The future ahead: Evolving cyber security priorities in India

August 2021

pwc

DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Preface

Dear reader,

It is our pleasure to bring to you our thought leadership report, ‘The future ahead: Evolving cyber security priorities in India’, which is a continuation of our ‘Cyber security: India market’ report. Launched in December 2019 during the Annual Information Security Summit (AISS), the previous report offered insights into the growth in domestic demand for cyber security in India. With the latest report, we have attempted to gauge how cyber security priorities are evolving during and post the pandemic.

The cyber security ecosystem is at a critical point. The increasing number and complexity of cyberattacks, coupled with rapid digitisation driven by the pandemic, have emphasised the importance of cyber security in businesses of all sectors and sizes. To find out what’s next in cyber security, we conducted a study with over 100 business and technology executives in India.

Based on our study, this paper highlights the key trends for the future of business, the evolving cyber security priorities and the various ways of optimising the cyber security function. In addition, it underlines the shift of focus towards digitisation, increasing significance of business resiliency, rapid adoption of cloud computing, localisation of supply chain ecosystems, and the need for optimised allocation of resources.

We hope you will find this report to be an insightful read.

Rama Vedashree

CEO, Data Security Council of India

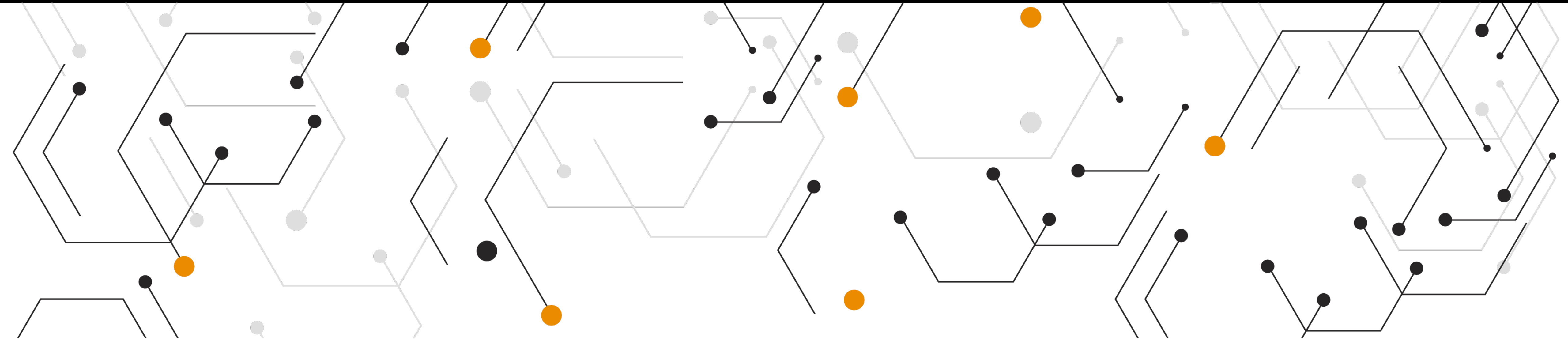
Sivarama Krishnan

Partner and Leader, APAC Cyber and India Risk Consulting, PwC

Siddharth Vishwanath

Partner and Leader, Cyber Security, PwC India

Table of contents



1 Introduction

Introduction

Businesses not just in India but across the globe are undergoing rapid transformation and adopting new technology-driven ways of working. Though technology intervention helps streamline processes and customer service delivery, it also expands the security threat landscape, necessitating a shift in cyber security priorities. As a result, organisations are looking to enhance their capabilities in order to successfully navigate the changing threat landscape and evolving priorities and ensure protection of their data and continuance of business.

Hence, to assess this evolving landscape, we conducted a survey and analysed responses from more than **100 Indian organisations** on the changing cyber security priorities in some key focus areas. This report presents an analysis of the responses, together with our point of view on the same.

We looked at the priorities of stakeholders (CIOs, CISOs, technology heads, among others), along with what drives the need to have effective cyber security mechanisms across different sectors. Our survey covered organisations across the following sectors: banking, financial services and insurance (BFSI); government and public sector (G&PS); consumer industrial products and services (CIPS, i.e. automotive, pharma, chemical, industrial manufacturing); technology, media and telecom (TMT); hospitality; leisure; transportation; logistics; infrastructure; and capital projects.

Domains of the study

Enabling the future of business

Gauges the point of view on the future of business of the survey respondents' industry/organisation.

Threat landscape

Seeks to understand how the security threat landscape is changing for the survey respondents' industry/organisation.

Cyber security priorities

Identifies the priorities for the survey respondents' organisations with respect to security initiatives and plans for enhancing the security posture.

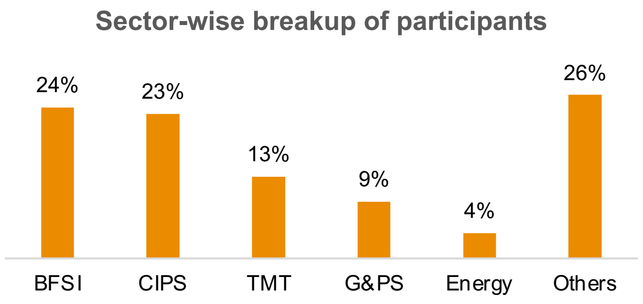
Security optimisation

Seeks to understand how executives are trying to optimise cyber security investments in their organisation.

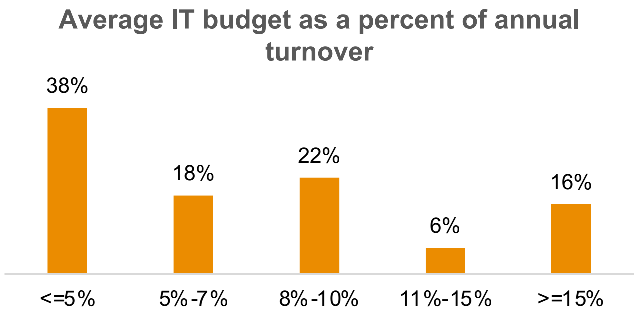
Demographics of survey participants

Organisations of varying sizes and from across various sectors participated in the survey. Participant demographics are shown below.

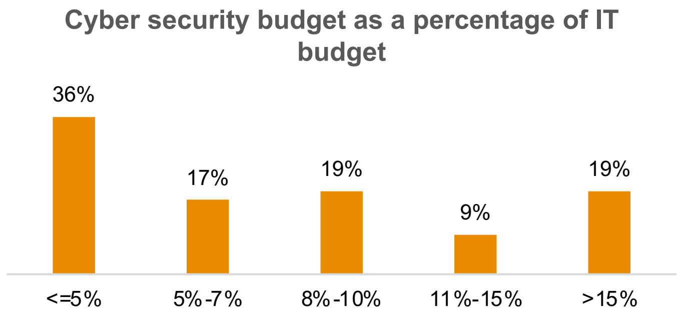
Question: What is your organisation's primary industry sector?*



Question: What is the average IT budget of your organisation as a percentage of the revenue?*

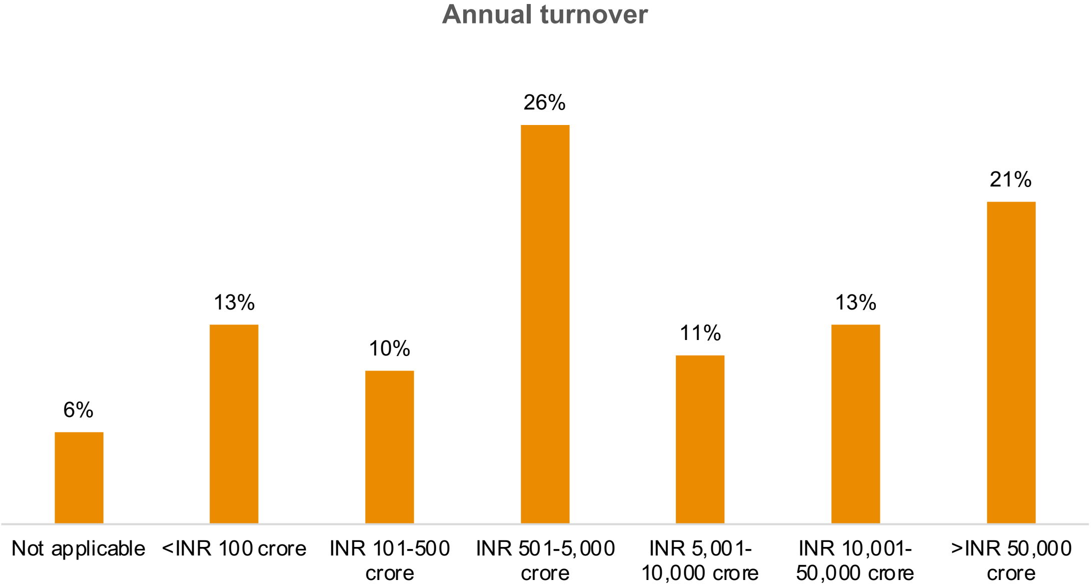


Question: What is the cyber security budget of your organisation as a percentage of the IT budget?*

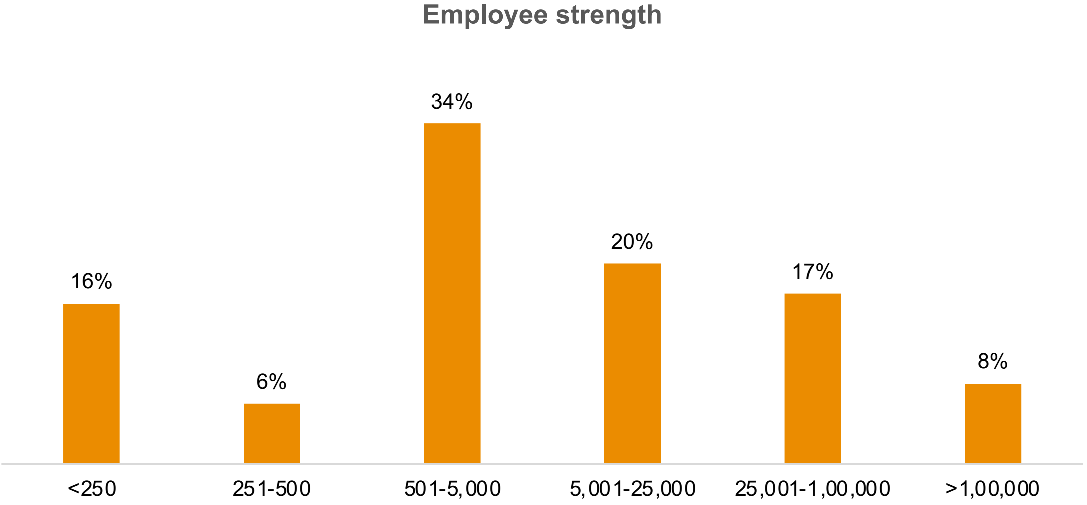


***Source**: DSCI-PwC survey

Question: What is the annual turnover of your organisation?*



Question: What is the overall employee strength of your organisation?*



***Source**: DSCI-PwC survey

2 Future of business and the evolving threat landscape

Organisations are transforming their ways of working

As India emerges from the ongoing impact of the pandemic, businesses, consumers and communities are changing their ways of working faster than ever before to address the profound challenges that they face, making the most of the tremendous opportunities ahead of them.

In our survey, we asked executives to respond to the following parameters surrounding the future of business:

01 Digital transformation

Nearly **49%** of the respondents strongly agree to the fact that digital transformation will play a key role going forward.

02 Business resilience

Over **43%** of the executives strongly agree that investing in building or enhancing business resilience.

03 Cloud adoption

Around **38%** of the executives strongly agree that cloud will play a major role in the future of business.

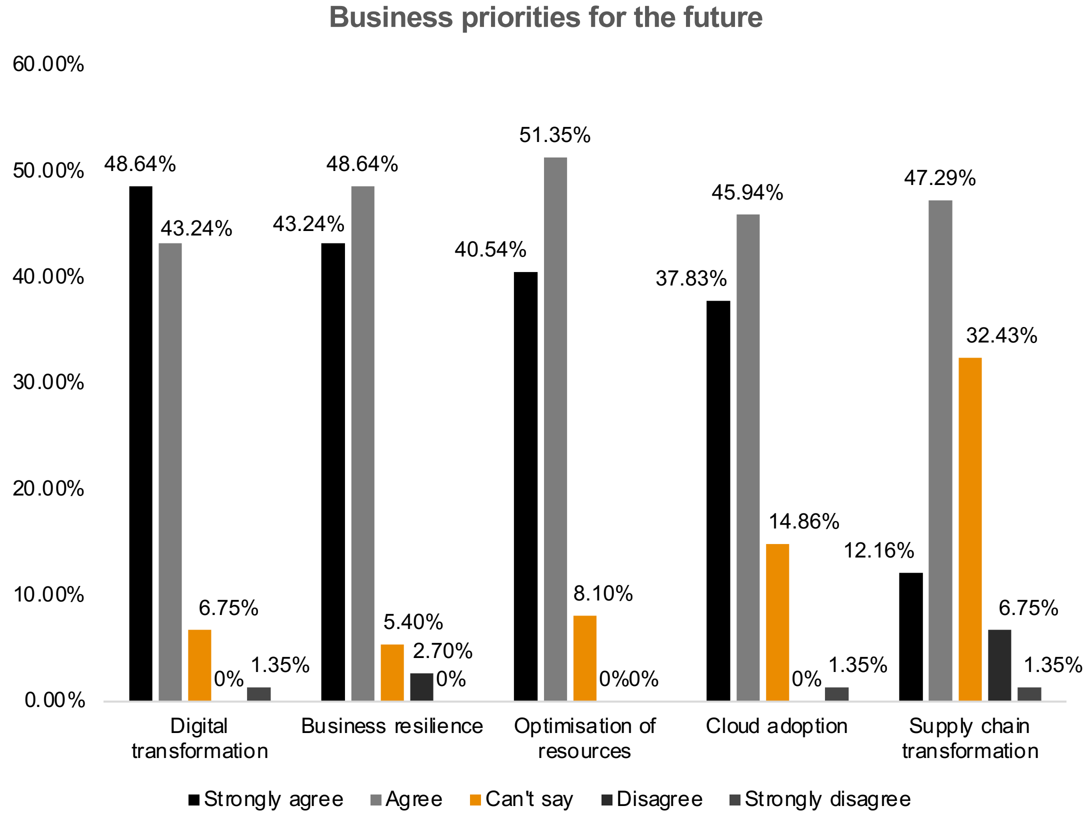
04 Supply chain transformation

Over **12%** of the executives strongly foresee a shift in the focus of procurement towards local suppliers.

05 Optimisation of resources

Efficient performance with optimised allocation of resources is one of the top priorities for nearly **41%** of the executives.

Question: From the parameters below, please choose those which are priorities for the future of your business.



Source: DSCI-PwC survey

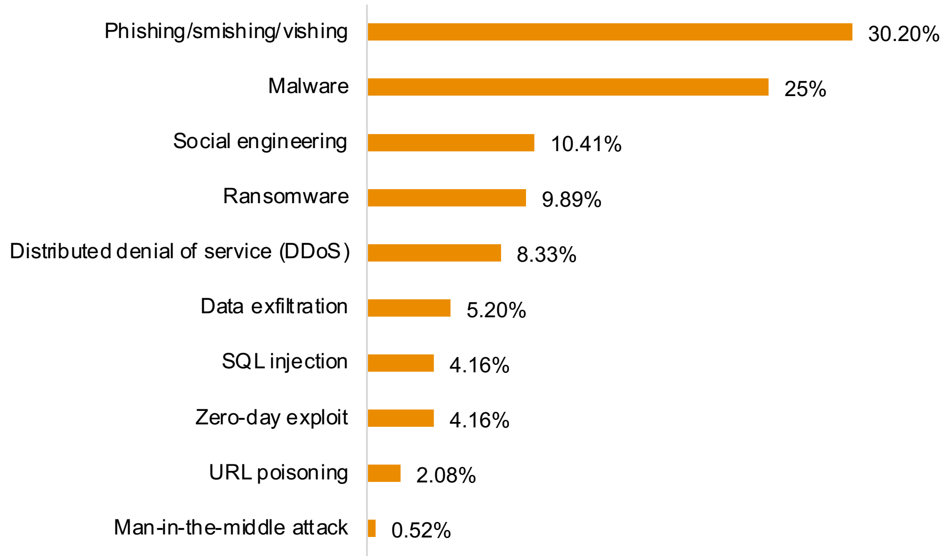
Cyberattacks, which were already on the rise, are increasing exponentially and becoming more targeted

Cyberattacks are not only increasing in number…

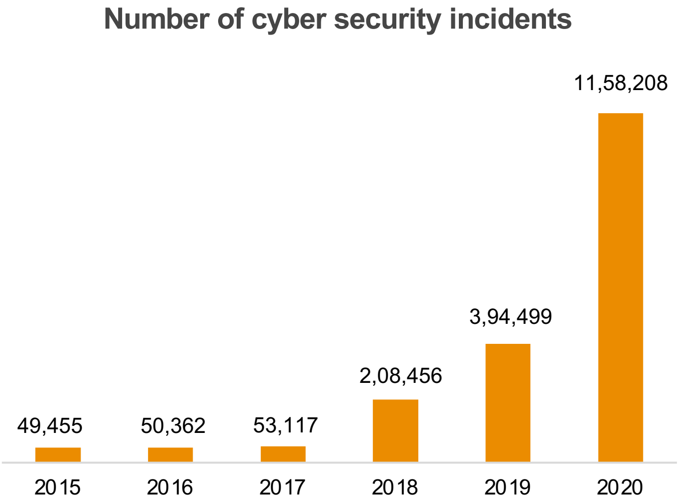
There has been a rise in cyber incidents following the COVID-19 outbreak. In the past few months, the number of cyberattacks on Indian organisations has increased significantly. The ongoing crisis has given malicious actors a favourable opportunity to launch cyberattacks as countries worldwide are busy handling the pandemic.

Question: What are the top types of cyberattacks that your industry/organisation is facing?

Top cyberthreats faced by Indian organisations



Source: DSCI-PwC survey



3X

increase in cyber security incidents in 2020 as compared to 2019

Source: CERT-In

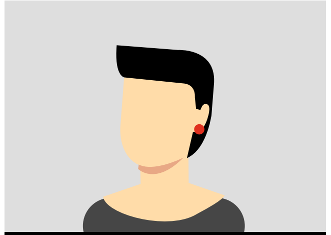
Note: *The figures reflect the number of cyber security incidents in India from the year 2015 to the year 2020.*

…but also becoming more and more targeted.

- There is a surge in cyber security attacks as well as a shift towards more targeted cyberattacks on businesses.
- Some of the types of pandemic-themed cyberattacks include COVID-19 themed phishing attacks, ransomware attacks and sharing of infected emails containing COVID-19 themed documents.
- Phishing, malware and social engineering are the top cyberattacks targeted at organisations.

Today, cyber security touches every part of the business, driving the need to re-calibrate cyber security priorities

Business leaders already had numerous concerns about cyberattacks…



Boardroom

Do we have the information we need to oversee cyber risks?

CEO

Are we compliant with the applicable laws and regulations?

COO

How do we establish a culture of shared cyber responsibility across the business?

CRO

Do we approach cyber security using a risk-based approach?

CIO/CISO

Are we taking appropriate steps to protect our organisation against cyber risks?

CPO

Are we following applicable privacy laws and regulations?

…and the pandemic and rising number of cyberattacks have further aggravated these concerns.

Are we still secure in this remote working scenario?

Are we resilient enough for a cyberattack?

Have we secured our supply chain, and are we prepared for a disruption in it?

Do we understand the risks emerging out of increasing digitisation and cyberattacks?

Owing to the changing cyber risk landscape, do we need to relook at our cyber security priorities?

Are we collecting more data than required or unnecessary data?

Hence, recalibration of cyber security priorities can help businesses sustain in the long run.

3 Changing cyber security priorities

Businesses are looking to re-prioritise their cyber security focus areas

Strategising cyber priorities

Our survey reveals that ‘improving threat management capabilities’ is the top priority for Indian businesses, with 67.86% of the executives listing it as one of their top three priorities.

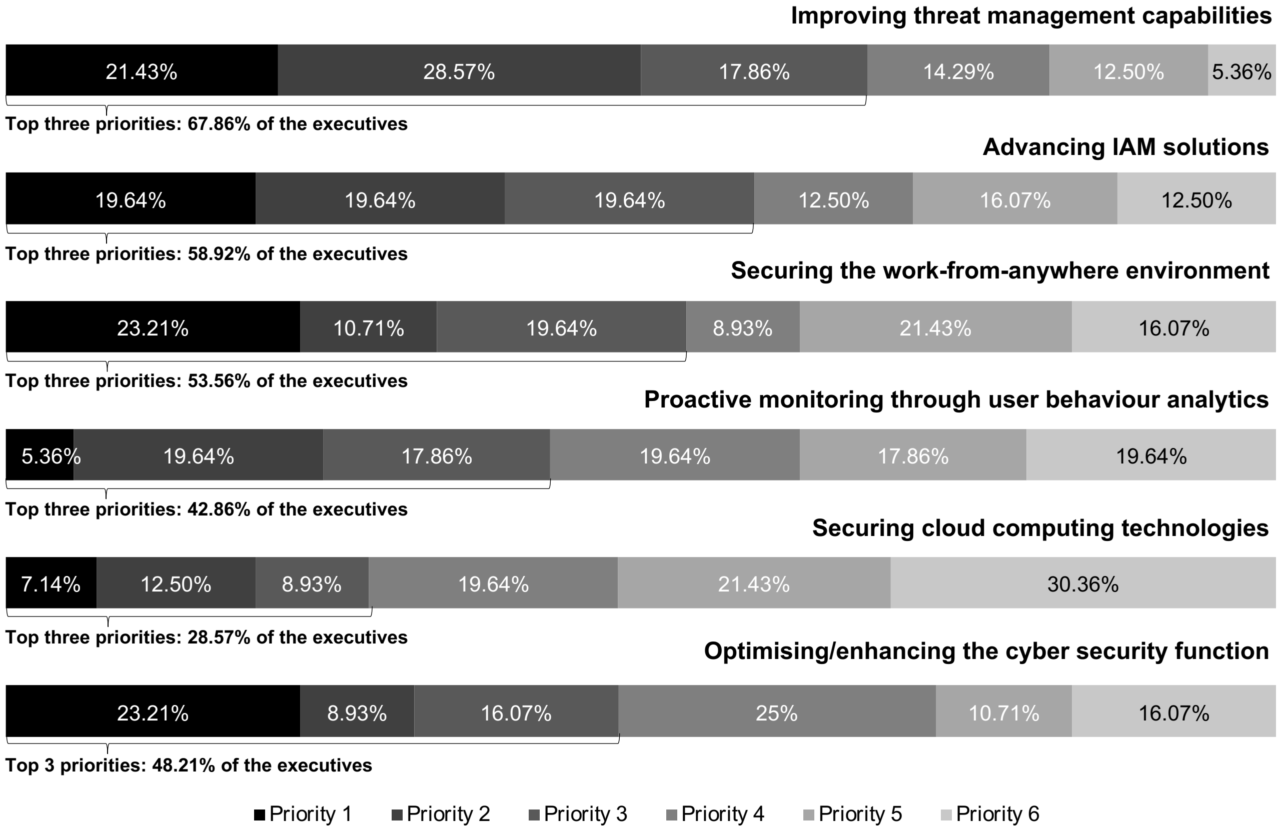
It is followed by ‘advancing identity and access management (IAM) solutions’ and ‘securing the work-from-anywhere environment’, which 58.92% and 53.56% of the survey respondents, respectively, ranked as one of their top three priorities.

We asked our survey respondents to rank the focus areas below in order of priority:

- improving threat management capabilities
- advancing IAM solutions
- securing the work-from-anywhere environment
- proactive monitoring through user behaviour analytics
- securing cloud computing technologies
- optimising/enhancing the cyber security function.

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).

Cyber security priorities of Indian organisations

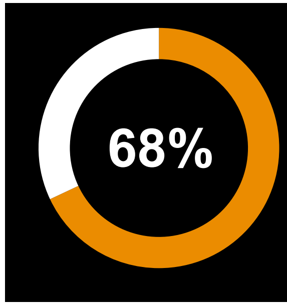


Source: DSCI-PwC survey

01: Improving threat management capabilities

Threat management with risk-based vulnerability prioritisation is currently the topmost priority of Indian executives

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



say improving their organisation's threat management capabilities is their topmost priority

Organisational priorities are shifting, with a focus on getting a complete view of the risk landscape and proactively responding to emerging threats.

Of the 68% of the executives who selected 'improving threat management capabilities' as one of their top three cyber security priorities, 50% have chosen 'risk-based vulnerability prioritisation' as a measure to do so. Further, many executives are moving towards automation, with over 21% selecting 'automated intelligent remediation' and over 13% selecting 'automated orchestration for remediation'.

Source: DSCI-PwC survey

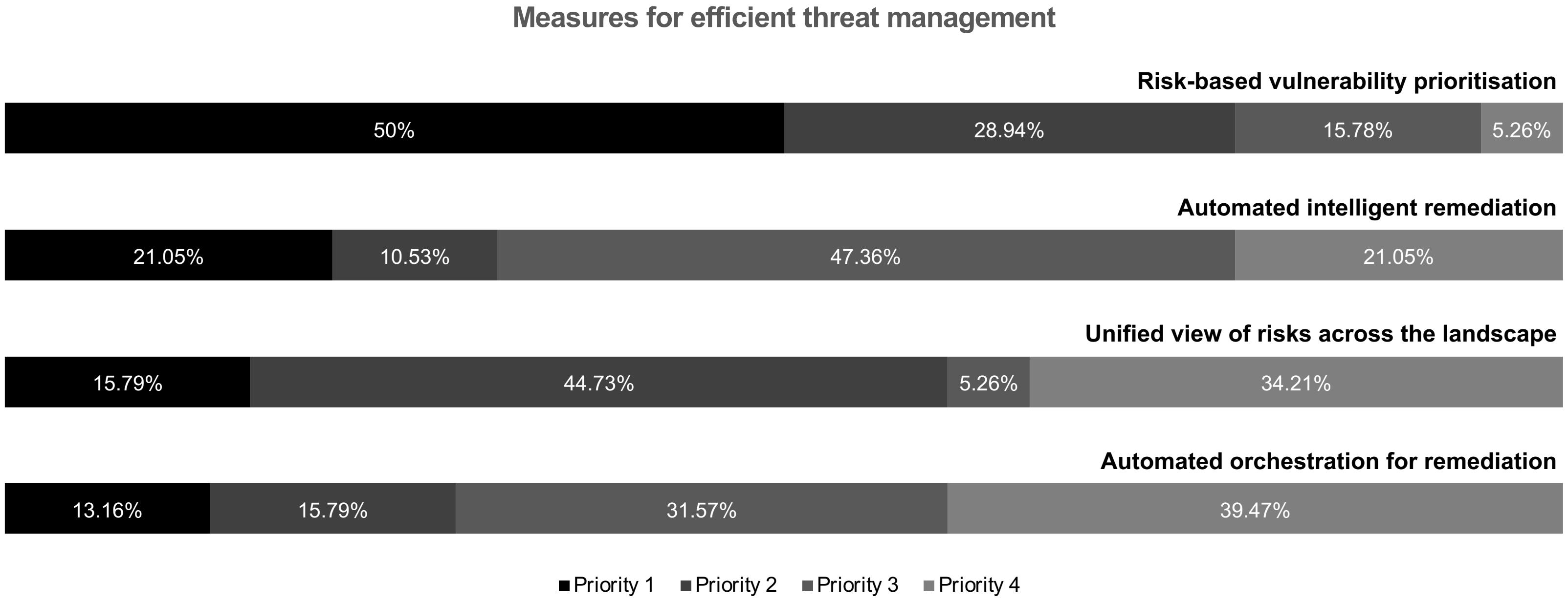
Note: *This figure indicates the percentage of executives, rounded to the nearest whole number, who selected 'improving threat management capabilities' as one of their top three priorities.*

We asked survey respondents to rank the following measures to address threat management requirements in order of priority:

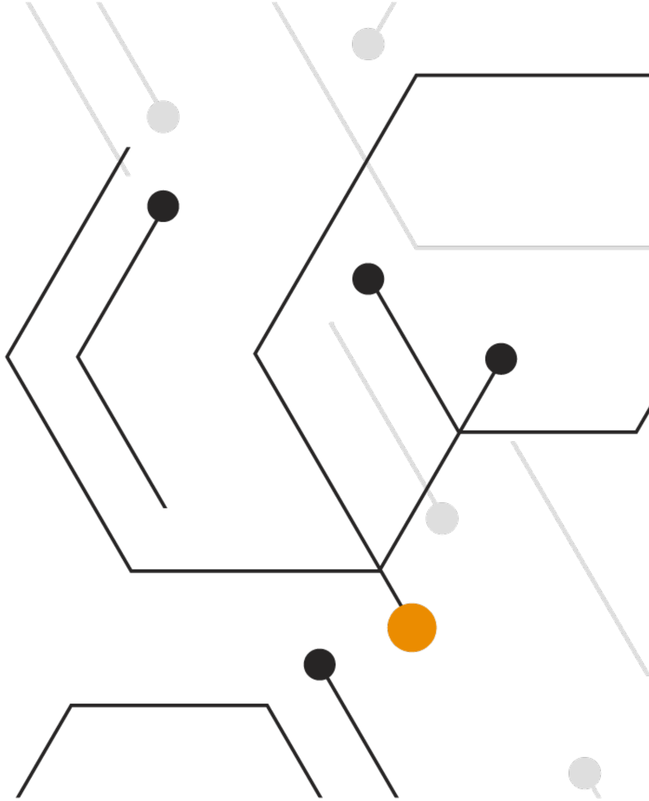
- automated intelligent remediation using machine learning to reduce remediation time and eliminate human errors
- remediation of security vulnerabilities through automated orchestration
- risk-based vulnerability prioritisation to reduce risk across the ecosystem by focusing on remediation efforts based on threats and available data
- a single, unified view of risks across the entire cyber security landscape.

__Note:__ The figures below reflect the views of the executives (68%) who chose 'improving threat management capabilities' as one of their top three cyber security priorities.

Question: Please rank the following measures for efficient threat management in order of priority for your organisation (1: highest priority, 4: lowest priority).



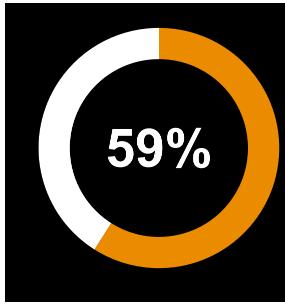
Source: DSCI-PwC survey



02: Advancing IAM solutions

Organisations are actively looking to enhance IAM solutions

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



say they are prioritising the advancement of IAM solutions

Organisations aim to governing complex ecosystems from anywhere and at any time:

- The industry has begun to recognise the importance of existing IAM solutions. Of the executives (59%) who selected advancing IAM as one of their top three cyber security priorities, over 42% have prioritised enhancement of these solutions.
- Businesses are focusing on agile solutions for IAM-specific necessities and implementing various turnkey solutions, with over 39% and over 18% of the executives prioritising these measures respectively.

Source: DSCI-PwC survey

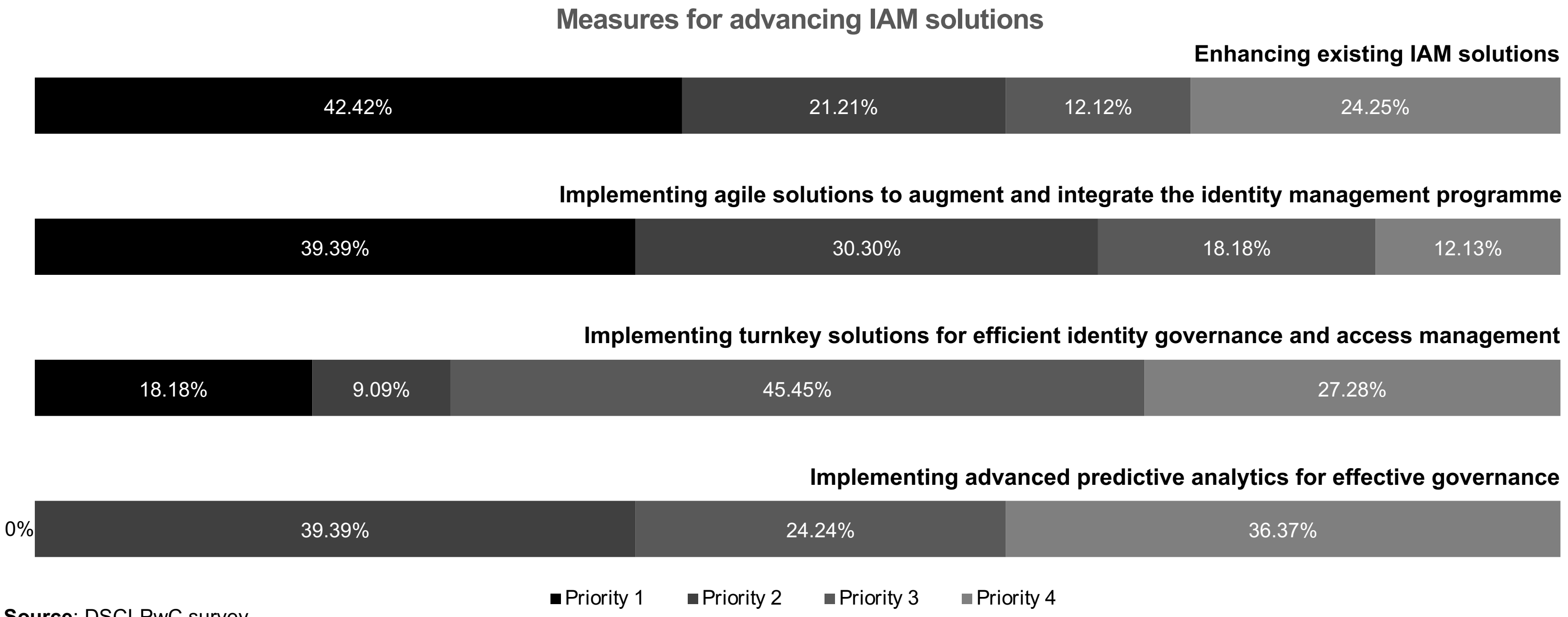
Note: *This figure indicates the percentage of executives, rounded to the nearest whole number, who selected 'advancing IAM solutions' as one of their top three priorities.*

We asked survey respondents to rank the following measures for addressing IAM requirements in order of priority:

- enhancing existing IAM solutions and focusing on increased control and security
- implementing agile IAM solutions to ensure flexibility and scalability
- implementing turnkey solutions for effective identity governance and access management
- implementing advanced predictive analytics to understand risk and user behaviour.

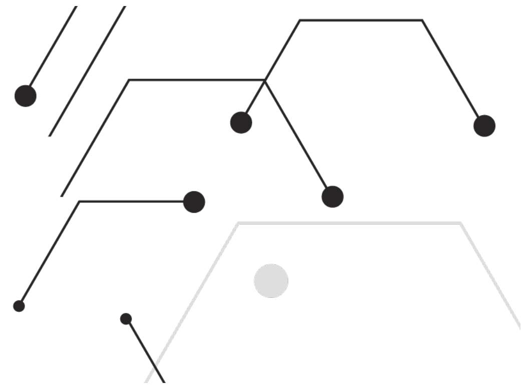
***Note:** The figures below reflect the view of the executives (59%) who selected advancing IAM as one of their top three cyber security priorities.*

Question: Please rank the following IAM measures in order of priority for your organisation (1: highest priority, 4: lowest priority).



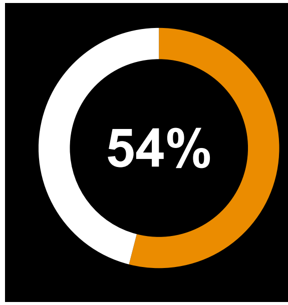
Source: DSCI-PwC survey

03: Securing the work-from-anywhere environment



Organisations are stepping up to the challenge of securing remote working, with an emphasis on creating a stronger security culture through awareness

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



are prioritising securing the work-from-anywhere environment

The number of employees working remotely has increased significantly. As per our survey, 54% of the executives expect over 50% of the workforce to work remotely in the near future. Additionally, nearly 14% of the executives indicate that the percentage of the remote workforce could go as high as 80%.

To secure these perimeter-less networks, of the executives (54%) who selected securing work-from-anywhere as one of their top three cyber security priorities, over 40% have prioritised promoting cyber security awareness and culture, and over 26% are focusing on data security.

Source: DSCI-PwC survey

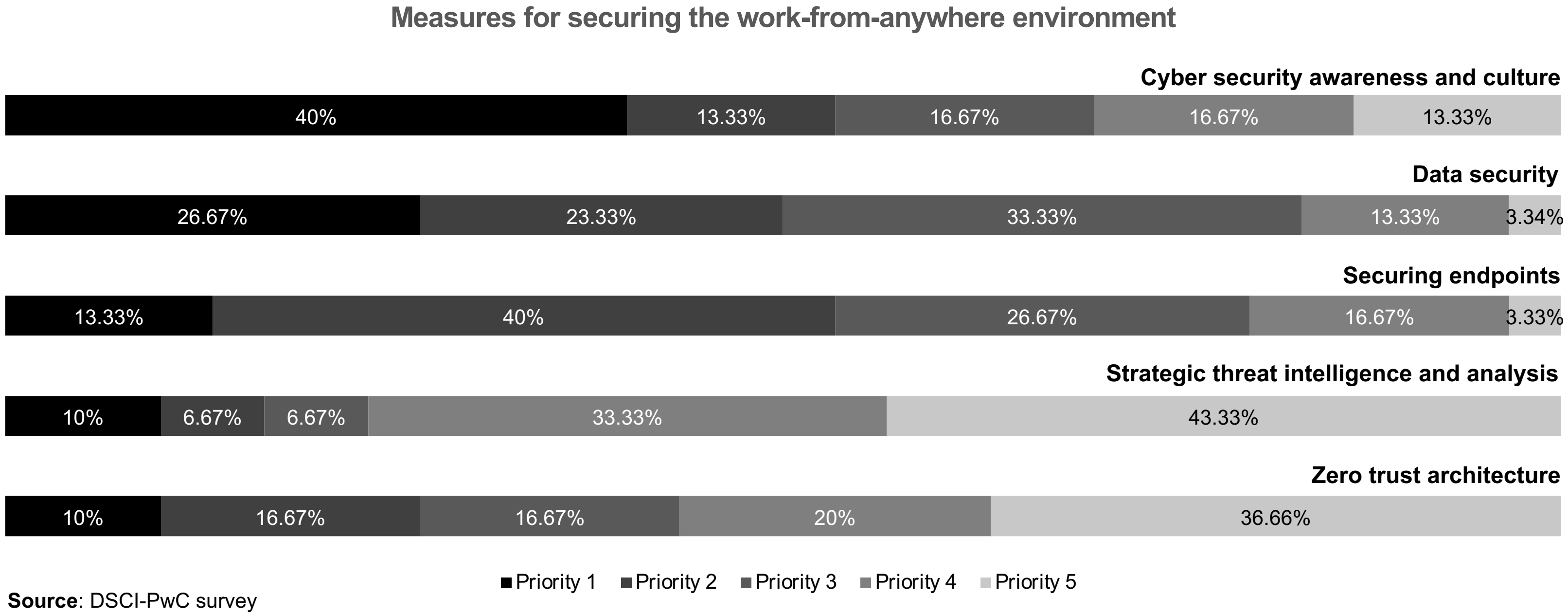
Note: *This figure provides the percentage of executives, rounded to the nearest whole number, who selected 'securing the work-from-anywhere environment' as one of their top three priorities.*

We asked survey respondents to rank the following measures for securing the work-from-anywhere environment in order of priority:

- cyber security awareness and culture for employees and associated partners
- data security to protect data from unauthorised sources
- endpoint security to protect employee end-user devices such as laptops
- implementation of zero-trust architecture by treating all users as potential cyberthreat sources
- strategic threat intelligence and analysis to drive high-level cyber security planning.

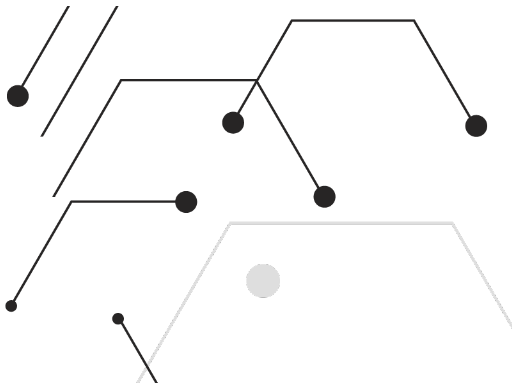
***Note:** The figures below reflect the views of the executives (54%) who selected securing work-from-anywhere as one of their top three cyber security priorities.*

Question: Please rank the following measures for securing the work-from-anywhere environment in order of priority for your organisation (1: highest priority, 5: lowest priority).



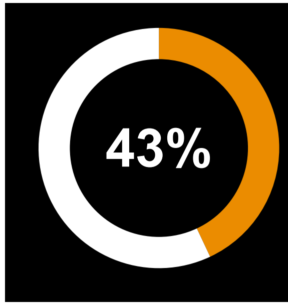
Source: DSCI-PwC survey

04: Proactive monitoring through user behaviour analytics



Organisations are looking to leverage advanced data analytics to proactively monitor anomalous user behaviour

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



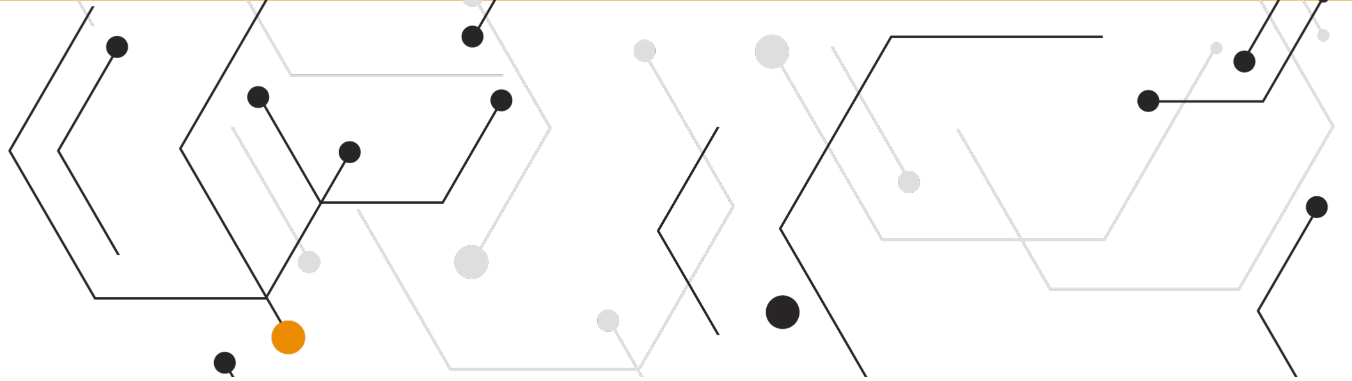
are prioritising proactive monitoring through user behaviour analytics

Of the 43% executives who chose monitoring through user behaviour analytics as one of their top three cyber security priorities, over 62% have prioritised advanced data and behaviour analytics to help detect anomalous user behaviour.

While the above is an obvious preference for most executives, for 12.5% of the respondents, implementation of artificial intelligence (AI) and machine learning (ML) to prioritise threats, advancement of the incident response mechanism and continuous threat detection are each a bigger focus area.

Source: DSCI-PwC survey

Note: *This figure provides the percentage of executives, rounded to the nearest whole number, who selected 'proactive monitoring through user behaviour analytics' as one of their top three priorities.*



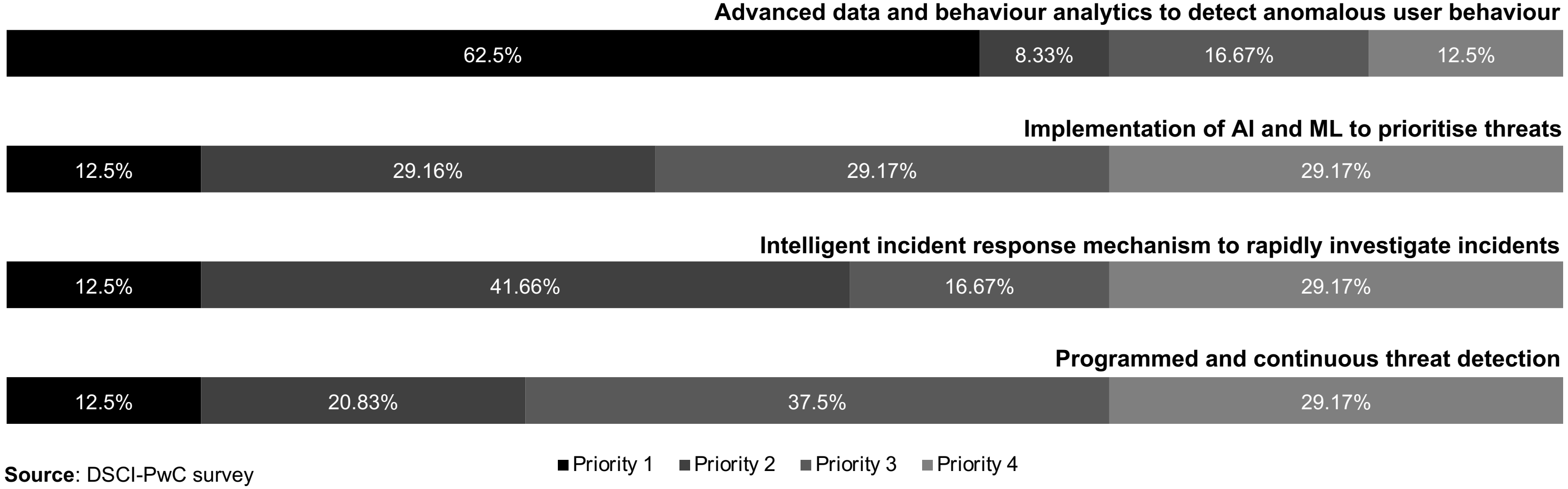
We asked survey respondents to rank the following measures for proactive monitoring through user behaviour analytics requirements in order of priority:

- advanced data and behavioural analytics to detect anomalous user behaviour, contextualising alerts in relation to users, devices and events
- use of AI and ML to filter billions of actions on a network and list down prioritised cyberthreats
- intelligent incident response mechanism, reviewing incidents by prioritising anomalous entities and tracing associated activities and events, to accelerate security investigations
- programmed and continuous threat detection for effective and quick remediation.

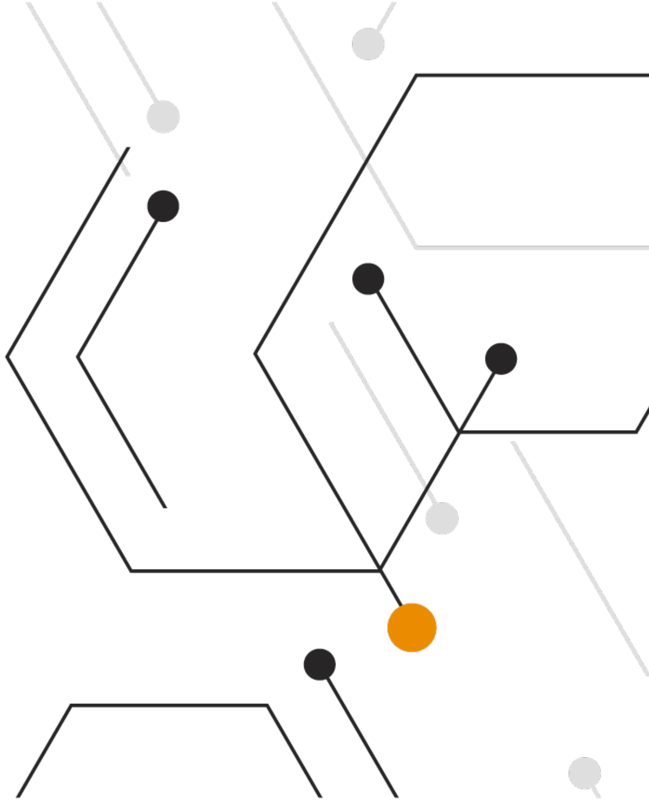
***Note:** The figures below reflect the views of the executives (43%) who chose monitoring through user behaviour analytics as one of their top three cyber security priorities.*

Question: Please rank the following measures for proactively leveraging user behaviour or analytics in order of priority for your organisation (1: highest priority, 4: lowest priority).

Measures for proactive monitoring through user behaviour analytics

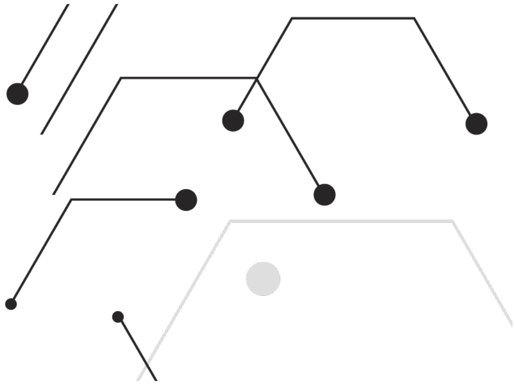


Source: DSCI-PwC survey

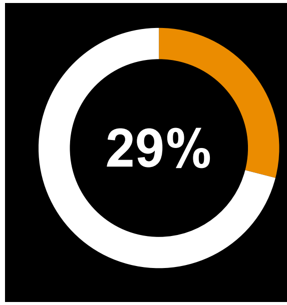


05: Securing cloud computing technologies

Organisations are considering enhancing the security maturity of their cloud environment



Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



are prioritising securing of cloud computing technologies

Businesses are seeking efficiency, reduced overheads and commercially viable solutions that guarantee cyber security.

Of the executives (29%) who chose securing cloud computing technologies as one of their top three cyber security priorities, nearly 43% are working towards enhancing the security maturity of their existing cloud environment, while over 28% are trying to accelerate secure cloud adoption.

Source: DSCI-PwC survey

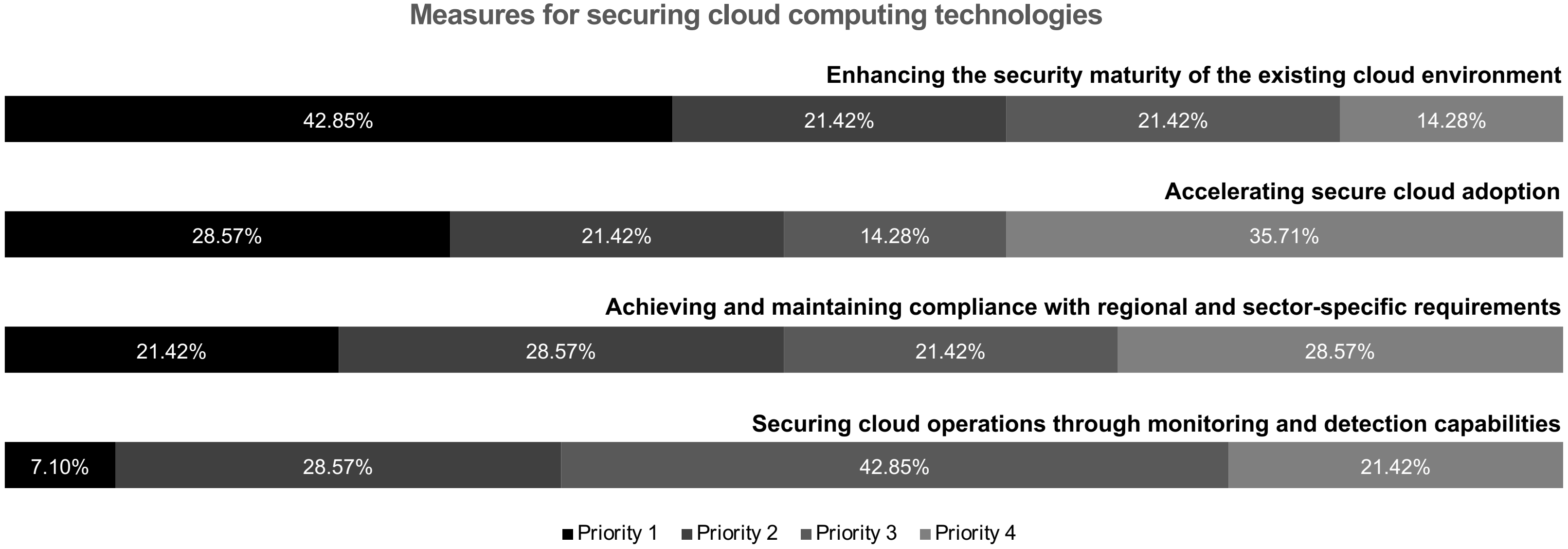
Note: *This figure indicates the percentage of executives, rounded to the nearest whole number, who selected 'securing cloud computing technologies' as one of their top three priorities.*

We asked survey respondents to rank the following measures to secure cloud computing technologies in order of priority:

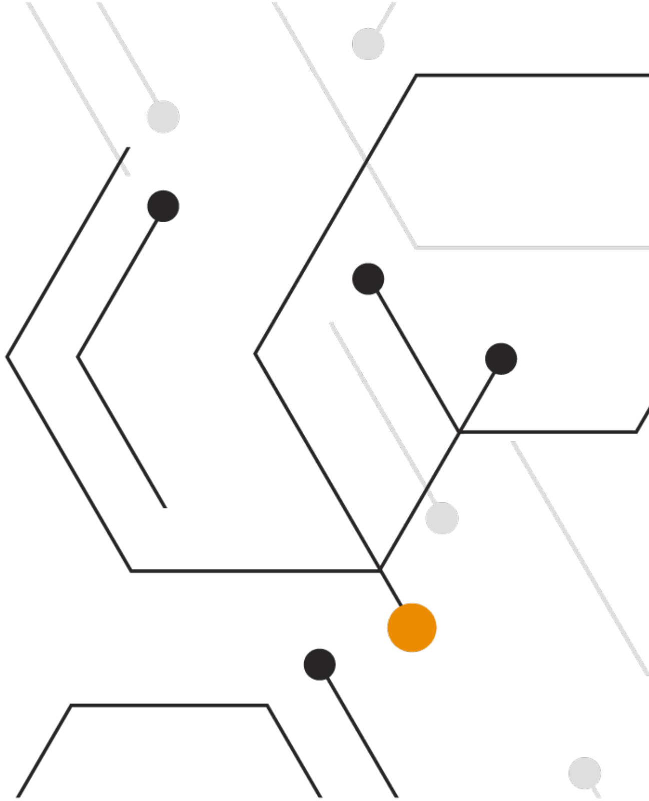
- enhancing the security maturity of existing cloud environments
- accelerating secure cloud adoption
- complying with relevant laws and sector-specific requirements
- securing cloud operations through monitoring and detection capabilities.

Note: *The figures below reflect the views of the executives (29%) who chose 'securing cloud computing technologies' as one of their top three cyber security priorities.*

Question: Please rank the following measures for securing the cloud ecosystem in order of priority for your organisation (1: highest priority, 5: lowest priority).



Source: DSCI-PwC survey



4 Dichotomy between enhanced security and optimisation

Though cyber security budgets are increasing, decision makers still face business pressure to optimise the cyber function

As cyber security priorities evolve, a dichotomy has emerged between enhancing the security capabilities of an organisation and optimising available resources.

Organisations are facing ever-increasing cyber risks and need to prioritise the enhancement of their security capabilities. At the same time, due to financial pressure, cyber security budgets are not increasing at the same pace as requirements. Hence, cyber spending may not be aligned with the most significant risks.

On one hand, 72% of the executives predict that the YoY cyber security budgets will increase by over 5%. On the other, for over 48%, optimising/enhancing the cyber security function is among their top three cyber security priorities.

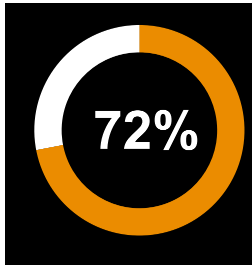
This has given rise to a dichotomy between enhancing cyber security capabilities on the one hand and optimising the available resources on the other.

Businesses face a dichotomy between

↑ enhancing cyber security capabilities

↓ optimising cyber security resources

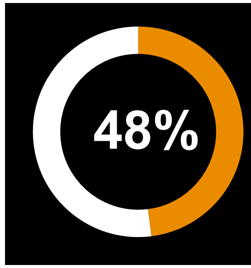
Question: What is your foresight on the cyber security budget (year-on-year) in the upcoming 3 years for your organisation?



predict that their YoY cyber security budget will increase by over 5% in the next three years

Source: DSCI-PwC survey

Question: Rank the areas below in order of priority for your organisation (1: highest priority, 6: lowest priority).



say that optimising/enhancing the cyber security function is one of their top three cyber security priorities

Source: DSCI-PwC survey

5 Optimisation as a key imperative

Organisations are working on three key levers to optimise cyber security spends

The DSCI-PwC survey asked executives to share their views on the three key dimensions of their cyber security functions.

We asked survey respondents to rank the following measures to optimise/enhance cyber security cost in order of priority:

- automation in cyber security
- technology optimisation/enhancement
- optimisation of security operations.

01 Automation

Leveraging automation as the foundation for managing security processes will help in optimising the effort and resources required for handling cyber security.

02 Technology optimisation/enhancement

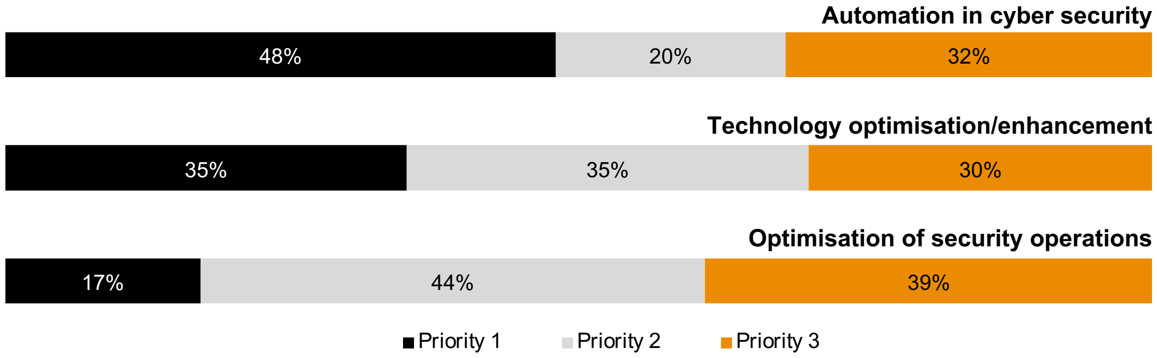
Businesses can optimise their security landscape through technology consolidation and leverage an open-source technology stack to reduce costs.

03 Optimisation of security operations

Security operations can be optimised through managed security services, cloud-based service delivery and transaction-based pricing models.

Question: Please rank the following measures for cyber security cost optimisation/enhancement in order of priority for your organisation (1: highest priority, 4: lowest priority).

Measures to optimise/enhance cyber security cost



Source: DSCI-PwC survey

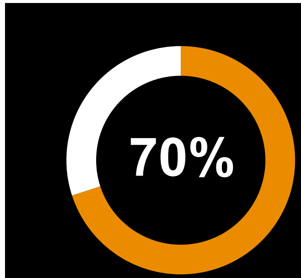
01 Leveraging automation for routine tasks

For 31% of the executives, automating threat detection and response capabilities is the number one priority, while the corresponding figure for automation in deployment leveraging continuous integration (CI) and continuous delivery (CD) is 35%. Similarly, for 31% of the executives, the first priority is automating security monitoring tools.

Nearly 92% of the executives are also looking at automating the security vulnerability management lifecycle and 92% are considering orchestration/automation, including DevSecOps/SOAR in the next 12 months.

These automation requirements stem from the fact that businesses are looking to automate repetitive functions, streamline workflows and orchestrate security tasks due to staff shortage and cost pressures.

Question: In your view, roughly what percentage of your manual work can be reduced through automation?



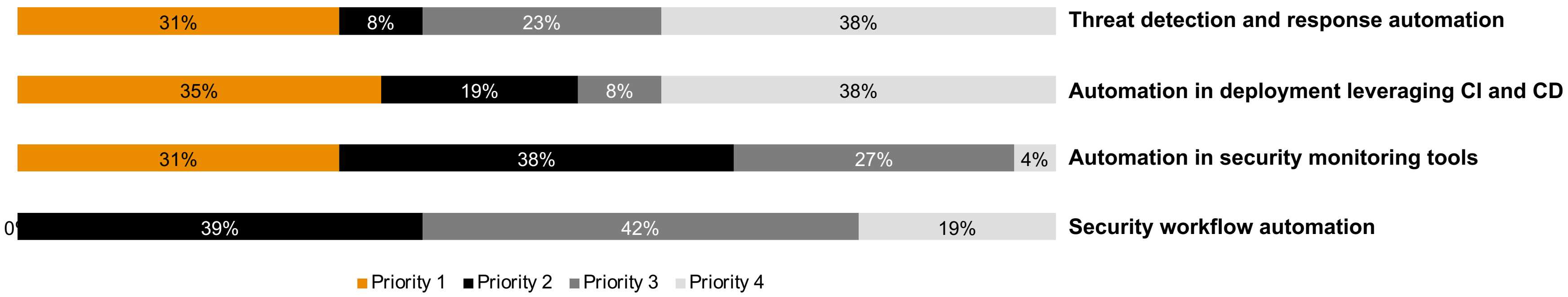
say that over 10% of manual work can be reduced through automation

Source: DSCI-PwC survey

Note: *The figures in the graphs above reflect the views of the executives (48%) who chose automation in cyber security as the first priority for cyber security cost optimisation/enhancement.*

Question: Rank in order of priority the areas of automation which would help enhance the cyber security posture of your organisation (1: highest priority, 4: lowest priority).

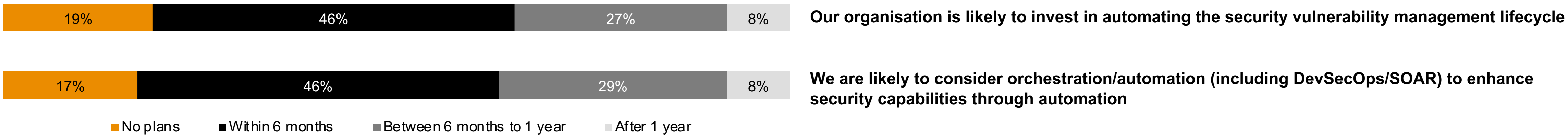
Areas of automation



Source: DSCI-PwC survey

Question: When do you plan to adopt/invest in security automation?
Option 1: Our organisation is likely to invest in automating the security vulnerability management lifecycle.
Option 2: We are likely to consider orchestration/automation (including DevSecOps/SOAR) to enhance security capabilities through automation.

Plan for automation



Source: DSCI-PwC survey

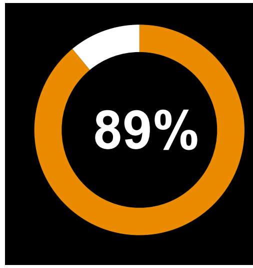
Note: *The figures in the graphs above reflect the views of the executives (48%) who chose automation in cyber security as the first priority for cyber security cost optimisation/enhancement.*

02 Understanding and consolidating the security technology landscape

Scope for improvement in redundant security tools and technologies

82% of the executives acknowledge the presence of redundant security tools and technologies in their businesses. They realise the need to regularly assess their existing security technology stack for relevance as the functions of various security solutions tend to overlap. Hence, it becomes imperative to optimise the implementation of security technologies across all the layers in an organisation for comprehensive security coverage.

Question: Is there scope for improving the redundant or underutilised tools/technologies/software licences in your organisation?



agree/strongly agree that there is scope for improvement in redundant or underutilised tools/technologies/software licences

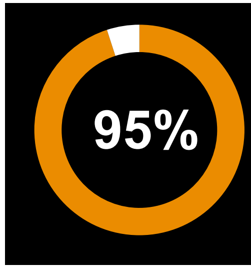
Source: DSCI-PwC survey

Note: *The figures in the charts above reflect the views of the executives (35%) who chose technology optimisation as the first priority for cyber security cost optimisation/enhancement.*

Consolidating security technologies can also support optimisation

91% of the executives agree that it is cumbersome to manage multiple security tools and technologies and prefer using a single technology that can offer many benefits. This is important as consolidation of technologies can help in optimising cyber security as security tools require seamless integration with multiple functions of a business and their management is an entirely different challenge.

Question: Is the management of numerous security tools and technologies a cumbersome task, and would you prefer to use a security tool that provides multiple capabilities?

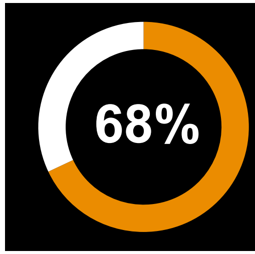


agree/strongly agree that they are more likely to use security tools providing multiple capabilities

Open-source security stacks are helping businesses keep pace with cyber security risks

Many businesses are already using open-source security software stacks. As per our survey, 82% of the executives say that they will consider the use of open-source software or cyber security solutions manufactured by domestic start-ups. Agility is a critical requirement in a highly dynamic function such as cyber security. Hence, businesses are looking at flexibility and innovation as a necessary requirements. This is where open-source security stacks establish their durability and advantage.

Question: Would you consider the use of economical security solutions (including open-source tools, Make in India/start-up cyber security solutions) to enhance the security posture of your organisation and ensure cost-effectiveness?



executives agree/strongly agree that they are more likely to use economical security solutions (open source, Make in India, start-ups)

Source: DSCI-PwC survey

Note: *The figures in the charts above reflect the views of the executives (35%) who chose technology optimisation as the first priority for cyber security cost optimisation/enhancement.*

03 Optimising cyber security operations

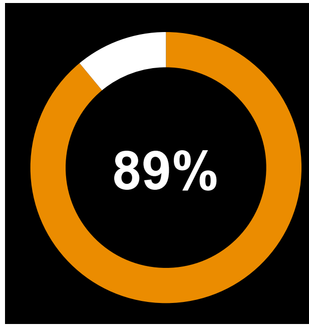
Transaction-based pricing models ensure that funds are allocated efficiently. As such, businesses (89%) are re-evaluating their security investments and exploring **variable cost models** for better return on investment.

Businesses today are exploring avenues to optimise their spending pattern as 67% executive strongly agree or agree that they are more likely to procure packaged and bundled services as compared to individual service offerings. **Bundling security services** allows vendors to offer a more cost-optimised package.

Currently, executives have outsourced vulnerability management activities, incident detection and response, incident investigation, malware and forensic analysis, data privacy, and regulatory compliances (33% each), closely followed by security operations centre (SOC), and user behaviour analytics (22% each).

In the near future, 44% of the executives are planning to outsource IAM, followed by security culture and SCADA/IoT security (33% each).

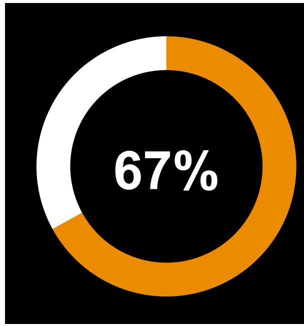
Question: Does the variable costing model allow cost-effective outsourcing of cyber security services as compared to an in-house function?



agree or strongly agree that they are more likely to adopt a variable costing model as compared to an in-house function for cost-effective outsourcing

Source: DSCI-PwC survey

Question: Is your organisation more likely to procure packaged and bundled services (e.g. managed security services) as compared to individual service offerings?



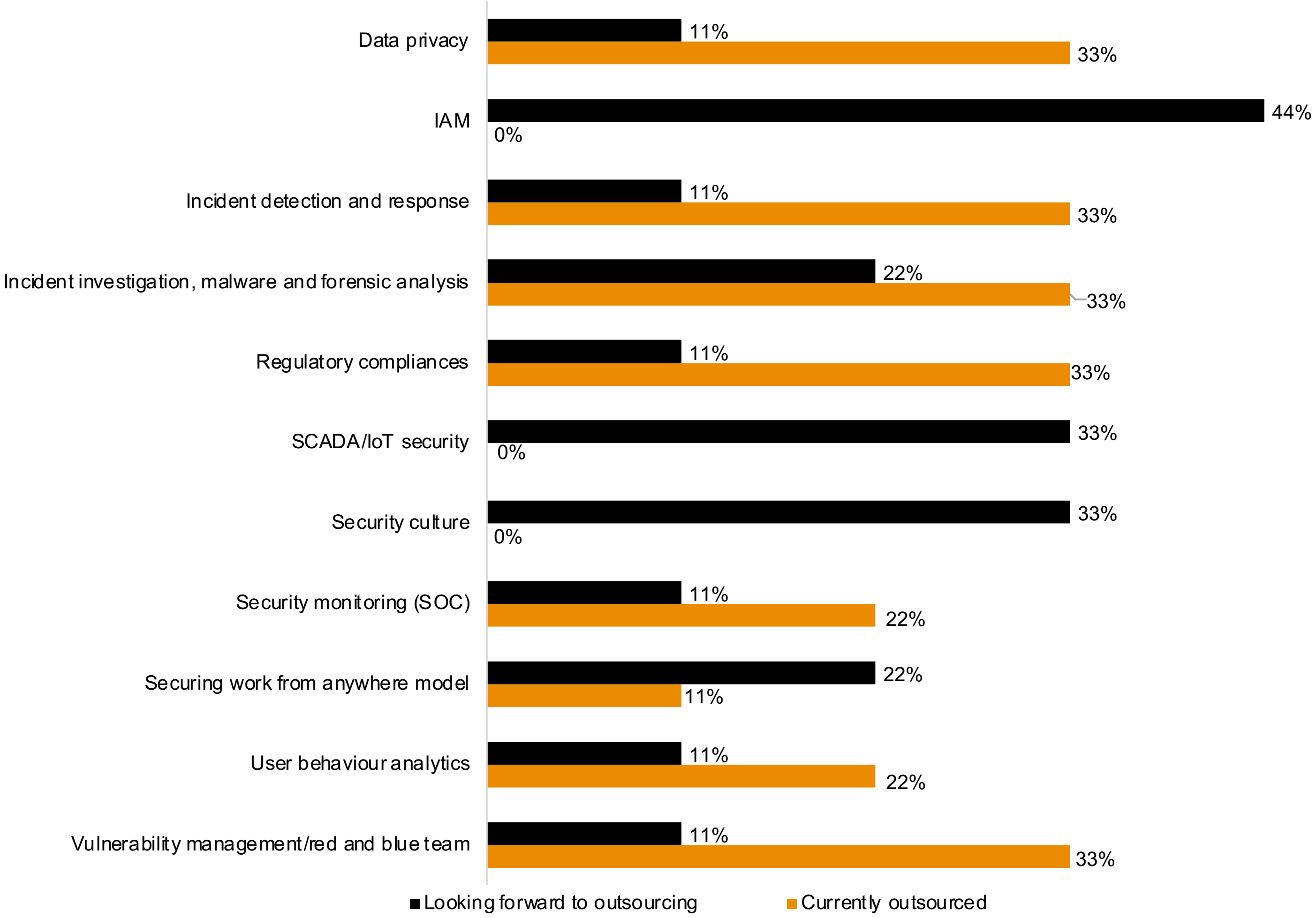
agree or strongly agree that they are more likely to procure packaged and bundled services as compared to individual service offerings

Source: DSCI-PwC survey

Note: *The figures in the charts above reflect the views of the executives (17%) who chose optimisation of security operations as the first priority for cyber security cost optimisation/enhancement.*

Question: Which cyber security areas have you currently outsourced/are looking forward to outsourcing in your organisation? Select all that apply.

Executives who have outsourced or are planning to outsource various cyber security areas



Source: DSCI-PwC survey

Note: *The figures in the charts above reflect the views of the executives (17%) who chose optimisation of security operations as the first priority for cyber security cost optimisation/enhancement.*

6 Conclusion

Emergence of new cyber security priorities

Across businesses, the ways of working are undergoing significant transformation. Organisations are migrating towards a work-from-anywhere-anytime model. Cyber security strategies should evolve with the changing business requirements. The need of the hour is to align an organisation’s visions and goals, and not only its IT requirements, with its cyber security strategy.

New cyber security priorities require organisations to focus on some key solutions for maximum effectiveness

Organisations are looking at enhancing threat management capabilities by leveraging risk-based vulnerability prioritisation and automated intelligent remediation.

Organisations with an existing IAM solution are aiming to enhance the same, and others are considering agile solutions and advanced predictive analytics for effective governance.

Organisations are doubling their efforts on security awareness and culture and focusing on endpoint protection in the context of the work-from-anywhere-anytime environment.

Organisations are leveraging advanced data and behaviour analytics to detect anomalous user behaviour.

Organisations with an existing cloud environment are focusing on enhancing its security maturity, and others are prioritising secure cloud adoption.

Organisations are looking to uphold digital trust and develop cyber security strategies that help in both creating and protecting business value. Meanwhile, cyberattacks have increased and become more targeted during the pandemic. Hence, there is a need to reset organisational cyber strategy in order to enhance capabilities and focus on key areas.

Cyber security priorities have evolved, and a few specific areas that require more attention are:

- threat management capabilities
- IAM solutions
- security of the work-from-anywhere environment
- monitoring through user behaviour analytics
- securing cloud computing technologies.

Increased focus on cyber security optimisation

Organisations should enhance their cyber security capabilities while optimising available resources. They need to prioritise the development of a cyber security programme that looks at the available resources holistically and tries to enhance operational excellence through optimisation.

Automation: Organisations can identify routine tasks within security processes and automate them to reduce the administrative burden and optimise overall security management.

Technology optimisation/enhancement: Organisations need to evaluate their network and optimally deploy technology based on their overall security posture.

Optimisation of security operations: Organisations can analyse how they handle security operations and associated costs by exploring managed security services, cloud-based service delivery and transaction-based pricing models.

The organic rate of **growth in cyber security budgets is not commensurate with current security requirements.** Organisations need to optimise resources and rethink their cyber budgets to meet evolving security requirements.

Authors

This report has been co-authored by **Anas Viquar, Atul Kumar, Anand Raman, Faiz Haque, Sameer Gupta and Rangoli Nigam**. The overall development of the report was steered by **Sivarama Krishnan, Rama Vedashree and Siddharth Vishwanath**.

Rama Vedashree is the CEO of the Data Security Council of India.

Sivarama Krishnan is Partner and Leader, APAC Cyber and India Risk Consulting, PwC.

Siddharth Vishwanath is the leader of the Cyber Security practice at PwC India.

About DSCI

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

Contact us

Rama Vedashree
Chief Executive Officer (CEO)
Data Security Council of India
ceo@dsci.in

Atul Kumar
Lead – Government Initiatives
Data Security Council of India
atul.kumar@dsci.in

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, 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.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in advisory, assurance and tax services. 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.

For more information about PwC India visit us at www.pwc.in

Contact us

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

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

pwc.in

Data classification: DC0 (Public)

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.

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.

KS/August 2021-M&C 14229