Securing the future of business

Cyber security solutions
Digital trust

August 2020
What will the future of business be like?

The COVID-19 crisis has resulted in widespread concerns amongst businesses, clients, consumers and communities worldwide, and is expected to have a significant impact on the global economy. Businesses worldwide have dealt with this unprecedented situation by helping their workforce to work from home (WFH)/work remotely and revamping their business continuity plans, among other steps. Many of these measures are not only point-in-time to deal with the current crisis, but also expected to continue in the post-COVID-19 future.

Future of business

Business resilience
Strengthening business systems and processes to perform seamlessly during a crisis

Low-touch business model
Digital transformation – driving minimum physical contact with customers

Work from anywhere and anytime
Increased emphasis on WFH model, allowing employees the flexibility and their safety

Resource optimisation
Optimal allocation of resources to deliver business outcomes

Supply chain transformation
Increased reliance on local procurement/greater control over supply chains
Security priorities of businesses will be transformed

From a cyber security point of view, we believe that the future of business will revolve around an altered world with seamless and borderless transformation. Organisations are expected to reanalyse cyber security priorities and strive to accordingly adjust to their redefined business requirements.

<table>
<thead>
<tr>
<th>Pre-COVID-19 era</th>
<th>Future of business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Siloed security investments</td>
<td>Security optimisation and consolidation</td>
</tr>
<tr>
<td>Secure organisation and data centres</td>
<td>Secure ‘work from anywhere’ model</td>
</tr>
<tr>
<td>Perimeter security/trusted endpoints</td>
<td>Zero trust architecture/ semi-trusted or untrusted personal devices and virtual desktop infrastructure (VDI) adoption</td>
</tr>
<tr>
<td>Traditional security monitoring</td>
<td>Predictive security monitoring</td>
</tr>
<tr>
<td>Mitigation of all risks</td>
<td>Risk-based focused remediation</td>
</tr>
<tr>
<td>Facility-dependent application access</td>
<td>Secure cloud adoption</td>
</tr>
<tr>
<td>Structured identity solutioning</td>
<td>Managing identities on the go</td>
</tr>
</tbody>
</table>
PwC’s cyber security solutions will aid in securing the future of business

Our cyber security solutions will help organisations enhance their security maturity and adjust to the future of their business requirements.

- Security optimisation
- Perimeter-less workforce security
- User behaviour monitoring
- Next-generation threat management
- SwiftSecure Cloud solution
- Intelligent identity and access management
The economic impact of the COVID-19 crisis may increase the cost pressure on businesses. Optimising cyber security investments would become an imperative for many businesses to enhance their security posture.

### Security technology optimisation

- Evaluate incumbent network security architecture and cast off non-essential/redundant security tools.
- Optimise licensing costs for products based on their usage.
- Consider open source/commercially competitive security products in the network.

### Fixed costs to variable costs

- Managed Security Services (MSS) ‘in-a-box’ for end-to-end security monitoring.
- Transform the on-premise security solutions landscape and move to cloud-based solutions (e.g. cloud firewall, privileged identity management [PIM]).

### Optimise security team structure

- Redesign security organisation structure.
- Institutionalise virtual security team on shared-model basis.
- Drive governance, security approvals and regulatory compliances through virtual collaboration.

### Automation and other opportunities

- Automate security processes (e.g. DevSecOps, user management).
- Automate/orchestrate incident detection and response (e.g. security orchestration, automation and response [SOAR]).
- Evaluate solutions to drive efficiency in a cost-effective manner (e.g. VDI solutions to cut costs on laptops).
As organisations move towards the future of business, conventional security may no longer be sufficient to address the changing threat landscape. Employees become the new perimeter for security, and protection from opportunistic threat actors becomes critical.

Flexible and rapid-to-deploy security solutions would be the need of the hour to meet cyber security requirements arising out of any unprecedented disruption.

**Zero trust architecture**
- Secure access to resources regardless of location.
- A least privilege and stringent access control strategy.
- Define attributes based on business and data sensitivity.
- Design micro-perimeters.
- Prevent untrusted communication.

**Secure endpoints**
- Assess endpoint security effectiveness
- Assess endpoint patching effectiveness
- Secure VDI implementation
- WFH policies and guidelines updates
- Bring your own device (BYOD) security operating model definition
- Mobile device management (MDM)

**Threat analysis**
- Discover indicators of compromise (such as COVID-themed communication).
- Strategic threat intelligence/dark web monitoring to identify compromise.
- Ready-to-integrate managed detection and response infrastructure.

**Secure culture**
- Web-enabled security awareness training.
- Conduct campaigns to sensitise employees on pseudo-phishing, SMS phishing (smishing) and voice phishing (vishing).
Traditional network and security monitoring will transform to include user behaviour monitoring as one of the critical components. Leveraging security analytics with machine learning (ML)/AI to cover user and entity behaviour to analyse, correlate and detect anomalous interactions among users, systems, applications and data will become the need of the hour.

### Advanced data and behaviour analytics
- Create behavioural baselining and risk scores to detect anomalous behaviours.
- Near real-time detection for compromised accounts, insider threats and data breaches.
- Turnkey solution for existing security event related to a data lake.

### Defend the enterprise with AI and ML
- Leverage advanced AI and ML to filter billions of actions on a network into a list of prioritised threats.
- Classify assets and users to segregate common and anomalous behaviour aligned with business practices.
- Use security analytics to bypass manual processes and spend time investigating risk-based prioritised alerts.

### Detect threats at the speed of business
- Contextualise alerts in relation to users, devices and events.
- Provide important perspectives for alert triaging to the security operations centre (SOC) teams.
- Programmed and continuous threat detection to monitor corporate data with behavioural analysis, threat intelligence and business context to uncover hidden threats.

### Intelligent incident response
- Rapidly investigate incidents by pivoting on anomalous entities and tracing associated activities and events.
- Accelerate investigations by correlating disjointed events and providing analysts with all relevant information in a single user interface.
While organisations add security measures to protect their businesses, emerging threats seek to derail or bypass these security controls. Next-generation threat management provides automated monitoring, protection and remediation measures. The focus is to provide a complete view of the risk landscape and proactively respond to emerging risks.

### Automated intelligent remediation

- Unified robotic process automation (RPA) based solution integrating different technologies/processes (e.g. scan engine, asset database, incident management tool, threat feed)
- Bot-managed tasks including automated scans, notification and monitoring of remediation
- Correlation and algorithms to prioritise remediation tasks
- Orchestrated remediation and closure validation

### On-the-go patch and configuration update

- Continuous scanning to identify vulnerabilities across the landscape based on a predefined baseline
- RPA-based patch management and configuration management

### One-click risk view across the landscape

- Correlation of vulnerabilities across the infrastructure and application
- Holistic view of vulnerabilities and related exploits
- Unified/single view of risk scores across the landscape, with the ability to drill down to asset level
- Intelligent reports mapping the vulnerabilities-asset applications

### Agility to integrate newer processes

- RPA-based automation with a process designer interface to customise/integrate new processes
- Integration capability with other processes such as a secure software development life cycle (SDLC), DevSecOps and configuration management to enable end-to-end and seamless vulnerability management
The SwiftSecure Cloud solution will help businesses drive efficiency, reduce overheads and make themselves commercially viable while ensuring that cyber security is incorporated appropriately across the journey.

**Accelerate secure cloud adoption, driven through PwC’s partnerships with leading cloud service providers (CSP) (AWS/Azure/GCP)**

- Security strategy, policies and guidelines aligned to a cloud adoption strategy
- Ready-to-deploy cloud security stack
- Security-enabled solution with reference architecture, Center for Internet Security (CIS) benchmarks and others for secure environment
- Cloud security assessment and management to provide assurance to businesses and IT

**Enhance maturity of existing cloud environment**

- Cloud identity integrated lifecycle management
- Cloud access management for secure access to cloud resources
- Secure configuration and operations in a multi-cloud environment
- Threat intelligence and vulnerability management

**Securing cloud operations**

- Cloud security monitoring for proactive identification of potential security threats
- Detect, prioritise and remediate vulnerabilities
- Incident management and forensics investigation for responding to securing issues
- Training and awareness for employees

**Achieve and maintain compliance**

- Compliance with regional and sector-specific requirements
- Privacy requirements for data transfer and access
- Third-party auditing for security assurance
Intelligent identity and access management

Managing identities on-the-go will become a prerogative for businesses to govern a complex ecosystem of stakeholders operating anywhere and anytime.

Comprehensive, automated and streamlined identity management solutions will help businesses drive process automations, efficient compliance fulfilment and other requirements.

**Lightweight ready-to-use platform**

- Turnkey solutions to solve end-to-end identity governance and access management challenges.
- Complete identity management (IDAM) with advanced product capabilities delivered as cloud-ready, on-premise and plug-and-play options.
- Workflows to automate processes for managing identities and accesses across enterprise applications.
- Secure single-click access to all applications across all platforms with single sign-on (SSO) and multifactor authentication (MFA) capabilities.

**Advanced analytics engine for effective governance**

- AI/ML to create accurate predictive and actionable insights for discovery and remediation
- Automated policy-driven access certification to enable remediation and reporting
- Audit-ready compliance-statutory solution for SOX, HIPAA, ISO27001 etc.
- Intelligent analytics engine for enhanced identity control with data mining and analytics
- Advanced user interface (UI) dashboard for 360-degree coverage

**Autonomous services for select adoption**

- Adoption of discrete solutions/services from the suite as per the requirements.
- Pricing flexibility with pay-as-you-go consumption-based models.
- Self-service for access request, password reset, etc., to optimise desk costs.
- Access provisioning and de-provisioning automation to streamline onboarding and offboarding processes.
- Access review as a service to eliminate manual efforts on IT audits and provide a more secure environment.
- Save time and decrease costs with reduced implementation cycles and ongoing maintenance costs.

**Flexible to augment, integrate or replace**

- Agile solution to address IDAM-specific necessities including identity governance and administration (IGA), access management (MFA and SSO), authorisation and PIM/privileged access management (PAM).
- Ability to integrate new related processes as per business needs
- Support any already-deployed identity access management (IAM) solution
- Agile effortless integration with IT service management solution
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.

© 2020 PwC. All rights reserved.

Contact us

Sivarama Krishnan
Risk Consulting Leader
PwC India
sivarama.krishnan@pwc.com

Amol Bhat
Partner, Cyber Security
PwC India
amol.bhat@pwc.com

Anirban Sengupta
Partner, Cyber Security
PwC India
anirban.sengupta@pwc.com

Hemant Arora
Partner, Cyber Security
PwC India
hemant.arora@pwc.com

Siddharth Vishwanath
Partner and Leader, Cyber Security
PwC India
siddharth.vishwanath@pwc.com

Manu Dwivedi
Partner, Cyber Security
PwC India
manu.dwivedi@pwc.com

Prashant Mehendru
Executive Director, Cyber Security
PwC India
prashant.mehendru@pwc.com

Rahul Aggarwal
Partner, Cyber Security
PwC India
rahul2.aggarwal@pwc.com

Ramanathan V. Periyagaram
Partner, Cyber Security
PwC India
ram.periyagaram@pwc.com

Sangram Gayal
Partner, Cyber Security
PwC India
sangram.gayal@pwc.com

Saritha N Auti
Executive Director, Cyber Security
PwC India
saritha.auti@pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
PwC India
sundareshwar.krishnamurthy@pwc.com

Unnikrishnan P
Partner, Cyber Security
PwC India
unnikrishnan.padinjyaroott@pwc.com

Venkateshwar Nippani
Partner, Cyber Security
PwC India
venkat.nippani@pwc.com

Data Classification: DC0 (Public)

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

© 2020 PricewaterhouseCoopers Private Limited. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

KS/August 2020 - M&C 5960