July 2020

Securing the future of business

A PwC point of view on perimeter-less security

pwc

Introduction

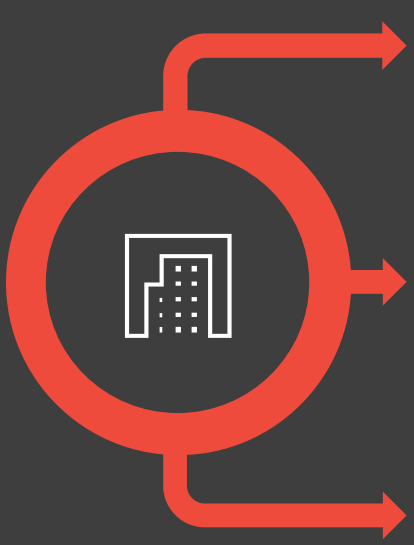
As organisations move towards the ‘future of business’, they will no longer be able to address the changing threat landscape using conventional approaches. They now need to enhance their threat management capabilities to sustain and protect critical resources.

With diminishing organisational boundaries, employees have become the new perimeter for security. Protection from opportunistic threat actors becomes critical, underlining the need for embedding a robust security culture in the organisation.

The current digital era is fuelled by the mobile and cloud ecosystem, which is emerging as the primary driver for computing, and the traditional mechanisms to protect this ecosystem have dissolved. This makes it even more important to have controls in place to protect the critical corporate infrastructure and establish secure network architecture.

However, the implementation of these measures is challenging due to the mobile nature of devices and operations, wherein users now access and share information across systems and cloud-based applications from outside the organisation. Such issues are making it imperative for organisations to focus on securing the endpoint devices used to access and share information.

Organisational boundaries are blurring rapidly



Low-touch business model

Digital transformation – driving minimum physical contact

Work from anywhere and anytime

Increased emphasis on WFH model, allowing employees flexibility and ensuring safety

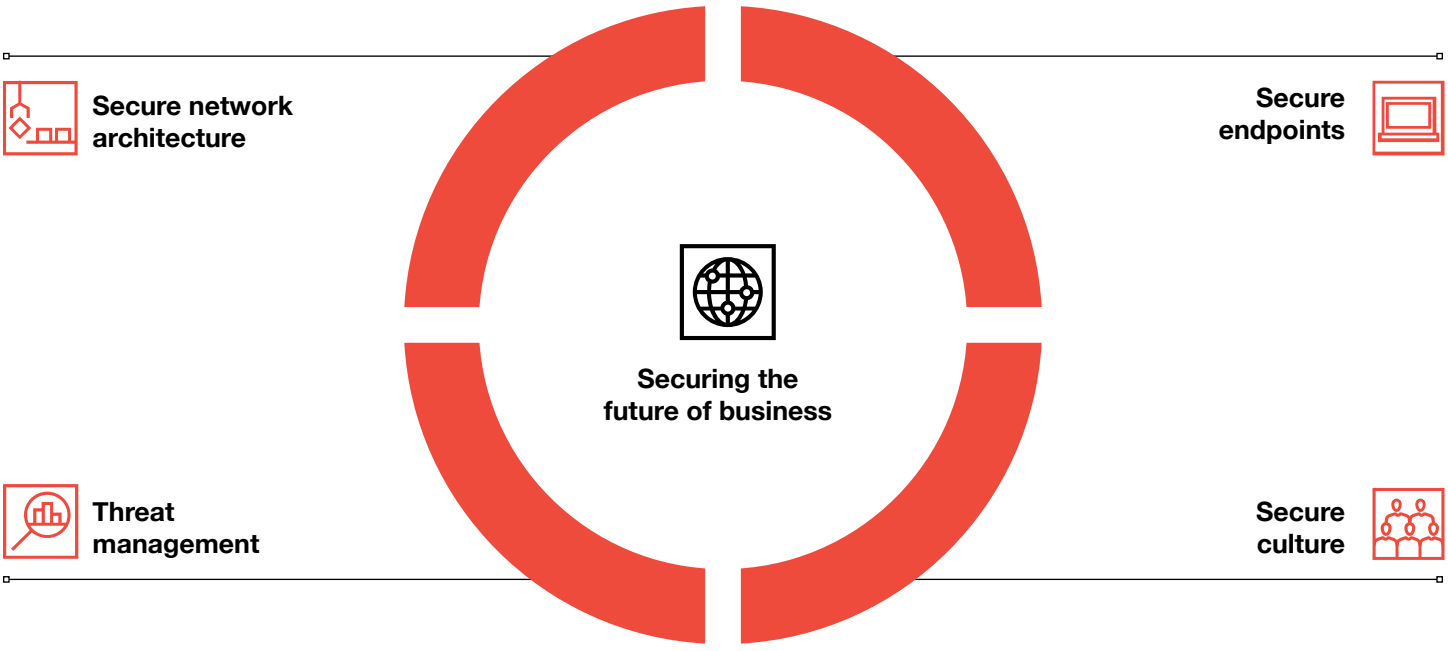
Business resilience

Strengthening business systems and processes to perform seamlessly during and post crisis

These factors will influence security management across the following four dimensions:

- Endpoint devices
- Network architecture
- Threat landscape
- Organisational culture

The above factors are prompting organisations to adopt a perimeter-less security approach in order to gear up for the 'next normal':



Secure network architecture

- **Applications, data, users and their devices** are **moving outside the zone** of **control** and the **organisation's perimeter.**
- **Attackers** on the outside can **penetrate** an organisation's **network** through various means such as **credential hacking of trusted users.**
- The **work from home** culture presents insiders with a **bigger opportunity** to **breach security controls** due to **less/limited direct oversight.**
- With **traditional networks,** everyone **inside** the network is **trusted by** default (thus allowing attacker to gain access once inside).
- **Traditional perimeters** are **less compatible** with today's **digital business** model and hence **pose greater risks.**

Secure endpoints

- With **compromised endpoint devices,** cyberattackers **easily gain access to an organisation's network infrastructure.**
- **Endpoints** are the **primary source for 'exfiltrating'** an organisation's sensitive data (intentionally or unintentionally).
- **Data-driven malware and ransomware** attacks are on the **increase.**
- **Under the bring your own device (BYOD) policy,** employees are increasingly using their own mobile and other semi-trusted and untrusted devices to access critical information.
- The digital era has led to the proliferation of **heterogeneous device types, which** makes the securing of endpoints more complex.

Threat management

- **Increased adoption of emerging technology** (e.g. 5G, autonomous vehicles, IoT, cloud computing, and AI) has made **cyber challenges more dynamic.**
- **Cyberattackers** have resorted to **sophisticated attacks** such as **COVID-themed attacks, impersonation and ransomware.**
- **The growing remote workforce** has rapidly transformed **the nature and vulnerability of enterprise networks.**

Secure culture

- **Employees** are **operating outside of the office premises** and are comparatively **more vulnerable.**
- **Increased COVID-19 themed phishing/smishing attacks** are targeting employees/contractors to **exfiltrate sensitive** information and important credentials.
- Moreover, employees are **unaware** of the cyber **security practices** of organisations.

Secure network architecture

The zero trust concept – ‘always verify and never trust’

In the past, **securing an organisation was about establishing walls** around the **data centre** that housed the core data and applications. Under this setup, **users** with **valid credentials** were considered to be **trusted users.**

With the **growing use of emerging technology coupled with mobile platforms, cyberattackers** are resorting to attacks such as **credentials hacking, targeted phishing and data mining malware** in order to obtain credentials and gain **access to an organisation’s network.**

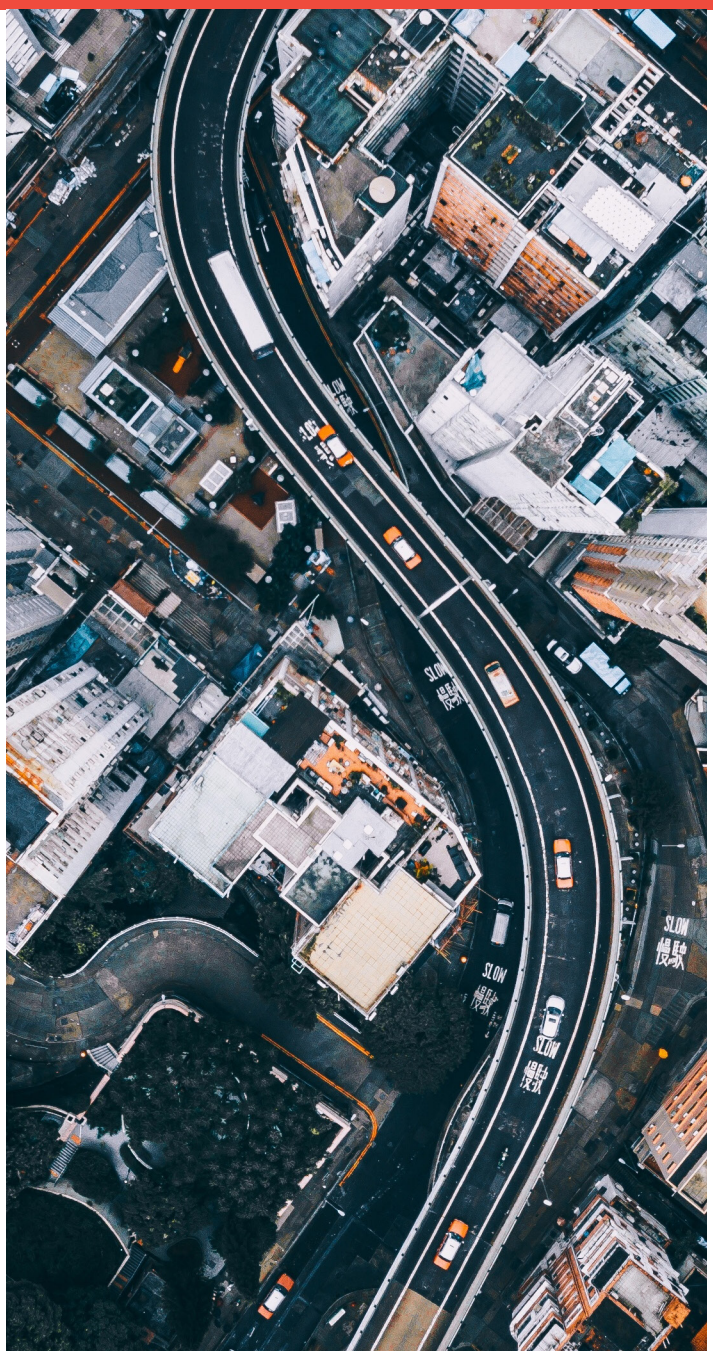
Traditionally, remote access to the corporate network, and thus the data centre, has been enabled by VPN. Once users have been authenticated, they gain **access to authorised information resources or ‘anything’ internally as they are ‘trusted’ by the ecosystem.**

Organisations should consider adopting **zero trust architecture (ZTA)** to fortify their **network architecture. ZTA principles** are based on the concept of **‘always verify and never trust’ anyone.** This approach requires **every user, account or device** attempting to gain access to the organisation’s infrastructure to **undergo verification prior to obtaining access.**

ZTA aims to enforce granular perimeters on data, user and location.

This lowers the potential for data breaches, as ZTA continuously focuses on application workload and the data asset rather than the endpoint device/server/perimeter.

Though ZTA may sound like a **single technology/solution,** it is **more of a holistic** approach to securely manage **organisational assets – namely endpoints, applications, network devices, databases and servers.**



Organisations could consider moving to **serverless architecture,** as with this approach, there is greater focus on **securing the application** rather than worrying about the **underlying infrastructure** (i.e. network components) **for patching and security controls. Behavioural protection and access permissions** then become the primary focus areas.

ZTA principles

Shift towards network micro-segmentation

In ZTA, there is a shift away from wide network perimeters to a more narrow focus on protecting individual or small groups of resources called network micro-segments. Further, it is ensured that no implicit trust is provided to systems/users based on their network location.

Location-independent outreach to resources

No traffic, irrespective of its origin or source, should be considered to be safe and trusted. Until the traffic is analysed and its authorisation verified, the content should considered to be unsafe. One of the key elements to enable ZTA is device trust, typically by controlling network-level access to the endpoint and by whitelisting processes and systems running on the endpoint.

While device trust verifies device authenticity, it is important to have secure transport protocols implemented to ensure that the conduit (device) is secured and data integrity is maintained. It is equally important to focus on establishing data trust for securing the data lifecycle through varied protection mechanisms.

Least privilege, stringent and dynamic access control strategy

A strict role-based access control (RBAC) approach should be adopted. It should be supported by privileged identity management for administrative and sensitive access. Multifactor authentication should be enabled across the ecosystem to ensure access to the information resources is controlled and validated, thereby establishing user trust. Organisations should implement an access control strategy focused on least privilege, stringent and dynamic access. Such a strategy allows for improved management of access as it takes into account the resource sensitivity, user's job role, configuration of the resource being accessed, and the user's location.

Robust monitoring

In ZTA, the monitoring needs to be extended to the entire ecosystem, including the applications, network, operating systems and databases. An advanced threat intelligence infused security operations centre (SOC) that leverages user behaviours, network access patterns and insider threat analytics would be a stepping stone to enhancing monitoring.

Implementing a zero trust approach

When establishing ZTA, an organisation should first start by identifying sensitive data within its environment and its flows between various systems.

The next step involves identifying people and groups based on their attributes (e.g. job role, location). Based on this information, organisations should construct zero trust micro-perimeters. This is an essential step in the entire ZTA ecosystem process.

Once ZTA is established, it is equally important to monitor the ecosystem with continuous security and behavioral analytics and also embrace security automation and orchestration.

Secure endpoints

Endpoint devices and mobile devices being used by organisations continue to increase in number, along with the amount of data being processed/stored on them. Every single device used to access an organisation's systems is yet another endpoint for the organisation to secure. Organisations need to opt for solutions that are sustainable and evolve with incoming threats.

Endpoints are nothing but a communication network node. While these nodes allow users to access corporate infrastructure and information, they could also be used to intentionally or unintentionally exfiltrate an organisation's sensitive data to unauthorised users. In addition, endpoints are targeted by cyberattackers trying to gain access to corporate infrastructure.

Due to the evolving threat landscape, endpoint devices themselves face a huge risk of compromise and hence need special attention.

"Your security is only as good as your weakest link!

A **multitude** of **security solutions** can help **prevent employees** and other users from f**alling prey to cyberattacks. Specially crafted endpoint security** (including untrusted or semi-trusted BYOD devices) ensure security consistency and control. The feeds from all the endpoints should be gated towards the SOC.

Such **controls** also **allow** an **organisation** to **identify** where the data is being **accessed and data-sharing patterns,** and **enable user behaviour analytics.**

BYOD security model

In the **new normal** – or what is now known as the next normal – it is essential for organisations to consider defining a BYOD security operating model.

The BYOD security operating model defines how **organisations should manage employees' personal devices while allowing them to access critical infrastructure.** Basic elements that organisations need to consider while defining the operating model include:

- BYOD security policy
- technical controls to be implemented
- managing security incidents
- staff sensitisation/awareness.

Remote working policies and guidelines

Organisations usually have adequate security guidelines. However, it is of utmost importance to ensure that the **security guidelines are transformed and available** as they undergo a transition.

Policies and procedures should be exercised and updated to include remote access, layered authentication, remote connection, personal device usage and security of an organisation's crown jewels.

Virtual desktop infrastructure (VDI)

In crisis situations like COVID-19, certain organisations find it challenging to **continue their business remotely** either due to **lack of endpoint infrastructure or due to limited VPN licences.**

Such organisations should consider **implementing** VDI which would allow users to **access critical infrastructure** through non-organisational assets in a **secure manner.**

Securing VDI infrastructure is also an important aspect of VDI implementation. Organisations should ensure that the **configuration is secure** and that **movement of content** to the user's local machine is **restricted.**

Enterprise mobility management (EMM)

EMM helps business reduce costs and manage risks by securing devices, data and the configuration of all mobile devices in the network.

Organisations should evaluate EMM solutions and expand their functionality to personal devices to **ensure enterprise data security** on **personal devices.**

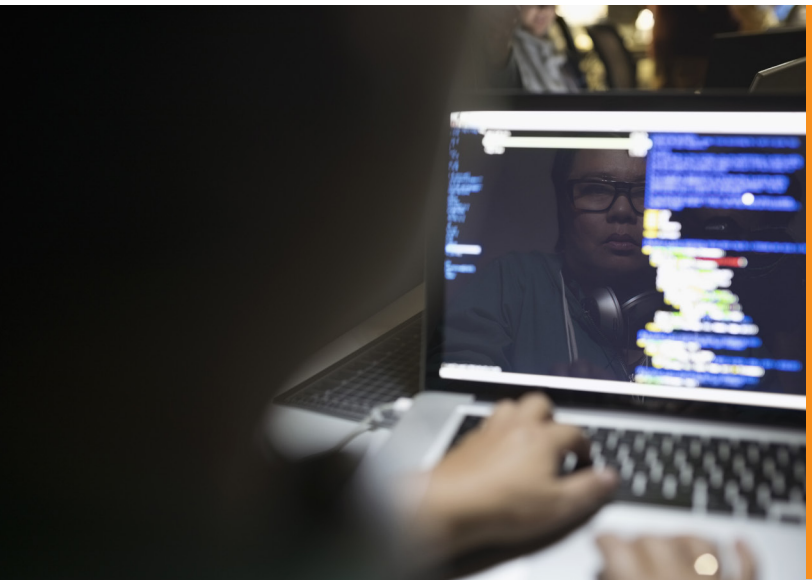
Where possible, **only approved devices** should **be allowed to connect to the organisation's network remotely,** as the level of security controls and policies on the personal devices of employees are unknown variables.

Endpoint detection and response (EDR)/endpoint protection

Organisations should consider **implementing full disk encryption** along with an **EDR** tool. This will help in investigating and containing attacks.

While detective and preventive controls are being implemented, it is also important for organisations to **continuously scan and patch/update these endpoint devices.**

Threat management



In today's dynamic environment, organisations are faced with two kind of challenges – external and internal. External challenges are of an evolving nature, and they often become the key source of security threats for organisations. On the other hand, internal challenges can range from unidentified threats to obsolete mitigation plans and untreated vulnerabilities in critical systems.

In the **advancing digital world** (i.e. future of business), it is of **utmost importance to address cyber security vulnerabilities and threats** to obtain the **best possible outcome** from **digital technological investments.**

Increasing implementation of emerging technology such as 5G, **autonomous vehicles, Internet of things (IoT), cloud computing, and AI** has increased the complexity of **cyber challenges** faced by organisations.

Threats are now **more sophisticated** and are **evolving** at a **pace faster** than an organisation's **coping mechanisms.** This requires organisations to **revisit their existing security controls** and adjust them to new cyberthreats.

Organisations need a **proactive and pragmatic approach** to manage risks and security concerns. The **'security by design'** approach will help organisations **establish an ecosystem of trust** and ensure **cyber security risks** are **continuously managed and monitored.**

A certain level of **automation and advanced algorithms** needs to be introduced by an organisation across processes such as 24x7 **security operations, threat intelligence, identity management** and **code reviews** to improve **detection and response while reducing cost.**

Managing evolving threat vectors

Indicators of compromise (IOCs)

Organisations should continuously perform identification of new IOCs. They need to detect the presence of known IOCs (e.g. COVID themed) as well as identify anomalies indicating the presence of rogue systems. Once this information is available, organisations should compare the data with available threat intelligence to identify new IOCs and incorporate those in the security monitoring.

Strategic threat intelligence/dark web monitoring

The dark web has been a major concern area for several organisations. While there are other cyberthreat vectors to be worried about, the dark web is a common location where stolen organisational data resides. Hence, it is important for organisations to implement dark web brand monitoring and protection services.

Managed detection and response infrastructure

With the transforming digital landscape, it is has become evident that organisations need next generation capabilities for cyberthreat detection and response. They also need proactive intelligence and insights into advanced threat vectors to cope with the widening threat landscape. This has made it important for organisations to continuously monitor all their infrastructure components through 24x7 SOC operations instead of 8x5 monitoring. Organisations should consider integrating their detection capabilities with the incident response process to enable seamless response to threats.

Secure culture

It is important for organisations to foster a culture that is risk aware. Thus, there is a need for a comprehensive security awareness programme that encompasses virtual training sessions and phishing/ vishing/smishing campaigns for development, continuous adaptation and sensitisation around security practices.

With **remote working culture having become the next normal,** users (employees and selected contractors) have **increased responsibility towards cyber security.** Users are **now operating** in a **less-secure environment** that is not totally in control of the organisation compared to the office premises.

Though organisations have security controls that can help manage the cyber security risks in the next normal, not all these risks can be managed. **Cyberattackers are constantly trying to find and exploit the smallest of opportunities** to gain access to an organisation's infrastructure. One such example is **phishing attacks** that are **tailored** to target users by providing them with **fake information/cures/advice** relating to COVID-19.

This makes it important for organisations to define a **strategy for training and awareness** of employees. The strategy should ideally cut across all the **three layers of an organisation – i.e. apex, tactical** (governance and technical teams), **and staff.**

Organisations should consider **gamification of awareness content to engage employees and increase their security awareness.** Gamification is nothing but applying a **gaming context to communicate business objectives.**

Simulating phishing attacks with employees or **threat scenarios** with the SOC team are certain **common examples** of areas where gamification can be introduced.

Awareness campaigns should also be aimed at deterring the advanced modus operandi of hackers.

While **one side of the coin is employee awareness, the other side is having the right resources with the right skills to manage cyberthreats** in the next normal. Organisations should **determine** if the **current teams have adequate knowledge/skills** and, if not, determine a **path for upskilling them.**

Cyber workforce training

As the first step, organisations should revisit their training material/content in order to make it more specific and detailed for the remote working environment. They should also consider gamification of the training content for better employee engagement. Next, organisations should make this learning module mandatory for all employees and select contractors. This e-learning module should be followed by a mandatory assessment of employees'/ contractors' knowledge.

As there might be limitations to rolling out the e-learning module across all employees/contractors, an alternative is conducting virtual training sessions targeted at specific audiences.

Cyber security workforce capabilities

Having the right set of people and capabilities to manage the advancing cyberthreat landscape is an important aspect for any organisation. While organisations have established business operations, it is important to consider how these people capabilities can be upskilled to manage cyber security challenges in the next normal.

Organisations should consider running diagnostics of their current cyber security organisation to understand current capabilities/skills and ways to manage the requirements for the future.

Awareness campaigns

Most cyberattacks start with a phishing, vishing or smishing attack. Hence, it's very important that employees are able to identify tailored, targeted phishing attacks (such as a COVID-19 themed attack).

Organisations should consider conducting a phishing simulation exercise to assess the capability of the whole organisation to respond to these phishing attacks.

About PwC

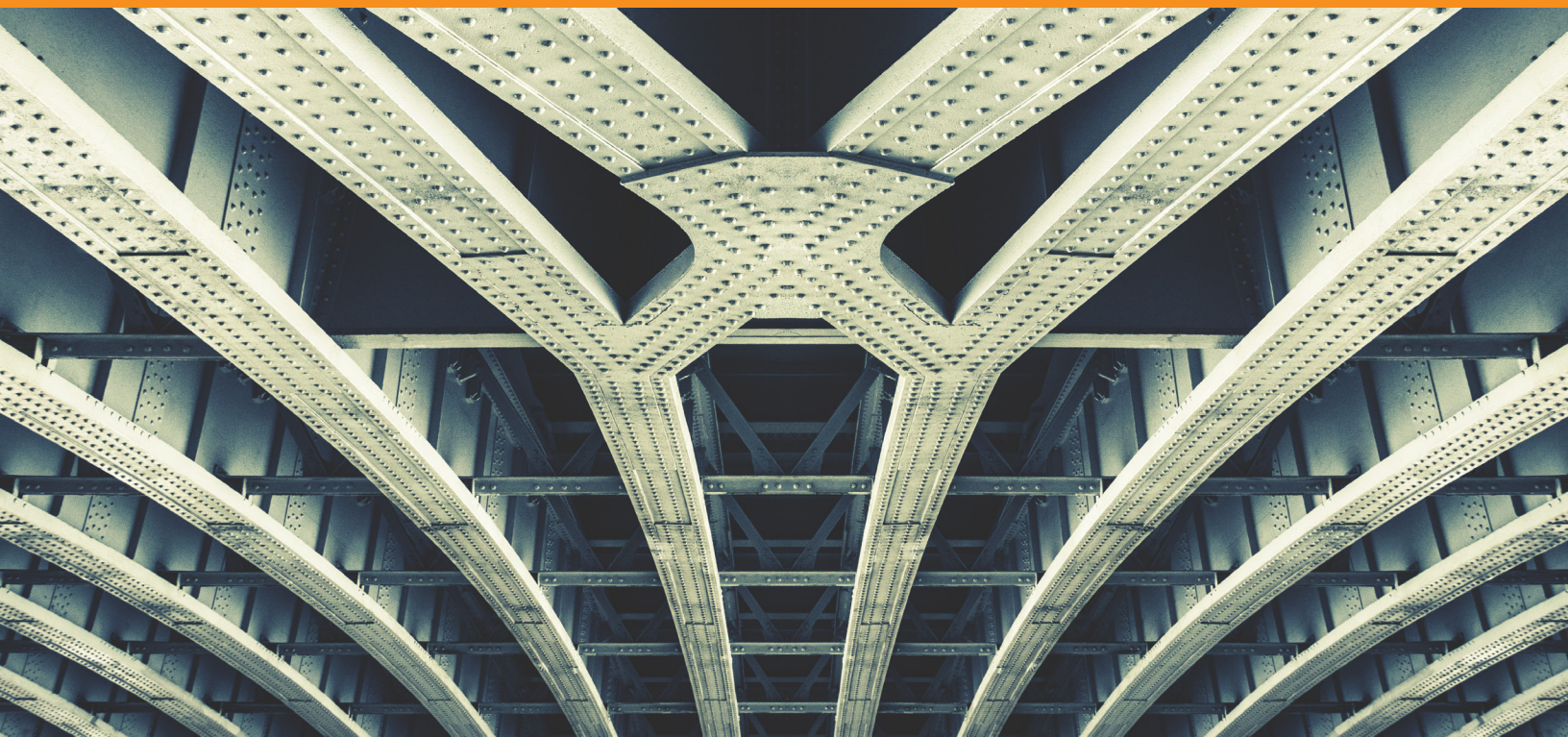
At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

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.

Siddharth Vishwanath
Partner and Cyber Advisory Leader
PwC India
Mobile: +91 91671 90944
siddharth.vishwanath@pwc.com

Ashish Bhugra
Director, Cyber Security
PwC India
Mobile: +91 9619 597 598
ashish.bhugra@pwc.com



pwc.in

Data Classification: DC0 (Public)

SG/July 2020/M&C-6798