KALINGA UNIVERSITY

BUSINESS PLAN TEMPLATE

Name of all the participants	01 DILSHAD AHMAD 02 MEGHAL PANDEY 03 ADRITA PATHAK 04 ANMOL KUMAR GUPTA
Email Address to contact	Dilshadahmad8877@outlook.com
Contact Nos.	8877623200
Name of School/ College	Asansol Engineering college
Program Name and Semester	B.Tech (5^{th} Sem)

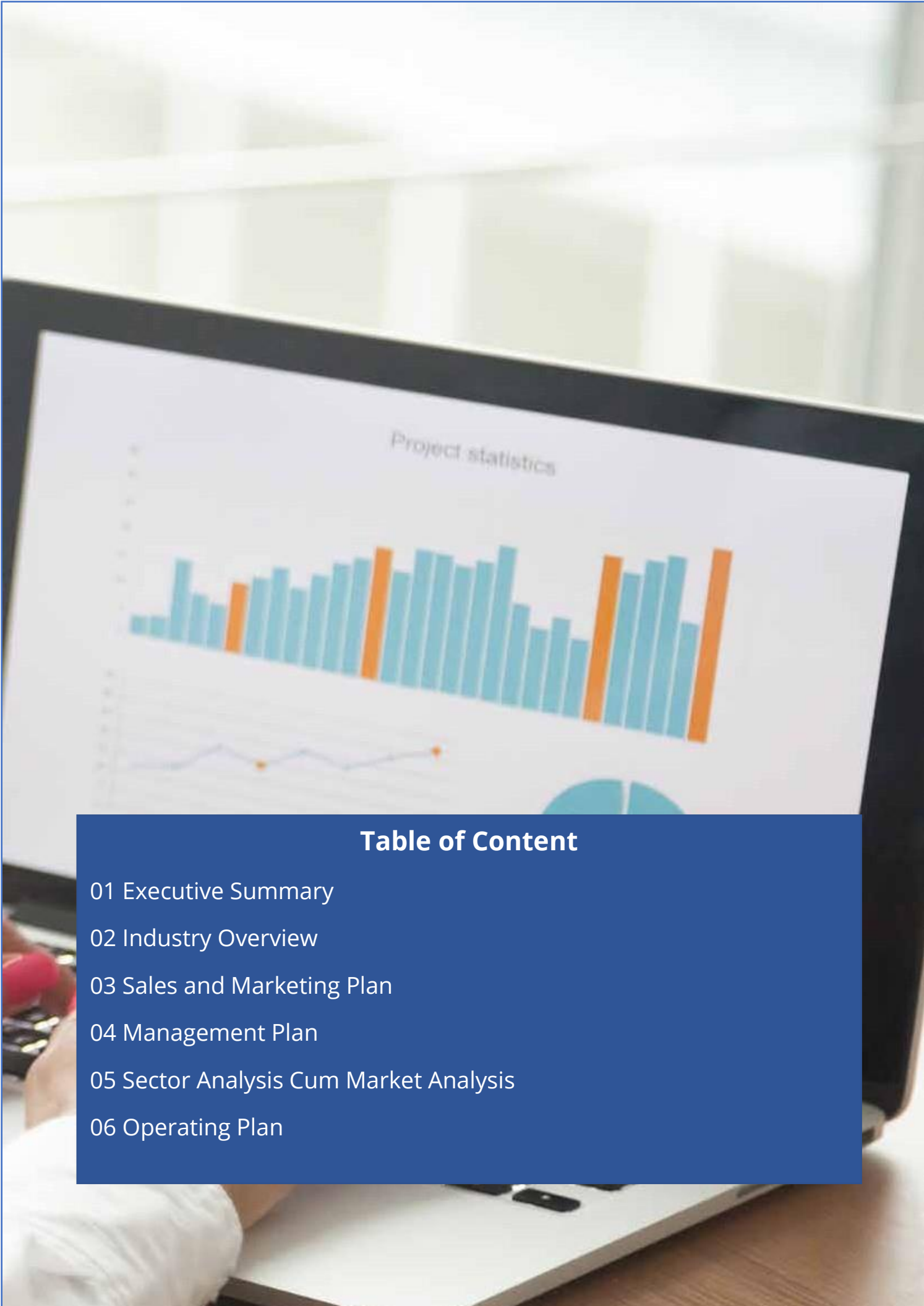


Table of Content

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 in2023.[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

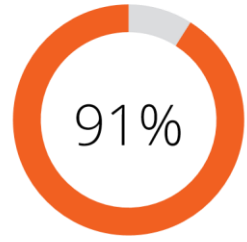
The cyber security market in India is expected to grow at one and a half times the global market growth rate.

Increasing attacks on cyber security systems

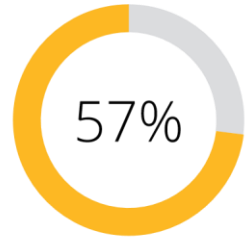
As systems get more interconnected, another significant factor the industry is grappling with is the increasing number of breaches and sophisticated cyberattacks, driven by different motives.

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

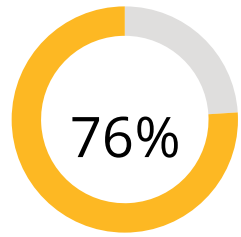
Threefold increase in cyber security incidents

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.



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

How cyber security products and services are expected to pan out

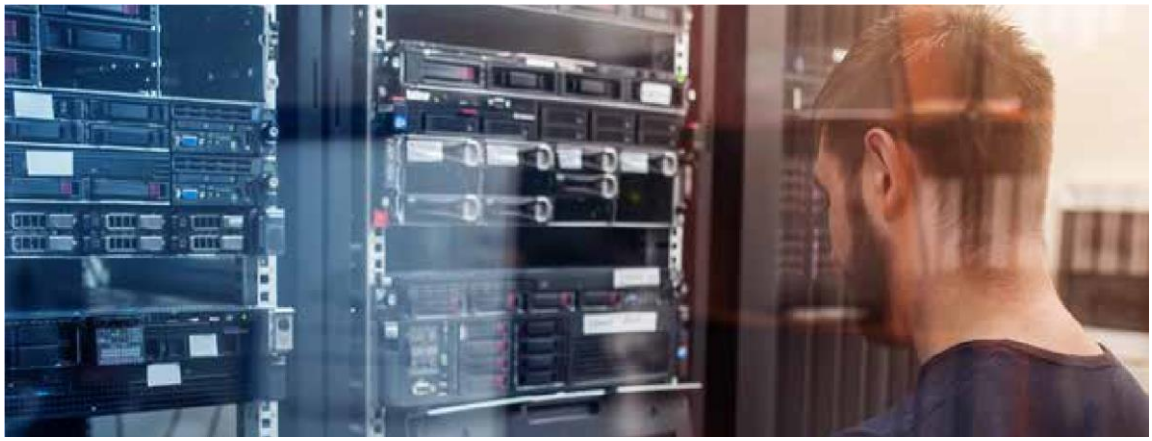
The study estimates that the market for cyber security products in India will grow at a higher rate than that for services. The existing portfolio of cyber spending will change with products becoming dominant, as organisations invest more in products powered by specialised technologies.

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.

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

While the products market is estimated to grow at a CAGR of 16.9% over three years and reach USD 1.64 billion by 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 these India, such as Make in India, Digital India and set of Skill India, aimed at economic galvanisation and instances of inclusion, have also begun to leverage emerging monetary gain, technologies to create efficiencies and increase include reputational reach. Automation in terms of bots, robotics further compounded by 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, digitisation efforts come with their own cyber security risks. While earlier cyberattacks were largely for reasons for attacks now also damage and power play, 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.

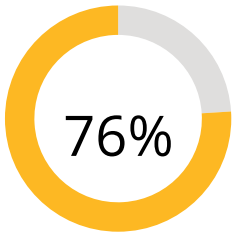
The average cost of a malicious insider attack rose by **15% in 2019 from last year**.

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

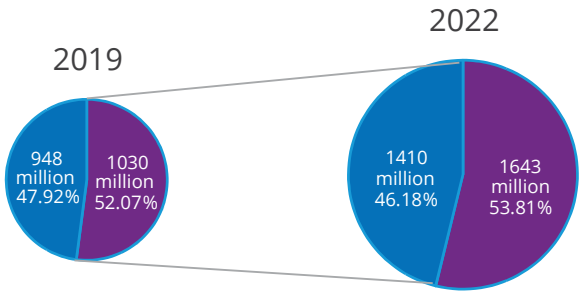
Gradual shift in favour of cyber security products

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.



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.

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.

03 Sales and Marketing Plan

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).

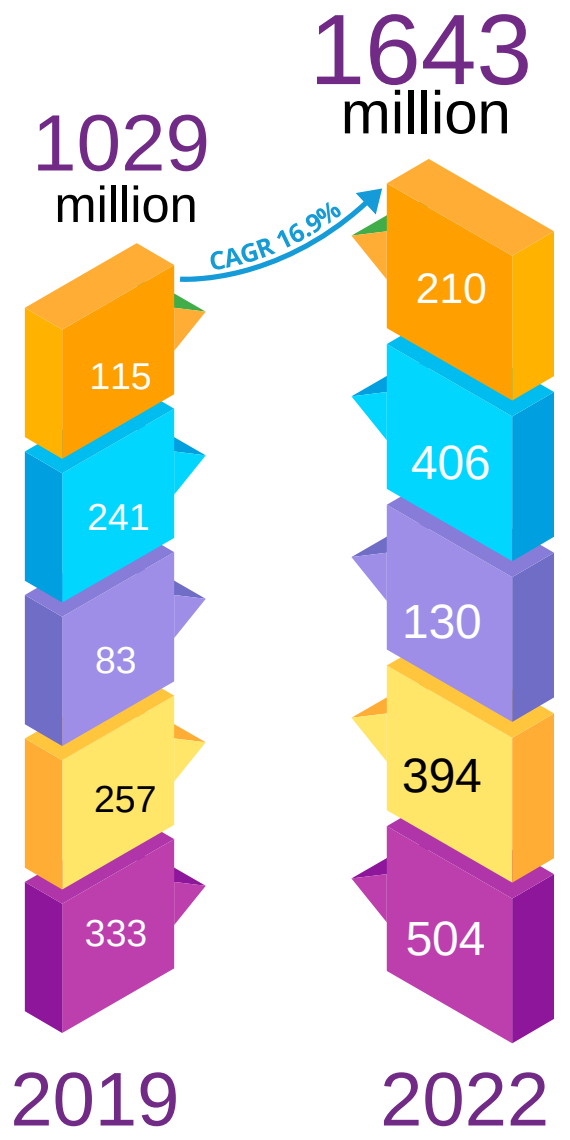
- Data security products are growing at the fastest rate, due to the expected regulatory evolution and focus on security and privacy of the product mix. This is due to the need of data.
- Endpoint security products are also growing faster than the overall market among enterprise point

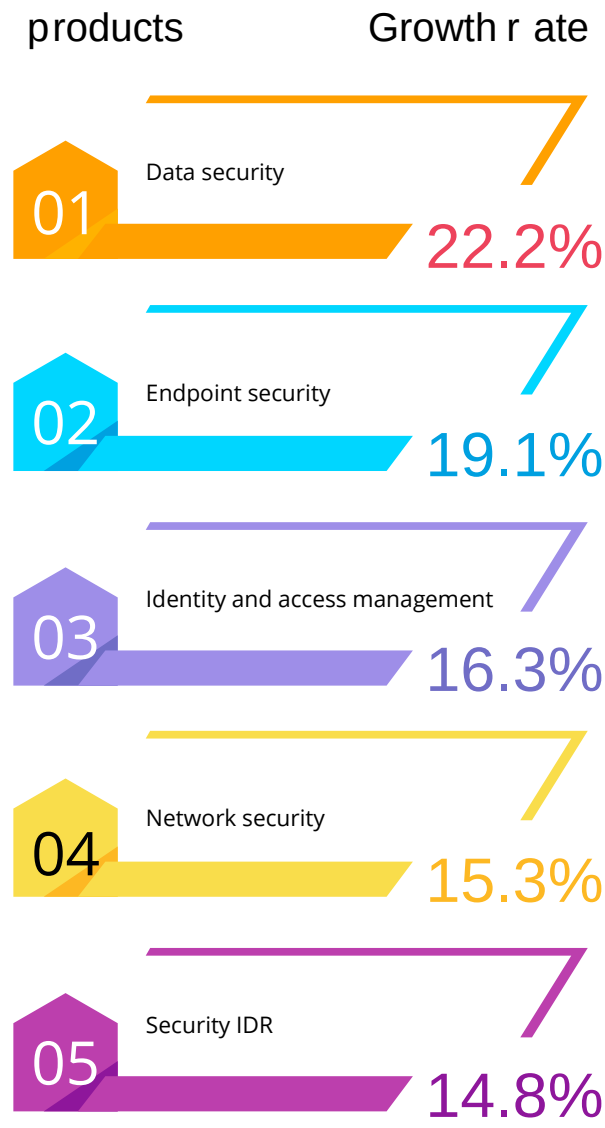
- Security IDR will continue to be the most dominant product category, occupying 32% of the product mix. This is due to the need for continuous innovation and automation in this space such as, threat intelligence capabilities, integration of governance risk compliance (GRC) capabilities, user mix for cyber security products. This is largely driven by concern behaviour analytics, use of big data and statistics to facilitate quick incident executives to safeguard the starting response. for most high-profile endpoints.


Global Stocks
Technology Stocks
Portfolio P1
Portfolio P2

Growth of the Cyber Security products market in India

Products consumption (in USD million)





Security IDR N/w Sec IAM
Endpoint Sec Data Sec

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

CYBER PRODUCT

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%.**

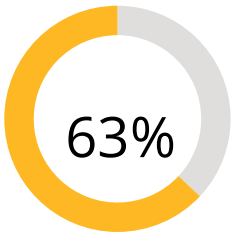
Data security products include encryption, tokenisation, data masking, data loss prevention, information rights management, file and data access monitoring.

- With number of digital services increasing, both volume 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 data protection expenditure will comprise:

increasing demand for context aware data security controls

breach reporting and response capabilities. The future of 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.

04 CYBER SECURITY SERVICES

Cyber Security Service Cum Management Plan

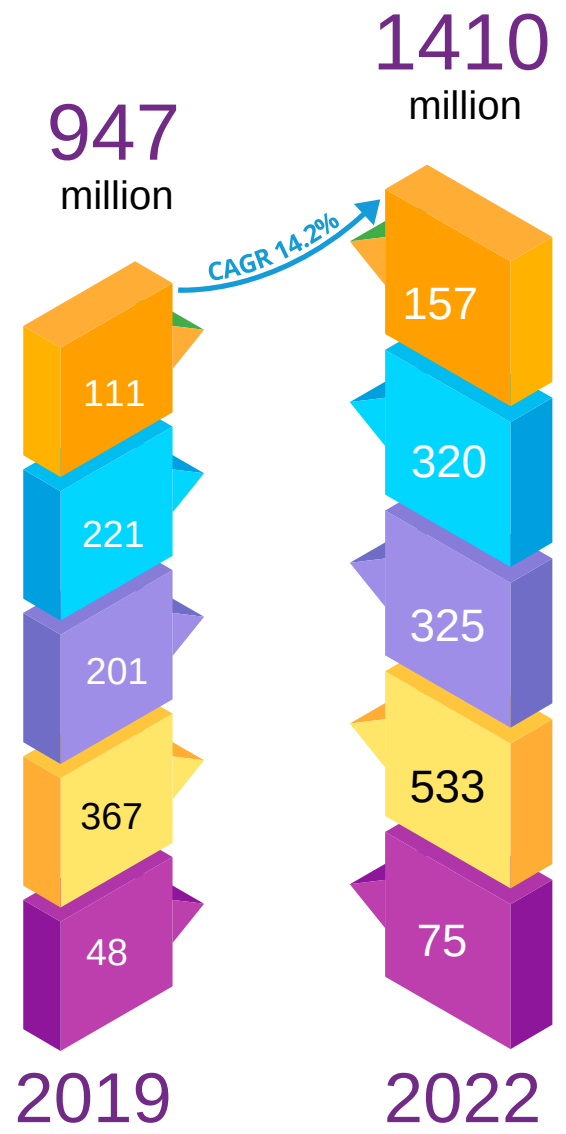
Security testing and incident response to lead growth in demand for cyber security services

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)

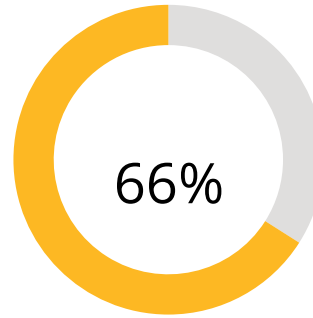


- Incident response
- Security testing
- Security consulting
- Security operations
- Security implementation

s ervices	Growth r ate
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%

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.

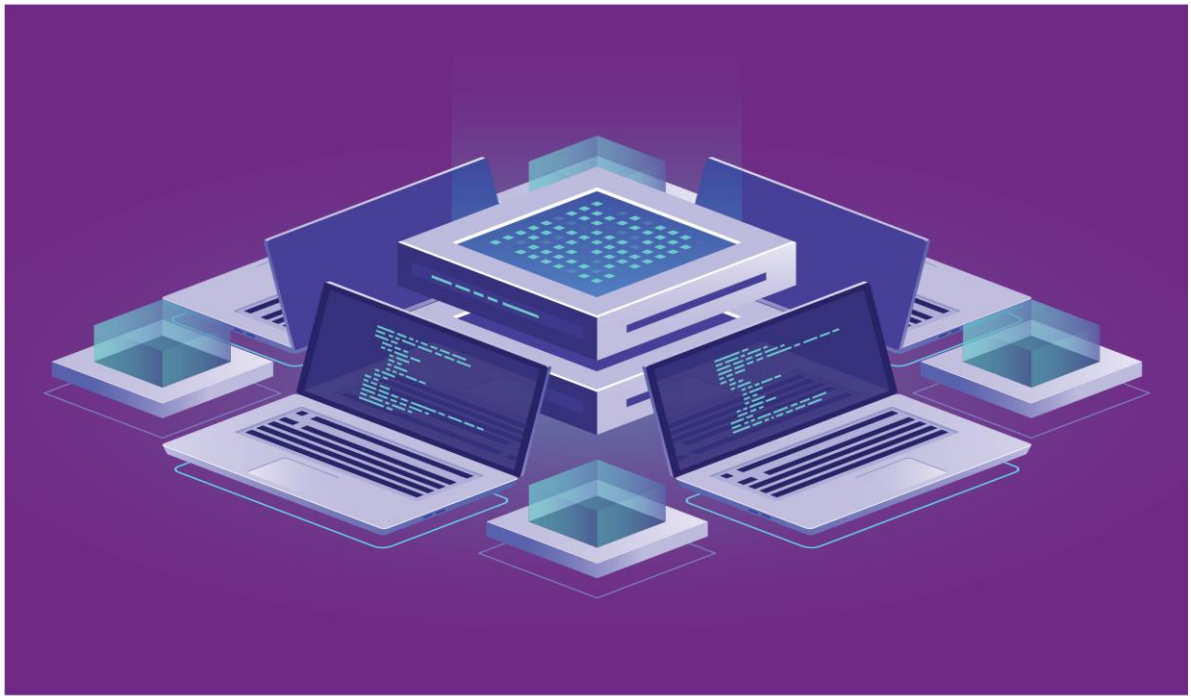
Security testing is one of the fastest growing services as organisations want to prevent attacks on their systems

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

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.



05 SECTOR ANALYSIS

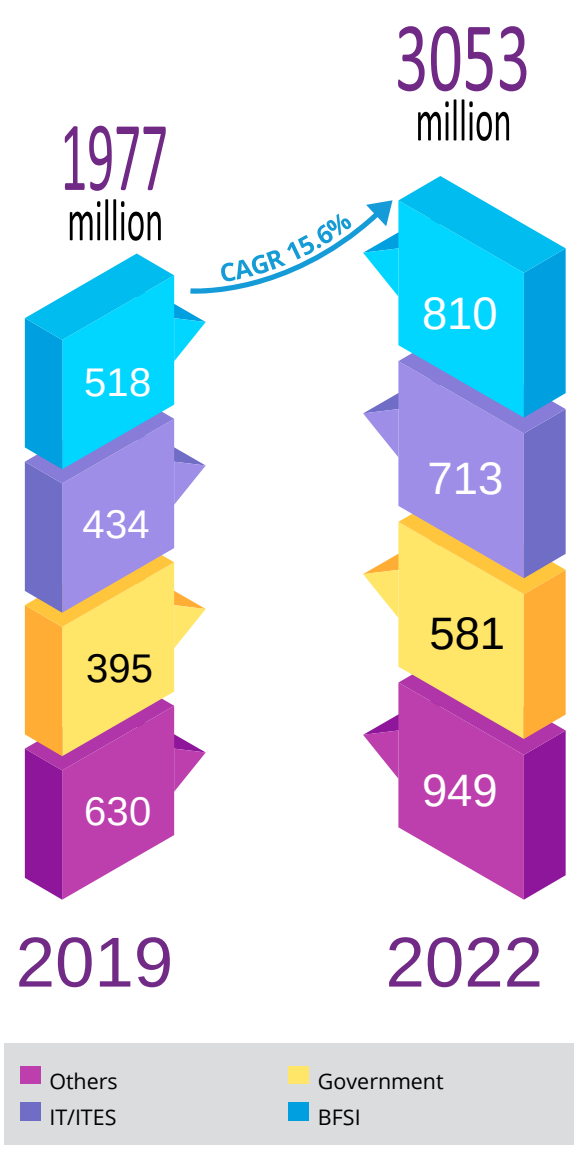
Sector Analysis

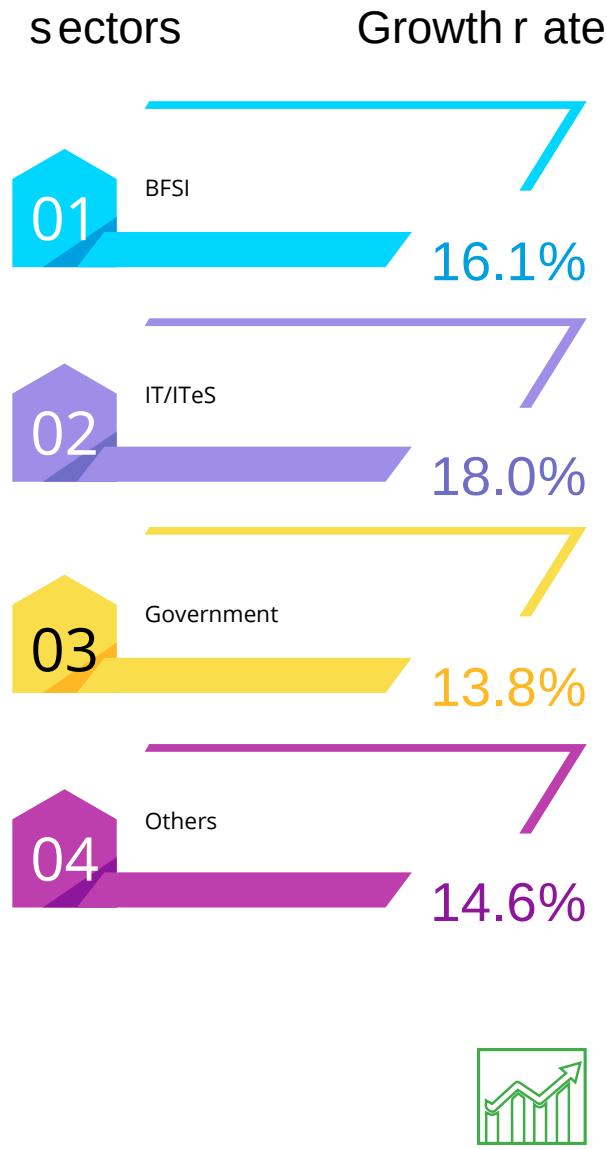
BFSI, IT/ITeS and Government are the top 3 sectors with the largest market share in cyber security expenditure in India

- 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)





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

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.

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

- 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.

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.

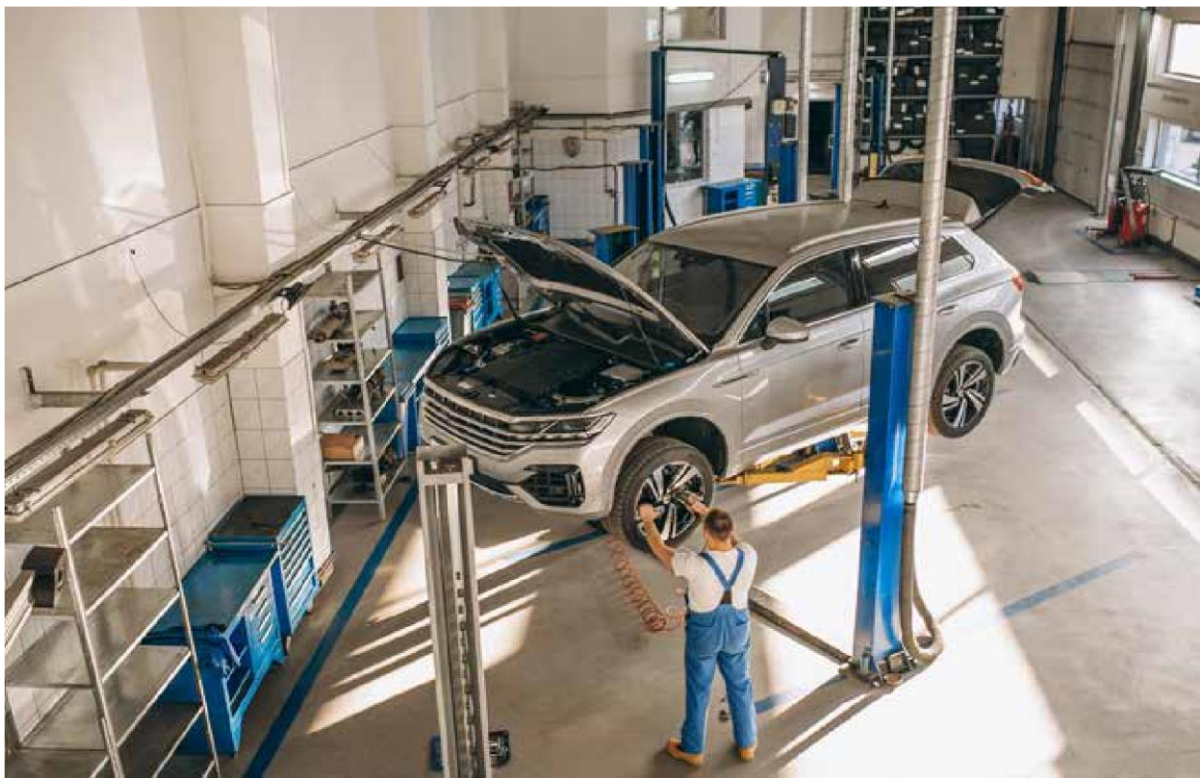
The Ministry of Power has mandated a CISO position for all utilities, released as per Indian Standard IS 16335 (Security Standard for Power Systems). The Ministry has also notified information sharing and directed relevant bodies to set up analysis centres. The Central Electricity

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).



1. Inform your employees about your cybersecurity policies.

Set up IT cybersecurity practices and policies for your employees. This includes requiring strong passwords and establishing appropriate Internet usage guidelines that comprehensively discuss your business cybersecurity policies.

2. Update your software.

Cybercriminals can enter your computer network through outdated apps with known vulnerabilities. Make sure you regularly install software updates and patches for applications and operating systems as soon as they're available.

3. Place a firewall.

One of the first lines of defense in a cyberattack is a sturdy firewall. We recommend that all small to medium-sized businesses set up a firewall to create a barrier between your data and cybercriminals. Installing internal firewalls is also an effective practice to provide additional protection.

4. Back up all your data regularly.

Always back up all your business data including those stored in the cloud. To have the latest backup, check your on-premise and cloud servers regularly to ensure that it is functioning correctly.

5. Secure your wi-fi networks.

Make sure your wi-fi network is secured, encrypted, and hidden. To hide your wi-fi network, set up your router so it does not broadcast the network name, and protect its access with a strong password.

6. Install anti-malware software.

Anyone can be a victim of data breach, no matter how vigilant one is. Since phishing attacks center on installing malware on the employee's computer, it's imperative to have anti-malware software installed on all devices and in your network.

7. Make an action plan for mobile devices.

Mobile devices can also impose cybersecurity threats, more so if they store confidential business data. It is best to require all employees to protect their devices with passwords, install security apps, and encrypt their data. In addition, establish protocols for reporting lost or stolen company equipment.

8. Implement strong data protection procedures.

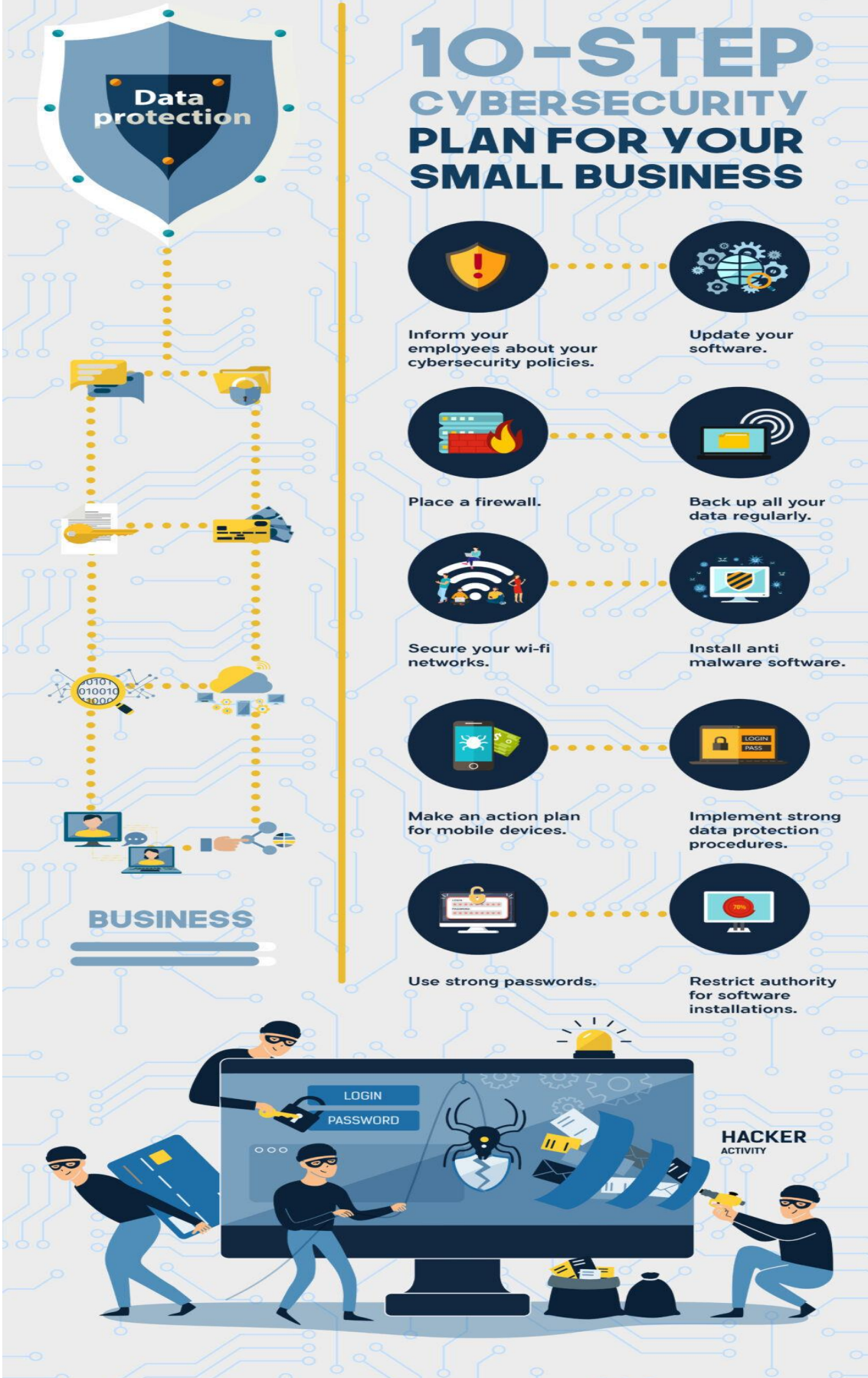
Running your office machines on the latest software, web browsers and operating systems are the best defense against cybersecurity threats. Devise and follow a business data protection strategy that encompasses strong security measures centered around the restriction of access.

9. Use strong passwords.

Basically, strong passwords are a complex combination of special characters, numbers, and letters that provides more security for all your online accounts. Require all employees to always use two-factor authentication when accessing sensitive business data. It's also best to encourage them to never disclose their usernames to third parties.

10. Restrict authority for software installations.

Employees should have limited access to all data systems and software installations. Any installation should only cater to their role's specific needs, and under the permission of the network administrator.


Data protection
BUSINESS
10-STEP
CYBERSECURITY
PLAN FOR YOUR
SMALL BUSINESS
Inform your employees about your cybersecurity policies.
Update your software.
Place a firewall.
Back up all your data regularly.
Secure your wi-fi networks.
Install anti malware software.
Make an action plan for mobile devices.
Implement strong data protection procedures.
Use strong passwords.
Restrict authority for software installations.
LOGIN
PASSWORD
HACKER
ACTIVITY
uniserve
IT SOLUTIONS

Operating Plan

- Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.
- Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.
- Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.
- Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.
- Ability to apply approved planning development and staffing processes.
- Ability to apply critical reading/thinking skills.
- Ability to collaborate effectively with others.
- Ability to coordinate cyber operations with other organization functions or support activities.

- Ability to develop or recommend planning solutions to problems and situations for which no precedent exists. Ability to effectively collaborate via virtual team.