Turnaround and transformation in cyber security
India update

www.pwc.in

Contents

Foreword

Sivarama Krishnan
Leader, Cyber Security,
PwC India

> *"Technological development is changing the way organisations do business, and cyber security is transforming to keep pace with it. The heightened and increasingly complex threat landscape is pushing organisations to change the security paradigm."*

The current dispensation's focus on cyber security is opportune. Organisations in India are hurting because of the growing number of untoward cyber incidents and their ramifications. It is only when the organisations, public or private, secure themselves that the country will be able to defend itself from this new form of warfare.

Interestingly, cyber postures of organisations in India are largely determined by their size. The larger organisations are often much ahead of the curve in deploying cyber defence strategies. The mid-market and smaller organisations are often seen to be struggling, more so because of the mindset: "If I am small, I am not interesting for the cybercriminal." In the absence of appropriate security controls, organisations have delayed incident detection and response and may sometimes even fail to detect incidents, only to be notified later by external parties.

Cyber security in India has come a long way in the past few years and has gained huge importance in recent times with the thrust on Digital India, e-commerce and mobile payments. Cyber security has been identified as one of the key areas of development by Prime Minister Narendra Modi. "Can we secure the world from the bloodless war? I'm talking about cyber security. India must take the lead in cyber security through innovation. I dream of Digital India where cyber security becomes an integral part of national security," he has said recently.[1]

With rapidly growing interconnected business operations and increasing digitisation, cyber security challenges are bound to intensify. Effective measures need to be taken to ensure protection against cyberattacks and threats. While the nation focusses on growth, our work as technologists, strategists and captains of industry is clearly cut out. We need to focus on the basics that will help keep the growth story on course. We hope that this report will play an important role in getting you to focus on cyber security, a fundamental pillar supporting organisational growth in this digital age.

[1] *Prime Minister Narendra Modi's quote on cyber security. Retrieved from http://www.ndtv.com/cheat-sheet/five-points-pm-narendra-modi-made-on-digital-india-777199 and http://www.assocham.org/eventdetail.php?id=1168#*

Cybercrimes push Indian companies to invest in security

increase in detected information security incidents as compared to the previous year

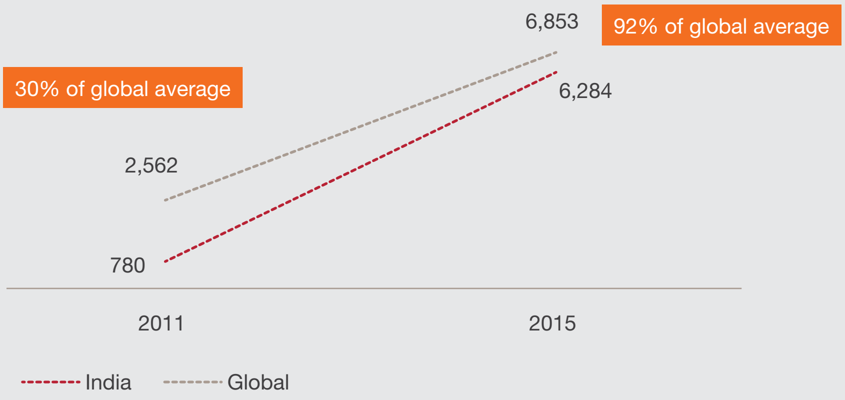
Number of incidents soar

Year after year, cyberattacks continue to escalate in frequency, severity and impact. Prevention and detection methods have proved largely ineffective against the increasingly adept assaults, and many organisations don't know what to do, or don't have the resources to combat today's highly skilled and aggressive cybercriminals. The asymmetric nature of cybercrime incentivises it; the cost of committing cybercrimes to intercept and/or modify information, degrade performance of assets, gain unauthorised access to systems, get information for personal gain or bring harm to an organisation is negligible compared to the investments required to safeguard against attackers.

Underestimating the level of risk an organisation is exposed to is usually a fatal mistake. Cyber security impacts all organisations, from fledgling start-ups to billion-dollar multinationals. Notable cyber incidents over the past year, such as that of the Indian music streaming service that compromised the records of more than 10 million users, or the vulnerability found in the routers of a popular networks company which allows attackers to spy on traffic, testify this.

Our survey reveals that acts of transgression in the Indian cyberspace have increased twofold over the past year. Indian organisations detected 117% more incidents over the previous year, shooting up from an average of 2,895 incidents to 6,284 incidents a year. This is a sharp deviation from the global trend, which saw a 39% increase in security incidents over the previous year.

Average number of incidents detected per respondent: India vs global



While earlier, developed nations were prime targets, Indian organisations have been barraged by attacks and are now on a par with other global companies at the receiving end of cyberattacks.

Indian firms have seen a steady increase in the average number of incidents detected over the past five years, with a compound annual growth rate (CAGR) of 68%.

Average number of security incidents detected per respondent in the past 12 months

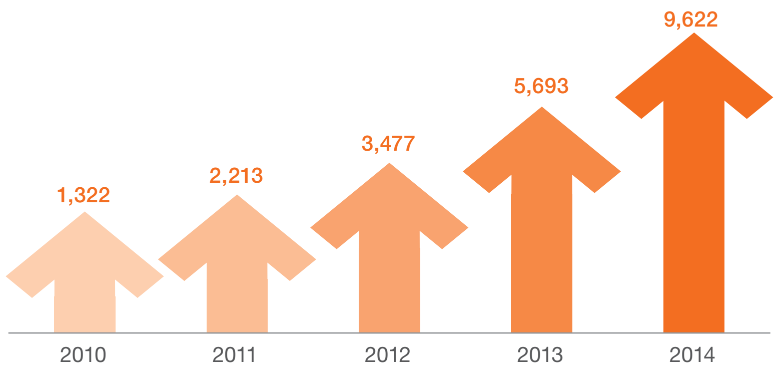
	World	India
2014	4,948	2,895
2015	6,853	6,284
Increase	39%	117%

A report by the National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India, titled *Crime in India-2014*, shows a 69% increase in cases reported under the Information Technology (IT) Act in 2014 from the year before. The number of cases recorded increased from 5,693 in 2013 to 9,622 in 2014.

69%

increase in reported cases under the IT Act

Cases reported under cybercrimes through the years

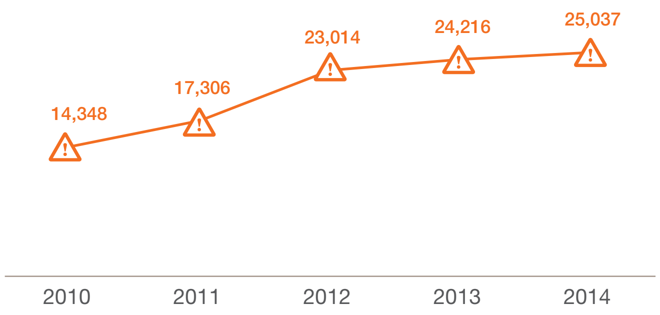


Source: National Crime Records Bureau (NCRB): Crime in India, PwC analysis

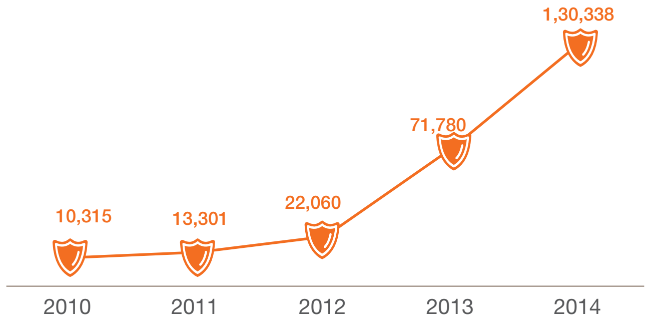
The number of security incidents that have been handled by Indian Computer Emergency Response Team (CERT-In) over the last few years has increased exponentially. If we compare the security incidents of 2014 with 2013, there has been a marked increase of 82%. The types of incidents handled were mostly related to malicious code, phishing, website intrusion, spam, network scanning and probing and malware propagation.[2]

[2] CERT-In. Retrieved from http://cert-in.org.in

Indian website defacement attacks



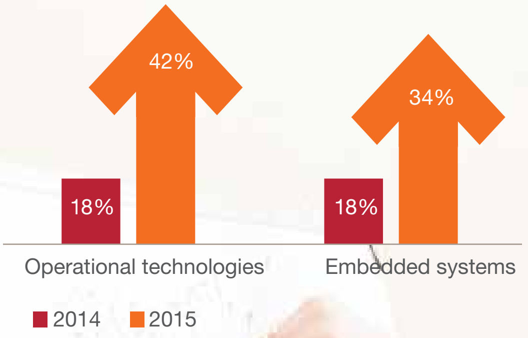
Security incidents handled by CERT-In



Source: CERT-In

Supervisory control and data acquisition (SCADA) systems and Industrial Control System (ICS) technologies are targeted more frequently by threat actors, whose motivations range from economic advantage to espionage to disruption and destruction. Cyber defences that were adequate a few years ago are now considered basic. Critical infrastructure asset owners need to deploy solutions and capabilities to neutralise such advanced threats. If we consider the security of embedded systems and operational technologies, the number of incidents caused by their exploitation has increased this year as compared to last.

Security incidents caused through embedded systems and operational technologies



Exploits of embedded systems and operational technologies nearly

doubled

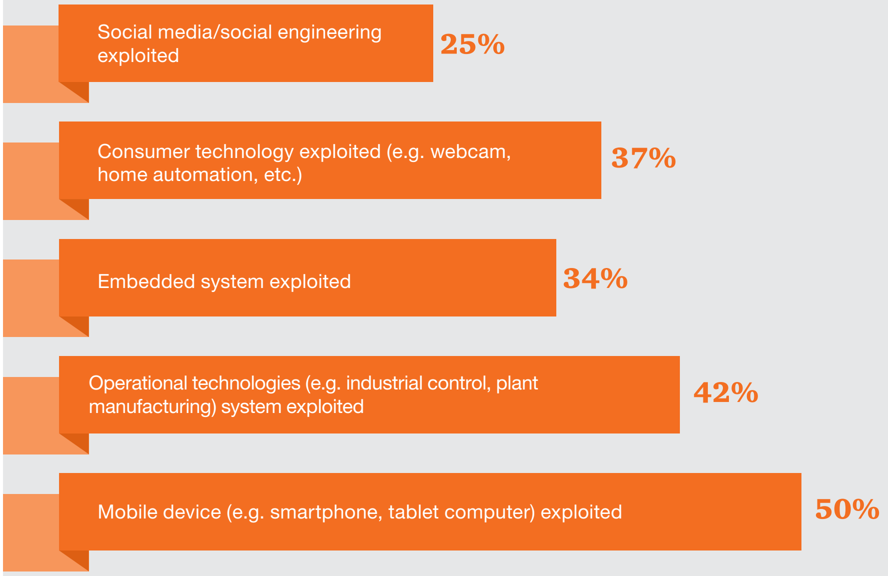
the year before

The drastic improvement in cyber technologies has helped organisations detect more incidents than before. An organisation can now detect attackers as they enter its network, whereas earlier it could only catch attackers on their way out, if at all.

Another reason for the detection of more incidents can be the convergence of information technology, operational technology and consumer technology, which has helped organisations adapt and evolve business models, however, without a complete understanding of the risks it entails. As a result, we have seen a proliferation of incidents from mobile devices, consumer devices, operational technologies and social media.

In the light of increasing incidents, it is noteworthy that Indian organisations are rethinking their cyber security requirements and preparing for advanced threats. The importance of cyber security has grown considerably over the past few years and has helped expand the influence and scope of cyber security functions.

Mediums through which security incidents occured



Organisations are responding with agility and conviction to remove existing constraints and strengthen the three pillars of people, processes and technology to enhance their security profiles.

Financial losses increase twofold

Financial losses as a result of cyber incidents increased by 135% over the previous year, which is a steep rise compared to the trend of 20-30% over the years before.

Not only has the number of incidents increased, but the average loss resulting from an incident borne by an Indian organisation has also increased by close to 8%.

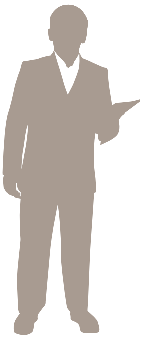
Performing a thorough evaluation of factors that contribute to the losses from cyber incidents remains a daunting task for organisations in the country, and hence, the true cost of cyber incidents is hard to calculate. Some factors that are typically used to estimate the financial loss from cyber incidents include loss of customer business, legal defence services, court settlements, investigations, forensics, and deployment of detection software, services and policies among others.

Our survey also reveals that 44% of respondents cited loss of customer records and almost 36% suffered financial losses as a consequence of security incidents. A small percentage of respondents, however, did not know about the tangible or intangible impact of such incidents on their organisation.

Further, almost 38% respondents claim to have suffered a loss of 'hard' intellectual property (IP), which includes strategic business plans, deal-related information and sensitive financial information. Such information in the wrong hands can severely impair competitive advantage and potentially change the dynamics of an industry. Our analysis reveals that an increasing number of organisations are putting in place mechanisms to estimate losses as a result of cyber incidents with greater accuracy, year after year.

135%

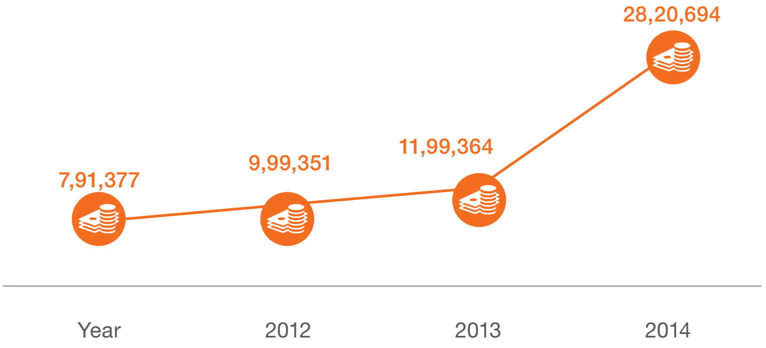
increase in average financial loss due to cyber incidents



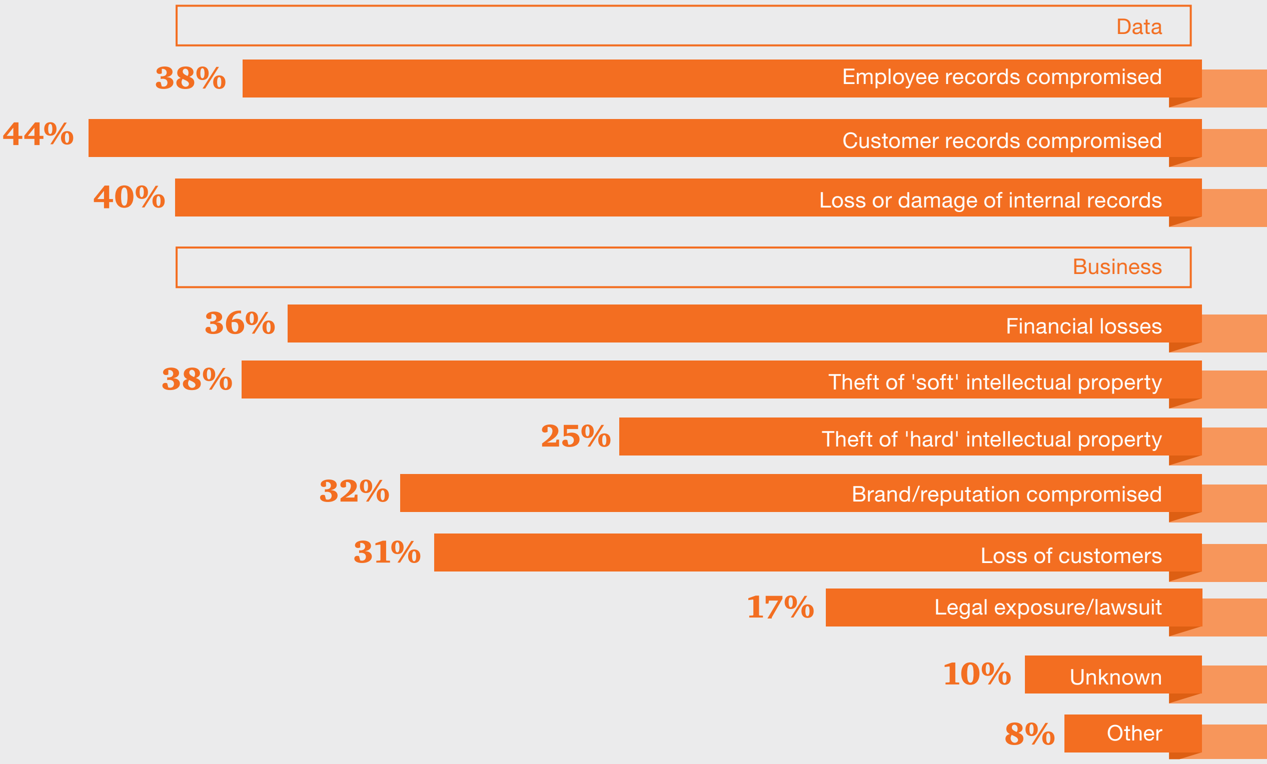
44%

have suffered loss of customer records

Estimated average financial loss as a result of security incidents per respondent: India (USD)



Impact of security incidents on business and data



Companies ramp up investments in security

Our survey revealed that the average information security budget has increased with a CAGR of 25% for Indian organisations over the last five years. This has helped the organisations in combatting security incidents by deploying newer and more robust technologies and processes. It has also assisted in capacity building as more security professionals are now getting hired to be a part of the information security team.

As organisations focus more on profitability, they have a proclivity towards investments in growth activities rather than defensive measures. However, the cost of ignoring cyber security can be considerable. Loss of IP and customers, and damage to reputation can be difficult to restore.

Cyber insurance holds promise

By now it seems clear that technically adept adversaries will always find new ways to circumvent security safeguards. That's why many businesses are purchasing cyber security insurance to help mitigate the financial impact of cybercrimes.

No wonder, then, that cyber security insurance is one of the fastest-growing sectors in the insurance market. In fact, a recent report by PwC forecasts that the global cyber insurance market will notch up 7.5 billion USD in annual sales by 2020, up from 2.5 billion USD this year.[3]

Today, first-party insurance products cover data destruction, denial of service attacks, theft and extortion; they may also include incident response and remediation, investigation and security-audit expenses. Other key areas of coverage include privacy notification, crisis and reputation management, forensic investigations, data restoration and business interruption. The insurance industry is attempting to expand into policies that cover the value of lost IP, reputation and brand image, as well as cyber-related infrastructure failures.

Organisations in India are expressing a keen interest in cyber insurance. Close to 55% of respondents have either purchased or are planning to purchase it.

25%

CAGR increase in information security budgets over the last five years

[3] PwC. (September 2015). *Insurance 2020 and beyond: Reaping the dividends of cyber resilience*

Insider threats tackled at multiple levels

15

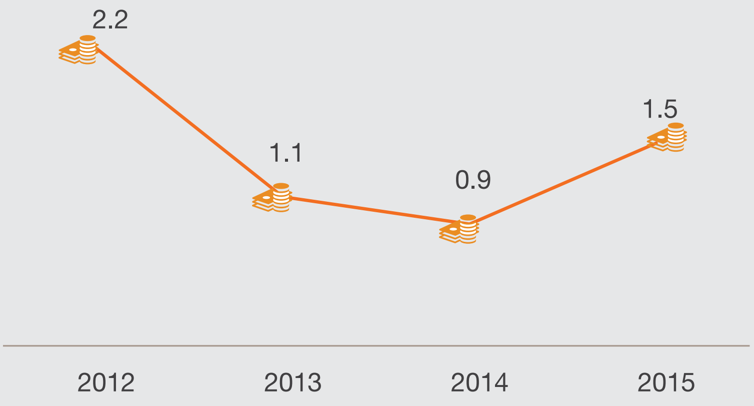
incidents caused by insiders for every 10 incidents caused by an outsider

Insider threats return to haunt organisations

When it comes to the sources of security incidents, those caused by external factors dominate news headlines. Agents like terrorist hacks, hacktivists, etc. have been all over the media over the previous years. However, it is important to understand that security breaches by insiders—employees, vendors and business partners with authorised access—can be even more harmful. As per the responses of the survey, an insider caused nearly 15 security incidents for every 10 incidents caused by an outsider in 2015. Yet, a majority of businesses are unprepared for insider threats.

The trend over the years also shows the same results as security incidents caused by insiders have dominated those caused by external actors. Though the trend has been declining over the last three years due to improvements in internal access controls, it appears that in the last 12 months, the number of incidents caused by insiders have once again increased due to the inability of the existing basic identity and access management controls to prevent modern techniques like social engineering used by attackers to exfiltrate confidential information.

Ratio of security incidents caused by insiders vis-à-vis external actors: Trend over the years



Insiders have an advantage as they have authorised access to information and hence have no need to breach any security controls. They also understand the organisation's competitive environment better than any other external actor. They know exactly where to look for the company's most valuable information.

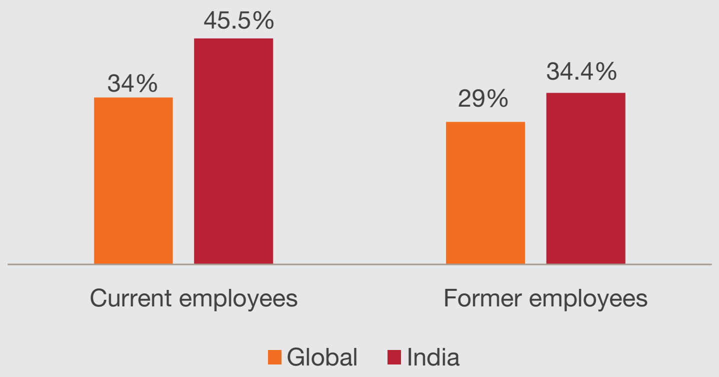
46%

believe that current employees expose organisations to security risks

Among the insider threat actors, a little less than half (46%) of the respondents said that current employees expose their organisation to security incidents. Even though this figure is slightly less than last year's (48%), still it is a massive 12 percentage points more than the global average. One of the major reasons for such a high percentage can be attributed to the lack of personnel background checks, as only 56% of the respondents say that it is carried out in their organisation.

Former employees were cited as another major security threat, with nearly 34% respondents holding them responsible for security incidents. This indicates that the companies need to establish greater rigour in their exit-related processes and make sure that all accounts and access of the users are deactivated upon separation.

Employees as sources of incidents



Access management, authentication and sensitisation: The key levers

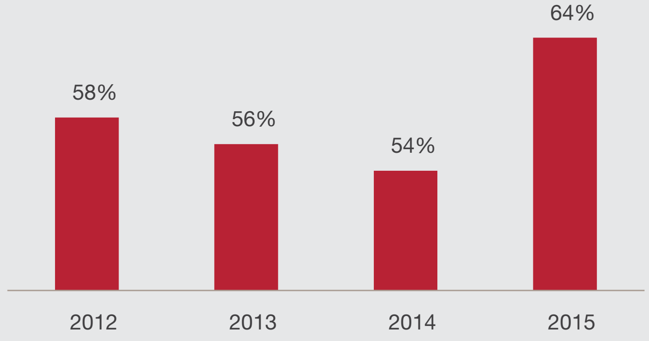
In an era where insider threats are rising, weak authentication mechanisms are usually held responsible. Organisations have already put in place controls to mitigate risks stemming from insider threats. However, with advancements in tools and techniques employed by internal actors, organisations need to continuously adapt and evolve to keep up.

It is easy to understand why many organisations are turning to advanced authentication techniques to address insider threats and boost the confidence of employees, customers and suppliers.

There has also been a steady increase in risk-based authentication systems as nearly 56% of respondents said that such systems were deployed at their organisation this year as compared to 50% the previous year. More advanced authentication technologies such as biometrics, facial and voice recognition have also been developed; however, their use is limited. Use of password-less authentication will require organisations to rethink their approach to identity management and focus solutions to build identity trust relationships with users. Furthermore, authentication solutions should be designed to correspond to the level of risk of access to systems and should not hinder the ease of use of systems.

Benefits of advanced authentication	
Improved customer/business partner confidence	66%
Online transactions are more secure	60%
Enhanced fraud protection/reduced fraud	56%
Improved customer experience	52%
Improved regulatory compliance	50%
Brand reputation protected	47%

Respondents who have received employee training and attended awareness programmes over the years



Unintentional breaches can be avoided by ensuring that employees are aware of the organisation's security and privacy policies, procedures and consequences of not adhering to them. As many as 64% of the respondents said they have a security awareness training programme, while 18% of them marked it as a top priority in their agenda for the next 12 months. Some 58% of our respondents said their organisations have made it compulsory for the employees to complete the training related to privacy policies and practices, even as 21% see this training as a priority in the next 12 months. Employee training and awareness is an important component and should be carried out by the organisations.

Organisations focus on cyber security

81%

have adopted security framework(s)

Over the years, cyber threats have evolved by leaps and bounds and will continue to do so. Criminal organisations are expected to become more sophisticated, mature and be able to migrate their activities online at a greater pace.[4] Outsourcing activity among Indian organisations is also expected to rise with more and more organisations focussing on their core business, thereby creating more complex and interconnected networks with suppliers, vendors, partners and other third parties, making them more prone to cyberattacks and data leakages. And hence, it is imperative for Indian organisations to gear up for the cyber security challenge by formulating security strategies and implementing technology solutions to monitor and manage security risks.

Rewards of a robust security framework

Recent advances in computer science and technologies are providing powerful opportunities for organisations to transform their cyber security programmes and create a holistic system of integrated safeguards. It all starts with a strategy and an underlying foundation based on risks. A detailed information security strategy allows the management to set long-term goals and have clear visibility of their targets so that focussed efforts are made and the progress is tracked.

A vast majority of Indian organisations (81%) have adopted a security framework or, more often, an amalgam of frameworks, mostly with very good results. The two most frequently implemented guidelines are ISO 27001 (53%) and the US National Institute of Standards and Technology (NIST) Cyber Security Framework. These guidelines enable organisations to identify and prioritise risks, detect and mitigate security incidents, gauge the maturity of their cyber security practices and better communicate and collaborate internally and externally. At the same time, around three-fourths of the respondents said that their organisations have an overall information security strategy in place.

Benefits of security frameworks	
Better able to identify and prioritise security risks	66%
Better able to quickly detect and mitigate security incidents	61%
Sensitive data more secure	62%
Better understanding of security gaps and how to improve them	47%
Improved internal and external collaboration and communications	51%
Better prepared to operate and compete across global markets	42%

Frameworks such as the NIST Cyber Security Framework and ISO not only bring together leading practices from across industry sectors and serve to improve risk-based security, but also provide a platform for internal communication and external collaboration.

Organisations are also leveraging risk-based guidelines to improve the security performance of third-party partners, which is a key concern. They have found that frameworks can enable companies to more easily exchange information with business partners and suppliers, and communicate expectations and concerns about the services they provide.

[4] *Information Security Forum (ISF). Threat Horizon 2017*

Over 60%

have invested in vulnerability management as well as intrusion detection tools

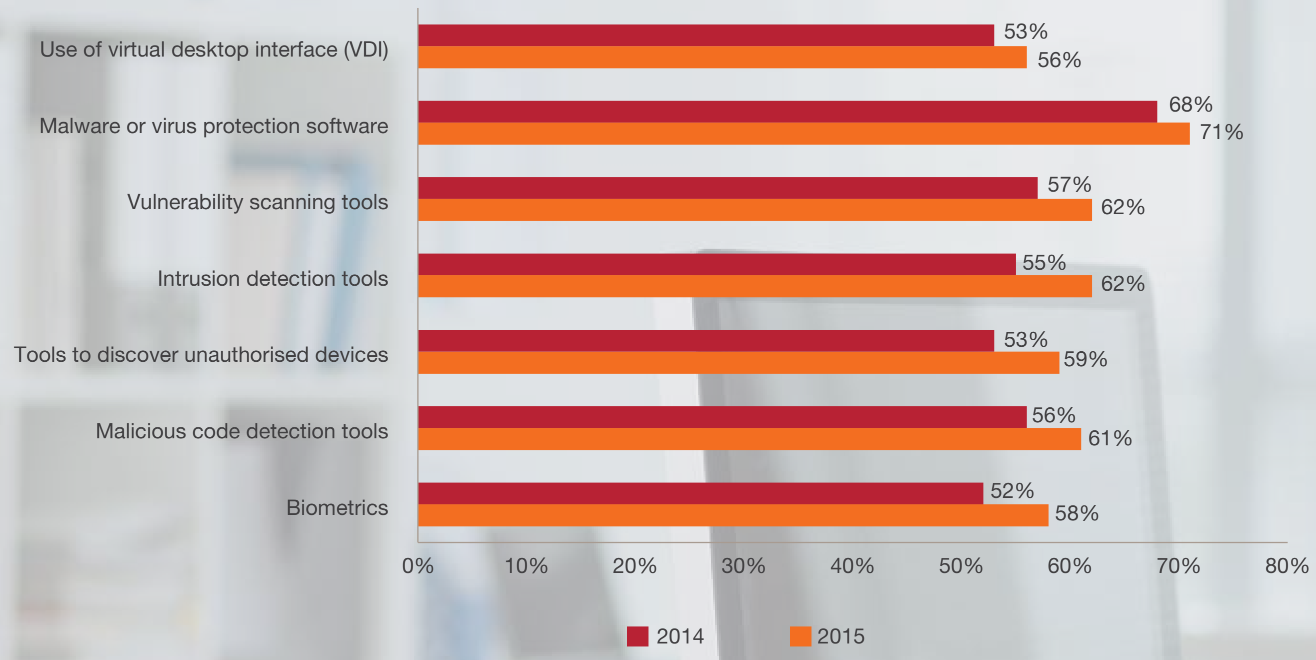
Technology investments: The core of cyber security

In today's rapidly evolving threat landscape, threat actors are becoming more sophisticated, breaching the defences of business ecosystems and leaving reputational, financial and competitive damage in their wake.

Organisations recognise its importance and have invested accordingly in the technological advances. Vulnerability scanning tools have seen an increase in adoption and are up from 57% to 62%. Intrusion detection tools have increased from 55% to 62%.

Other major categories which have gained importance are malicious code

Respondents adopting various security technologies



Security event correlation and behavioural profiling tools will be top priorities in the next 12 months

detection tools, malware software and use of virtual desktop interface (VDI).

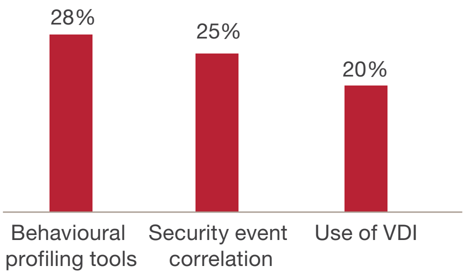
Some organisations are exploring the use of data analytics for identity and access management to monitor employee usage patterns and flag outliers. In this scenario, the data analysis solution looks for patterns around the employee access entitlements and then identifies unwanted access.

Organisations are already realising the benefits of advanced technologies to improve their information security environment and a sizeable number of them (53%) have listed implementation of newer technologies as their top priority in the next 12 months.

50%

cited suppliers/ customers as likely sources of security incidents

Top technology implementation priorities in the next 12 months



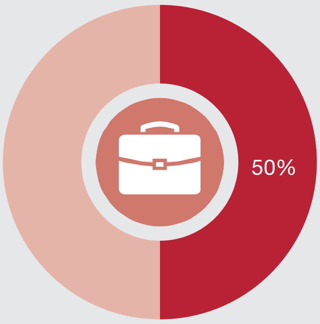
Third party security focus not yet pervasive

While over 50% of respondents cited suppliers and/or customers as likely sources of incidents, most Indian organisations (over 85%) are confident around the information security practices of their business partners and suppliers.

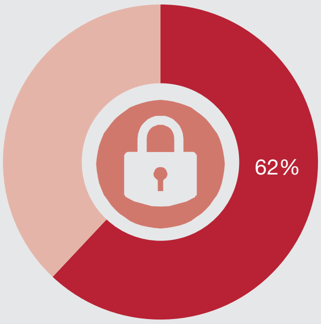
In the absence of strong compliance requirements or baseline security standards for third parties, information once shared with third parties may still be at risk. Over 24% of respondents cited former business partners and suppliers as causes of incidents.

In today's interconnected ecosystem, the compliance of third parties to relevant security policies and procedures is important to maintain the overall security posture of the organisation. Surprisingly, we noted that 50% of companies do not ensure that third parties comply with their privacy policies, and around 40% of total organisations do not have established baseline standards for third parties.

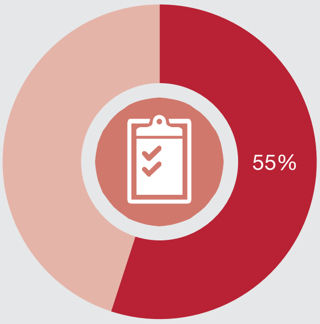
Compliance with privacy policies



Compliance audit to check safeguards for personally identifiable information (PII)



Established security baselines/standards



70%

collaborate with others to improve security

Organisations partner to sharpen cyber security intelligence

As more businesses share more data with an expanding roster of partners and customers, it makes sense for them to swap intelligence on cyber security threats and responses. Indeed, over the past three years, the number of organisations embracing external collaboration has steadily increased.

These collaborations have proven to be highly beneficial for all parties.

Most organisations say external collaborations allows them to share and receive more actionable information from industry peers, as well as government agencies such as CERT-In. Many say that information sharing has improved their threat awareness and intelligence.

Organisations that do not collaborate often cite the lack of information-sharing framework and standards as well as incompatible data formats and platforms among public and private entities as the reason. Another weakness is that cyber security updates are not communicated at network speed.

Policies and regulations on data privacy vary widely across the globe, and *some organisations also worry that sharing certain types of data can violate the privacy of customers, employees and other individuals.* And, of course, validation of intelligence is a concern for all.

In India, the CERT-In functions at the national level to coordinate cyber security emergency response and facilitates communication between other CERTs. CERT-In also issues guidelines, advisories and vulnerability notes to help organisations strengthen cyber security.[5] The National Cyber Coordination Centre (NCCC) was recently approved by the government to coordinate intelligence gathering between agencies and handle issues related to national security.[6]

For example, security challenges often do not differ by sector but by an entity's size or constituency—a big bank might have much more in common with a large pharmaceutical company than it does with a regional bank.

Benefits of external collaboration	
Share and receive information from industry peers	63%
Improved threat intelligence and awareness	58%
Share and receive information from government	46%
Share and receive more information from law enforcement	46%
Receive more timely threat intelligence alerts	49%

The evolving involvement of executives and the board

When it comes to cyber security, there is no other pivotal player than the top information security officer, typically the chief information security officer (CISO) or chief security officer (CSO). The responsibilities and competencies associated with this role has become visible and critical.

Today's CISO or CSO should be a senior business manager who has the expertise not only in cyber security but also risk management, corporate governance and overall business objectives. He or she should have the expertise of key executives to provide insights into business risks and should be able to competently articulate risk-based cyber security issues to the C-Suite and board. Simply put, the cyber security leader should have the ability to effect change on par with C-level executives.

Today's cyber security incidents often leave behind a broad swath of operational, reputational and financial damages. Consequently, many board of directors and the C-Suite have begun to address cyber security as a serious risk oversight issue that has strategic, cross-functional, legal and financial implications.

[5] *CERT–In. Retrieved from www.cert-in.org.in*

[6] *The Economic Times*

Our survey reveals that today's board of directors and C-Suite are actively involved in addressing cyber risk. Over 61% of respondents believe that their boards are vigorously involved in formulating the overall information security strategy, which is significantly higher than the global average of 45%.

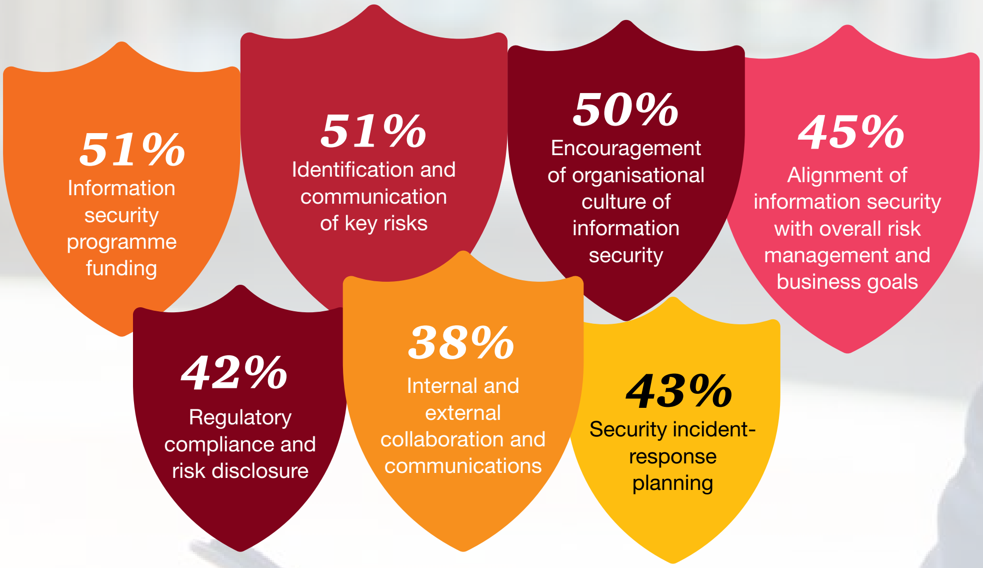
While defining the return on security investments (ROSI), which continues to be difficult to justify, our survey reveals that boards are supportive of cyber security programmes. Fifty-one per cent of respondents admitted that their board's active participation has helped improve the funding process.

The surge in average information security budgets over the last five years show that CISOs/CIOs, and heads of information security today find it easier to obtain funds for their programmes, and the growing number and intensity of attacks has only helped their cause.

CEOs too have played their part. Almost 54% of respondents believe that their CEO promotes cyber security as a corporate governance imperative and not simply an IT issue. Almost 55% of respondents believed that CEOs understand that cyber security is a top business risk.

Such trends, such as the involvement of the boards and C-Suite in cyber security, mark a shift in the attitude of the top level management and is a significant boost to cyber security programmes within organisations.

How the board's participation has helped improve the organisation's information security programme



51% Information security programme funding

51% Identification and communication of key risks

50% Encouragement of organisational culture of information security

45% Alignment of information security with overall risk management and business goals

42% Regulatory compliance and risk disclosure

38% Internal and external collaboration and communications

43% Security incident-response planning

Emerging technologies: New risks

Technological change continues to disrupt how organisations compete and create value in ways that often alter operating models. Some of the most significant business trends today, including the explosion of data analytics, the digitisation of business functions, and a blend of service offerings across industries, have expanded the use of technologies and data that is creating more risk than ever before.

Gearing up for the Internet of Things (IoT)

The ecosystem of Internet-connected devices, operational tools and facilities is poised to soar in the coming years. Research firm IDC predicts that the number of devices connected to the Internet will reach 30 billion in 2020, up from an estimated 10.3 billion last year.[7] The Government of India recently launched the Digital India Programme and the Smart Cities Mission. Digital India aims at transforming India into a digitally empowered society while the smart city concept aims at developing 100 smart cities in India. These initiatives will boost the IoT industry in India. Citizens and business leveraging this technology will serve as a fillip to this industry.

IoT has indeed come a long way from being a futuristic concept just a few years ago to transforming into real products, services, and applications. Smart watches, fitness bands and trackers, smart glasses, self-driving cars and drones are just the beginning of the endless possibilities.

As IoT continues to expand, analysis of machine-to-machine (M2M) data will become critical. In this type of data-centric environment, the importance of strong encryption cannot be underestimated. The security and privacy risks have been highly publicised. Hackers can hijack connected cars and control them remotely; digital snoopers can infiltrate home surveillance systems and monitor the behaviour of residents; and threat actors can compromise connected medical equipment and potentially impact the health and safety of patients. Vulnerabilities left unattended can result in grave repercussions from business losses to catastrophic establishment attacks.

[7] International Data Corporation (IDC). (June 2015). Connecting the IoT: The road to success

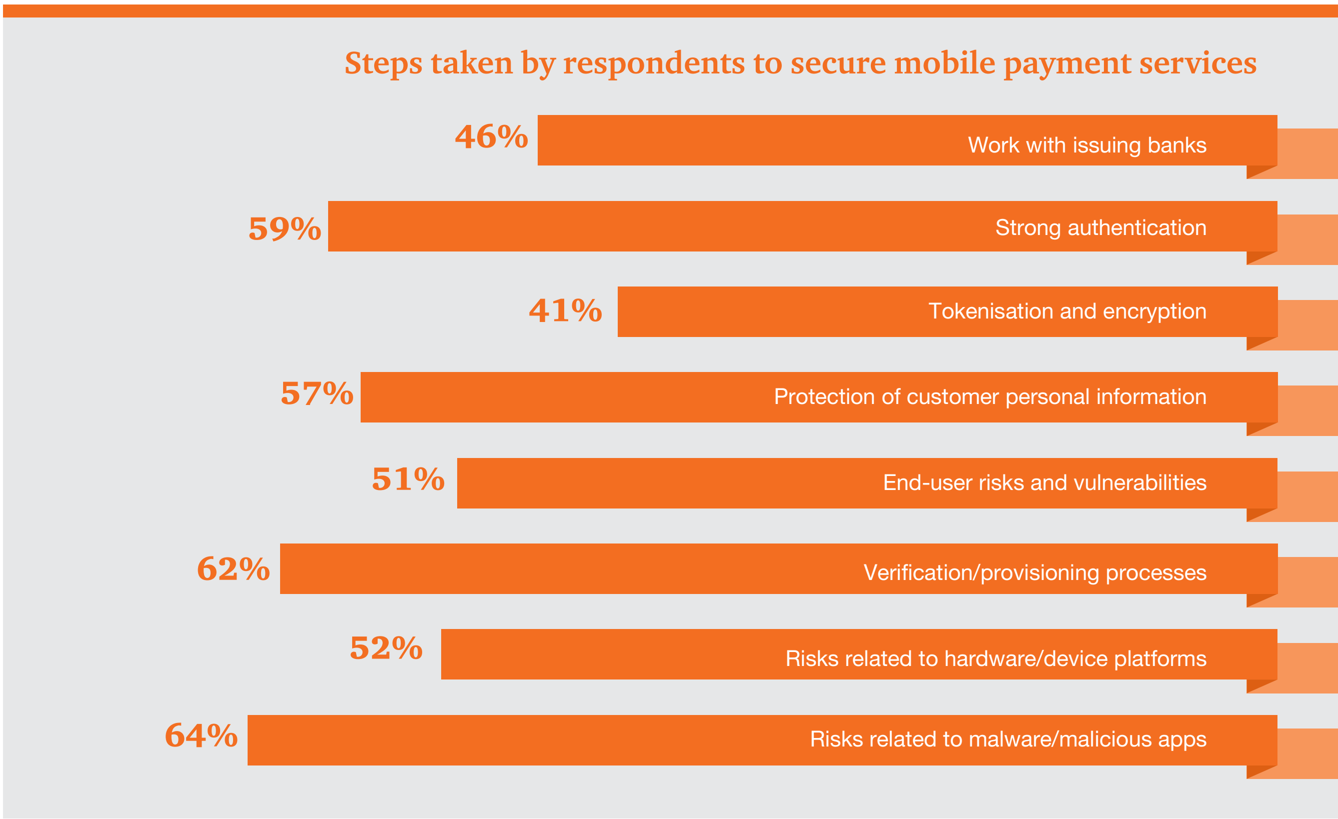
Going mobile with payments

With the increase in sales of smartphones and access to the Internet, m-commerce, m-payment is set to grow rapidly. It is still in its nascent stage however, the ecosystem is continuously and rapidly evolving as new partnerships are formed among a constellation of technology, financial, retail and telecommunications firms.

M-payments along with value added services such a m-coupons, m-commerce, mobile analytics, mobile wallets and virtual currencies present a huge opportunity for a develpoing countries like India. However, it also brings with it cyber, privacy and compliance risks that organisations need to address.

M-payments present a strong case for financial inclusion by assisting in the ease of operation related services to cash handling, storage and transfers. Reserve Bank of India (RBI) has already recommended banks to increase access to banking services for the unbanked population by leveraging m-payment systems. In continuation of its efforts, RBI granted ‘in-principle’ approval to 11 organisations to set up payment banks and begin their operations.

As per the survey conducted, 59% of respondents said that their organisation was accepting m-payment services which are in sync with the global average of 57%. At the same time, officials of many organisations worry that this might also mean new security concerns for the m-payment ecosystem such as weak cryptography, mobile application server threats, SIM card application attacks, and m-payment application database threat among others. As a consequence, adequate steps are being taken to improve the security of m-payments. Some of the steps undertaken include strong authentication (59%), verification/provisioning process (62%), addressing risks related to malware and malicious apps (64%) among others.



Reclaiming cyber security through innovation

59%

actively monitor/ analyse information security intelligence

Cyber security centres (CSCs) bring actionable intelligence

The last couple of years have witnessed the advent of the new generation security information and event management (SIEM) solutions and rise of cyber security standards. Criminals are using technology to give crime a completely new dimension. The dynamic of the cyber security threat landscape is compelling the industry to develop better systems and solutions beyond the traditional security operation centre (SOC).

An effective SOC should not only contain state-of-the-art tools and technologies but also have mechanisms for threat intelligence reporting, profiling, detection and response. This need has given rise to new age CSCs, which fundamentally focus on integrating all internal events and global threats and provide insights or actionable intelligence, and quick and decisive remediation action.

CSCs focus on providing threat intelligence by collecting and correlating information from internal and external sources and continuous strategic threat profiling through data enrichment. CSCs improve threat response capabilities by supporting forensic evidence collection, incident classification and forensic analysis and help bolster the organisation’s threat management process.

71%

employ cloud-based security services in India

Adoption of cloud-based service model for cyber security

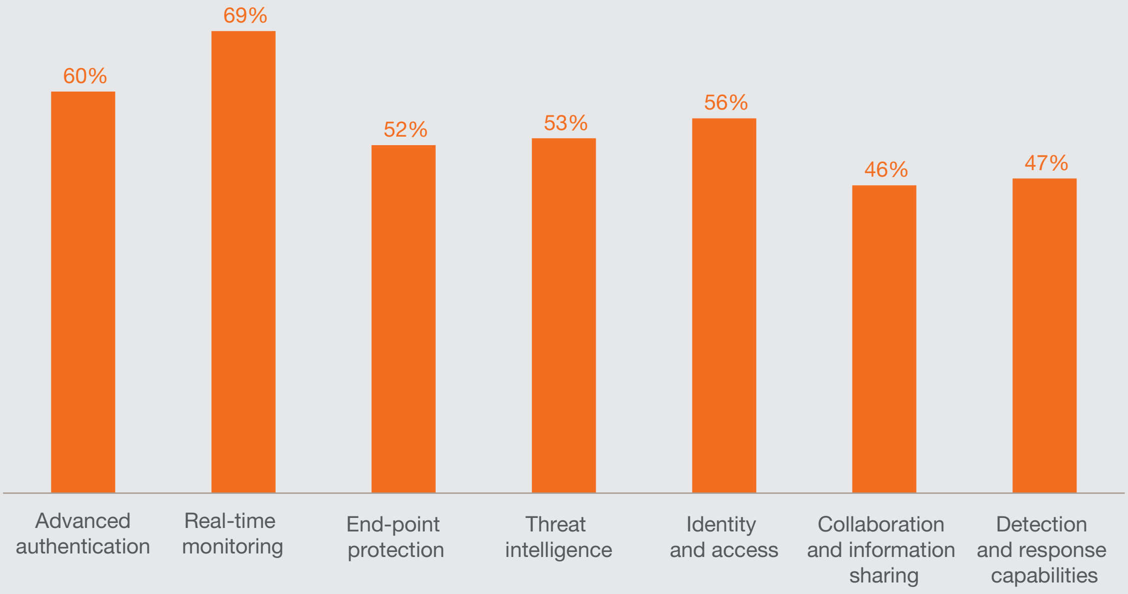
Cloud computing is changing the way businesses operate by presenting new avenues for delivering services, information sharing and enhancing operational efficiencies. It is also helping organisations stay cyber secure.

Cloud-based models have emerged as an effective way for organisations to effectively manage cyber threat costs. A majority of survey respondents entrust a broadening range of critical services to the cloud, including real-time monitoring and analytics, advanced authentication and identity and access management. Many companies are adopting cloud-based cyber security that is delivered by managed service providers, often using private cloud architecture.

Globally, cloud-based IT security solutions are also in demand, especially from small and medium businesses.

As per the global survey results, 70% of respondents say that their organisations use some form of cloud-based security solutions. According to respondents based in India, cloud-based security services are being used for a wide range of solutions like threat intelligence activities, setting up of advanced identity and access management capabilities, end point encryption, etc.

Respondents who have adopted various cloud-based security components



The big impact of Big Data

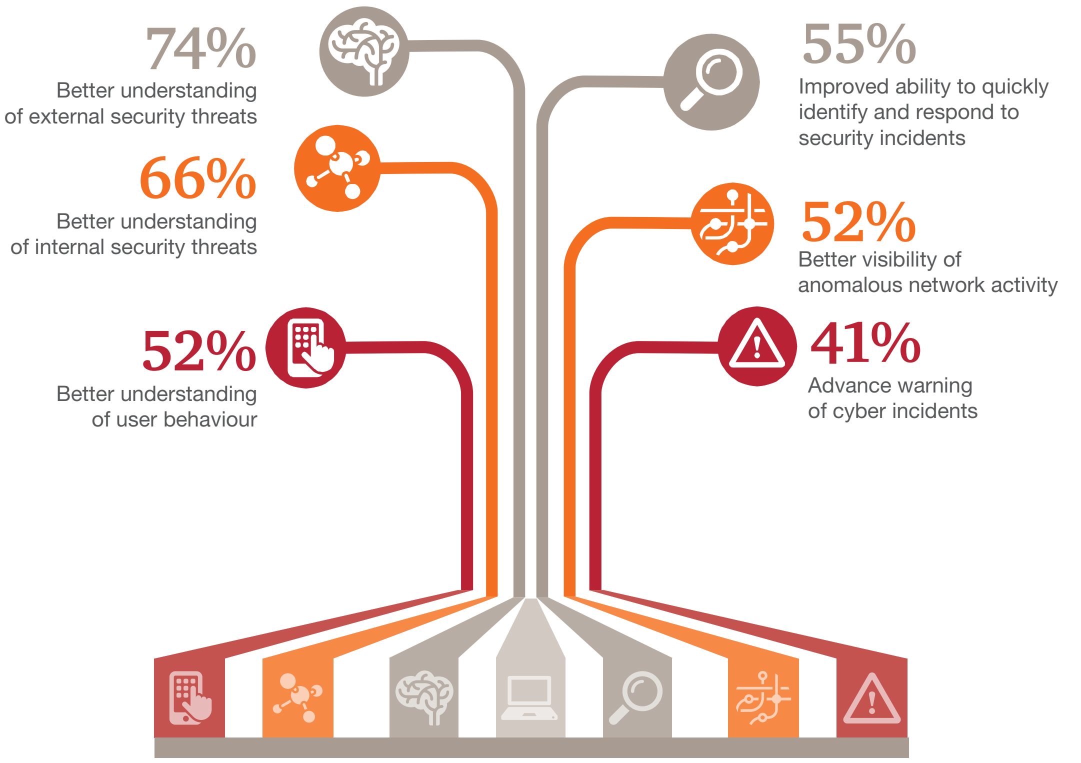
In a world where data is gaining importance, and companies are leveraging big data analytics for business decision, a growing number of organisations are also employing big data analytics to monitor securit threats, quickly respond to incidents and audit and review data to understand how it is used, by whom and when.

A data-driven approach can shift security away from perimeter-based defences and enable organisations to put real-time information to use in ways that can help predict security incidents. Data-driven security enables companies to better understand anomalous network activity and more quickly identify and respond to security incidents. It can also be effective in reducing or quickly detecting employee security incidents by monitoring their behaviour for suspicious activity. In India, we noted that over 1/4th of respondents have plans to employ big data analytics for improving their security programmes in the next 12 months.

Big data analytics often require an enormous commitment to computing resources and software expertise. Data analytics also can be combined with existing SIEM technologies to generate a more customisable and extensive view of network activity.

Organisations are exploring the use of data analytics to identity and access management to monitor employee usage patterns and flag outliers. In this scenario, the data analysis solution looks for patterns around the employee access entitlements and then identifies unwanted access.

Results for best perceived benefit of leveraging Big Data analytics in security



Fit for the future of cyber security

An advanced and enhanced information security programme will not only enable companies to better protect themselves against cyber threats in the future, but also help create competitive advantages and foster trust among customers and business partners.

The challenge, of course, is that it is exceedingly difficult to predict the future of cyber security when many aspects of its present state are uncertain and continually shifting. Nonetheless, we believe there are some assumptions that organisations should consider while preparing to enhance their cyber security over the next five years.

First, any discussion of the future should be predicated on the premise that personal lives will be increasingly digitised, creating even greater avalanches of data that can be collected, analysed and potentially compromised. Businesses too will continue to generate and share more information about people and processes, and IoT will unleash a torrent of (M2M) data. Amid this escalation of data, individual and corporate identity, and privacy will begin to converge. In this type of data-centric environment, the importance of strong encryption cannot be underestimated.

It's safe to assume that future threat actors will wield an attack kit of technically sophisticated tools and tactics. For governments and businesses, espionage and political hacking will merge as hacking techniques will become highly nuanced and aggressive. At the same time, increasingly brazen attacks by nation-state and politically motivated hacktivists will result in economic sanctions or possibly even cyber warfare. In fact, it's not entirely unlikely that a catastrophic cyber security incident will precipitate demand and support for government-controlled identity management.

Furthermore, governments are working to improve their ability to trace and directly attribute intrusions to responsible threat actors. Empty indictments of individual cybercriminals or governments hasn't worked in the past and similarly will be ineffective in the future. Enforceable international treaties will be a necessity.

Authentication and identity management are the juggernauts that pose the greatest perils to cyber security and promise the greatest payoffs. Mustering the right defences will require new solutions based on big data, cloud computing and heuristic approaches.

Forward-thinking companies are already shifting away from traditional perimeter defences in favour of cloud-enabled cyber security based on real-time analysis of data and user-behaviour patterns. Thinking ahead can help organisations stimulate discussion, explore possible scenarios and develop a strategy for cyber resilience. Doing so will help businesses build a forward-looking cyber security programme that is based on the right balance of technologies, processes and people skills—all supplemented with an ample measure of innovation. With these components in place, organisations are likely to be better prepared for the future of cyber security.

Methodology

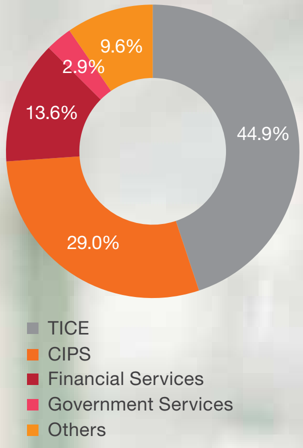
The Indian update of the Global State of Information Security® Survey 2016, which is a worldwide study by PwC, CIO and CSO, was conducted online from 7 May 2015 to 12 June 2015. Readers of CIO, CSO and clients of PwC from around the globe were invited via email to participate in the survey.

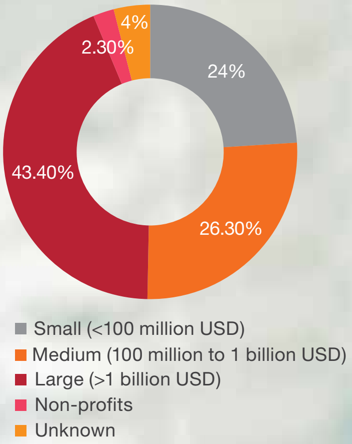
The results discussed in this report are based on the responses of more than 480 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices from across 17 industry sectors in India. The margin of error is less than 1%. All figures and graphics in this report were sourced from the survey results.

The respondents belong to the following four major industry verticals:

- Consumer, industrial products and services (CIPS)
- Technology, information, communications and entertainment (TICE)
- Financial services (FS)
- Government and others

Around 43% of our respondents had annual gross revenues of over 1 billion USD and another 26% (approximately) had revenues between 100 million USD and 1 billion USD. Almost a quarter (24%) of our respondents were small enterprises with annual gross revenues of less than 100 million USD, making it an inclusive survey with a distributed respondent base.





For an overview of global cyber security trends, refer to our global report at www.pwc.com/gsiss

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bangalore, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity in separate lines of service. Please see www.pwc.com/structure for further details.

Contacts

Sivarama Krishnan
Leader, Cyber Security
sivarama.krishnan@in.pwc.com

Siddharth Vishwanath
Partner, Cyber Security
siddharth.vishwanath@in.pwc.com

Vishal Salvi
Partner, Cyber Security
vishal.salvi@in.pwc.com

Balaji Venketeshwar
Executive Director, Cyber Security
balaji.venketeshwar@in.pwc.com

Akkaiah Janagaraj
Director, Cyber Security
akkaiah.janagaraj@in.pwc.com

Amol Bhat
Director, Cyber Security
amol.bhat@in.pwc.com

Manu Dwivedi
Director, Cyber Security
manu.dwivedi@in.pwc.com

Prashant Mehendru
Director, Cyber Security
prashant.mehendru@in.pwc.com

Rahul Aggarwal
Director, Cyber Security
rahul2.aggarwal@in.pwc.com

Sangram Gayal
Director, Cyber Security
sangram.gayal@in.pwc.com

Sundareshwar Krishnamurthy
Director, Cyber Security
sundareshwar.krishnamurthy@in.pwc.com

Tarun Kumar
Director, Cyber Security
tarun.k@in.pwc.com

pwc.in

Data Classification: DC0

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

PD 445 - October 2015 Turnaround and transformation in cyber security.indd
Designed by Corporate Communications, India