pwc

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

CYBER SECURITY INDIA MARKET

What lies beneath

December 2019

Disclaimer

This report has been jointly developed by Data Security Council of India (DSCI) and PricewaterhouseCoopers Private Limited (PwCPL) India.

Data Security Council of India

The information contained herein has been obtained or derived from sources believed by DSCI to be reliable. However, DSCI disclaims all warranties as to the accuracy, completeness or adequacy of such information. DSCI shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof.

The material in this publication is copyrighted. You may not, however, distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without DSCI's written consent.

PwC India

This presentation has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this presentation without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this presentation, and, to the extent permitted by law, PwC, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this presentation or for any decision based on it.

PwC has taken all reasonable steps to ensure that the information contained herein has been obtained from reliable sources and that this publication is accurate and authoritative in all respects. However, this publication is not intended to give legal, tax, accounting or other professional advice. No reader should act on the basis of any information contained in this publication without considering and, if necessary, taking appropriate advice upon their own particular circumstances. If such advice or other expert assistance is required, the services of a competent professional person should be sought.

Foreword

Rama Vedashree
CEO, Data Security
Council of India

Siddharth Vishwanath
Leader, Cyber Security
PwC India

Over half a billion people in India use the internet today, and this number is expected to register double-digit growth in the next few years. Rising internet usage, together with millions of smartphone users and growing mobile data traffic, sets the context for transformational change in the country.

The new generation in India is clearly 'mobile first', with 1.16 billion mobile phone subscriptions[1] and more than 12.3 billion apps being downloaded in 2018[2] alone.

Corporate India is gearing up to meet these growing needs, through its investments in various initiatives and emerging technologies. Realising the several benefits of emerging technologies, the government has also enrolled more than 1.24 billion Indians in its biometric digital identity programme Aadhaar[3], and brought more than 10.3 million businesses under a common digital platform, through the Goods and Services Tax (GST)[4]. The average daily government eTransactions has moved up from 20 million in 2015, to close to 143 million in 2019[5].

In the last few years, cyber criminals have shifted their focus to developing markets like India—which has boarded the digital bandwagon in a big way and where different organisations are at different levels of maturity to fight off cyberattacks. As a result, Indian organisations across sectors are vulnerable to cyber-attacks and there have been reported breaches in the recent past causing concern to both governments and businesses.

Alarmed by these developments, regulatory attention towards cyber security has gradually increased and there is a greater focus on pushing more organisations into adopting the minimum security baseline. While banks have already started feeling the heat after the Reserve Bank of India (RBI) imposed penalties over non-compliance in the last one year, other industries are not far behind. Regulators are taking cues from global headwinds and crafting their cyber security mandates. Both central and state governments have also stepped up their vigil to protect against and respond to breaches.

However, the effect of these three drivers, viz. rapid digitisation, increasing cyber threats and regulatory focus on cyber security, varies widely across sectors and enterprises. Larger and more mature organisations have already undergone the initial grind and have incorporated cyber security as part of their strategic initiatives. Sectors such as energy, healthcare and manufacturing are emerging with their own unique cyber security challenges. Although the demand from these sectors for strong security mechanisms is still catching up, they hold a promising future for cyber security.

We felt this is an opportune moment to understand the domestic cyber security market and the various trends shaping it. This joint study by PwC India and Data Security Council of India (DSCI) gives detailed insights into how the domestic demand for cyber security in India is going to evolve in the next few years and, in effect, shape adoption and implementation of cyber security products and services. We wish to place on record our sincere thanks to several security and business leaders from the Industry, who have significantly contributed to this study.

Table of Contents


SUM

01 EXECUTIVE SUMMARY

Executive Summary

The advancements in technology and its usage have connected people, businesses and organisations in India and brought them closer, leading to economic progress. However, these advancements come with critical vulnerabilities which can be exploited by those who are experts in misusing technology for economic gains. Cyber security breaches across organisations have become commonplace, regularly grabbing headlines that alarm both consumers and leaders. As our reliance on data and interconnectivity swells, developing strong resilience to withstand cyberattacks has never been more important.

Cyber security market in India – driving factors

The cyber security market is crucial to ensuring India's stature as one of the world's leading investment hubs, as well as the security of its major sectors, and is expected to become more pronounced and grow exponentially. This is in part driven by nationwide initiatives such as Digital India, and increasing digitisation of the country's business environment and daily life. According to estimates, the cyber security market in India is expected to grow from **USD 1.97 billion** in **2019** to **USD 3.05 billion** by **2022**, at a compound annual growth rate (CAGR) of **15.6%**—almost one and a half times the global rate.

While many factors are contributing to this high growth rate, the study shows that three factors are significantly driving the cyber security demand market in India—digital growth, increase in cyberattacks and stringent regulatory mandates.

Digital growth necessitating security investments

A favourable demographic dividend and an increasing literacy rate have resulted in an accelerated adoption of digital lifestyle and data consumption. Newer business models and delivery channels have gained wide audience and acceptance—propelled by both public and private sectors. For instance, various citizen services have been digitised by national and state level e-governance initiatives. These, in turn, have resulted in an expansion of cyberattack surface and the need for introducing defence mechanisms at multiple touchpoints, including networks, endpoints, applications, cloud, bots, and internet of things (IoT) environments.

Over 12.3 billion mobile applications were downloaded in India in 2018.[6]

The digital payments' transaction value is estimated to grow at a CAGR of 20.2% from approximately USD 64.8 billion in 2019 to USD 135.2 billion in 2023.[7]

The number of social network users in the country is expected to grow from 326 million in 2018 to 422 million in 2022, second only to China.[8]

47.5 billion national e-transactions have been recorded in 2019, until November.[9]

1.5x

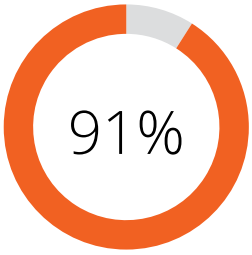
The cyber security market in India is expected to grow at one and a half times the global market growth rate.

Increasing attacks on cyber security systems

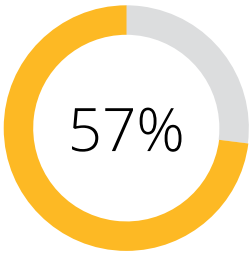
As systems get more interconnected, another significant factor the industry is grappling with is the increasing number of breaches and sophisticated cyberattacks, driven by different motives.

This is evident from the rise in cyberattack incidents reported by the Indian Computer Emergency Response Team (CERT-In)—from 53,081 in 2017 to 2,08,456 in 2018, an increase of about 292%. Network scanning, probing, and vulnerable services accounted for over 61% of these incidents.

The survey also indicates that business executives acknowledged the increasing high stakes on account of these breaches, and hence the need for them to evaluate their digital risk, and focus on building resilience for the same.

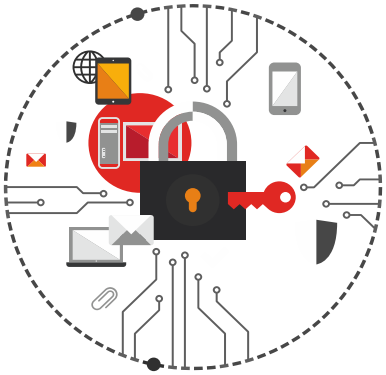


Respondents believe that **Cyber Attacks** will increase in their sector by 2022



Respondents have expressed that **Securing the Cloud** will be top priority by 2022

Threefold increase in cyber security incidents



Reported by CERT-In

Regulatory norms driving security market needs

Owing to the increasing frequency and sophistication of cyberthreats, regulators are beginning to play an active role in formulating directives, tightening regulatory controls and increasing supervisory coverage across sectors.

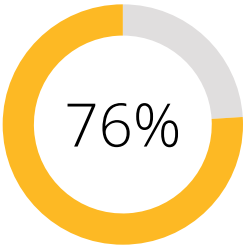
Regulatory institutions are taking cognisance of evolving risks and technological advancements, and integrating these into directives and guidelines. RBI's controls for cloud, multi-factor authentication (MFA) for secure card payments (card-not-present transactions)[10] and the Securities and Exchange Board of India's (SEBI's) cyber resilience framework directives[11] are some examples of such guidelines.

How cyber security products and services are expected to pan out

The study estimates that the market for cyber security products in India will grow at a higher rate than that for services. The existing portfolio of cyber spending will change with products becoming dominant, as organisations invest more in products powered by specialised technologies.

Artificial intelligence (AI) and machine learning (ML) applications are being embedded into the cyber suite of offerings—especially in security intelligence, detection and response (IDR), endpoint security and security testing. The key use cases stem from the ability to use predictive analytics and heuristics in drawing quick statistical inferences, thereby helping in detecting and lessening threats with optimised number of resources and savings. A natural outcome of such developments is the emergence of products and platforms specialising in these areas.

While the products market is estimated to grow at a CAGR of 16.9% over three years and reach USD 1.64 billion by 2022, the market for cyber security services will grow to USD 1.41 billion by 2022, at a CAGR 14.2%.



Respondents believe they don't have adequate budgets to counter cyberthreats, and would need to increase investments in cyber security.

The cyber security products market is estimated to grow faster than the services market.

CAGR of 16.9% over three years

Data protection and endpoint security to see relatively higher growth

In products, data protection and endpoint security tools will grow at a CAGR of 22.2% and 19.1% respectively over 3 years, as compared to the overall category growth rate of 16.9%.

Compliance requirements, risk of reputation loss in case of data breaches, loss of competitive advantage owing to data loss and increasing data volumes are some of the key factors driving investments in **data security and privacy**.

47% of the survey respondents have highlighted data security and privacy as primary areas of concern and investment. Regulations such as the Personal Data Protection Bill of 2018, compliance with the Aadhaar Act and the Digital Information Security and Healthcare Act (DISHA) of 2018 are also being considered as factors driving data security and privacy requirements.

The rising number of connected and mobile devices have created the need to guard the rising number of endpoints having access to critical enterprise data. This, together with rising adoption of IoT and escalating demand for smart devices, is likely to drive the endpoint security market. In most of the breaches, the endpoint has been found to be the most vulnerable weak link and the conduit for the attacks.

Over 34% survey respondents were of the view that there was a need to increase investments in their respective organisations in endpoint security products.

Security IDR will continue to be the most dominant product category, occupying 32% of the product mix characterised by advanced analytics in detection and response capabilities.

Incident response and security testing services slated to be the core engines, fuelling demand for services.

Security testing and incident response continue to grow at a higher rate than rest of the services—at a CAGR of 17.4% and 16.3% respectively over 3 years, as compared to the overall category growth rate of 14.2%.

Given the rapid introduction of features and services for consumers, organisations are realising the need to integrate security testing at every stage of the security development lifecycle. Further, enhanced deployment of IoT devices in industrial systems and exponential increase in consumer IoT will lead to improved focus on security testing.

The fact that some breaches and incidents will happen is a given, and hence despite protection being built in, services revolving around response and resilience capabilities that help an organisation recover quickly from an attack are in high demand. Further, regulatory mandates requiring transparency in reporting security incidents are also driving the market.

Security operations will continue to be the most dominant category, occupying 38% of the service mix driven by prescriptive regulations and the need to strengthen resilience capabilities.

A look at the key sectors

The study estimates that the cyber security market in India will be defined by three key sectors—banking and financial services industry (BFSI), information technology (IT) and information technology enabled services (ITeS), and government. These sectors will constitute 68% of the cyber market share.

01 'Tightening' of regulations in the BFSI sector

02 IT/ITeS organisations handling critical client information from 90+ countries and having to conform to various regulatory and government mandates

03 Government concerns such as attacks from state actors, need to increase citizen awareness and roll-out of smart cities

BFSI sector continues to be the bellwether

There is a plethora of cyber security related action in the BFSI sector in terms of spending, directives by regulators, rapid adoption of technology such as digital payments, peer to peer (P2P) lending platforms and crowdfunding.

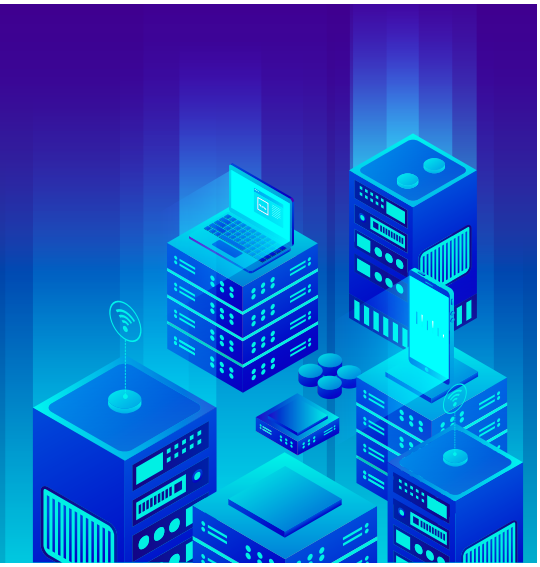
Evolving threats to digital trust arising from increasing interactions with new stakeholders will further drive cyber security demand—for example, third-party digital wallet service providers and cardless payment solution vendors.[12]

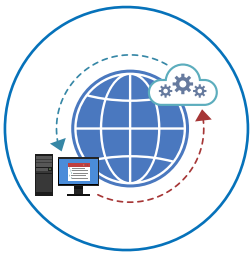
Deployment of security frameworks with adherence to safe transaction principles, implementation of audit log management systems and clear procedures for responding to incidents will come into focus.

The survey also reflects that increased cyberthreats are the core drivers for heightened expenditure in this sector. Over 67% of BFSI respondents cited cyberthreats due to digitisation as the biggest reason for cyber security spending.

Over 64%

of respondents in IT/ ITeS held supply chain related weaknesses responsible for data leakages.





IT/ITeS sector enterprises being targeted as channels to pilfer global client information

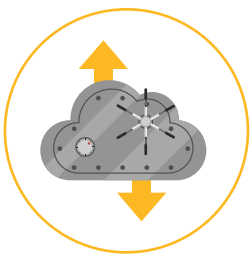
Service organisations that hold valuable client information have become a target of recent cyberattacks. Many of these are caused by targeted or unintended security exposure of client information due to security risks owning to distributed nature of the services supply chain.

The IT/ITeS sector is likely to witness growth in its security spend from USD 434 million in 2019 to USD 713 million by 2022, at a CAGR of 18%.

Thwarting attacks from state actors on government agenda

Significant security spendings in the government sector will revolve around investments in defensive measures to counter threats to critical infrastructure by state actors or external governmental bodies. Creating consumer awareness and smart city initiatives will also drive substantial momentum and investments around cyber security.

The market for cyber security demand from the government sector is expected to reach USD 581 million by 2022, at a growth rate of 13.8% CAGR.



Rapid technology adoption in other sectors increasing cyber security investments

Operational technology and industrial automation are increasingly getting interconnected with IT to meet business requirements. Adoption of smart meters and advanced metering infrastructure, use of drones, virtual reality (VR) and augmented reality (AR) are making it necessary for the sector to be secure.

Recent steps taken by the government, such as launching of the National Health Protection Scheme (Ayushman Bharat), where protecting of healthcare information is crucial, are expected to drive spending on cyber security in this sector.

02 MARKET ANALYSIS

Market Analysis

Key factors driving the growth of the Indian cyber security market

Digitisation is rapidly changing the cyberthreat landscape

India's growth trajectory and the growing influence of Indian enterprises globally, makes it an attractive target for cyber criminals. The large-scale initiatives of the government and corporate India, such as Make in India, Digital India and Skill India, aimed at economic galvanisation and inclusion, have also begun to leverage emerging technologies to create efficiencies and increase reach. Automation in terms of bots, robotics process automation (RPA), AI and ML are driving productivity in services across India.

However, increased adoption of digital technologies has also resulted in multi-fold increase of sensitive information being stored online. Though positive for the economy, these digitisation efforts come with their own set of cyber security risks. While earlier instances of cyberattacks were largely for monetary gain, reasons for attacks now also include reputational damage and power play, further compounded by state actors.

Tightening of regulatory norms

- While cyberattacks are growing and becoming more sophisticated, regulators are taking active note and are not only formulating frameworks and guidelines, but also tightening controls over organisations across different sectors.
- Platforms for interactions between regulatory authorities, industry veterans, academics and businesses have been setup to discuss topical issues and fine-tune the regulations.
- Certain critical sectors are looking at regulations which are beginning to increase the scope of regulations within that particular sector, and are more 'granular' and 'tighter'—e.g. In BFSI sector, existing and upcoming regulations from RBI, SEBI and the Insurance Regulatory and Development Authority of India (IRDAI).
- Global regulations such as General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST) will also continue to have an increasing impact on the Indian market, considering exchange of services and data.
- Increasing regulation is leading to demand for compliance—whether via cyber security products or services—and will further drive the market demand.

Cyberattacks on the rise

India is becoming a vulnerable destination for ransomware attacks.

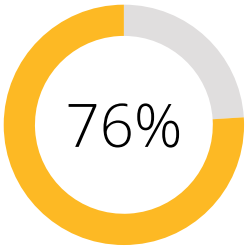
The average cost of a malicious insider attack rose by **15% in 2019 from last year**.

The average cost of a data breach in India has **gone up to INR 119 million,** an increase of 7.9% from 2017.

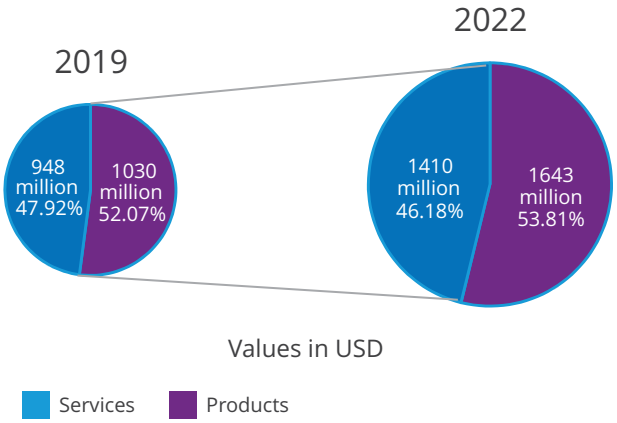
Gradual shift in favour of cyber security products

As per study estimates, the cyber security market in India is expected to grow from USD 1.97 billion in 2019 to USD 3.05 billion by 2022 at a CAGR of 15.6%—almost one and half times the global rate.

- As organisations strive to bring technology and skilled resources together in the most cost-effective way to counter growing cyber security threats, a mix of products and services will contribute to the growing demand within organisations.
- The products segment slightly dominates the overall portfolio in 2019, and it is expected to remain dominant during the forecast period attributable to improved product innovations and prescriptive regulations.
- The study shows an increasing trend amongst organisations to invest in tailored cyber security technology for their specific needs, besides proactively including security as an investment in annual budgets.



Respondents felt current investments in cyber security in their enterprises were inadequate and foresee security budgets increasing in future.



Products and Services

Steady growth is estimated in both the segments, with cyber security products growing at 16.9% CAGR and services at 14.2% CAGR. However with technology innovation, the scale is slightly tilted in favour of cyber security products, which occupy a wider market share as compared to cyber security services.

The study analysis reveals that market contribution of cyber security products to the overall demand will increase from 52% of the mix in 2019 to 54% by 2022.

- Within products, data protection and endpoint security will see relatively higher growth (network security, identity and access management, and security intelligence, detection and response [IDR] make up the rest of the market for this study). The growing popularity of connected devices, bring your own device (BYOD), and IoT technologies is projected to increase impact in the endpoint segment. Regulations and increasing volume of data are driving interest in data security.

- Within services, incident response and security testing are slated to be the core services fuelling demand (security consulting, security implementation and security operations make up the rest of the services pie for this study). Increasing breaches and the need to integrate testing as a significant part of the development lifecycle are anticipated to propel this segment's growth.

03 CYBER SECURITY PRODUCTS

Cyber Security Products

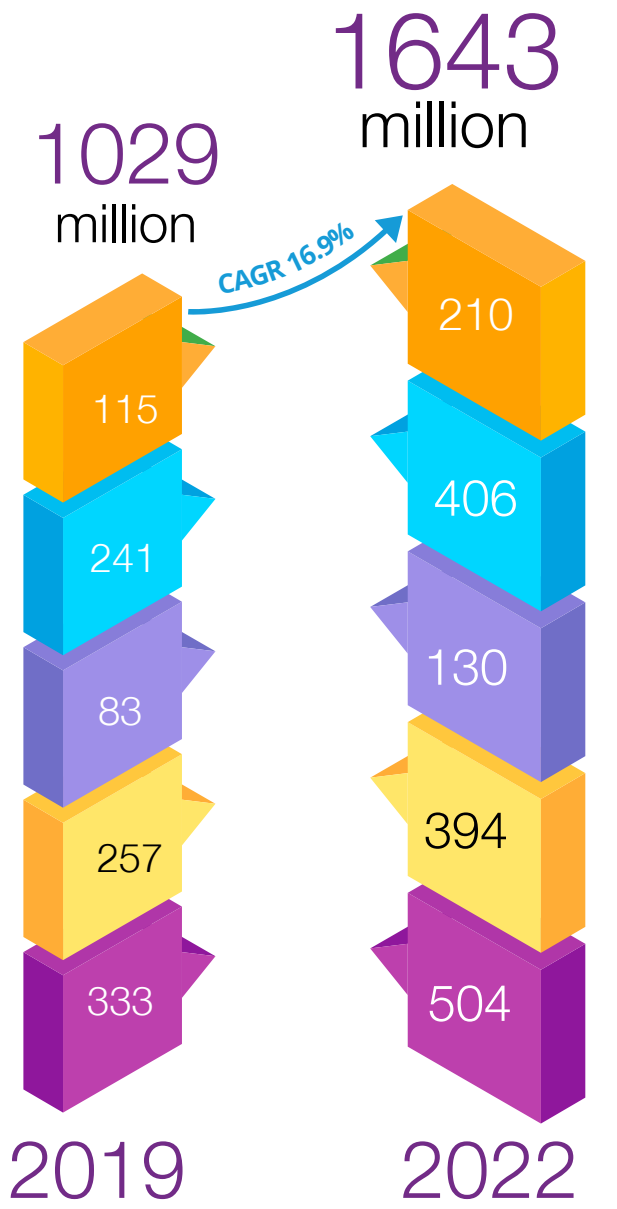
Growth of the Cyber Security products market in India

The cyber security products market in India is expected to grow at a CAGR of 16.9% by 2022. For the purpose of the survey, the cyber security products market has been classified in five categories, viz. data security, endpoint security, network security, identity and access management, and security intelligence detection and response (IDR).

- Data security products are growing at the fastest rate, due to the expected regulatory evolution and focus on security and privacy of data.
- Endpoint security products are also growing faster than the overall market mix for cyber security products. This is largely driven by concern among enterprise executives to safeguard the starting point for most high-profile endpoints.
- Security IDR will continue to be the most dominant product category, occupying 32% of the product mix. This is due to the need for continuous innovation and automation in this space such as, threat intelligence capabilities, integration of governance risk compliance (GRC) capabilities, user behaviour analytics, use of big data and statistics to facilitate quick incident response.

Growth of the Cyber Security products market in India

Products consumption (in USD million)



Products	Growth Rate
01 Data security	22.2%
02 Endpoint security	19.1%
03 Identity and access management	16.3%
04 Network security	15.3%
05 Security IDR	14.8%

Data security products: Growth fuelled by emphasis on privacy and confidentiality

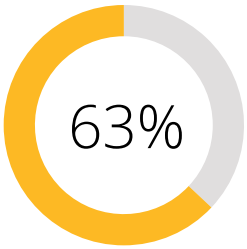
It is expected that the data security products market in India will increase from **USD 115** million in 2019 to **USD 210** million in 2022 at a CAGR of **22.2%.**

Data security products include encryption, tokenisation, data masking, data loss prevention, information rights management, file and data access monitoring.

- With number of digital services increasing, both volume and value of data produced is increasing exponentially. For example, as per a recent RBI report, digital transactions in India grew in value by 19.5% and the volume by 58.8% in 2018-19.[13]
- Regulatory requirements are becoming stringent, as can be seen in the forms of the Personal Data Protection Bill,[14] the Aadhaar Act,[15] and DISHA (Healthcare),[16] the updated IT Act,[17] among others. This will result in enterprises investing more in areas such as data discovery, data lifecycle management and cryptography, as organisations will have to put in more efforts to comply with regulatory norms, which can be automated using cyber security products..

Traditionally, data security measures have focused on encryption, masking and leakage prevention based on static set of rules. In future, we will see ML based dynamic data breach reporting and response capabilities. The future of data protection expenditure will comprise:

- increasing demand for context aware data security controls
- focusing on categorisation, classification and analysis of data access permission due to growth of unstructured data growing across organisations.



Respondents saw data security and privacy as primary areas of concern and investment.

Attacks leveraging endpoints are increasing rapidly.

Endpoint security products prioritised after script-based attacks on end users

It is expected that the endpoint security products market in India will increase from USD 241 million in 2019 to USD 406 million in 2022 at a CAGR of 19.1%.

With rapid digitisation, and high number of smartphone (340 million in 2018)[18] and internet users (525 million in 2019)[19], the number of endpoints have also increased.

Attacks against endpoints are rapidly increasing, especially in the form of script based attacks such as powershell attacks (increased by over 1000%)[20] and file less malwares.

With growing BYOD (bring your own device) ecosystems, the focus has increased on native hardening and monitoring of endpoints, rather than enterprises controlling system security through the backend. 15% of the survey respondents said they were looking to improve visibility and response to cyberattacks, through automated endpoint detection and response solutions.

The endpoint security

market is made up of products such as anti-virus and anti-spam software, host intrusion prevention software (HIPS), exploit protection, behavioural analysis of memory and continuous monitoring.

Traditionally, endpoint solutions have focused only on protection mechanisms. In future, there will be a strong focus on automated response.

- Signature-based protection mechanisms are now making way for endpoint security solutions, which are at present based mostly on trial and error methods.
- Organisations now want to detect endpoint attacks in real-time and quarantine the endpoints. For these reasons, endpoint detection and response (EDR) solutions will gain further prominence.
- Gradual shift to integrated security products, that include multiple endpoint security tools in a single, centrally managed package such as anti-virus, anti-spyware, algorithmic behavioural analysis, desktop firewall and HIPS.

Network security products are in focus as more organisations adopt digital technologies

It is estimated that the market for network security products in India will increase from **USD 257 million** in 2019 to **USD 394 million** in 2022, at a CAGR of **15.3%**.

- The number of network devices in India is expected to reach 2 billion by 2021. Similarly, network devices per user is predicted to be 1.5 by 2021.[21]
- Machine-to-machine (M2M) modules of information exchange will account for 22% (445 million) of all networked devices in 2021, growing at a CAGR of 21.1%.[22]
- CERT-In handled 1,27,481[23] security incidents (61% of total incidents) in 2018 due to network scanning/ probing/vulnerable services.
- Organisations are expected to allocate at least 20% of their overall cyber security budget for network security.

Network security

is defined as security measures undertaken by implementing a combination of software, hardware, and networking technologies such as firewall, unified threat management, network intrusion detection and prevention, virtual private network (VPN), content inspection, web content security.

Demand of enterprises for security solutions catering to complex hybrid models covering both on-premise systems and on cloud services, is on the rise. This makes it more important for network security controls to transcend into and between boundaries of physical systems and cloud services.

- With growing digitisation of businesses, more users, devices, applications, services and data are located outside of an enterprise than inside.
- Adoption of zero-trust architecture by enterprises by implementing strategies such as micro-segmentation and ML capabilities, using concepts such as software defined security architecture to manage and operate.

Identity management

is a suite of solutions related to user and device identities.

The importance of IAM products for a strong security framework

It is expected that the market for identity and access management (IAM) products in India will increase from **USD 83** million in 2019 to **USD 130** million in 2022, at a CAGR of **16.3%**.

- 30% of survey respondents are looking to increase their expenditure in the IAM segment with proliferation of IoT devices and edge computing capabilities.
- With increasing M2M interactions, managing non-human identities has become crucial for many organisations. Further, with federated identities becoming a norm, IAM products are expected to utilise mobile and cloud computing technologies to manage the new identities.

Many enterprises are using context-based identity management, coupled with AI, to reduce risks of fraudulent access

Whereas traditional adaptive authentication was rule-based, the next generation of adaptive access services combine rules with ML and advanced analytics

Identity analytics, especially user and behavioural analytics is expected to witness a convergence with security information and event management (SIEM)/security orchestration, automation and response (SOAR) platforms for managing risks.

Increase in the number of IoT devices will see shifting of security functions to trusted gateways, as many such devices will not have the adequate processing power or sophistication to support high-trust authentication or secure device communication.

Cyber resilience and the rising demand for IDR products

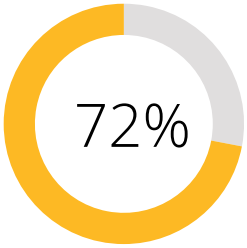
It is expected that the market for intelligence detection and response (IDR) products in India will increase from **USD 333** million in 2019 to **USD 504** million in 2022, at a CAGR of **14.8%**.

Quick reporting of breaches in cyber security, and compliance requirements mandated by regulators are pushing organisations to respond quickly after a breach is detected.

Shortage of staff skilled in handling cyber security is compelling organisations to use automation and orchestration to strengthen security systems

Organisations are expected to move towards using self-healing systems with:

- **Advanced intelligence**
- **Automating and orchestrating the response to a security breach**
- **ML-based use cases as opposed to rule-based use cases**



Respondents were looking to increase expenditure in the security IDR category.

Security IDR

includes a variety of product categories such as SIEM, threat analytics, forensics, vulnerability management among others.


CYBER
SECURITY
50%
50%
STEP 01
STEP 02
70%
20%
90%

04 CYBER SECURITY SERVICES

Cyber Security Services

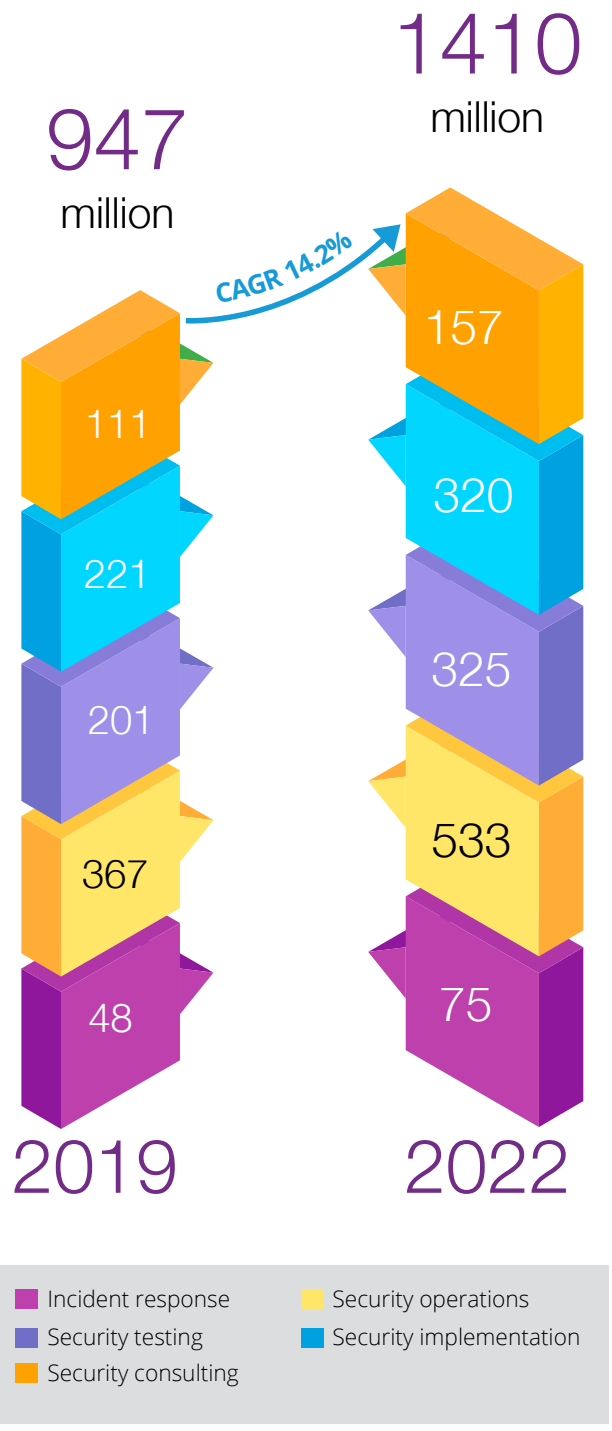
Security testing and incident response to lead growth in demand for cyber security services

The cyber security services market has been classified in five categories for clearer understanding, viz. security consulting, security implementation, security testing, security operations and incident response:

- Security testing is expected to grow at the fastest rate due to rapid digitisation, increase in the number of connected devices and increased integration between information technology and operational technology.
- Incident response related services are growing due to increase in number and complexity of security breaches. Organisations proactively resort to cyber forensics to address vulnerabilities in security systems, post a breach.
- Security operations continues to be the most dominant service category, occupying 38% of the service mix. Organisations are investing in services for visualizing new threats, monitoring them continuously, adhering to compliance guidelines and defusing potential breach incidents in the consistently widening zone of cyberthreats.

Security testing and incident response to lead growth in demand for cyber security services

Services consumption (in USD million)



Services	Growth Rate
01 Security consulting	12.2%
02 Security implementation	13.2%
03 Security testing	17.4%
04 Security operations	13.3%
05 Incident response	16.3%

Security consulting to help digitising businesses draw effective risk management plans

Security consulting services are expected to grow at a CAGR of **12.2%** over 3 years to become a market worth **USD 157** million by 2022.

- New technology-led business models and increasing digitisation means a broader surface for potential cyberthreats, requiring enhanced cyber risk management.
- Adoption of emerging technologies such as cloud, chatbots, RPA, blockchain would result in organisations spending more on security consulting.
- More enterprise boards and senior management are expected to actively consider cyber security risks, leading to the need for structured assessments and benchmarking.
- Increased focus on cyber security awareness and training by both government and private enterprises. As per our survey respondents, 14% budget of cyber security consulting services has been allocated to security awareness and training.

Security consulting services are expected to see a gradual shift from ‘optimising existing security’ to ‘distribute and virtualise security’, as more organisations adopt cloud/virtual environments and extended ecosystems, such as third-party suppliers and vendors

Security awareness and training delivery mechanisms will see a drift from classroom and web-based training modules to more interactive ones, such as gamification, simulations and on-demand training.

- 55% respondents said that by 2022, they will adopt gamification as a preferred mode for training people on security awareness.

Drawing up effective cyber security strategies depend on successful security implementation

The security implementation services market in India is estimated to increase from **221** million in 2019 to **USD 320** million by 2022, at a CAGR of **13.2%**.

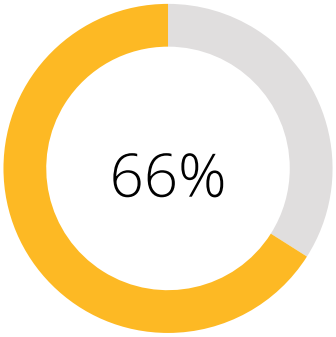
- Growth of cyber security implementation service is directly related to the increased adoption of cyber security products. By 2022, the security products market is expected to grow at a CAGR of 16.9%.
- Tightened regulatory restrictions with rigid controls will also increase the demand for security implementation. For example, the RBI Cyber Security framework asked banks in 2016 to set up and operationalise Security Operations Centers (SOCs), to monitor and manage cyber risks in real time, and ensure additional authentication for card-not-present (CNP) transactions.[24]

Traditionally, security implementation centered around a plug and play model, where security issues for a device mattered once they were plugged in. However, security implementations are getting increasingly complex given the interplay between hybrid environments such as public and private cloud services, increasing configurations, need to accommodate user context and integration of AI and ML technologies.

- Implementation pedagogy will experience a shift from 'trust but verify' to 'never trust, always verify' (following the zero trust security model) due to:
  - organisation perimeters continuously getting blurred with extended ecosystems and changing business models
  - concerns arising out of trustworthiness of internal data traffic.

The security implementation

market involves services such as information security architecture design, deployment and support for hardware and software, integration and subsequent functional and performance testing.



Respondents were looking to increase expenditure on security implementation services by 2022.

Security testing is one of the fastest growing services as organisations want to prevent attacks on their systems

The security testing services market includes penetration testing, web testing, application security, audits and reviews.

It is estimated that the security testing services market in India would increase from **USD 201** million in 2019 to **USD 325** million by 2022, at a CAGR of **17.4%**. Security testing services will comprise **23%** of the services market share, as against **21%** share in 2019.

01

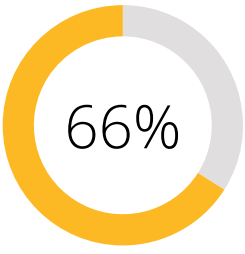
Connected devices and rapid increase of IoT requires better security testing of the same. According to a NASSCOM report, the number of IoT devices in India are expected to reach 1.9 billion by 2020.[25]

02

Stringent regulatory mandates related to cyber security have made it essential for organisations to invest in security testing. The RBI started this regulatory practice and more regulations across industries are expected.

03

Businesses are expected to plan spending a significant share in performing Red/Blue and Purple team assessments to test detection and response capabilities of security systems.



Respondents will prefer to outsource security testing services by 2022.

Security testing is expected to transform into a highly automated service, operating in real-time, with latest intelligence capabilities of threat detection, and perhaps equipped with self-healing capabilities.

DevSecOps and agile security testing were cited as emerging trends by the survey respondents

There is an increased expectation to minimise the window of exploiting security vulnerabilities.

Coders rely heavily on open source platforms for security testing.

Digital businesses require a shorter cycle of healing from cyberattacks.

Security operations to remain the largest amongst cyber security services

It is expected that the security operations market in India will grow from **USD 367** million in 2019 to **USD 533** million by 2022, at a CAGR of **13.3%** and occupy **38%** of India's cyber security services market.

- Cyberattacks have evolved and increased in volume over the years. Attacks have become sophisticated in nature and types of attacks such as APT, Zero Day, malwares, multi-vector attacks have become common, targeting core infrastructure such as ATM switches, payment interfaces.
- Increased expectation from security systems to reduce response time, contain and remediate security incidents. For example, ransomware, is a threat that can get exponentially worse with time.
- 37% of respondents said that they will increase their spend on security operations services to stop loss of intellectual property, frauds, leakage of customer data and other sensitive information.
- Niche security technologies are looking to automate repeatable tasks, streamline workflows and orchestrate security tasks due to shortage of staff.

From a 'keeping the lights on' point of view, security operations will increasingly get automated. However, security services will focus on advanced threat detection and response capabilities.

With the use of AI becoming more prominent, the focus will move from passive monitoring of threats to active neutralising of threats.

Security operations services involve managing and monitoring the configuration and health of security devices.

Effective incident response is the key to effective cyber security in the era of inevitable cyber breaches

The incident response and forensics services space in India is expected to grow from **USD 48** million in 2019 to **USD 75** million by 2022, at a CAGR of **16.3%**.

- Nearly 77% of the respondents were looking to increase their expenditure in the areas of cyber forensics and incident response.
- There was a threefold increase in reported cyber incidents (as per CERT-In) last year and cyberattack trends suggest further increase in such incidents, fuelling the need for enhanced incident response services.[26]
- With technology landscape becoming more complex and varied, there is an increased focus on investigation of digital breaches and preservation of evidence.
- There is an increasing need to follow due regulations while reporting security breaches – for example, making it mandatory for data fiduciary in case of personal data breach.[27]
- Organisations are looking at ensuring they have an active retainership arrangement for incident response services.
- More organisations are expected to engage on compromise detection to proactively identify breaches.

Incident response capabilities are expected to evolve from merely analysing the root cause of an incident to a holistic business response including precaution, prevention and self-healing and to go further as a service model because of the intensity of cyberattacks, which require highly trained teams to respond at short notices.

The incident response market involves areas such as incident management, digital forensics, evidence capturing and breach reporting.


ONLINE:USER A
08:54:30
VOICE FEED:NETWORK:12.38.73
Profits:
ANALYTICS
Evolution:
SECURITY
Actual vs Target
Data Availa
KPI:Produc
FRONT-CAMERA-IP:143.453.
01:43:55
ADDRESS:
Market Share
TIME-DATE 00:38:29
Customers Sa

05 SECTORAL ANALYSIS

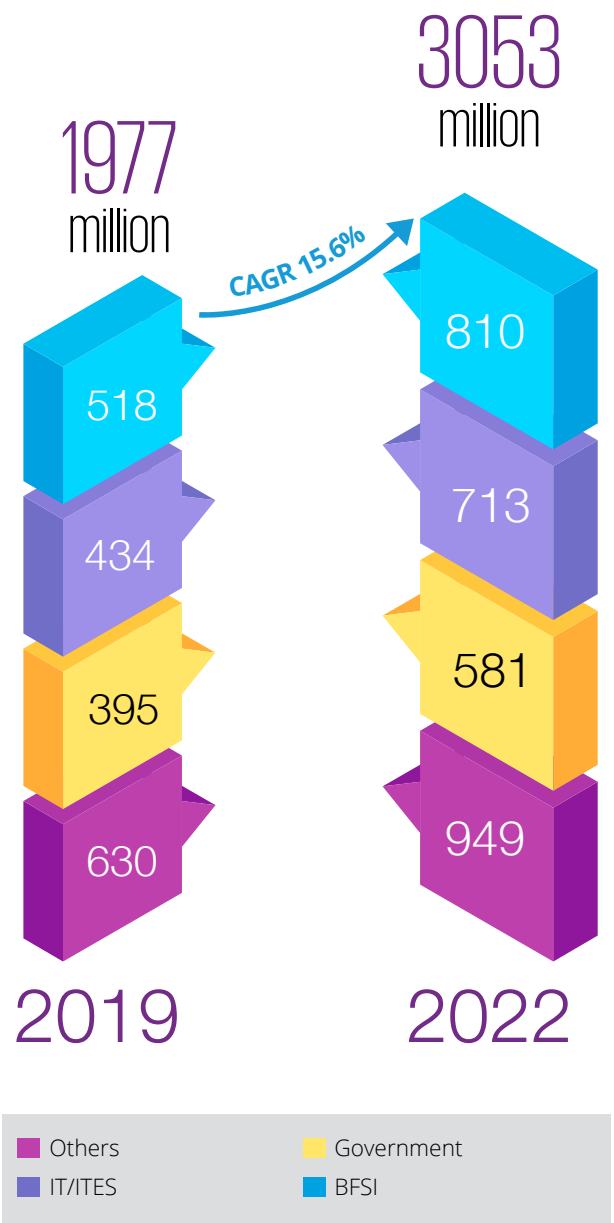
Sectoral Analysis

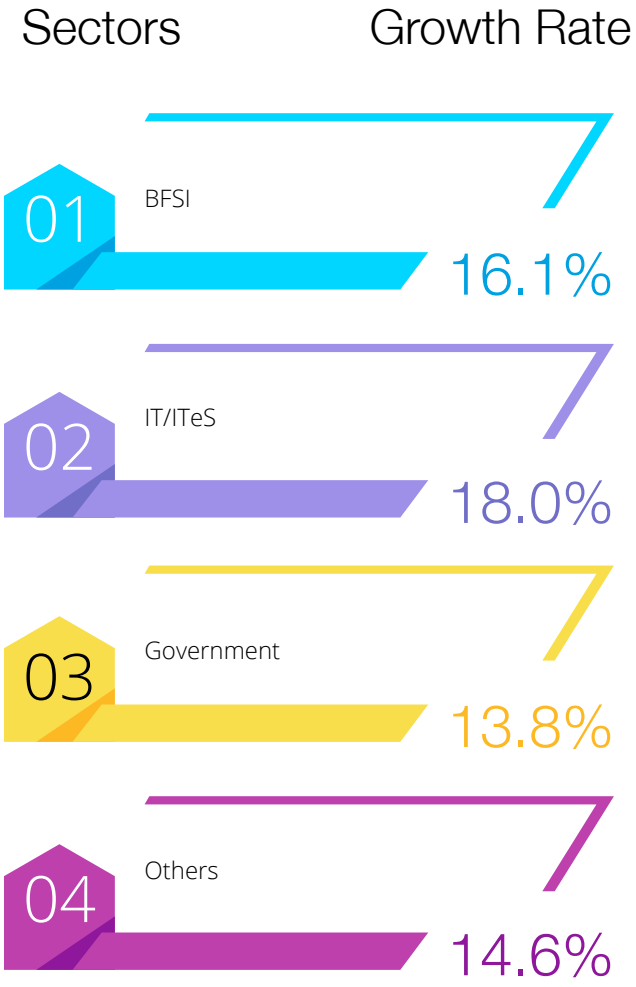
BFSI, IT/ITeS and Government are the top 3 sectors with the largest market share in cyber security expenditure in India

- The survey looked at the following sectors, viz. BFSI, IT and ITeS, government and others.
- The BFSI sector's expenditure on cyber security is driven by adherence to regulatory norms, rapid adoption of technology in services and increased cyberthreats. BFSI, with 26% share has the largest cyber security expenditure.
- IT/ITeS organisations store plethora of valuable client information and are hence targeted by cyber hackers. Many of these are caused by targeted or unintended security exposure of client information due to security risks owning to distributed nature of the services supply chain.. This sector grew the fastest at a CAGR of 18%.
- Significant security spending in the government sector will revolve around investments in defensive measures to counter threats by state actors to critical infrastructure. Digitisation of citizen services, creating consumer awareness and smart city initiatives, which are bound to utilise technological innovations, will also drive substantial momentum and investments around cyber security.
- Other sectors apart from the three mentioned above include energy, healthcare and automobile.

BFSI, IT/ITeS and Government are the top 3 sectors with the largest market share in cyber security expenditure in India

Sectoral segmentation (in USD million)





The importance of India's BFSI sector makes it a prime target for hackers

The BFSI sector accounts for **26%** of the total expenditure in the cyber security market. The sector is expected to increase its expenditure to **USD 810** million from the existing **USD 518** million by 2022, at a CAGR of **16.1%**. The growth can be attributed to several factors such as tightened directives from regulators, rapid adoption of technologies like digital lending, utility payments, e-commerce, online insurance marketplaces and mobile banking—to drive operational efficiency and customer convenience.

Digital disruption has forced companies to take a look at their digital strategies.

- Digital payments in India will increase from USD 64.8 billion in 2019 to USD 135.2 billion in 2023, at a CAGR of 20.2%.[28]
- Innovation in payments technology using AI, blockchain, IoT and real-time payments, and the introduction of mobile point of sale (POS) devices has also contributed to the growth of potential security risks.

The nature of services provided by the BFSI sector has resulted in the sector being governed by detailed prescriptive guidelines and regulations.

- Regulations are becoming 'granular' and 'tighter' and at the same time, more segments of regulations are coming into the ambit.
- Risks due to usage of legacy systems and applications remain high, but regulators are also considering risks being brought by emerging technologies to the BFSI sector.
- Increased enforcement of cyber security laws and rules. For example, between January and February 2019, the RBI levied stringent fines (USD ~10.16 million) on 36 public, private and foreign banks for non-compliance with cyber security rules.[29]

Evolution of attacks

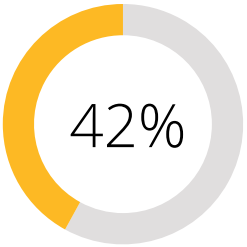
2006	2014	2018
Banking trojans (ZeuS, Dridex, Shylock)	ATM network attacks (Carbanak malware)	SWIFT payment attacks (Lazarus)

Cyberattacks in the BFSI sector have evolved from merely being about cyber crime to efforts in crippling the economy.

- Sophistication of cyberattacks are increasing as financial institutions (FIs) continue to learn and bounce back from less sophisticated attacks.
- Hackers are exploring new attack channels and deploying multi-vector attacks.
- In-order to maximise returns from cyberattacks, hackers are increasingly targeting 'core banking systems'.

Threats and awareness on privacy are driving the demand for cyber security in the IT and ITeS sector

The cyber security spend in the IT/ITeS sector is expected to grow from **USD 434** million in 2019 to **USD 713** million by 2022, at a CAGR of **18%** – the highest among all sectors.



Respondents felt cyber incidents in IT/ITeS sector were caused due to weak access control mechanisms.

Cyber threats have become a major challenge in the IT/ITeS sector as:

- Adversaries are targeting IT and software supply chains to infiltrate into secured corporate perimeters, exploiting vulnerabilities in open source components utilised during system development.
- Hackers are targeting this sector to get access to the ecosystem of global clients they serve.
- Besides a dent in their reputation due to exposure of client data, IT and ITeS organisations also stand the risk of facing backlash from multiple global regulations such as General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).

The IT/ITeS sector is witnessing increased awareness on user privacy and is preparing for further regulations on data privacy. For example, the forthcoming legislation on the Personal Data Protection Act in India is expected to be further in favour of personal data protection.

It is estimated that by 2021, there will be **1.5** networked devices per individual.[30] With the IT sector being one of the largest employers globally, there is a huge upsurge expected in the number of end points, which have lately been identified as the most vulnerable point of entry for cyberattacks.

Government's push for cyber security is largely driven by the Digital India initiatives

The cyber security market in the government sector is estimated to grow from **USD 395** million in 2019 to **USD 581** million by 2022, at a CAGR of **13.8%**. This growth is primarily driven by increased focus on digitisation of government systems and rising cyberattacks on critical state infrastructure.

Digital delivery of services is transforming the way citizens interact with the government. Some of the major digital services provided by the Government of India are:

- More than 275 government services are leveraging 1.24 billion Aadhaar enrolments[31] to provide benefits to citizens. Digital inclusion has been enhanced with 337 million Jan Dhan accounts[32] and 93 million health insurances already linked to Aadhaar.
- 3.12 lakh Common Service Centres (CSCs) have been established to bring e-services (such as Permanent Account Number [PAN], passport services, etc.) to the doorstep.[33]
- The smart cities project is using technology to improve the ease of living of citizens through smart water management, smart waste management, smart traffic management, smart command and control centre to name a few.

The government sector is one of the most attacked sectors globally.

The threat landscape is now changing from defacement of websites to attacks on critical state infrastructure from state actors to destabilise the country.

- The threat spectrum in the government sector is very wide, ranging from state actors motivated to wage cyber wars to hacktivists pushing their own agenda.
- The government is highly prone to cyber espionage as adversaries are not just aiming to obtain state secrets, but also access citizens' personal data.
- Cyberattacks can hurt the economy, derailing India from its projected growth trajectory and worsen relations with our neighbours.

Government's strong commitment to cyber security is resulting in prescriptive mandates and guidelines. Some steps taken by the government to address cyber security issues are:

- Formulating new regulations related to cyber security such as a new National Cyber Security Policy, the updated IT Act, the Personal Data Protection Bill, the Digital Information Security in Healthcare Act (DISHA).
- The Ministry of Electronics and Information Technology (MeitY) asking all ministries to spend 10% of their IT budgets on cyber security and suggesting the appointment of Chief Information Security Officers (CISOs) in each ministry.[34]
- Steps taken by state governments to strengthen their security setup, including mandates such as CISO appointment, defined security budget, security monitoring.

Healthcare and energy are two sectors likely to fuel the growth driven by need for privacy and safety

The cyber security spend in other sectors is expected to grow from **USD 630** million in 2019 to **USD 949** million by 2022, at a CAGR of **14.6%**. The major sectors under this ambit include energy, healthcare and automotive. This growth can be attributed to rapid adoption of emerging digital technologies, increased cyberthreats and upcoming regulations.

Globally, the healthcare sector is one of the key sectors and second only to BFSI in driving the cyber security market. In India, the sector has not been primarily targeted by hackers, so far. However, the recent developments with regard to use of technology are expected to increase demand of cyber security safeguards in the sector.

- Schemes such as Ayushman Bharat have kickstarted the digitisation of health records. Under the scheme, more than 67.5 million e-cards have been issued so far.[35]
- The government is in the process of formalising the Digital Information Security in Healthcare Act (DISHA) and has already released a draft version for the same. The Act will promote and adopt e-health standards, as well as enforce security and privacy measures for the electronic health data.

India is on the cusp of digital health transformation, which in turn will increase the threat landscape, driving expenditure on cyber security in this sector.

Energy is another key sector (including oil and gas, power and utilities) in which cyber security expenditure is expected to increase. Some of the areas in the energy sector where use of technology and cyberthreats are growing are:

- Adoption of smart meters, advanced metering infrastructure and decentralised renewable generation (DER) are increasing the attack surface for data theft, fraud, tampering and man-in the middle (MITM) attacks.
- Use of drones to track vast pipeline networks in order to detect leakages has reduced the clean-up cost, but also opened the sector to newer forms of attacks. Additionally, increased usage of virtual reality and augmented reality is increasing the threat landscape for the energy sector.

The Ministry of Power has mandated a CISO position for all utilities, released as per Indian Standard IS 16335 (Security Standard for Power Systems). The Ministry has also notified information sharing and directed relevant bodies to set up analysis centres. The Central Electricity Authority (CEA) is developing a cyber security manual for auditing power utilities.

The automotive industry is facing an inflection point—as risks for cyber security, privacy and safety will increase with internet connectivity in the sector and automotive products becoming commonplace.

- Developments in automobiles, such as the emergence of connected cars (internet-enabled) and predictive maintenance (using telematics), are only expanding the cyberthreat surface.
- Mobility as a service (rise of shared cabs) is collecting data about drivers, passengers, destinations and routes, thereby leading to increased concerns on privacy.

The automobile ecosystem has used technology to transform into an integrated supply chain. On one hand, this has helped in reducing cycle time and improving rate of manufacturing; on the other, it has also resulted in increased threat for intellectual property rights (IPR).


FILE
EDIT
SELECT
START
FINISH

Appendix

Study approach

The study aims to understand the current and future size of India's cyber security market. As part of our approach towards the study, we have looked at the market from a demand standpoint, focusing on cyber security products and cyber security services. We undertook a primary survey of enterprises across sectors. This was complemented with interviews of cyber security experts and secondary research.

We looked into the priorities of stakeholders (CIOs, CISOs, technology heads, to name a few), along with what drives the need to have effective cyber security mechanisms in different sectors. Our survey covered 100+ organisations, with one-third of them being followed with interviews. Some of the key areas studied in the survey are listed here:

Areas

- **Digitisation**
- **Threat quotient**
- **Cyber preparedness**
- **Regulatory stringency**
- **Security spending**

- Drivers of cyber security requirements, top priorities and key challenges
- Current cyber security position and future expectations
- Trends for cyber security services and products

Glossary

AI	Artificial Intelligence
IDR	Intelligence, Detection and Response
APT	Advanced Persistent Threat
BFSI	Banking Financial Services and Insurance
BYOD	Bring Your Own Device
CISO	Chief Information Security Officer
CAGR	Compound Annual Growth Rate
CBS	Core Banking Solutions
CEA	Central Electricity Authority
CERT-In	Indian Computer Emergency Response Team
DDoS	Distributed Denial of Service
DISHA	Digital Information Security Health Care Act
DRG	Decentralised Renewable Generation
GDPR	General Data Protection Regulation
IoT	Internet of Things
IPR	Intellectual Property Rights
IRDAI	Insurance Regulatory and Development Authority of India
IT-ITeS	Information Technology – Information Technology enabled Services
ML	Machine Learning
m-PoS	Mobile Point of Sale
OTP	One Time Password
PAN	Permanent Account Number
RBI	Reserve Bank of India
SEBI	Securities and Exchange Board of India
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UCB	Urban Cooperative Bank
USD	United States dollar

References

Sn. no.	Source
1	TRAI (https://main.trai.gov.in/sites/default/files/PR_No.74of2019.pdf)
2	'Digital India - Technology to transform a connected nation' by McKinsey Global Institute (March, 2019) (https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf)
3	'Aadhaar' (https://uidai.gov.in/)
4	'Digital India - Technology to transform a connected nation' by McKinsey Global Institute (March, 2019) (https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf)
5	Etaal – Electronic Transaction Aggregation & Analysis Layer (http://etaal.gov.in/etaal/YearlyChartIndex.aspx)
6	'Digital India - Technology to transform a connected nation' by McKinsey Global Institute (March, 2019) (https://meity.gov.in/writereaddata/files/india_trillion-dollar_digital_opportunity.pdf)
7	'Emerging technologies disrupting the financial sector' by Assocham-PwC (May 2019) (https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/emerging-technologies-disrupting-the-financial-sector.pdf)
8	'Number of social network users in India' by Statista (23 September, 2019) (https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/)
9	Etaal – Electronic Transaction Aggregation & Analysis Layer (http://etaal.gov.in/etaal/YearlyChartIndex.aspx)
10	RBI on Multifactor Authentication, (6 December 2016) (https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=10766&Mode=0)
11	SEBI - Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants (https://www.sebi.gov.in/legal/circulars/dec-2018/cyber-security-and-cyber-resilience-framework-for-stock-brokers-depository-participants_41215.html)
12	RBI 'Report of the Working Group on FinTech and Digital Banking' (pg 71) (https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF)
13	RBI: Payment and Settlement: The Plumbing in the Architecture of India's Financial System (11 June 2019) (https://m.rbi.org.in/Scripts/BS_ViewBulletin.aspx?Id=18290)
14	The Personal Data Protection Bill 2018 (https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf)
15	The Aadhaar Act (https://www.uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf)
16	Digital Information Security in Healthcare Act 2018 (DISHA) (https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf)
17	The Information Technology Act 2000 (Amendment 2008) (http://nagapol.gov.in/PDF/IT%20Act%20(Amendments)2008.pdf)
18	Forecast for smartphones (https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/)
19	Forecast for number of internet users in India (https://www.statista.com/statistics/255146/number-of-internet-users-in-india/)
20	Symantec's 2019 Internet Security Threat Report (https://www.symantec.com/security-center/threat-report)
21	CISCO's VNI (https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/India_2021_Forecast_Highlights.pdf)
22	CISCO's VNI (https://www.cisco.com/c/dam/m/en_us/solutions/service-provider/vni-forecast-highlights/pdf/India_2021_Forecast_Highlights.pdf)
23	Annual Report (2018), CERT-In (https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2019-0123.pdf)

Sn. no.	Source
24	RBI's 'Cyber Security Framework in Banks' (2 June, 2016) (https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF)
25	IoT: Landscape and NASSCOM Initiatives by NASSCOM (May 2017) (https://www.wfeo.org/wp-content/uploads/stc-information/L3-IoT_Landscape-by-S_Malhotra.pdf)
26	Annual Report (2018), CERT-In (https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2019-0123.pdf)
27	The Personal Data Protection Bill 2018 (https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf)
28	Emerging technologies disrupting the financial sector (May 2019) (https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/publications/emerging-technologies-disrupting-the-financial-sector.pdf)
29	RBI slaps penalty on 36 banks, (9 March, 2019) (https://economictimes.indiatimes.com/news/economy/finance/rbi-slaps-penalty-on-36-banks-for-swift-non-compliance/articleshow/68328956.cms?from=mdr)
30	CISCO's VNI (https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/1213-business-services-ckn.pdf)
31	UIDAI (https://uidai.gov.in/)
32	PM Jan Dhan Yojana (https://www.pmjdy.gov.in/)
33	Common Service Centers (CSCs) (https://www.csc.gov.in/)
34	Ministries must spend 10% of IT budget on Cybersecurity: MeitY (September 2017) (https://tech.economictimes.indiatimes.com/news/internet/ministries-must-spend-10-of-it-budget-on-cybersecurity-meity/60333964)
35	Ayushman Bharat, Pradhan Mantri Jan Arogya Yojana (https://www.pmjay.gov.in/)

Acknowledgement

We would like to acknowledge the efforts of various core members from BFSI, IT/ITeS, Government, Energy, Healthcare, Manufacturing and Automotive sectors who provided their valuable inputs and guidance throughout the study.

On behalf of DSCI and PwC India, we would like to express our gratitude to all the individuals and firms for their valuable time and insights without which this report would not have been possible.

About the Authors

This report has been co-authored by Manishree Bhattacharya, Shubham Agarwal, Venkatakrishnan Iyer and Abhishek Bansal. The development of the overall report has been mentored by Rama Vedashree and Siddharth Vishwanath.

Siddharth Vishwanath is leader of the Cyber Security practice at PwC India. **Venkatakrishnan Iyer** is Director of Cyber Security practice at PwC India and **Abhishek Bansal** was formerly associated with PwC India as an Associate Director of Cyber Security practice.

Rama Vedashree is the CEO of Data Security Council of India (DSCI). **Manishree Bhattacharya** is Manager Research at DSCI and **Shubham Agarwal** was formerly associated with DSCI as a fellow.

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 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, Bengaluru, Bhopal, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai, Pune and Raipur. For more information about PwC India's service offerings, visit www.pwc.in

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

Data Security Council of India (DSCI) is a premier industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

For more information, visit: www.dsci.in

DATA SECURITY COUNCIL OF INDIA

NASSCOM CAMPUS, 3rd Floor, Plot. No. 7-10, Sector 126, Noida, UP - 201303

For any queries contact

P: +91-120-4990253 | E: info@dsci.in | W: www.dsci.in

DSCI_Connect dsci.connect dsci.connect

data-security-council-of-india dscivideo

yuktiprints@gmail.com