis/internet-service-providers-in-mumbai-targeted-in-ddos-attack-326708.html
4. https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/
5. https://www.rt.com/viral/360989-ddos-attack-iot-hackers/
6. https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
7. https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/
8. http://thehackernews.com/2015/10/cctv-camera-hacking.html
9. https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks
10. https://securelist.com/analysis/quarterly-malware-reports/75513/kaspersky-ddos-intelligence-report-for-q2-2016/
11. http://venturebeat.com/2014/12/30/lizard-squad-launches-ddos-tool-that-lets-anyone-take-down-online-services-starting-at-5-99-per-month/
12. https://wsandco.com/cyber-liability/cyber-basics/
13. http://cambridgeriskframework.com/getdocument/39
14. https://www.researchgate.net/publication/1958890_The_Evolution_of_Cyberinsurance
15. http://www.iii.org/sites/default/files/docs/pdf/cyber_risk_wp_final_102015.pdf
16. https://www.privacyrights.org/data-breaches
17. http://www.foxnews.com/tech/2016/01/08/time-warner-cable-says-320000-customer-passwords-at-risk-after-suspected-hack.html
18. http://arstechnica.com/security/2016/11/adultfriendfinder-hacked-exposes-400-million-hookup-users/
19. https://arstechnica.com/security/2016/09/plaintext-passwords-and-wealth-of-other-data-for-6-6-million-people-go-public/
20. http://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/
21. https://www.symantec.com/security_response/landing/azlisting.jsp
22. https://aws.amazon.com/blogs/aws/new-bring-your-own-keys-with-aws-key-management-service/
23. https://blogs.technet.microsoft.com/enterprisemobility/2016/08/10/azure-information-protection-with-hyok-hold-your-own-key/
24. http://cve.mitre.org
25. http://www.cvedetails.com
26. https://www.qualys.com/research/vulnlaws/
27. https://www.faa.gov/uas/media/Part_107_Summary.pdf
28. https://infoscience.epfl.ch/record/204987/files/DronesInSecurity.pdf
29. http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/
30. http://www.informationweek.com/iot/10-iot-startups-you-need-to-know/d/d-id/1325235?image_number=11
31. https://downloads.nymi.com/sdkDoc/doc-v3.1.5.403-403_1d2a591/index.html#the-nymi-band
32. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
33. http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20(ALRC%20Report%20108)%20/51-data-br'
34. https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/
35. https://www.cnil.fr/en/home

36. https://www.cnil.fr/en/rights-and-obligations

37. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

38. http://www.cert-in.org.in/

39. http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/act2000.pdf

40. http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

41. http://eng.rkn.gov.ru/personal_data/

42. http://www.ppc.go.jp/en/

43. http://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Infomration.pdf

44. https://www.pdpc.gov.sg/legislation-and-guidelines/overview

45. http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3Aea8b8b45-51b8-48cf-83bf-81d01478e50b%20Depth%3A0%20Status%3Ainforce;rec=0#legis

46. http://www.gesetze-im-internet.de/englisch_bdsg/

47. http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf

48. https://www.datatilsynet.no/english/

49. https://www.datatilsynet.no/English/Regulations/Personal-Data-Act-/

50. http://www.datainspektionen.se/

51. http://www.datainspektionen.se/lagar-och-regler/eus-dataskyddsreform/forberedelser-for-personuppgiftsansvariga/

52. https://www.edoeb.admin.ch/datenschutz/index.html?lang=en

53. https://www.admin.ch/opc/en/classified-compilation/19920153/index.html

54. http://www.gov.za/documents/protection-personal-information-act

55. http://www.gov.za/sites/www.gov.za/files/37067_2611_Act4of2013ProtectionOfPersonalInfor_correct.pdf

56. http://inicio.ifai.org.mx/SitePages/English_Section.aspx

57. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

58. https://www.difc.ae/files/7814/5517/4119/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf

59. http://www.npc.gov.cn/englishnpc/Law/Frameset-page2.html

60. http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_77459.pdf

61. http://blog.ventureradar.com/2015/12/29/20-commercial-drone-use-cases-and-leading-innovators/

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 a dedicated workforce of over 170,000, 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