The Value of Identity in the Digital Environment

AN IDC INFOBRIEF | MAY 2020

IDC ANALYZE THE FUTURE

Sponsored by LastPass by LogMeIn

Executive Summary

A person's digital life is rapidly becoming a critical asset that, should it be compromised in any way, will severely restrict one's ability to function effectively in society. This is true as much for one's personal identity as it is for the identity of a commercial organisation. In the commercial space, any negative impact to an organisation's identity, such as a data breach, can result in not just lost business, which goes without saying, but potentially lawsuits, prison time, and a total closure of the business if the impact is severe enough.

The re-use of personal passwords for work, work passwords for personal sites, and the ability to keep track of all this in a secure manner, is rapidly outpacing most people's abilities.

Unified security can address many, if not most, of these issues. Poor employee credential management remains a fundamental challenge for businesses. All too often people use the same passwords because "it's just too difficult" to create unique and random passwords in the variety of formats that online sites demand.

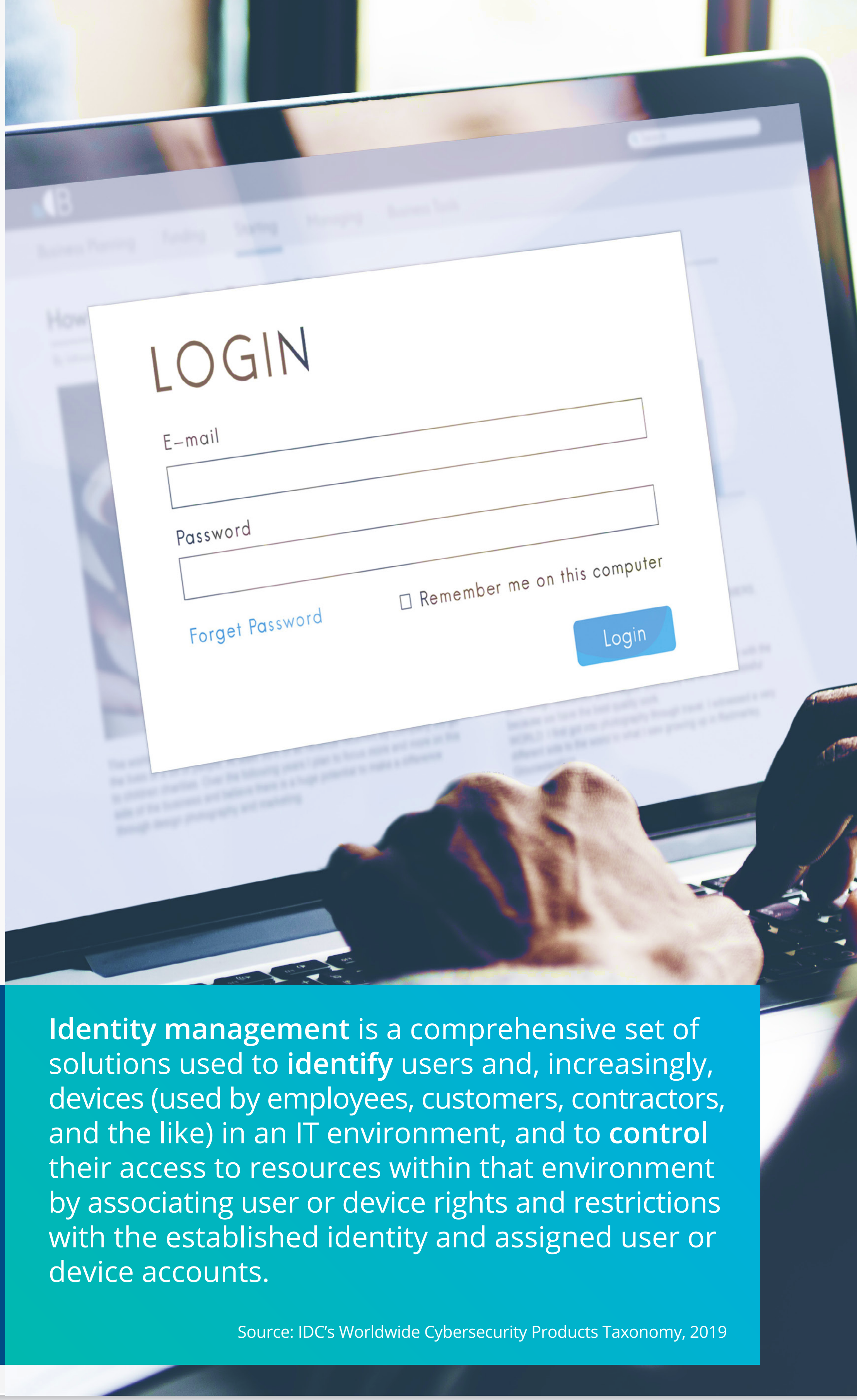
Organisations must change before well-funded and well-motivated threat actors, for whom the rewards are economic and bountiful, find a way to compromise employees' passwords and gain unlawful access to data, networks, and online transactions that require little effort to access.

For chief security officers and their teams, the rise in the number of devices, networks, and users increases the complexity of managing—and protecting—user access. This complexity can be addressed and, if done well, takes the security conversation to a new level. It becomes a business conversation.

This **IDC InfoBrief** will take a closer look at the commercial value and issues around identity and provide insight into how this seemingly innocuous part of an organisation's cybersecurity strategy is the vital lynchpin that is holding it all together. Today, the imperative of security goes beyond risks and is the core of business. Identity and access management (IAM) unlocks major opportunities for the business, particularly in the digital era which requires identity assurance more than ever, and core to this issue is the ability to provide a seamless user experience in which single sign-on (SSO), enterprise password management (EPM), and multi-factor authentication (MFA) combine to deliver unified security.

Senior business leaders need to accept that protecting the corporate identity starts with protecting the identity of every employee; neglecting one can have serious ramifications for the other.

Asia/Pacific organisations' tactical and short-term approach to their security investments should change, as today's unprecedented new focus by the C-Suite calls for more effective and well-funded investments in the future.



Identity management is a comprehensive set of solutions used to **identify** users and, increasingly, devices (used by employees, customers, contractors, and the like) in an IT environment, and to **control** their access to resources within that environment by associating user or device rights and restrictions with the established identity and assigned user or device accounts.

Source: IDC's Worldwide Cybersecurity Products Taxonomy, 2019

Six Drivers Accelerating the Boardroom's Security Agenda

IDC identifies six external drivers that are calling on boardrooms to pay greater attention to security as a business enabler and for building trustworthy businesses.

Operating in a climate of uncertainties

Natural disasters, cyberattacks, and a global pandemic are a stark reminder of the importance of business resiliency. The extended uncertainty period of the COVID-19 pandemic has placed pressures on businesses to operate in an unprecedented manner. According to IDC's Future of Work Employee Survey 2020, in countries like Singapore, India, Hong Kong, Australia, and New Zealand, a work-from-home mandate has pushed an uptake of video meetings, audio conference calls, and collaboration platforms. Securing and validating the identity of the end user accessing services remotely is more critical than ever, as not all organisations have the culture, the experience, or the technologies to enable a remote office.

Crisis of digital trust

Bad decisions, poor leadership, complexity, and cybercrime result in breaches that have a significant impact on businesses and customers. New approaches such as zero trust and distributed integrity are proving themselves. IAM is the number 2 investment priority for Asia/Pacific organisations.[2] Moving the security strategy from system or device to the new control points of data, application, and identity is considered to be the best strategic and comprehensive approach.

Borderless organisations

By 2024, 25% of Asia's top 1000 companies in the Asia/Pacific will rely on a global, secure, intelligent, highly integrated, and collaborative ecosystem that enables enterprises to function as borderless organisations.[1] This will require IT security systems that support an online collaborative environment to drive business outcomes, including ideation, productivity, faster time-to-market/project completion, and better employee experience (EX). Corporate IT security will need a holistic strategy to ensure access and control. Perimeter-focused security investments will also need to evolve to refocus on identity, data, and applications.

Lack of IT and security skills

More than one-third of organisations globally are struggling to implement new technologies to support their digital transformation efforts — and Asia/Pacific is no different.[3] The fast-changing technology landscape and scarce talent pool put businesses and their digital transformation plans at risk.

Rising expectations of superior digital experiences

Security issues abound as businesses race to capture new opportunities that come from combining digital technology with physical assets. Businesses will need to adopt and master digital technologies while ensuring reliable digital services, superior experiences, and frictionless security technologies. A key investment area to deliver on digital transformation goals is security, with 51% of Asia/Pacific organisations making this their number 1 investment area.[5] In so doing, secure-by-design principles must be core to success. Adopting a "highest level compliance" approach, even if it is not mandated, is a driver to engendering trust and transforming the business for competitive agility.

Future workforce

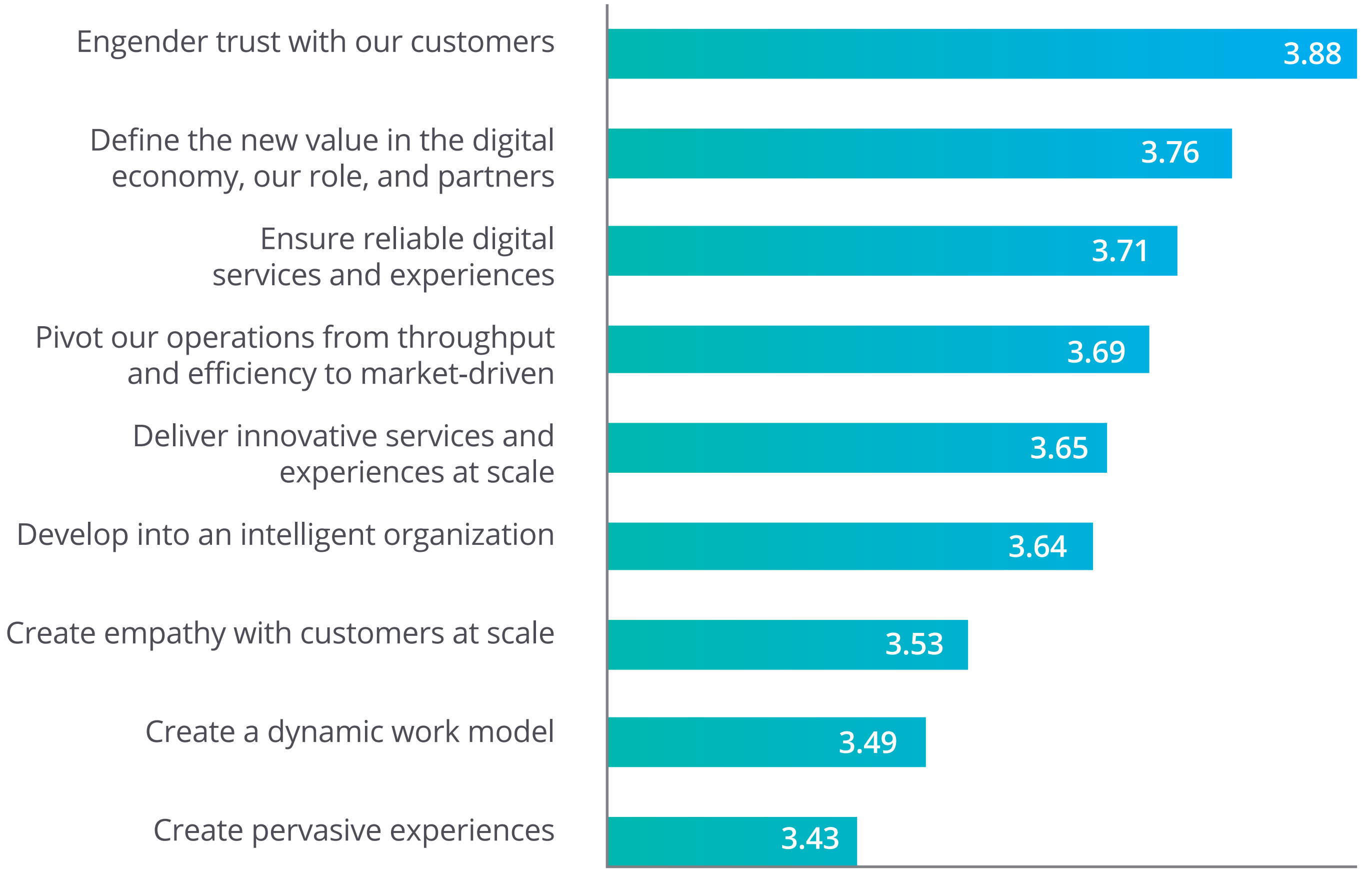
According to IDC's Asia/Pacific Future of Work Survey, 45% of organisations surveyed have implemented or are planning to implement contingent or project-based hiring policies to fill the digital skills gap.[4] The growing pool of contingent workers, the move toward collaborative workspaces, and rising millennial workforce call for new flexible workplace policies without sacrificing security.

Sources:
[1] IDC FutureScape: Worldwide Future of Work 2020 Predictions — Asia/Pacific (Excluding Japan) Implications)
[2-4,5] APeJ Future of Work Survey 2018
[3] IDC Worldwide CXO View of the Future Enterprise in the Digital Economy Survey 2020

Asia/Pacific CEOs' New Mandate in the Digital Economy: Trust

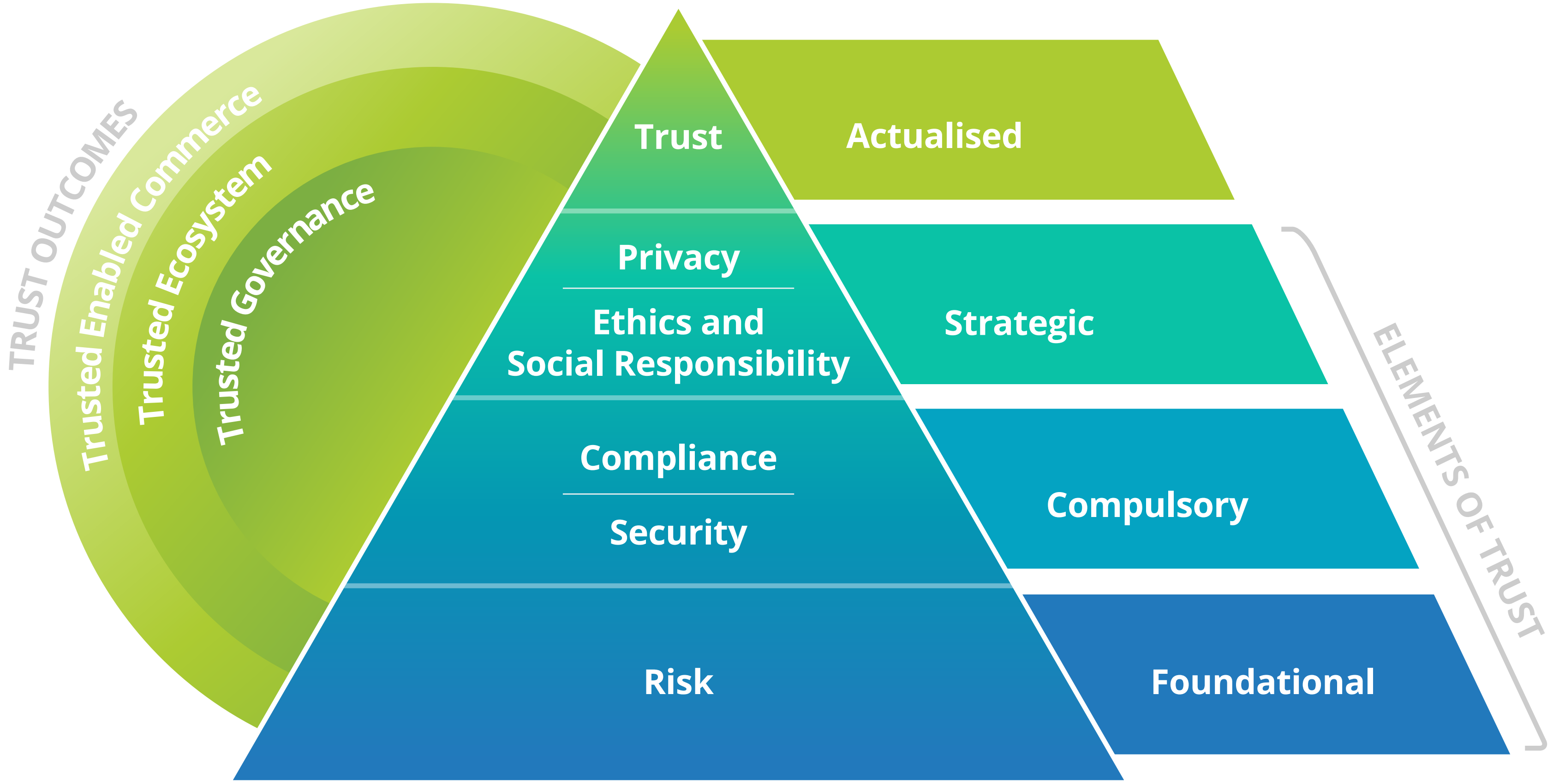
The pace of digital transformation has accelerated in the Asia/Pacific region since 2018. According to IDC's Asia/Pacific Future Enterprise Benchmark research, more than half (56%) of organisations are in the middle (*Digital Players*) to advanced stages (*Digital Transformers/Disruptors*) of their journeys. Trust, which matures with organisations as they embark on their digital transformation journey, is a critical focus for CEOs and is recognised as the single, most important ingredient necessary to gain loyal, profitable customers in the digital era. Trust is built upon a strategic approach to IT security, notwithstanding cultural aspects. Those that succeed in engendering trust with their internal and external stakeholders, including employees, customers, and partners, will reap benefits of a more favourable perception and more rewarding business engagements.

Engendering trust, defining new value, and ensuring reliable digital services and experiences rank highest in importance to the overall business vision.



Respondents were asked to rank their strategic business priorities, with 1 being the least important and 5 being the most important

Source: IDC's Asia/Pacific CEO Priorities Survey, January-February 2020 (N=80)



Source: IDC's Trust Framework, 2020

Security Challenges and Implications for the Business

A significant challenge has, for a long time, been the inability to realise the value of security. As a result, most organisations end up taking a tactical, not strategic, approach to IT security. The consequences are underfunding and underresourcing of security, an inaccurate focus on securing endpoints and an overburdened identity and access management (IAM) team.

Security resource issues

30% of Asia/Pacific organisations suffer from a lack of skills to ensure reliable and secure digital services. The talent shortage is more critical in Singapore, while Australia and New Zealand are in line with the regional average.[1]

Asia/Pacific average	Singapore	Australia	New Zealand
30%	55.6%	33.2%	33%

Insufficient security management focus

<10% of organisations have a dedicated chief information security officer (CSO or CISO).[2]

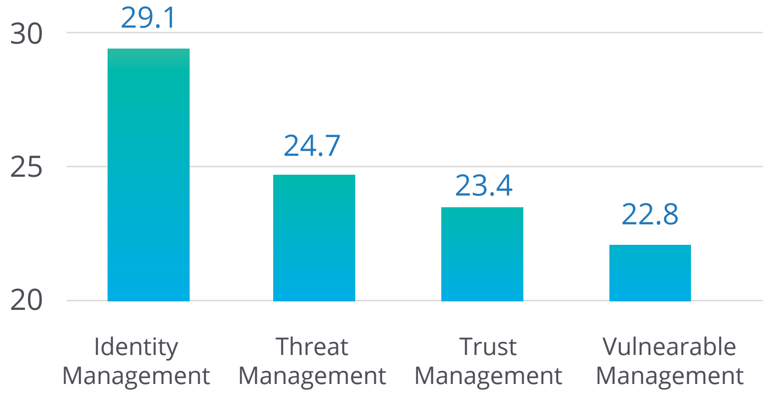
For **80%** of organisations, the head of IT (CIO or IT director) is also the head of security.[3]

IAM headcount

Enterprises with at least 500+ employees surveyed by IDC have an average of 23 full-time employees in the IT security department, with **more resources focused on IAM than any other area of IT security.**[4]

Considering the importance of threat identification, the ability to transfer valuable resources by improving IAM efficiencies would be considered a strategic move.

Percentage of Time Spent By Security Role[5]



Identity solutions with improved ease of use and greater automation can help cut down time spent on managing users and identities, which, in turn, ensures better use of security resources elsewhere.

Looming identity crisis

Businesses are still warming up to MFA and federation for enhanced security.[7]

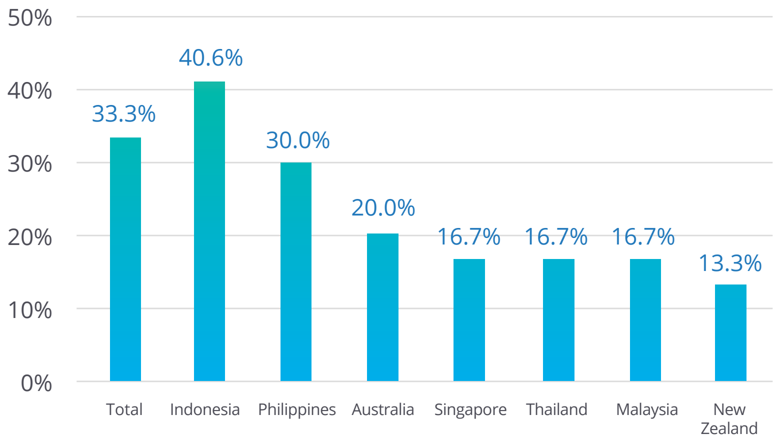
23.4% of Asia/Pacific organisations plan to deploy MFA for all users accessing sensitive data.[6]

30.4% of Asia/Pacific organisations are considering or piloting identity federation plans.[7]

Disconcertingly **29.1%** surveyed are not even considering this.[8]

Federation, the linking of a person's single authentication across multiple systems, will increase in adoption as more organisations realise its value in simplifying security and reducing the amount of administration to free resources up for other critical security roles.

Implemented Identity Federation[9]



- Indonesia stands out with **41%** of respondents having implemented identity federation, the only country higher than the regional average.
- Federated identity has yet to come of age in the mature IT markets of Australia, New Zealand, and Singapore.

Source:
[1] IDC's Future of Work Employee Survey 2020
[6] APeJ DX Executive Sentiment Survey 2019
[2-5, 7-9] APeJ Digital Trust and Cyber Economics Study 2018

Another Spanner in the Works: Remote Working

The shift to remote working, while a boost to employees' work-life balance, puts unprecedented burden on the business and throws out questions around connectivity and access. *Are employees given the right levels of access, and if they are and the appropriate security controls are in place, could they be more productive?* With remote working emerging as a permanent fixture in corporate policies, finding a way to mitigate the security-productivity trade-off is needed to prepare for the worst-case scenario and minimise business disruption.

In today's cloud era, working remotely is more than having a laptop to work on. Keeping employees productive requires giving them secure remote connectivity and access to the same applications and networks as they do in the office.

IDC's research bears out the importance and value of ensuring employees have secure remote access.

60% of Asia/Pacific employees surveyed want remote access but only 40% have it.

The **banking and financial services industry (BFSI) has the highest demand for remote access (71.5%),** but only 32% of those surveyed have deployed remote access technology, while those in telecommunications and transport seem to be more aligned with employee expectations – 47% cited a need and 40% have deployed remote access.

Further data quashes concerns over worker productivity: **44% of BFSI respondents cited productivity gains and more than half (58%) in telecommunications/transportation and public sector** also cited productivity gains.

Source: IDC's Future of Work Employee Survey 2020

Even for a highly regulated industry like banking which has strict policies to guard against potential risk exposure arising from improper handling of personally identifiable information in the event of loss of data or leakage, the boundaries of work continue to be adjusted to meet the needs of banking customers who demand immediate attention and service.

As organisations globally are finding out, remote working is no longer a nice-to-have but a critical piece to their business resilience and continuity plans. A crisis like the COVID-19 pandemic can strike any time, which is why enabling employees to work from anywhere and keeping the business running smoothly are top on the agenda for every business leader today.

With benefits of work-life balance and even productivity, remote working is here to stay and calls on business and IT leaders to address the following security challenges head on:

- Control over corporate network access from employees' managed and unmanaged devices.
- Addressing the complexities of authentication and compliance.
- Adopting a strong cyber risk governance practice.

Building a Trust Agenda for the Future Enterprise

This era of digital transformation thrives not simply on data but active participation in data sharing between stakeholders. IDC believes a trust agenda is more important than ever in order to achieve this goal. Today's boardroom agenda calls for a prioritisation on driving security, specifically identity, as a pillar for success of what IDC calls the "Future Enterprise", a business that successfully thrives with a digitally native culture, effectively competes through their ecosystems, generates revenue from empathy at scale, and demonstrates an ability to adapt operating models enabled by an intelligent, empowered and agile workforce. For many this will be a considerable challenge, but addressing key issues will define leaders and deliver significant competitive advantage.

Security as the foundation

Trust in the digital era is built upon a strong base of cybersecurity. Identity, along with applications and data, are emerging as the new control points. Ensuring data privacy is about who has access to what data, and in today's environment, from where; and data security is a key control point as it relates to both compliance and trustworthiness.

Changing models of IAM solutions

An identity management solution that provides a suite of services, as opposed to a collection of isolated applications, is the preferred option as security teams need to move away from single solution deployments towards a more consolidated suite of services that integrate seamlessly with other vendors. This delivers significantly increased value. As many services move to the cloud, there are some that will not or cannot, yet they still need to be afforded the same level of access controls as the more modern services.

Adopting a solution set that can span the modern hybrid IT environment and that adds little friction for the end user will ensure that adoption is high and that the risk landscape is significantly reduced. MFA, EPM, and SSO, used in combination, offer a level of control and visibility to the security team that is needed in the modern business.

The right tools

Unprecedented demand for remote access amid a global pandemic will sustain long after the crippling health crisis ends, creating demand for identity management tools.

These tools can address the over-population of IAM-focused employees, allowing them to refocus on other critical security roles such as threat hunting and remediation.

Cloud is maturing at a pace that makes it a more secure option than on-premises for many organisations. According to IDC's Security Software Tracker, cloud-based IAM will grow nearly 3 times as fast as on-premises IAM by 2023.

Likewise, many security solutions are being delivered from the cloud due to its scalability and security. The shortage of skills is driving new sourcing options for a range of solutions, like security, that had not previously been considered.

Reframing Cybersecurity as an Opportunity for Strategic Business

For senior business leaders too busy fighting fires to see where the next hot spot may occur, the security challenges of today need not be the same old story but a call for change. As IDC's survey shows, only through the implementation of automated solutions, and with strong C-Suite support, can there be an efficient way to address the onslaught of cybersecurity threats and improve an organisation's security posture amid the pressures of today's trading environment that demands digital business resiliency.

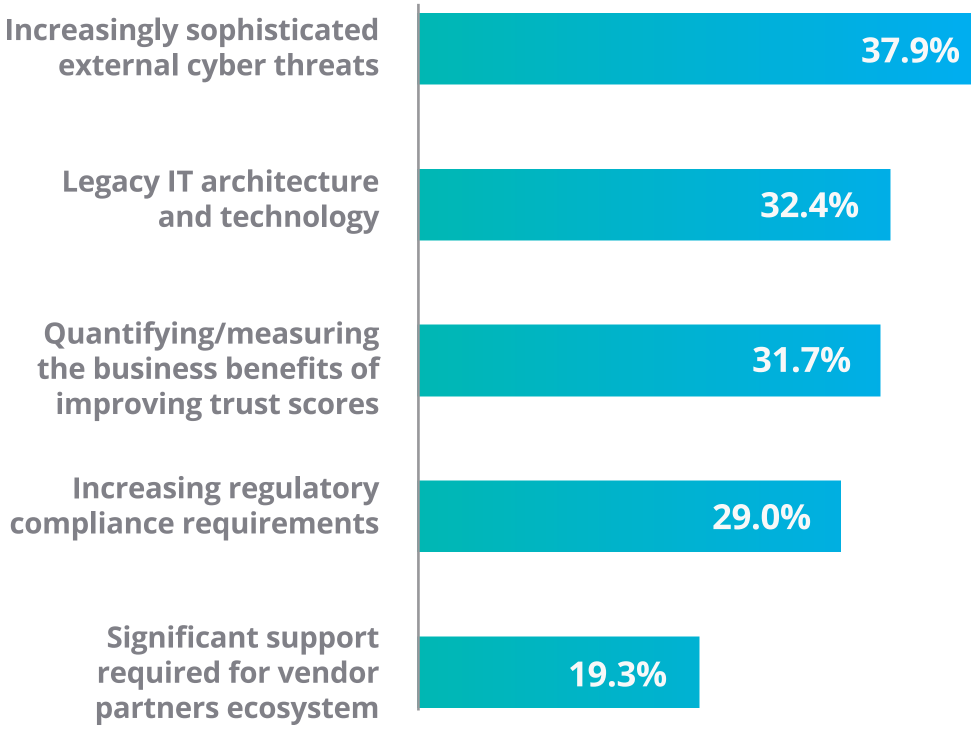
Beyond the omnipresent challenge of defining the value of security, there are other major challenges that C-Suite leaders seek to address in 2020–2021, namely the increasing complexity of threats, legacy systems, and compliance.

Strategic investment in IAM is one way to address many of these issues, particularly where users and identities are validated and monitored. The ability to track validated and legitimate users' actions can help speed up the ability to identify a potential hack, as valid activity can be eliminated much earlier in the process.

Unified security can help address compliance, by ensuring only legitimate identities have access to critical and sensitive data.

Deploying low or easy maintenance solutions, such as SaaS or cloud-based, can also help to address the issue of a sprawling security vendor ecosystem, whilst relieving internal teams of the need to manage on-premise equipment.

Future of Trust: Top 5 Challenges for 2020–2021

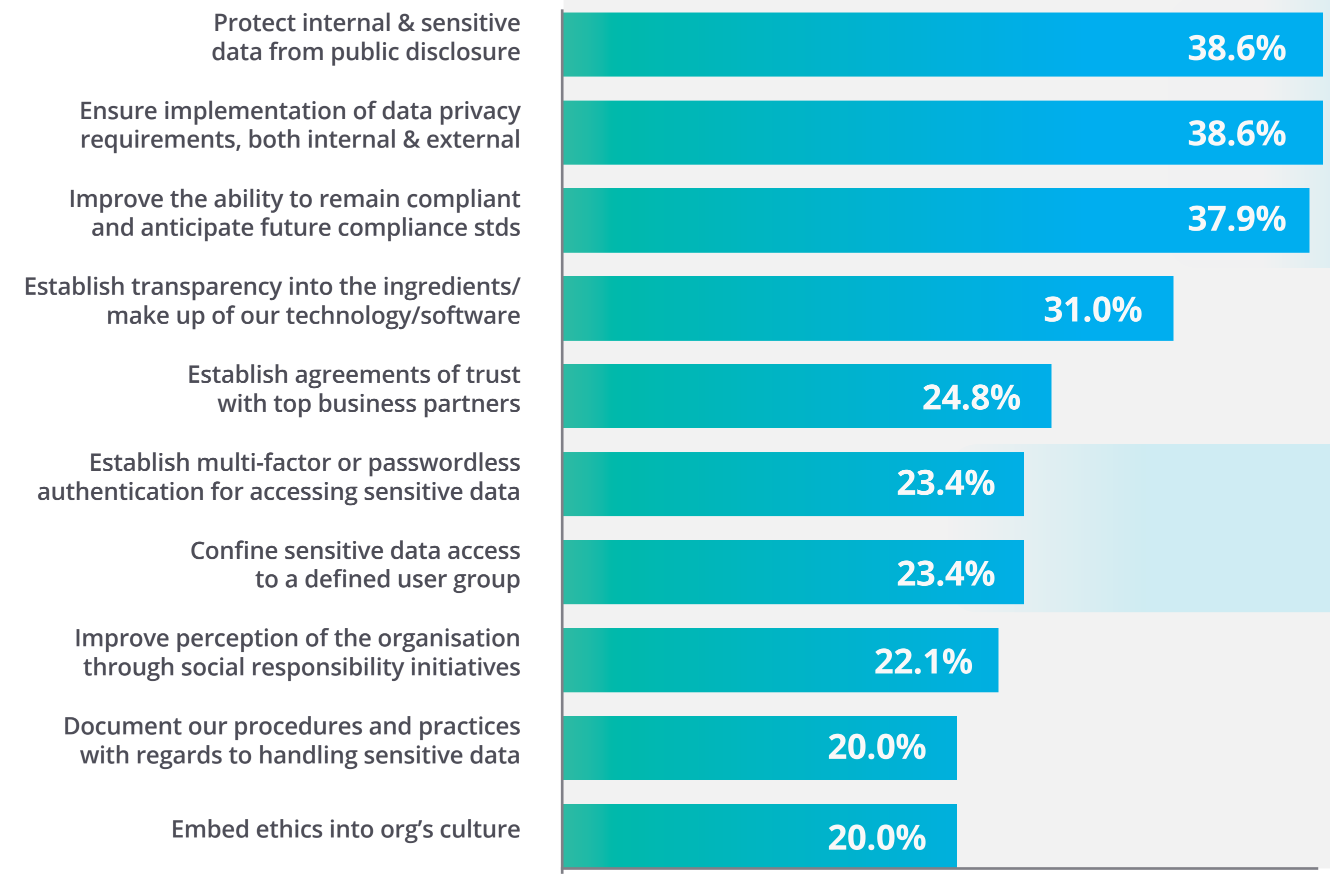


Source: IDC's CXO View of the Future Enterprise in the Digital Economy 2020

IT Impact Calls for Stronger Identity for Privacy Protection

Delivering on CEOs' number 1 agenda item of engendering trust — protecting internal and sensitive data from public disclosure — requires an understanding of digital trust. Whilst this is a new concept, many are struggling. Much of current investment plans to align to the requirement are focused on what customers are perceived to care about — data privacy. What is missing here is the security and monitoring of those that will be accessing the data, being down at sixth place, according to IDC's research. Unified security delivered though identity management along with monitoring, will be key to security success in the future.

Future of Trust: Top Goals for 2020-2021



Data security and data privacy rely on user semantics, which means authentication of users is critical.

Passwords are still the ubiquitous method of accessing secure systems and so, naturally, become a critical asset, and a target for threat actors.

With security control points shifting to data, application and **identity**, the need for stronger identity management and security tools is paramount.

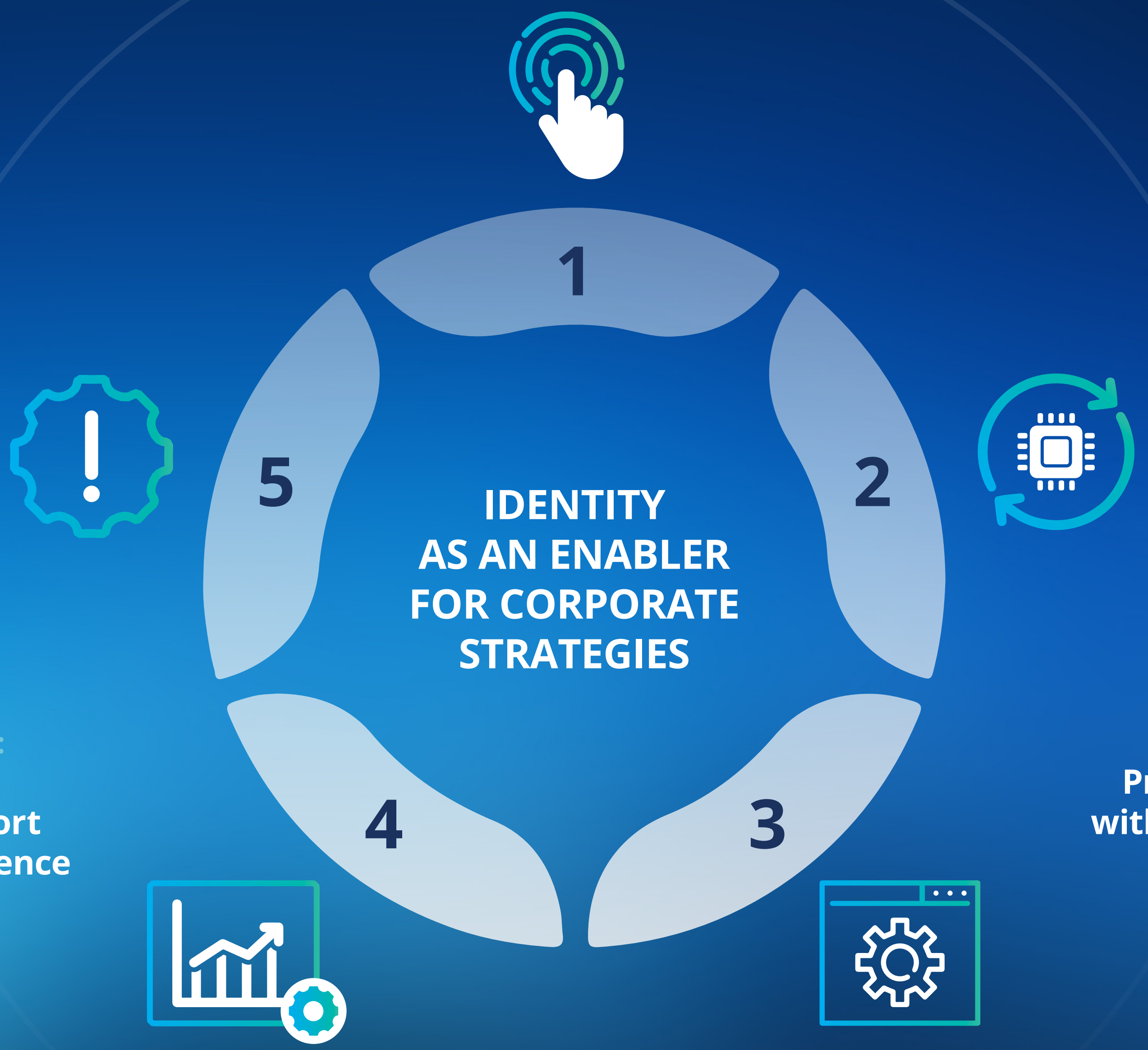
Identity is a unifier across the new security control points of identity, data, and application, so addressing IAM issues early can help to quickly resolve other areas of concern.

Source: IDC's CXO View of the Future Enterprise in the Digital Economy 2020

Five Drivers of Identity Supporting the Business (1/3)

Businesses need to understand how, and why, to fund security investments and to not think of them as insurance. Cybersecurity is a business risk that the IT security team can help address. Approaching identity as an enabler for corporate strategies elevates security to a new level.

IDC's research identifies five themes that demonstrate security's role in shifting perception away from business blockers, towards becoming business enablers.



IDENTITY AS AN ENABLER FOR CORPORATE STRATEGIES

Identity Driver 1:
Optimised user/customer experience

Identity Driver 2:
Managing identity at digital scale to enable DX

Identity Driver 3:
Propagating compliance without sacrificing usability

Identity Driver 4:
Integrating identity to support operational excellence

Identity Driver 5:
Managing enterprise risk through trusted identity

Five Drivers of Identity Supporting the Business (2/3)

Identity Driver 1: Optimising the user and customer experience

Business enabler: Engendering trust with all stakeholders.

Identity management: Improve employee efficiency with a combination of SSO and EPM, removing barriers to access without sacrificing security, and leverage MFA to authenticate the access request, confirming it is from a genuine and valid source.

- The Board is interested in the concept of "trust" so now is the time to educate them on the need for enhanced identity management as a key enabler of trust for both employee and customer experiences.
- The pressure is on to cater to the needs of today's multigenerational workforce, from mobile-first millennials to the less technology savvy workers.
- All employees need a simple and elegant solution for accessing multiple secure accounts across both on- and off-premise assets, whilst the internal IT team need an approach that ensures security and user friendliness whilst scaling and requiring minimal intervention.
- Addressing inertia and helping employees respond positively to new security solutions makes a difference in an organisation's security defence.

Identity Driver 2: Managing identity at digital scale to enable DX

Business enabler: Supporting the borderless organisation and distributed workforce.

Identity management: Deploy in-depth identity management and monitoring as a strategy to enable remote work-sourcing, in areas the business may not have the in-house resources: innovation, ideation, security — such skills can easily be outsourced with strong password controls.

In the era of increased remote working, organisation-wide digital dexterity is the goal. Identity management and monitoring tools enable administrators to easily manage access privileges for various groups of employees, including:

- **Providing a consistent approach to diverse application environments**: Utilising SSO technology to simplify access for users to on- and off-premises applications.
- **Supporting mobile-first strategies**: Recognising a single identity for each user regardless of the device or form function used.
- **Accounting for fragmenting definitions of who/what a user is**: Providing a consistent approach to identity for all users, regardless of location. This is a critical concern given inconsistent approaches across supply chains which can be used as a channel to cripple not just one linked organisation but the entire ecosystem.
- **Combating the risk of insider threats**: Ensuring the right levels of access is provided to only those who need to access company-sensitive applications and data can reduce the potential of the organisation being compromised from the inside, either maliciously or via compromised credentials.

Five Drivers of Identity Supporting the Business (3/3)

Identity Driver 3 Propagating compliance without sacrificing usability

Business enabler: Meeting the demand of the remote workforce and in times of business continuity/business preparedness.

Identity management: Remain compliant without over-burdening employees. MFA around sensitive data as an additional security layer can reduce risk without overly impacting productivity.

- Limiting an organisation's risk exposure to potential threats is all the more important in the digital era. With new laws emerging across the Asia/Pacific region to protect and secure personally identifiable information, taking the high road and being compliant to the highest available standard (such as GDPR), will ease the burden of localisation, meeting and exceeding customer expectations (and thereby engendering trust) and help drive towards uniform regulations.
- Begin with identity, and who has, and should have, access to sensitive data.
- Consider the impact of enhanced security on employee productivity, but balance the need to secure highly sensitive data and resources with user-friendly authentication methods.

Identity Driver 4: Integrating identity to support operational excellence

Business enabler: Toward the goal of a Future Enterprise.

Identity management: Robust password management enables multiple identities to be managed more effectively with fewer resources. Become more efficient with the limited security resources available. Embracing MFA and SSO all contribute to a more robust operating environment.

- Today's digital era has forced a change on organisations to strive for an optimised strategy that aims to free up IT resources to focus on strategic and growth-focused initiatives.
- Robust password management leads to not only more efficient identity management but unified security.
- Adopt a platform for MFA, SSO, and enterprise password management to ensure minimum stress on the limited resources.
- Robust IAM enables multiple identities to be managed more effectively with fewer resources. Become more efficient with the limited security resources available.
- Embrace the automation inherent in key solutions to provide a welcome relief to the over-stretched IT security teams, with an opportunity to repurpose these roles to more valuable or thought-intensive security challenges.

Identity Driver 5: Managing enterprise risk through trusted identity

Business enabler: Engendering trust with all stakeholders.

Identity management: Trusted identities enable improved productivity without sacrificing security; however a strategy around how "trusted identity" is defined will be critical.

- With the rise of the gig economy and contract working, many identities are also transient but require full access. Contextually aware-authentication solutions and the ability to apply policies based on user conditions ensure that access can be tuned in line with an organisation's appetite for risk.
- Ignoring the risks — and the availability of solutions — means giving up on the opportunity to have identity management capabilities designed to enable businesses to simply and securely address current and emerging access and authentication challenges.
- Applying consistent identity and access approaches to both internal and external users is a critical means of reducing exposure to risks, given that 40% of Asia/Pacific organisations are using outsourced contractors and gig workers to fulfil digital skills needs, and this is only set to grow, creating an increased demand for a holistic IAM offering.

Engaging The CEO and The Board

Security is a complex area, and speaking the right language of security is key to getting the support and approval of the board. This means *not* saying security as much as talking about the **business risk that the IT team can help address**. With engendering trust with customers being the number 1 agenda item for CEOs, the conversation throws the spotlight on “trust as an enabler for better business outcomes”.

Strategy:

IDC defines trust as the condition that enables decisions to be made between two or more entities that reflects the level of confidence (risk and reputation) between parties. In short, trust is the glue of relationships.

When engaging the CEO and the board, trust is an **up-levelling of the security conversation to include attributes such as risk, compliance, privacy, and even business ethics**. These elements transform the conversation from what *must* a company do to prevent negative outcomes to what *should* a company do. Thus, traditional approaches to security, risk, compliance, and privacy are facing challenges in both scope and scale.

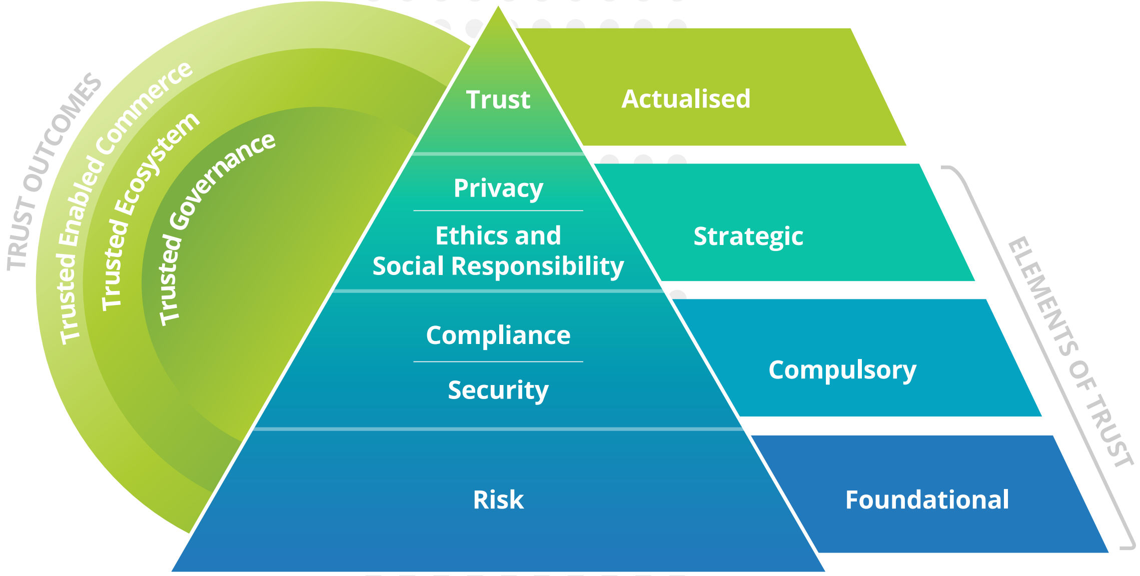
In IDC’s Trust Framework, the five elements of trust are not approached individually. These elements of trust have layers of implementation, much like the hierarchy that Maslow proposed for human needs. Today’s digital leaders — be they digital unicorns or traditional conglomerates that have reinvented themselves — have successfully built their digital success on trust.

When executed successfully, trust is also about maximising return, creating a quantifiable impact on revenue, expenses, and shareholder value.

Action:

Therefore, when speaking about identity management, this is about **managing enterprise risk through trusted identity, or identity integrity assuring security**:

- Define the returns on corporate “trust”, which is more about corporate culture.
- Define KPIs that the board can understand, such as the value of assets at risk, partner risk, as well as the core and value of risk mitigated. These become drivers of investment and enablement.
- Integrate identity to support operational excellence — permitting access to sensitive systems, securely.
- Propagate compliance without sacrificing usability — alignment of identities with protected data, and ensuring compliance through monitoring.
- Optimise user/customer experience — ease of use ensures employee efficiency, driving customer satisfaction.
- Manage identity at digital scale to enable digital transformation — delivering on the ability to leverage the gig economy and deliver distributed innovation.



Source: IDC’s Trust Framework, 2020

Speak the Language of Compliance, Privacy, Risk Management

One of the roles of the board is to help the business steer clear of risks. Identify key topics into regular discussions about both strategy and risk to enhance their knowledge and competency for more decisive decision making.

Tactic:

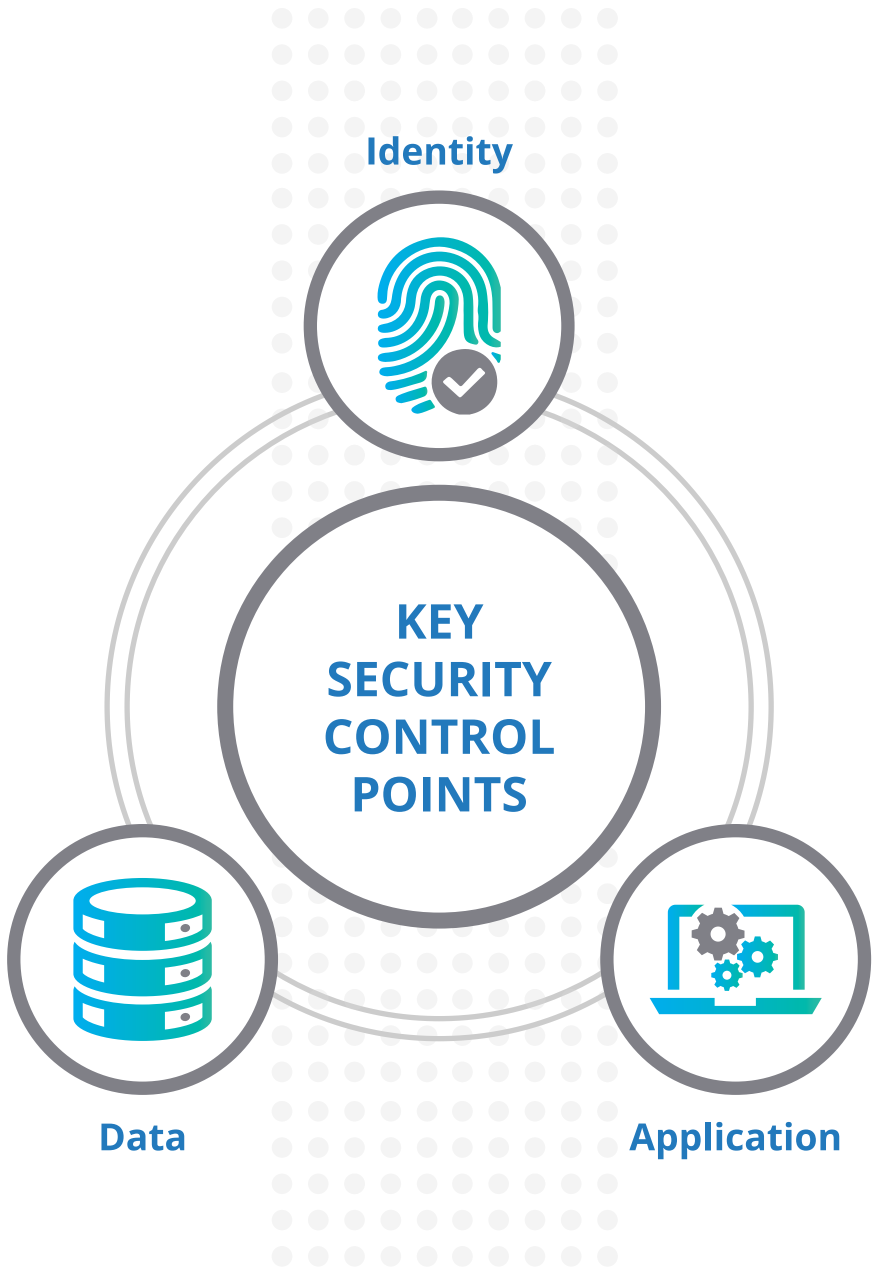
Risk management has shown to be an emerging skill in the Asia/Pacific, with most organisations focusing on financial risk whilst few, if any, consider cyber risk. This is a board issue, so **work with the committee** to:

- Identify how best to quantity cyber risk and embed into regular reporting. As regulations increase, the ability to define the "cost of assets at risk" increases.
- Identify who inside the organisation is tracking consumer data legislation. Personal data, for instance, is coming under legislation in most markets and is already covered under the GDPR for data on citizens of the European Union.
- IDC considers that GDPR is the "gold standard" for personally identifiable information (PII) data management practices. By adopting these guidelines, the ability to comply with the myriad of local legislation becomes a more simple procedure.
- Understand how the board has addressed this to date.
- Craft a remote working and remote access strategy for current business operations and have contingency plans in place for other unforeseeable external challenges that could impact the business.
- Outline a framework that ensures all people, networks and systems are being secured, especially at a time when remote access is now critical for most organisations.

Educate the Board:

Demonstrate IT's further foundational role in supporting the organisation to address resourcing and risk management imperatives:

- **Security of data and applications:** It is vital that the identity of all who access a company's systems are validated securely and in an efficient and productive manner. This will go a long way to ensuring the security of data and applications, whist offering efficiencies to the heavy investment in personnel managing this critical element of the security stack.
- **Removing the risk of rogue accounts:** Repurposing security staff from identity to other areas such as data security and threat hunting addresses the reality that attackers are getting smarter and may already be inside corporate networks. According to Singapore's Cyber Security Agency May 2019 report, attackers stay on networks in Asia, undetected, for up to 498 days.
- **Employee awareness and education:** Explaining the issue is only half the problem, and in most cases, the greatest threat to one's cybersecurity defence is from within. The other half is to provide solutions that the board can act upon, beginning with addressing the weakest link: employees.
- **Keeping abreast of the latest.** Updating the board in a meaningful manner will not only earn their trust, and confidence, but it will also help everyone make better decisions.



Next Steps

The sudden shift of the workforce to remote working has its security challenges, but those that see this as an opportunity to leverage identity as a unified security strategy to engender trust with customers and employees have a distinct advantage.

Review current identity and access management controls.

- How do you cater for multiple, and sometimes, personal, passwords across the organisation.
- What are your current IAM investments in terms of people and resources? Is this optimal?
- What levels of automation are you utilising, and can this be improved?

Realise that draconian measures will not meet the business needs.

- Adapt the technologies to meet the employee demands – it is more successful than trying to create rules that will be evaded in the name of productivity.
- Recognise today's challenges. Resource constraints, a younger workforce, and remote access are defining many business and IT decisions. For example, segregating personal and business use of devices is almost impossible today, and will become more challenging with a younger workforce.

Prepare for the new normal.

- Craft a strategy that looks at remote working for the long term.
- Have a strong cyber risk governance practice to mitigate risk.
- Look strategically at identity management and the value that can be realised across the organisation.
- Designing a solution that affords enhanced security, improved manageability, and end-user satisfaction is not impossible. See this as delivering a secure mobile workforce that can excel in a range of harsh, and benign, environments.

Engage the Board and CEO.

- Get buy-in from the committee by speaking the language of managing enterprise risk through trusted identities.
- Reimagine identity management in the broader context for enhanced employee experience and productivity as trustworthiness becomes embedded into the organisation's DNA.

Identity for Security That Enables the Business

Are you ready to elevate the security conversation into a business one?

Learn more about LastPass for Business

Click here to download the infographic

IDC ANALYZE THE FUTURE

Sponsored by LastPass by LogMeIn