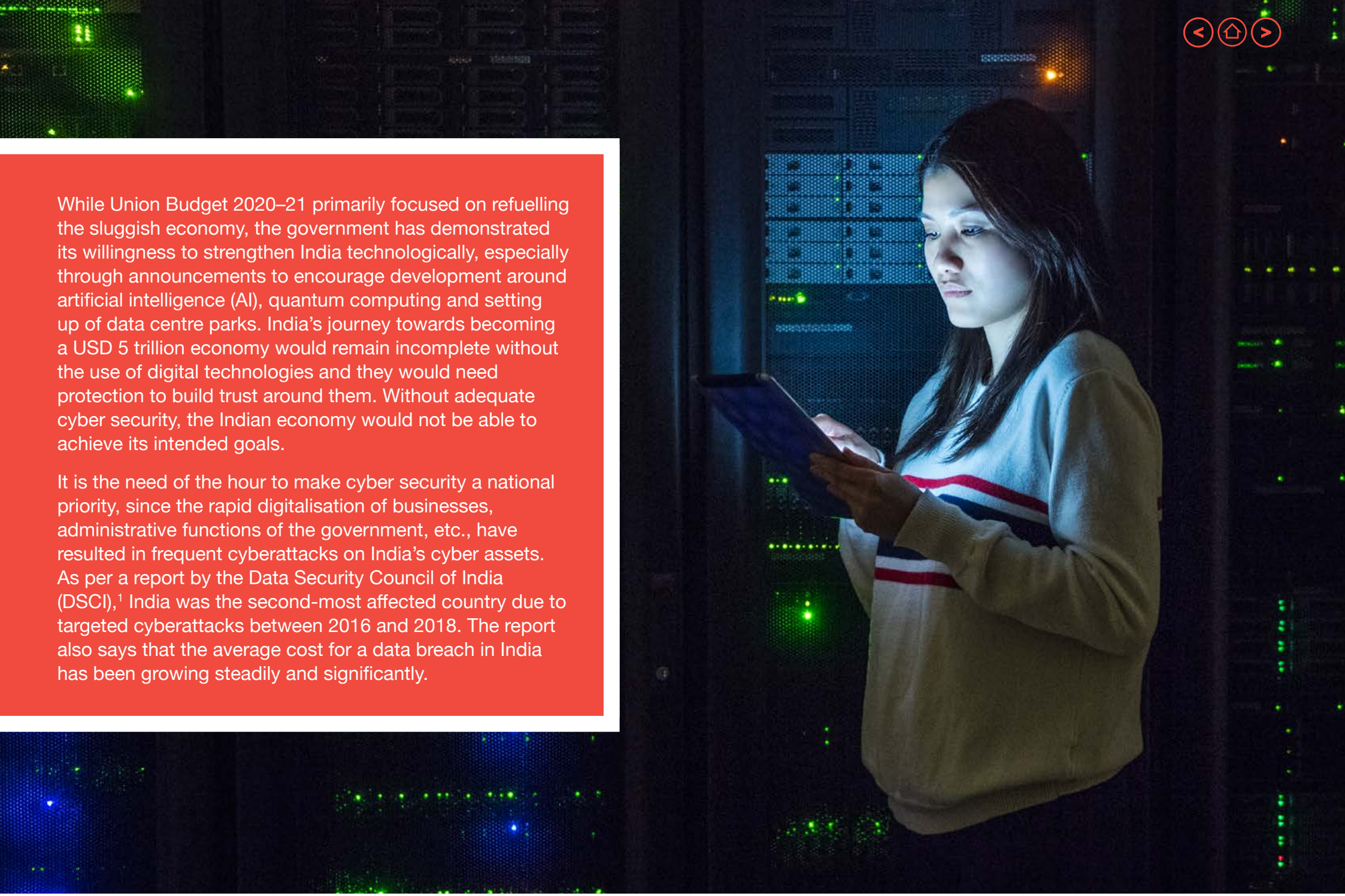
Need of the hour: Why cyber security should be a national priority

Cyber in Perspective

pwc

Click to launch

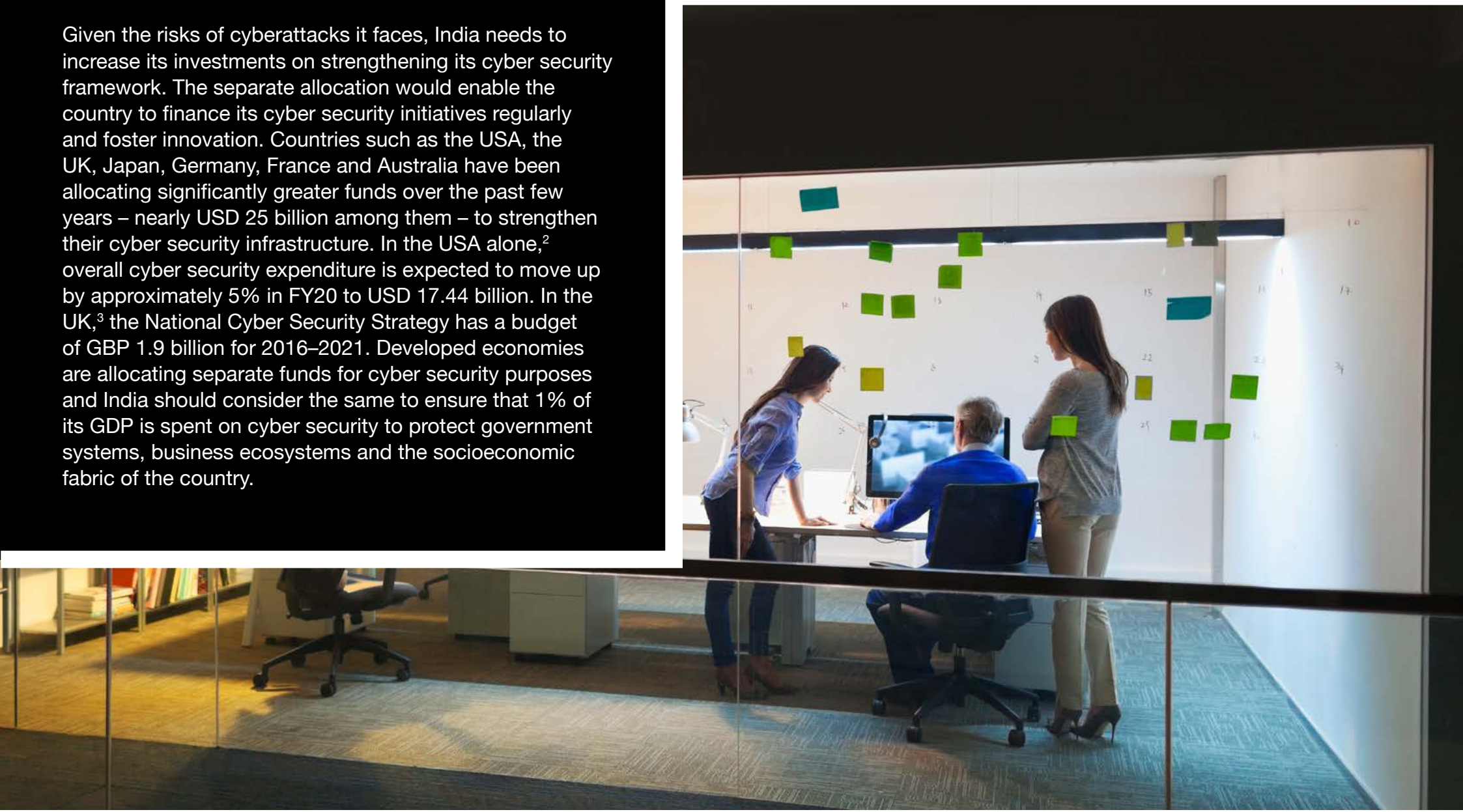


While Union Budget 2020–21 primarily focused on refuelling the sluggish economy, the government has demonstrated its willingness to strengthen India technologically, especially through announcements to encourage development around artificial intelligence (AI), quantum computing and setting up of data centre parks. India's journey towards becoming a USD 5 trillion economy would remain incomplete without the use of digital technologies and they would need protection to build trust around them. Without adequate cyber security, the Indian economy would not be able to achieve its intended goals.

It is the need of the hour to make cyber security a national priority, since the rapid digitalisation of businesses, administrative functions of the government, etc., have resulted in frequent cyberattacks on India's cyber assets. As per a report by the Data Security Council of India (DSCI),[1] India was the second-most affected country due to targeted cyberattacks between 2016 and 2018. The report also says that the average cost for a data breach in India has been growing steadily and significantly.

Additional investments required

Given the risks of cyberattacks it faces, India needs to increase its investments on strengthening its cyber security framework. The separate allocation would enable the country to finance its cyber security initiatives regularly and foster innovation. Countries such as the USA, the UK, Japan, Germany, France and Australia have been allocating significantly greater funds over the past few years – nearly USD 25 billion among them – to strengthen their cyber security infrastructure. In the USA alone,[2] overall cyber security expenditure is expected to move up by approximately 5% in FY20 to USD 17.44 billion. In the UK,[3] the National Cyber Security Strategy has a budget of GBP 1.9 billion for 2016–2021. Developed economies are allocating separate funds for cyber security purposes and India should consider the same to ensure that 1% of its GDP is spent on cyber security to protect government systems, business ecosystems and the socioeconomic fabric of the country.



Spending funds judiciously

If the government decides to increase expenditure to strengthen cyber security, the funds should be spent on the following areas:

1.

Building an effective legal framework to handle cyber security cases

At present, there isn't any specific legislation in India that provides protection against cybercrimes. The Information Technology Act, 2011, needs to be revisited as the scale and the modus operandi of cybercrimes have evolved and will continue to do so. India needs a law to tackle cases of cybercrime. This legal framework must be designed keeping in mind the ever-changing nature of technology.

It is also necessary to ensure that conviction rates increase in cases related to cybercrime. This could be done through capacity building in the legal circles. It will be necessary to invest more in the capacity building of legal professionals and law enforcement agencies. Expenditure could be routed towards equipping law enforcement agencies with necessary tools and technologies.

2.

Capacity building in the domain of cyber security

There is a dearth of adequately skilled cyber security professionals in India. A study conducted by the Information Systems Audit and Control Association (ISACA)[4] in the past year shows that 58% of the organisations worldwide have vacant cyber security positions. This shortage, which is felt at both the government and the industry level, can affect India's fight against cybercrimes. The government should encourage research and education related to cyber security skills.

If the government invests in capacity building of cyber security professionals, it is likely to result in the development of a robust cyber security ecosystem in India.

3.

Protecting critical infrastructure with deep monitoring and response capabilities

Critical Information Infrastructure (CII)[5] involves assets, systems, or parts thereof, that are deemed to be critical for the normal functioning of a country. As new technologies like the Internet of things (IoT) are integrated into our national critical infrastructure, new cyber security threats emerge, which are required to be handled by specific security solutions. This, coupled with a growing trend for convergence and multi-system interconnectedness, has introduced several security issues that threaten normal economic and social functions.

There are growing concerns and debates about the protection of the country's critical infrastructure and adequate budgetary allocation is required to build deep monitoring and response capabilities.

4.

Building and strengthening cyber defence and deterrence

State-sponsored cyberattacks are growing by the day and becoming a covert method of warfare, allowing countries to deny accusations and blame citizens. For the sake of sustainability and reliability in the digital age, the government needs to make India cyber-resilient by encouraging indigenous cyber security products and research and development (R&D).

Coordination and cooperation with other countries through bilateral and multilateral agreements to tackle cyber incidents is another critical step towards achieving cyber resilience and tracking cyberattacks originating from foreign countries. India needs to go through diplomatic channels to address this issue but at the same time, funds must be allocated towards setting up infrastructure dedicated to blocking malicious traffic from shadow locations. India should shut down safe havens for cybercriminals by barring internet traffic from suspected locations. India can identify countries where there are no laws against cybercrimes and block traffic originating from such countries by employing techniques such as geo-fencing.

5.

Bringing sectoral agencies and regulators under one roof

Another important area that demands urgent attention is the necessity of a national-level agency for protection from cybercrimes. While India has several sector-specific regulators and agencies focusing on their respective areas, there is clearly a need for a central authority at the national level, given that cybercrimes have evolved to penetrate various sectors and regulatory regimes. This gap needs to be filled in for swifter action against cyberattacks. The overarching agency should be empowered with sufficient funds to deal with cybercrime cases.

6.

Public awareness

Australia's cyber security strategy and Singapore's Digital Defence Department greatly emphasise citizens' awareness against cybercrime. In India, the government too should launch result-oriented cyber awareness campaigns to provide individuals one-to-one assistance and cyber security support. The awareness drives can include the formation of guidelines and provide people with government-recognised security applications which can be installed to secure devices.

There must be comprehensive drives to spread awareness about cybercrimes and how they can be prevented. Furthermore, the government could also consider making cyber security a part of school curriculums, so that students are aware of cyberthreats and precautions they should take when using the internet and mobile phones.

[1] https://www.dsci.in/ucch/resource/download-attachment/13/Cyber%20Insurance%20in%20India

[2] https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf

[3] https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1745/1745.pdf

[4] http://m.isaca.org/Knowledge-Center/Research/Documents/cyber/state-of-cybersecurity-2019-part-1_res_eng_0319a.pdf

[5] The National Critical Information Infrastructure Protection Centre (NCIIPC), the National Nodal Agency for Critical Information Infrastructure Protection, identifies power and energy, BFSI, telecom, transport, government and strategic and public enterprises as 'critical sectors'.

Author

Siddharth Vishwanath
Leader, Cyber Security
PwC India

Onkar Chand
Manager, Cyber Security
PwC India

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with 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.

pwc.in

Data Classification: DC0

SUB/February-M&C4625/4816