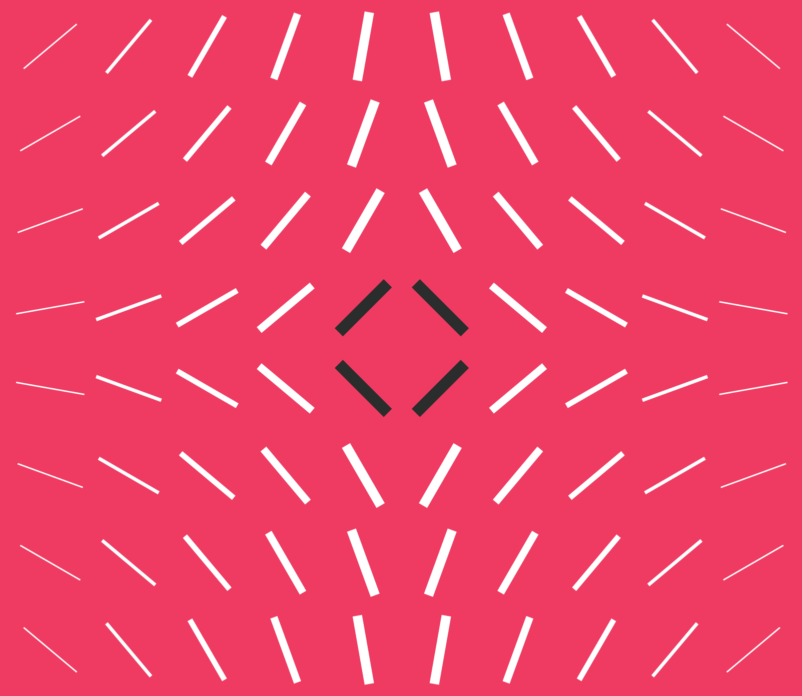
www.pwc.com/gx/en/issues/cybersecurity.html

PwC power sector cybersecurity trends and insights for 2021

Insights, leading practices and recommendations to address cybersecurity challenges in the power sector cybersecurity in 2021



April 2021

Topics

Power sector cybersecurity – 2020 in review and predictions for 2021

While many may see 2020 as a year to quickly put behind us, our PwC Power Sector report points out a few benefits from this unorthodox period.

Despite power company cash flow challenges and reduced revenues, this past year did prove that power sector workforces could change their operating model and work remotely with success. Cybersecurity systems were implemented through remote workshops and communications and progress was still made. Congratulations to all – your perseverance paid off and you did move the needle on your programs.

This past year was also a time to regroup. We saw a re-baseline of cybersecurity maturity and risk levels and the development of risk-based security plans for boards and executive teams. There was a greater ability to connect security spending and resourcing recommendations to risk targets, which gave leadership teams a clearer understanding of why these investments were important.

The last few years saw significant focus on Identity and Access Management and Privileged Access Management. We see this trend continuing for the next couple of years. 2021 will also be a significant year for data protection and cloud security enhancements, which appear on many security plans.

PwC expects to see a major reconciliation of managed security services in 2021. We have seen a lot of concern across the power sector with the legacy security monitoring services that are currently in place. They are delivering low or moderate value related to the costs. As a result, we predict a fairly dramatic turnover in managed security service providers in the next 12 months, moving to those that deliver much more than just eyes on glass with routine alerts.

And finally, we are starting to see constructive security discussions occurring between Information Technology (IT) and Operational Technology (OT). The dialogue is shifting away from ‘who owns what’, to finding solutions to better secure the OT environments through collaboration. Well done!

Richard Wilson

Cybersecurity and Privacy Energy, Utilities and Resources – Americas

Bram van Tiel

Cybersecurity and Privacy Energy, Utilities and Resources – EMEA

Jason Knott

Cybersecurity and Privacy Energy, Utilities and Resources – AsiaPAC

Setting the stage: Power Sector outlook

Setting the stage: Power sector outlook

Major trends

- Focus on new clean, distributed sources of energy, nuclear decommissioning
- Quest for digitally supported business models in the transformed utility value chain (digital grid, customer centric platforms)
- Become a services and solutions provider for energy customers
- Sustainable power beyond energy, e.g. automotive/ transportation
- Sector convergence with e.g. chemicals (circularity), Oil & Gas (new energies play) and others

Strategic essentials

Platforms and solutions

Using network assets as an intelligent, integrated network

Market shaping

Develop capacity for continuous market sensing, constant innovation, commercial mindset, aggressive branding and speedy decision making

Virtual supply

Potential long-term solution of storage in combination with renewables as virtual power plant

Value models

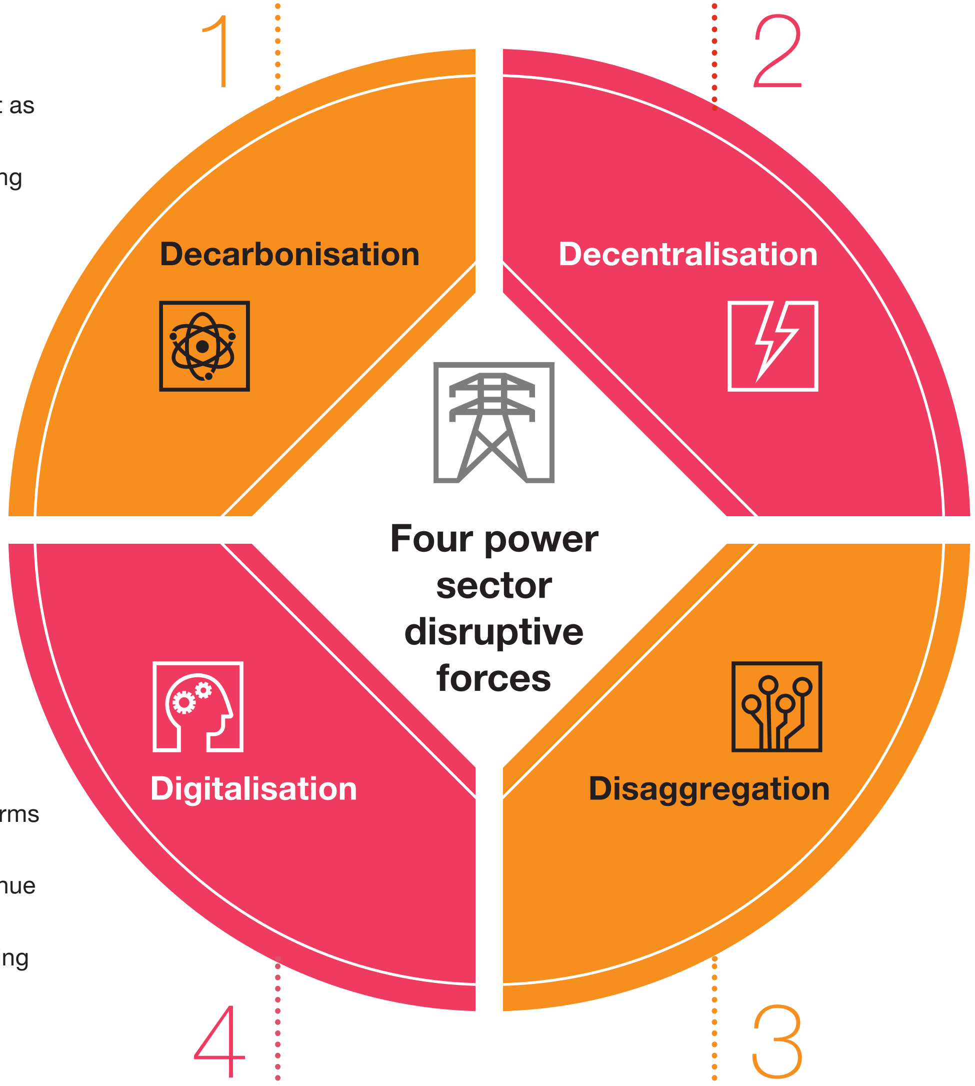
Bundling of services with a risk-adjusted pricing model

Home hubs

Creating ubiquitous market positions in large and undeserved customer group of residential customers

> “Global energy transformation is gathering pace, driven by the twin forces of changing customer expectations and rapid technological evolution.

Setting the stage: Power sector disruptive forces



Four power sector disruptive forces

1

Decarbonisation

- Zero carbon goals proliferating across most continents and accelerating in achievement.
- Coal and gas economics causing displacement as renewables prices drop.
- Planned and unplanned retirements, accelerating and creating energy gaps.
- Battery cost economics decline rapidly driving distributed generation.

2

Decentralisation

- Large scale centralised assets no longer price advantaged.
- Assets miniaturising and enabling broad adoption and distribution.
- Sites, buildings and premises emerging as battery-based supply.
- Virtual power plants resulting from integrating renewables and storage.

3

Disaggregation

- Technology enabling decomposition of load consumption patterns.
- Customer control of local energy supply decisions growing exponentially.
- Commercial and industrial customers active with renewables sourcing.
- Mass customisation emerging as necessary to match customer needs.

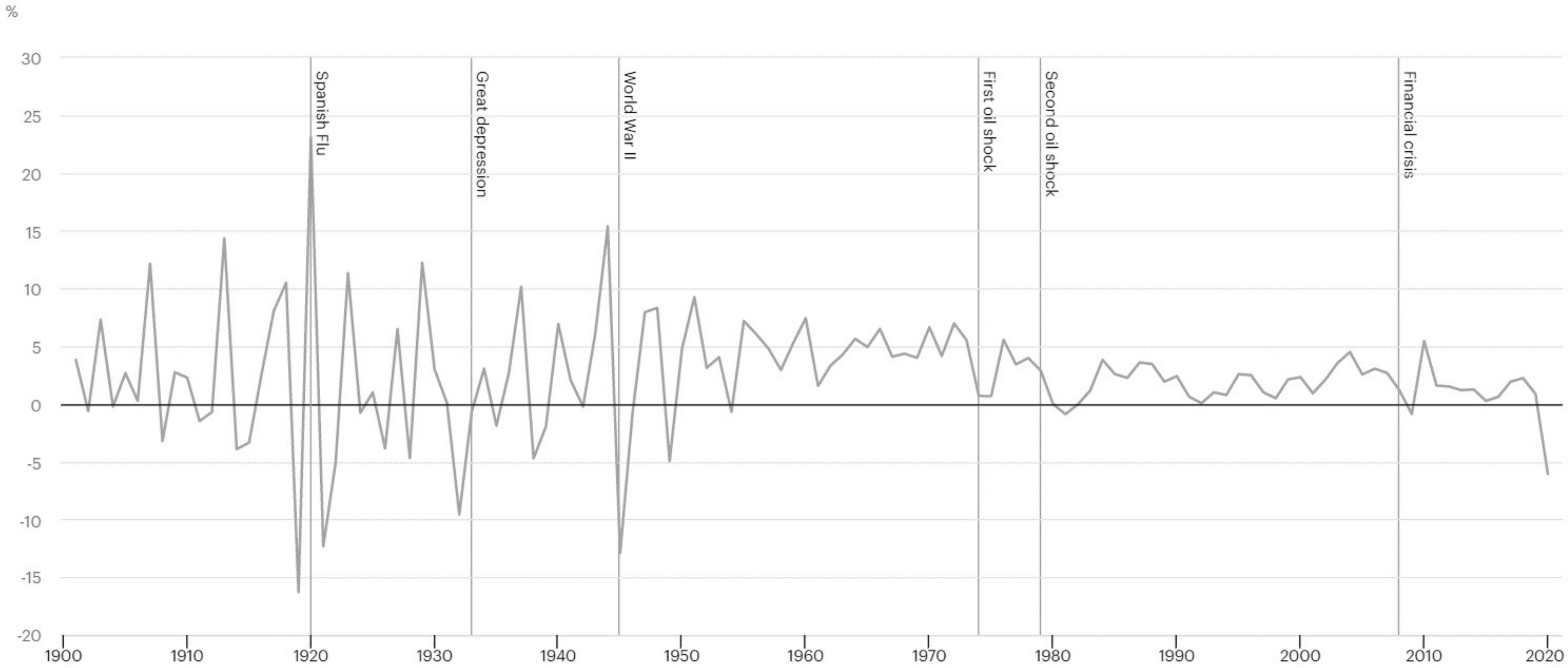
4

Digitalisation

- Vendors accelerating the shift from large platforms to value applications.
- Data analytics platforms a centrepiece for revenue growth and preservation.
- Customer acumen exceeding utilities and causing interface gaps.
- Companies repurposing capabilities to fit for purpose business value.

Setting the stage: Power demand in a COVID-19 era

Rate of change of global primary energy demand, 1900-2020

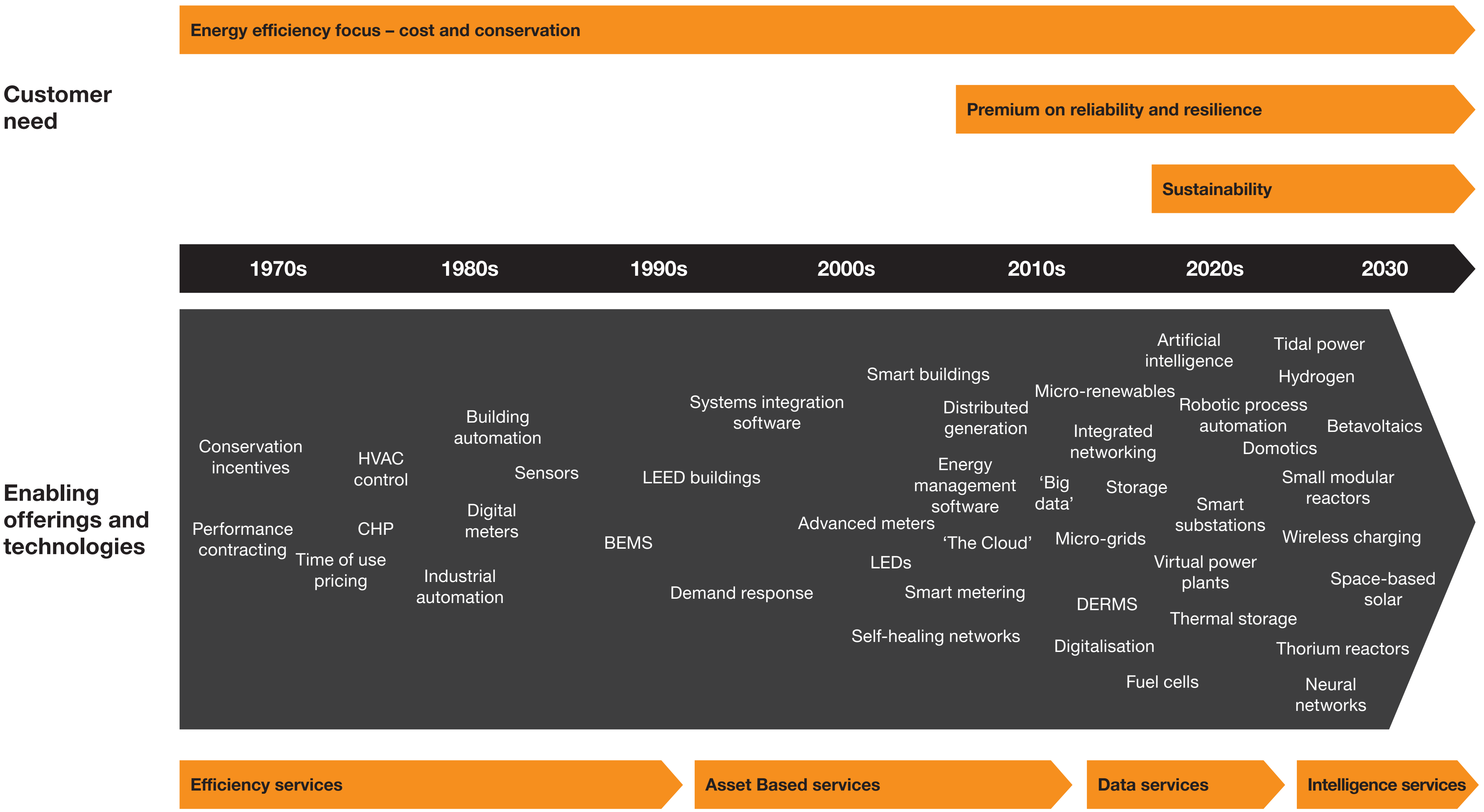


Source: IEA. Global Energy Review 2020: The impacts of the COVID-19 crisis on global energy demand and CO2 emissions

> “
>
> The shock to energy demand in 2020 is set to be the largest in 70 years. In our estimate, global energy demand declined by 6%, a fall seven times greater than the 2008 financial crisis.

How technologies are evolving within the power sector…

…and the question CISOs are asking: How do we secure these technologies?



Customer need

Energy efficiency focus – cost and conservation

Premium on reliability and resilience

Sustainability

1970s **1980s** **1990s** **2000s** **2010s** **2020s** **2030**

Enabling offerings and technologies

Conservation incentives

Performance contracting

HVAC control

CHP

Time of use pricing

Building automation

Sensors

Digital meters

Industrial automation

BEMS

LEED buildings

Systems integration software

Demand response

Advanced meters

LEDs

Smart buildings

Distributed generation

Energy management software

'The Cloud'

Smart metering

Self-healing networks

Micro-renewables

Integrated networking

'Big data'

Storage

Micro-grids

DERMS

Digitalisation

Fuel cells

Artificial intelligence

Robotic process automation

Smart substations

Virtual power plants

Thermal storage

Tidal power

Hydrogen

Betavoltaics

Domotics

Small modular reactors

Wireless charging

Space-based solar

Thorium reactors

Neural networks

Efficiency services

Asset Based services

Data services

Intelligence services

Business transformations are more sweeping and rapid

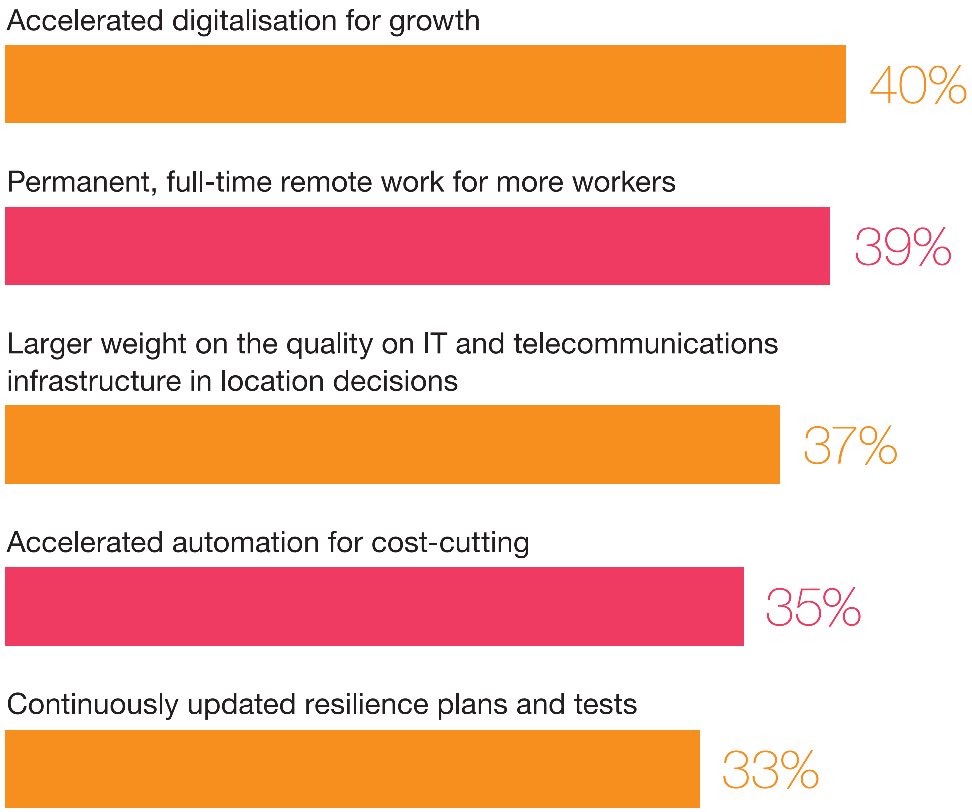
In the first three months of the COVID-19 pandemic, Chief Executive Officers (CEOs) reported that their organisations digitised at surprising speed, advancing to year two or three of their five-year plans. The future is now: digital health, industrial automation and robotics, enhanced ecommerce, customer service chat bots, virtual reality-based entertainment, cloud kitchens, fintech, and more.

The pandemic and economic recession have stoked further change, according to PwC's Global Digital Trust Insights 2021 survey: 40% of executives say they're accelerating digitisation – perhaps taking on business strategies they hadn't imagined before.

Their digital ambitions have skyrocketed. Twenty-one percent are changing their core business model and redefining their organisations (the 'redefiners'), while 18% are breaking into new markets or industries (the 'explorers'). Both categories have doubled since last year.

Doing things faster and more efficiently is the top digital ambition for 29% of executives ('efficiency seekers'), while 31% are modernising with new capabilities ('modernisers'). More than one-third – 35% – say they're speeding up automation to cut costs, which is no surprise at a time when revenues are down.

The businesses that CISOs protect are changing:



Source: PwC Global Trusts Insights Survey 2021, October 2020: base 3,249

Q. Which of the following changes are most likely to be impacts of the COVID-19 experience in your industry?

Cybersecurity trends in the power sector

How power sector CISOs are planning ahead

Just decades after coming out from under IT's wing, the cybersecurity profession has matured. Since the Massachusetts Institute of Technology was granted the first US patent for a cryptographic communication system in 1983, the industry has grown by leaps and bounds — with a long list of growing pains.

Armed with the insight and foresight that only experience and wisdom can provide, cyber stands at a critical, pivotal and exciting time for the power sector and the organisations and ratepayers it serves. The findings from PwC's Global Digital Trust Insights 2021 survey of 3,249 business and technology executives around the world describes what's changing and what's next in cybersecurity. Relevant excerpts from that study are included in this report.

No longer solely reactive, cybersecurity has become more risk-based and forward-thinking. Power Sector Chief Information Security Officers (CISOs) are building top-down, strategic cybersecurity plans that resonate more effectively with their management team and their board.

No longer technology-focused — although technology is very much in the picture — Power Sector security leaders are working closely with business teams to strengthen and increase the resilience of the organisation as a whole. As a result, operating unit leaders are becoming more accountable for the cyber risk they carry.

The timing couldn't be better. As the Power Sector quickly evolves, it is prompting many generators, transmitters and distributors to speed up their digitisation programs. CEOs and boards are turning to their CISOs to secure this change. Security teams are becoming seen as enablers of change, not just protectors.

Security technology is maturing too – which is simplifying cybersecurity's work and integrating it with the business as a whole. Digital solutions are adding layers of protection and continuously monitoring systems automatically for a simpler, more integrated approach to security.

Power Sector CISOs have an opportunity to reposition themselves as forward-looking strategic planners. And when spot fires are not demanding their attention, security managers are able to collaborate with their business leads.

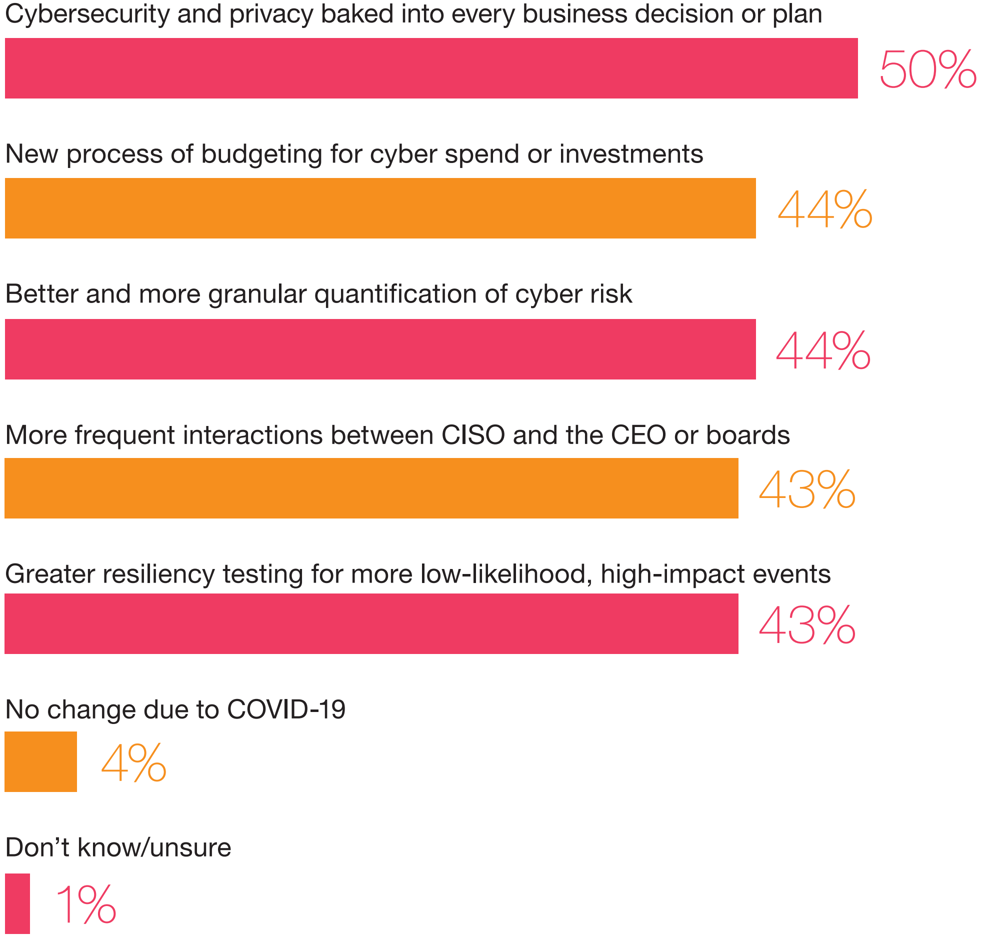
Business transformations are more sweeping and rapid

New technologies and business models in the power sector are challenging CISOs and their security teams to keep pace and secure rapidly changing environments.

COVID-19 added an immediate new set of security needs beginning in March 2020. Nearly all (96%) business leaders say they'll adjust their cybersecurity strategy due to COVID-19. Half are more likely now to consider cybersecurity in every business decision — that's up 25% from last year's survey.

CISOs must engage with management to understand where the business is headed, in order to keep in step with the vision and goals of their enterprise and keep it secure.

CISO strategies in 2020:



Source: PwC Global Trust Insights Survey 2021, October 2020: base 3,249

Q: Which of the following changes are most likely to be impacts of the COVID-19 experience on cybersecurity in your industry?

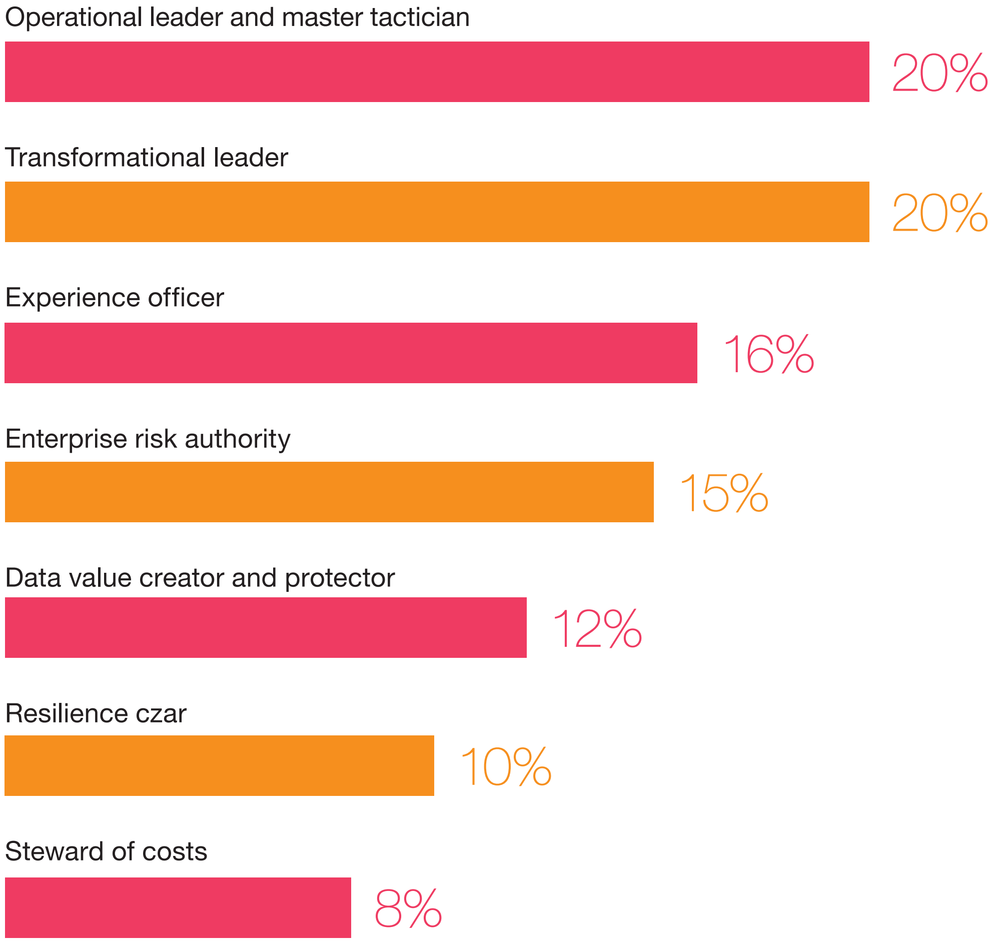
The current job description for CISOs

New times also call for new CISO leadership modes. Forty percent of executives say they need the CISO to be a transformational leader (20%) or an operational leader and master tactician (20%).

These roles are encompassing and call for the multifaceted expertise that CISOs have built. The transformational CISO leads cross-functional teams to match the speed and boldness of digital transformations with agile, forward-thinking security and privacy strategies, investments and plans. The operational leader and master tactician is a tech-savvy and business-savvy CISO who can deliver consistent system performance, with security and privacy throughout the organisation and its ecosystem amid constant and changing threats.

Some CISOs already inhabit these roles and are exhibiting four qualities most prized by executives: strategic thinking (38%), the ability to take smart risks (38%), leadership skills (36%) and the ability to recognise and nurture innovation (34%).

What executives expect CISOs to be:



Source: PwC Global Trust Insights Survey 2021, October 2020: Base 3,249

Q: What is the primary role your organisation's CISO needs to play to help your organisation achieve its growth and strategic objectives in the next two years?

Phishing trends in utilities

Phishing phase	Relationship between training and clicks-in-error	Utilities with 1 – 249 employees	Utilities with 250 – 999 employees	Utilities with 1000+ employees
Phase one: Baseline phishing security test Results	The **initial baseline phishing security test** was administered within utilities that hadn't conducted any security awareness training. Users received no warning and the tests were administered on untrained, unaware people going about their regular job duties.	39.6%	41.2%	39.2%
Phase two: Phishing security test results within 90 Days of Training	When organisations implemented a combination of **training** and **simulated phishing security testing** after their initial baseline testing, results changed dramatically. In the 90 days after completed security training events, the phish-prone percentage was cut by more than half to **14.1%**.	12.5%	13.2%	14.7%
Phase three: Phishing security test results after one year-plus of ongoing training	Measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests. The results were dramatic – **a consistent, mature security awareness training program reduced clicks-in-error from 39.6% down to 4.7%**. This demonstrates dramatic effectiveness across all utility sizes.	5.4%	4.9%	5.2%

Source: KnowBe4 phishing by industry 2020 benchmarking report

Guidance for power sector CISOs to plan and acquire budgets

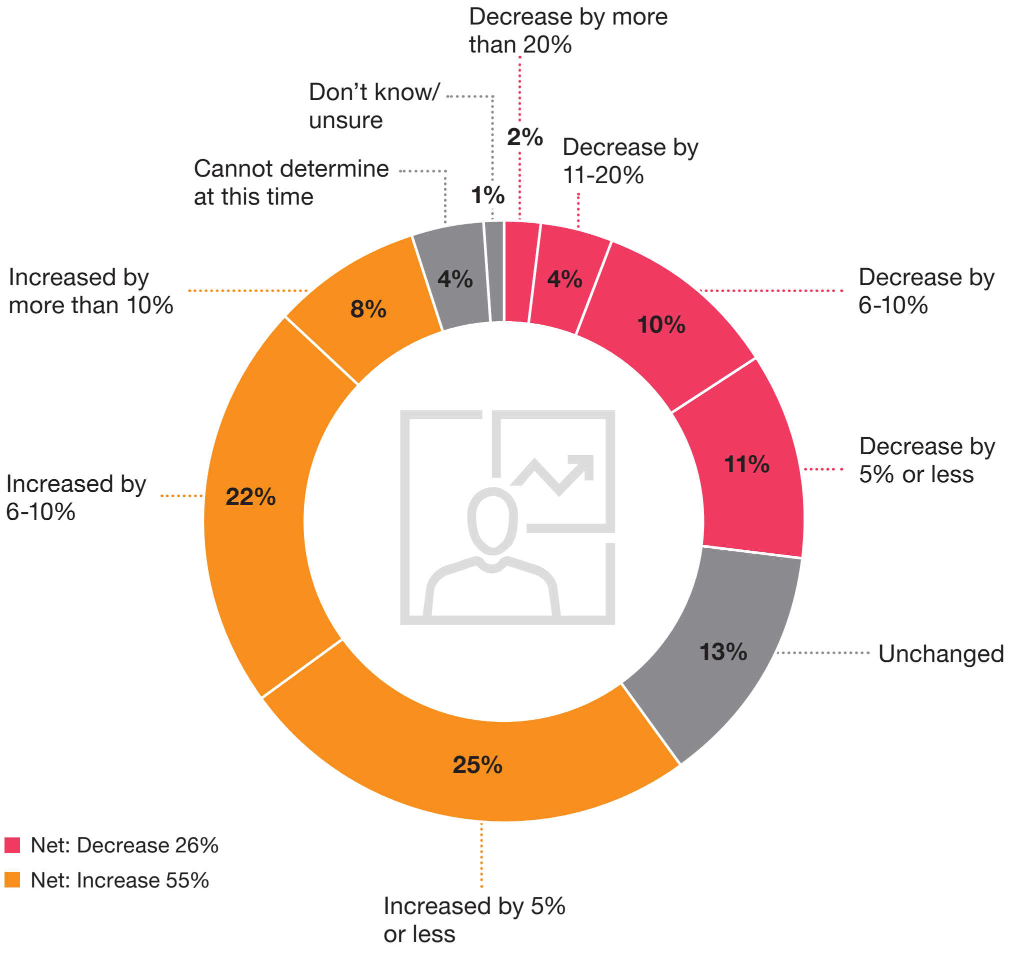
Building a compelling story for your budget

Fifty-five percent of technology and security executives who participated in the Global Digital Trust 2021 survey plan to increase their cybersecurity budgets, with 51% adding full-time cyber staff in 2021 — even as most (64%) executives expect business revenues to decline.

Clearly, cybersecurity is more business-critical than ever before. Still, 26% will need to do more with less and 13% will have to make do with static budgets.

The power sector has been hit with declining revenues and cash flows as a result of COVID-19. A compelling case for security budget increases are more important than ever. And getting the most value for every cybersecurity dollar spent is more essential as power companies digitise: every new digital process and asset becomes a new vulnerability for cyber attack.

Security budgets – not all are increasing



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249

Q: How is your cyber budget changing in 2021? base 1,414

Most executives lack confidence in the security budgeting process

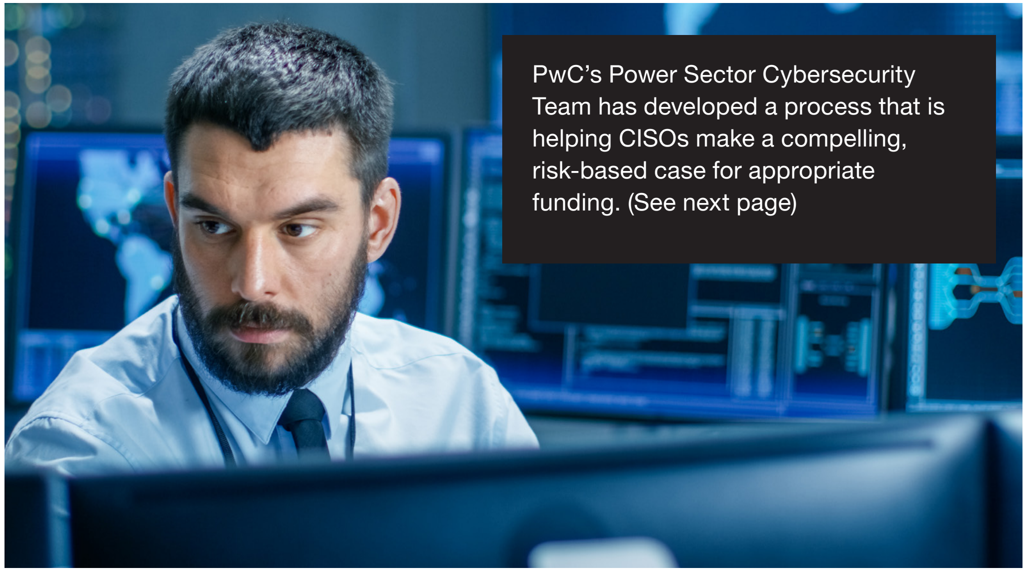
More than half (55%) of business and tech/ security executives:

- **Lack confidence that cyber spending is aligned to the most significant risks,** or
- That their budget funds remediation, risk mitigation and/or response techniques that **will provide the best return on investment (ROI)** (55%), or
- That budgets provide the **resources needed for a severe cyber event** (55%), or
- That the process **monitors the cyber program's effectiveness compared to expenditures** (54%).

Cyber budgets could and should link to overall enterprise or business unit budgets in a strategic, risk-aligned and data-driven way, but 53% lack confidence that their current process does this.

And with regard to preparedness for future risks, executives are not confident that cyber budgets provide adequate controls over emerging technologies (58%). **The executive team (and board) are a CISO's 'investors'. When investor confidence is low, they don't invest!**

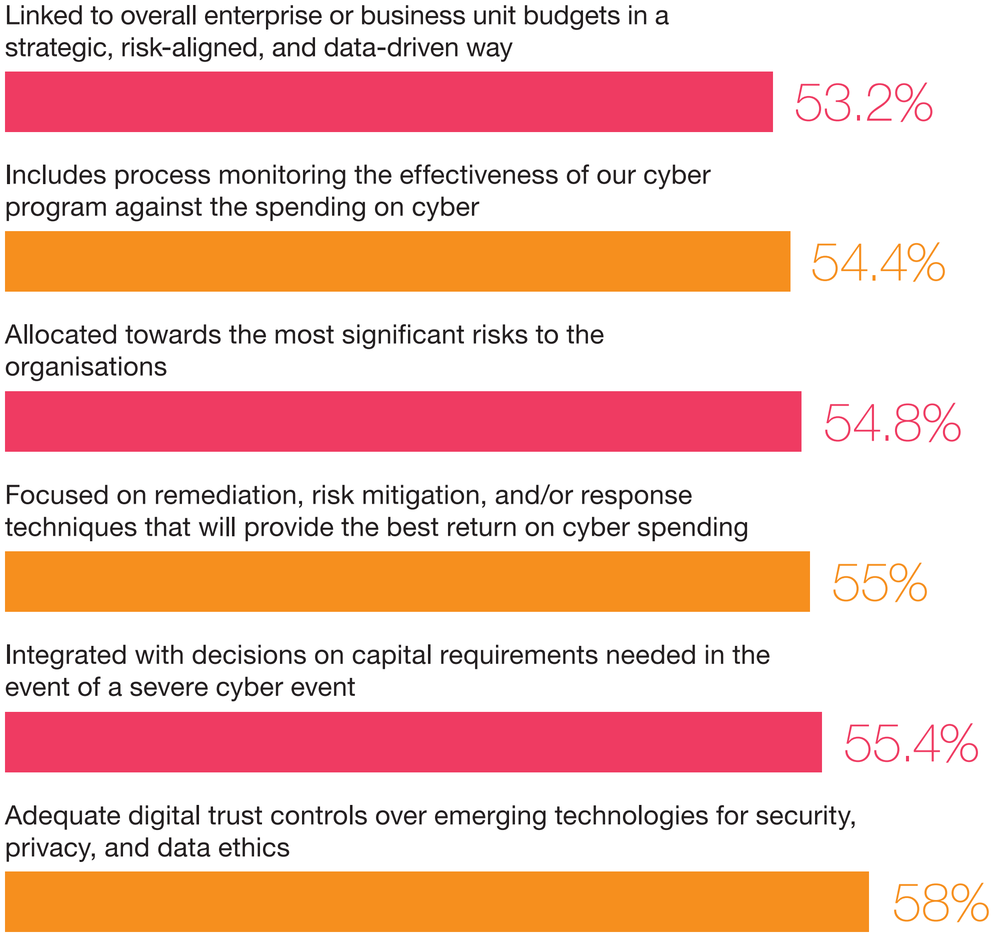
Not surprisingly, 44% of CISOs say they're trying new budgeting processes and considering how best to convince the CEO and board to assign needed funds.



PwC's Power Sector Cybersecurity Team has developed a process that is helping CISOs make a compelling, risk-based case for appropriate funding. (See next page)

Confidence in current cyber budgets and processes is low today

(% of respondents who are 'not very confident')



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249.

Q: Regarding your organisation's current cyber budget and processes, how confident are you with regard to the following?

Building a compelling story for your cybersecurity budget

1

Confirm cyber maturity level and identify your vulnerabilities.

2

Conduct a cyber risk assessment (current risk levels).

Then, confirm your target risk levels with management (desired risk levels of impact and likelihood on same heatmap).

3

Identify which controls to enhance, or add, to bring your current cyber risk down to target risk levels.

4

Draft a resourcing plan to implement the identified controls (in-sourced/co-sourced/out-sourced?).

5

Draft a roadmap by month/year to implement the controls.

6

Calculate the necessary budget to implement the controls, by year, using your resourcing assumptions.

Did management approve your security budget?

Yes, budget approved

No, budget not approved

7a

Remove unfunded controls from your plan. Then, show your executives the higher target risk level they will need to accept with the lower budget (see step 2).

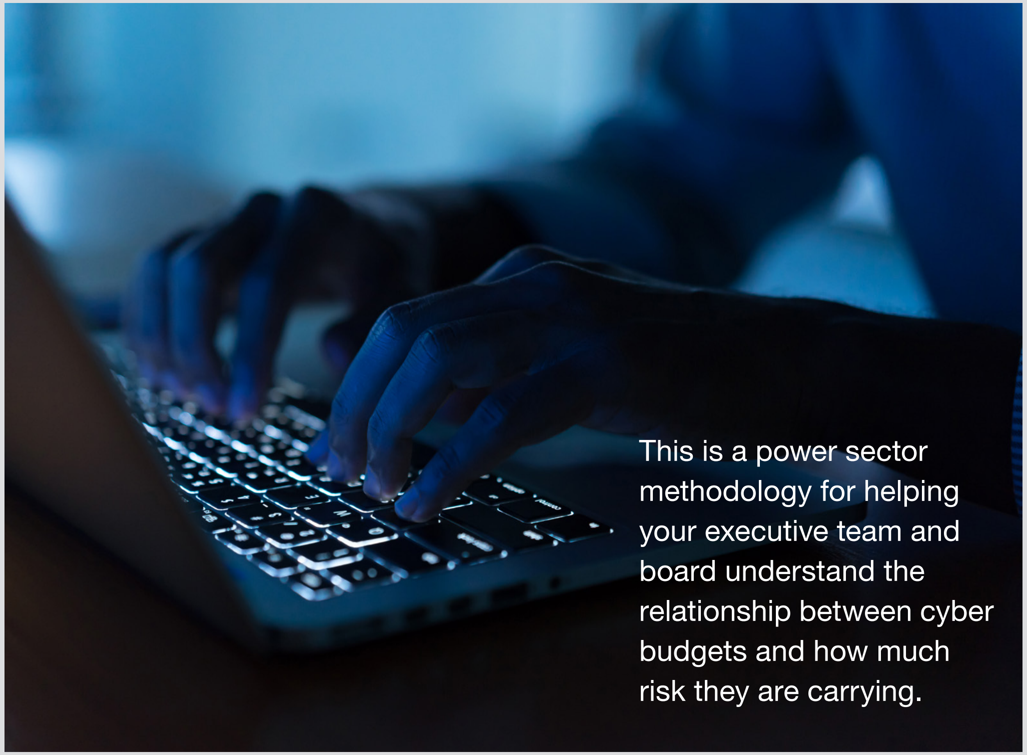
If your executives are uncomfortable with the higher risk level then you can renegotiate a higher budget.

7b

Execute the budgeted work.

8

Re-assess cyber risk annually to show how it is being reduced via the new controls.



This is a power sector methodology for helping your executive team and board understand the relationship between cyber budgets and how much risk they are carrying.

Guidance for C-Suites and Boards to effectively engage CISOs

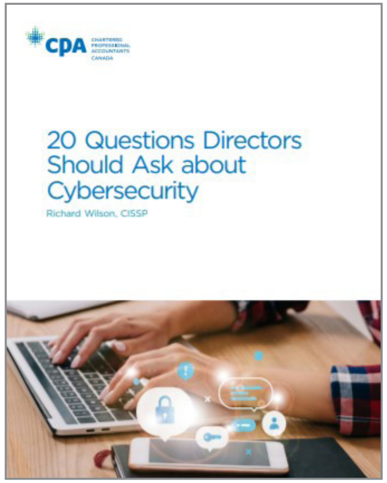
Good security requires effective collaboration and communication among boards, C-suites and CISOs. While this statement is obvious, the execution can be more complex.

There are often requests for CISOs to bring more business-centric reports and metrics to leaders. Boards speak ‘risk’, so overly technical information can be confusing. If reports don’t demonstrate how much security investments will lower risk, then the value of the investment is unclear. This is a major cause of security underfunding for CISOs who fail to show the connection. (See page 18 for a power sector methodology.)

If this communication is to truly be two-way, how can boards and C-suites also play a role in creating clarity? Here are a few suggestions, along with a helpful publication to equip you with the right cybersecurity questions to ask.

To assist boards and C-suites, team members from PwC authored the guide, 20 Questions Directors Should Ask about Cybersecurity for CPA Canada. It equips directors and leaders with important questions to better understand:

- Developing an effective cybersecurity strategy;
- Board cyber governance recommendations;
- The link between cybersecurity spending and risk reduction;
- Rationale for resourcing (what is an appropriate headcount for a power company?);
- A framework for planning cybersecurity programs in non-technical terms (NIST);
- Recommendations for intuitive cyber reporting.



CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

20 Questions Directors Should Ask about Cybersecurity

Richard Wilson, CISSP

CISO challenge:

The role of a power sector CISO is complex. Power, water and gas are essential to society, and a major cybersecurity event could cause significant public harm. The risk appetite for a cyber event is extremely low, but funding for security has its limits.

Leadership response:

Leaders need to work with CISOs to strike the right balance. Assess cyber risk and agree on how much risk is appropriate. Then, review what controls need to be in place to achieve the risk level and have conversations about adequate funding to lower cyber risk to desired levels.

CISO challenge:

A majority of power company CISOs share concerns about under-resourced security teams.

Leadership response:

Security headcount challenges stem from looking at the issue from the wrong angle. The sequence of questions should be:

1. What is our desired risk target?
2. What processes and technologies are required to achieve this risk level?
3. When do we need to have these controls in place, what is an appropriate time frame?
4. What is the best ratio of in-sourced resources (vs. co-sourced or outsourced)?
5. Based upon steps 1-4, determine how many in-sourced resources are required to both implement and operate the program.

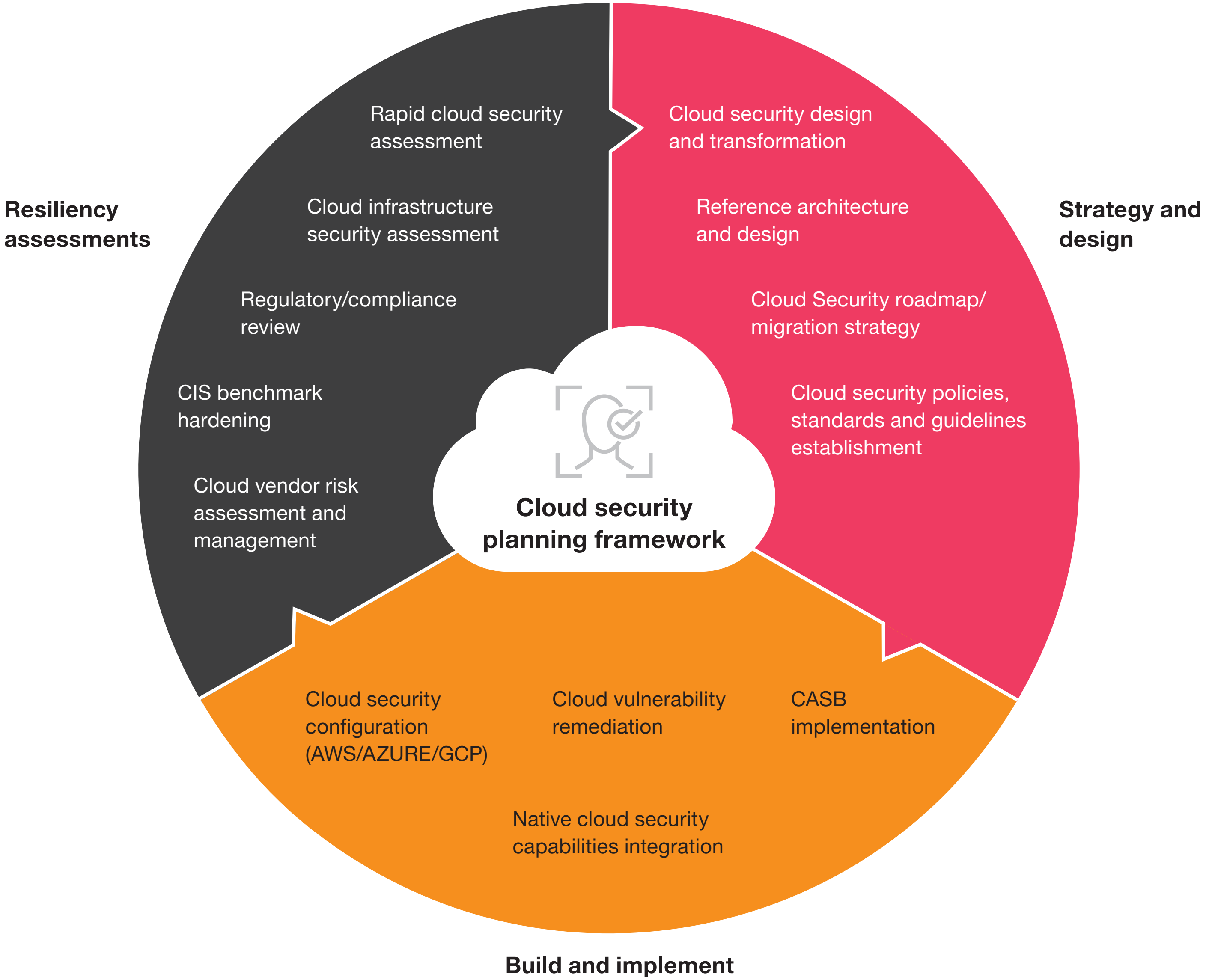
As you can see, security risk targets, plus the time to achieve it, is the root question to determine headcount.

Five Technical priorities for power sector cybersecurity

1. Strong power sector migration to the cloud

We are seeing power companies rapidly moving more of their environment to the cloud. They're doing away with static legacy systems in favour of more dynamic, nimble integrated cloud/network systems that are secure by design. Aging technical infrastructure, mobile workforce and asset management, customer-centric data analytics and relationship management, and evolving human resource (HR) systems are four drivers moving utilities to the cloud.

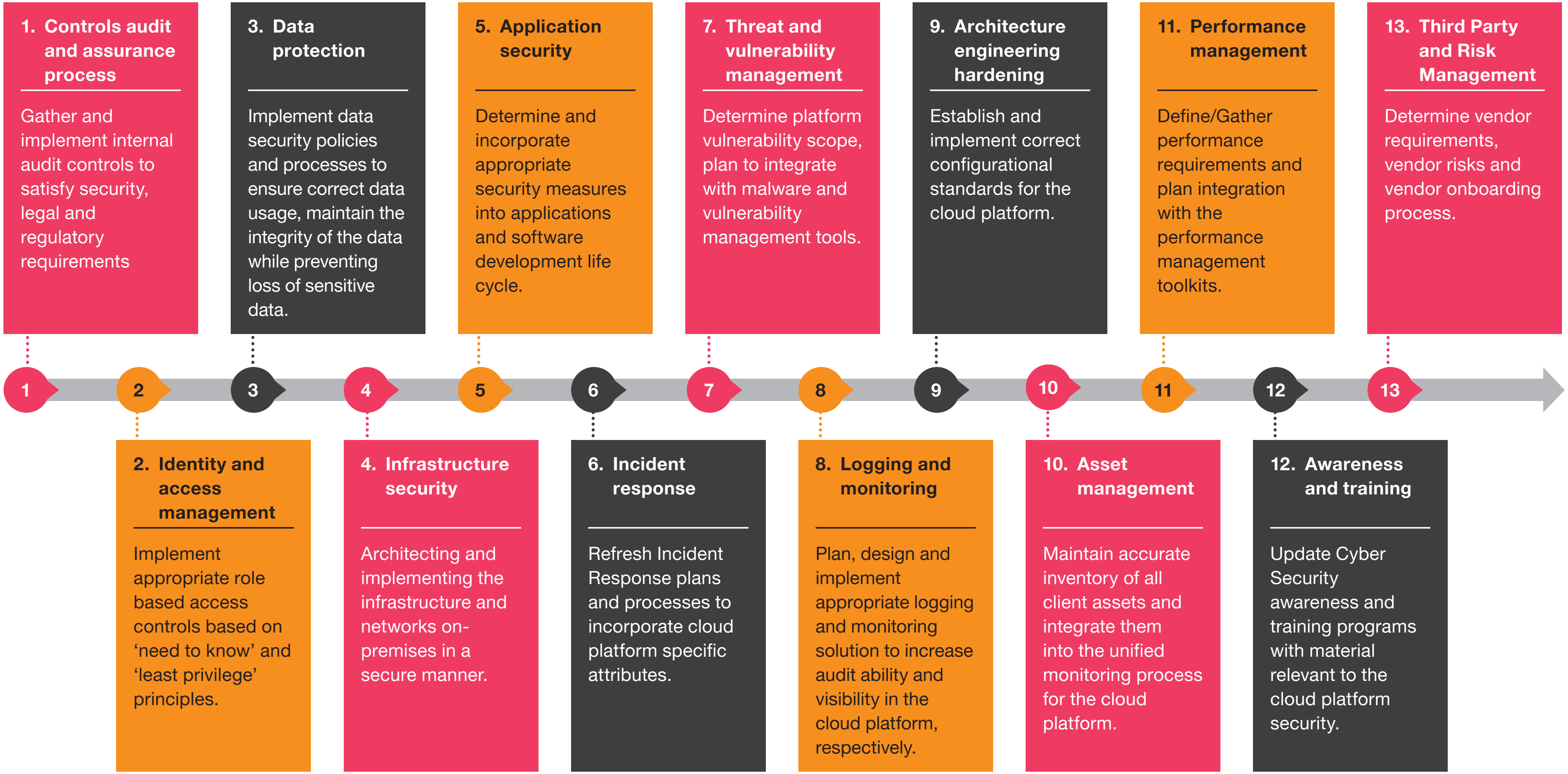
More than a third (35%) of executives strongly agree that moving to the cloud is foundational for the next generation of business solutions for their organisation. And 36% strongly agree that new solutions exist to secure cloud infrastructures better than they have ever been in the past.



Resiliency assessments
Rapid cloud security assessment
Cloud infrastructure security assessment
Regulatory/compliance review
CIS benchmark hardening
Cloud vendor risk assessment and management
Strategy and design
Cloud security design and transformation
Reference architecture and design
Cloud Security roadmap/ migration strategy
Cloud security policies, standards and guidelines establishment
Cloud security planning framework
Build and implement
Cloud security configuration (AWS/AZURE/GCP)
Cloud vulnerability remediation
CASB implementation
Native cloud security capabilities integration

1. Strong power sector migration to the cloud

Cloud security capabilities development plan



1. Controls audit and assurance process

Gather and implement internal audit controls to satisfy security, legal and regulatory requirements

2. Identity and access management

Implement appropriate role based access controls based on ‘need to know’ and ‘least privilege’ principles.

3. Data protection

Implement data security policies and processes to ensure correct data usage, maintain the integrity of the data while preventing loss of sensitive data.

4. Infrastructure security

Architecting and implementing the infrastructure and networks on-premises in a secure manner.

5. Application security

Determine and incorporate appropriate security measures into applications and software development life cycle.

6. Incident response

Refresh Incident Response plans and processes to incorporate cloud platform specific attributes.

7. Threat and vulnerability management

Determine platform vulnerability scope, plan to integrate with malware and vulnerability management tools.

8. Logging and monitoring

Plan, design and implement appropriate logging and monitoring solution to increase audit ability and visibility in the cloud platform, respectively.

9. Architecture engineering hardening

Establish and implement correct configurational standards for the cloud platform.

10. Asset management

Maintain accurate inventory of all client assets and integrate them into the unified monitoring process for the cloud platform.

11. Performance management

Define/Gather performance requirements and plan integration with the performance management toolkits.

12. Awareness and training

Update Cyber Security awareness and training programs with material relevant to the cloud platform security.

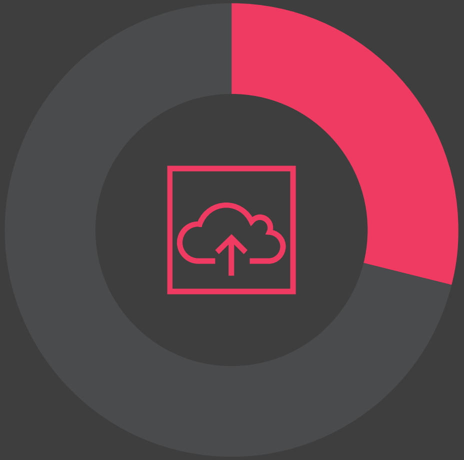
13. Third Party and Risk Management

Determine vendor requirements, vendor risks and vendor onboarding process.

Listed are 13 cloud security requirements that CISOs should consider to design, configure and operate your cloud environment securely.

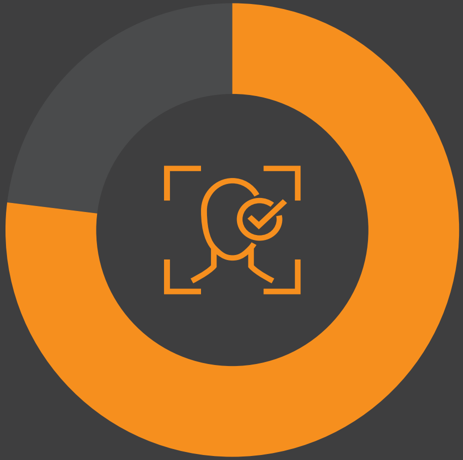
1. Cloud Security – A technical perspective

Public cloud adoption in 2021 is being driven by Infrastructure-as-a-Service (IaaS) and cybersecurity remains a major challenge for cloud adoption



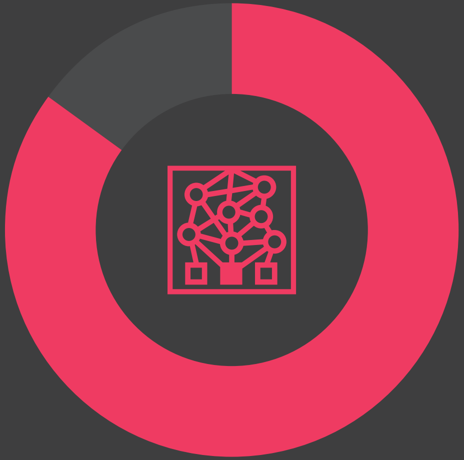
29%

IaaS is the fastest growing cloud segment in 2021



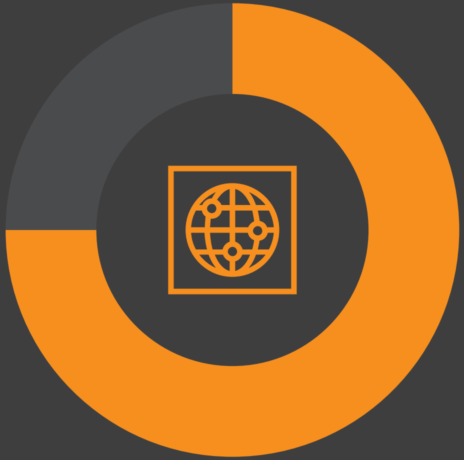
77%

IT professionals consider security a major challenge



85%

Enterprise workloads to be in cloud by 2020



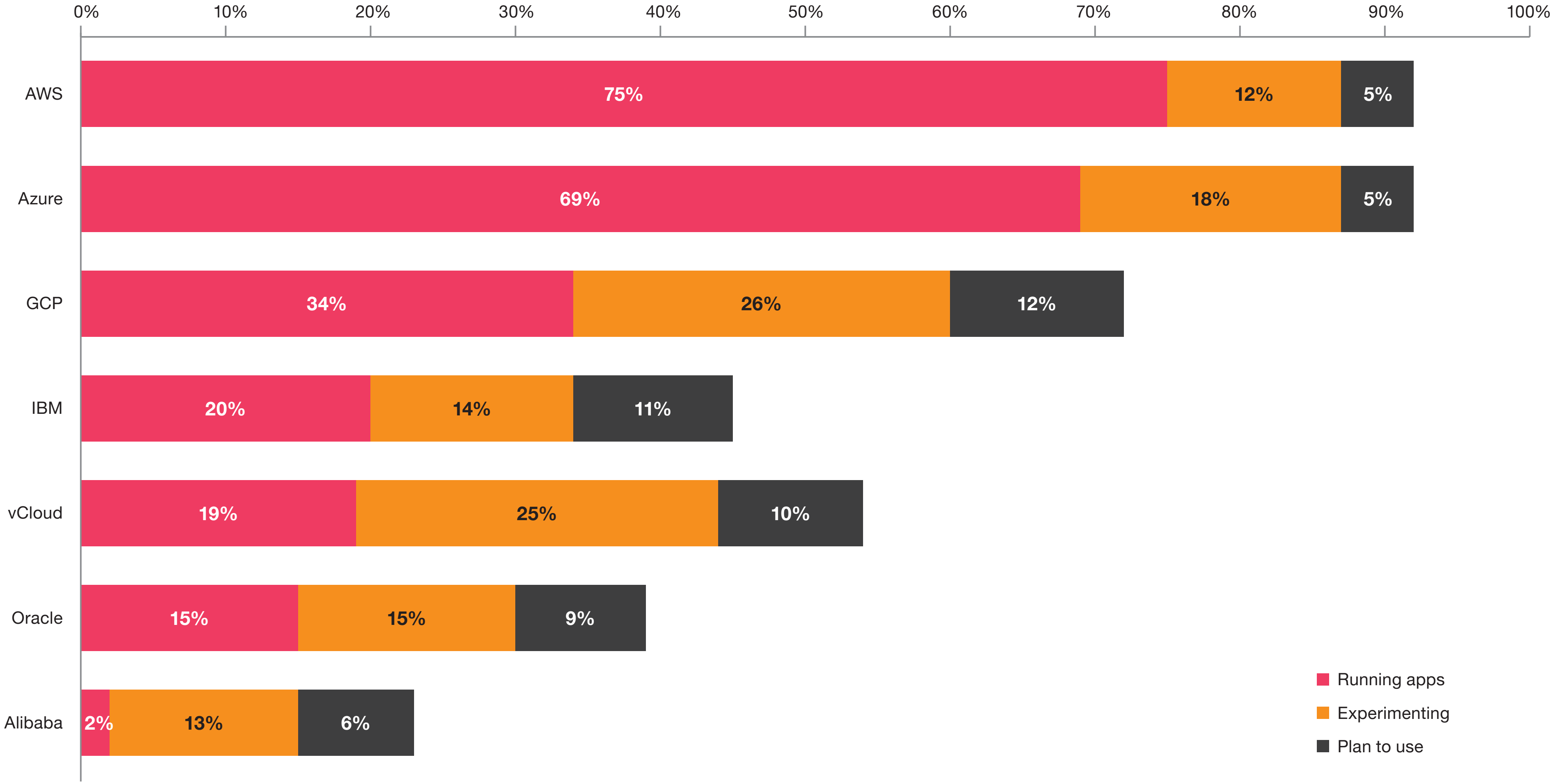
75%

Global organisations will have containerised applications in production

1. Cloud Security – Public cloud platform usage

Multi-cloud architecture is gaining traction

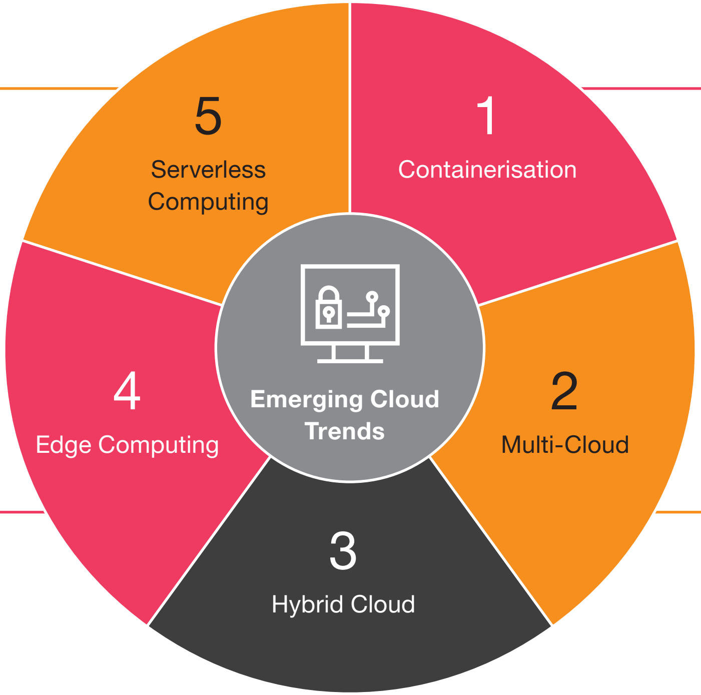
Public cloud platform usage worldwide, 2020



Source: Flexera, 2020, Forbes.com

1. Cloud Security – Cloud adoption in 2021

As the cloud landscape evolves, there are five trends driving cloud adoption in 2021



Serverless is the next evolution from monolithic application architecture after service-oriented architecture and micro services architectures. Serverless was among the top five fastest-growing Platform as a Service (PaaS) cloud services for 2020, according to the Flexera 2020 State of the Cloud report.

Enterprise container adoption expanded rapidly in 2018. As per Cloud Foundry survey, 47% of organisations have more than 100 containers deployed in production. The number is expected to increase in the years to come.

Edge pushes the computing power to the edge of what devices can handle. Internet of Things (IoT) is a well-known use case. It helps eliminate traditional issues like bandwidth, cost and latency and enables real-time customer engagement, sensor analytics, etc.

International Data Corporation (IDC) states, over 90% of enterprises worldwide rely on a mix of on-premises/dedicated private clouds, several public clouds and legacy platforms to meet their infrastructure needs. It affords enterprises the freedom from vendor lock-in, which is a big concern for over 80% of enterprises.

Making a full transition to the public cloud has proved more challenging than anticipated, so hybrid cloud solutions can help companies to transition to the public cloud at their own pace, with less risk and possibly at a lower cost.

Source: Flexera, Forbes.com

1. Cloud security technical challenges

Given the dynamic nature of the cloud, cloud applications and infrastructure are prone to configuration drift. This refers to the change in the configuration of applications and infrastructure resources from desired, compliant standards due to unmerged/poorly managed changes in the environment.

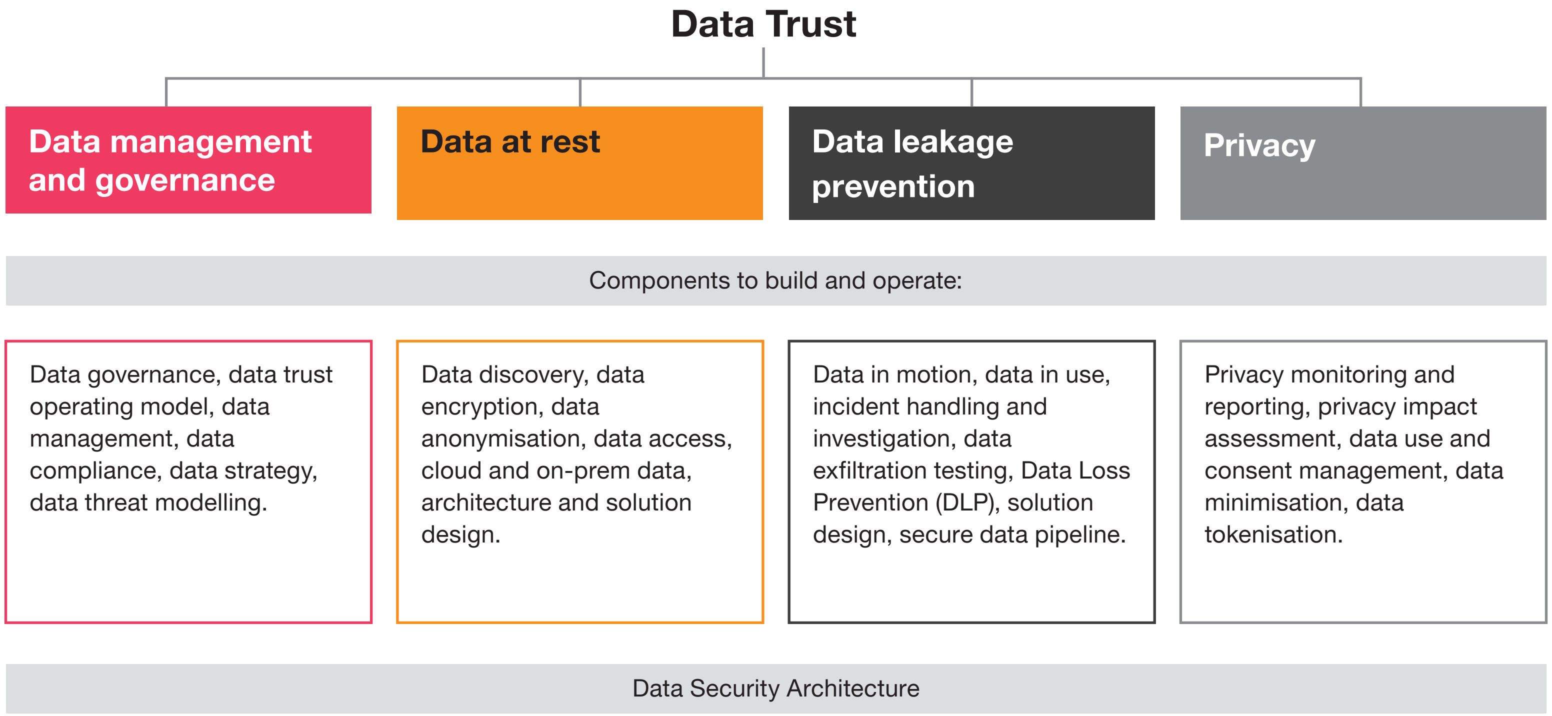
1	**Broken access model**	• Overly permissive and ambiguous principal and resource roles • Hardcoded credentials and secrets in Infrastructure as Cloud (IaC) scripts	• Automated cloud identity lifecycle management • Cloud secrets management solutions
2	**Network and communication**	• Security groups permitting remote access over internet • Unauthorised FaC changes • Sensitive traffic over internet	• Cloud flow logs monitoring • Cloud firewall management solutions • Cloud providers' private endpoints
3	**Storage and data services**	• Public storage buckets with sensitive data • Unencrypted backup snapshots • Unauthorised cross-region data replication	• Cloud compliance monitoring solutions • Cloud firewall management solutions • Resource policies and guardrails
4	**Compute, container and serverless**	• Instance launch from insecure image build • Unpatched/unsecure vulnerability managements/ machine images • Insecure container build pushed to container registry	• Cloud service catalogues • Image registry scanning • Container registry scanning and secure operations
5	**CI/CD pipelines**	• Secrets check-in Source Code Repositories • Unverified open source libraries in custom software or Infrastructure as Code scripts	• Source-code scanning tools • Secure Git operations for IaC • Compliance as code (CaC)
6	**Applications and APIs**	• Unhardened applications/middleware • Source code vulnerabilities in custom apps • Private endpoint application programming interface (API) exposed over internet	• Cloud hardening and vulnerability scanners • Source-code scanning tools • Application and API proxies

2. Merging of data protection, privacy, and governance

An interesting merger of activities has occurred in recent years. PwC's Data Protection team kept intersecting with our Data Governance team and Privacy team within the same clients. **Why?** Because these topics have significant overlap and collaboration needs to happen among them in order to start managing data effectively and securely. Regardless of where you start, all of these stakeholders and processes converge.

Power companies should think about a Data Trust strategy to address the interconnected areas as one strategy.

If you combine these four elements together, it becomes a single strategy to manage and protect data enterprise wide. PwC now calls this…



Data Trust

Data management and governance

Data at rest

Data leakage prevention

Privacy

Components to build and operate:

Data governance, data trust operating model, data management, data compliance, data strategy, data threat modelling.

Data discovery, data encryption, data anonymisation, data access, cloud and on-prem data, architecture and solution design.

Data in motion, data in use, incident handling and investigation, data exfiltration testing, Data Loss Prevention (DLP), solution design, secure data pipeline.

Privacy monitoring and reporting, privacy impact assessment, data use and consent management, data minimisation, data tokenisation.

Data Security Architecture

Benefits for power companies to adopt the Data Trust approach:

- A single data strategy reduces redundancy and effort.
- Business unit leads are not approached repeatedly by different data teams.
- CISOs get a full view of data locations and flows across the enterprise.
- Fewer data silos or gaps.

Important note:

While CISOs should stakeholder parties in each areas, it is recommended to execute one or two of the Data Trust components at a time

2. Data Trust – How power companies are evolving

As power companies transition into a single strategy around data, **new technologies and capabilities have emerged** to create an ecosystem that facilitates the creation, usage, sharing and retirement of data in a secure, trusted and transparent manner.

The Data Trust challenge

- Lack of visibility into the collection, dissemination and use of consumer data
- Integrity of data-centric processes supporting safety, reputation and health
- Data leakage and breaches
- Regulatory compliance and concept of 'privacy as a human right'
- 'Weaponised' data – geopolitics, disinformation campaigns

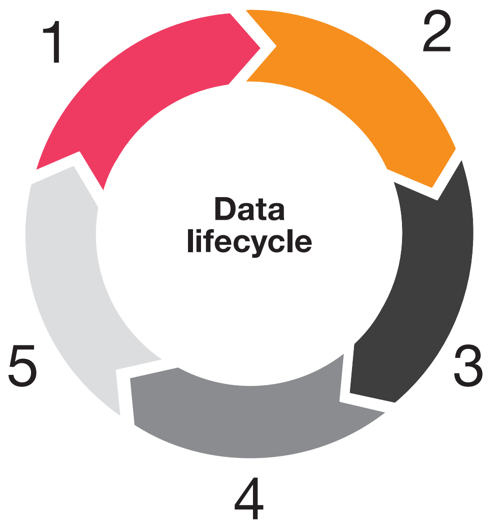
What's influencing Data Trust?

- Secure 3rd party data collaboration*
- Data integrity - deepfakes and disinformation*
- Dynamic data inventory
- AI-driven data classification and tagging
- Data encryption and protection

- Identity proofing and verification
- Consumer consent and data access requests
- Sensitive data monitoring
- Data anonymisation and de-identification
- Data retention, archival and deletion

2. Data Trust – Leading practices

The key guiding principle to establishing a successful data program is to incorporate the appropriate enablers throughout the data lifecycle.



- Define data
- Create data
- Use data
- Share data
- Retire data

Data Lifecycle

Define	Create	Use	Share	Retire
Data Protection Enabler				
Data Catalogue	Data Catalogue	Data Catalogue	Data Catalogue	Data Catalogue
	Automated and Contextual Classification	Data Access Management	Data Access Management	De-Identification
	DLP	DLP	DLP	Data Discovery
	Data Discovery		System Configuration	Encryption
	Encryption		Encryption	

Data Governance

Enabling Cross-Functional Capabilities

Chief Privacy Officer (CPO) + Legal/General Counsel (GC) + Chief Information Security Officer (CISO)

2. Data Trust – How it aligns to key three roles

Data trust enables distinct, yet interrelated cross-functional capabilities

Chief Privacy Officer (CPO)

- Data discovery (individual rights request) ✓
- Data inventory (consumers) ✓
- Data classification (consent, preferences) ✓
- Data breach safeguards ✓
- Privacy compliance ✓
- Personal Data (PII) protection ✓
- Privacy by design ✓
- Data deletion requests ✓
- Data breach notification ✓
- Responsible and ethical data use ✓

+

Legal/General Counsel (GC)

- Data discovery (eDiscovery, legal matters) ✓
- Data inventory (workforce) ✓
- Data classification (retention period) ✓
- Liability and insurance ✓
- Legal hold management ✓
- Intellectual property (IP) protection ✓
- Defensible legal posture ✓
- Data retention, archival and disposition ✓
- Data breach notification ✓
- Supplier Contracts ✓

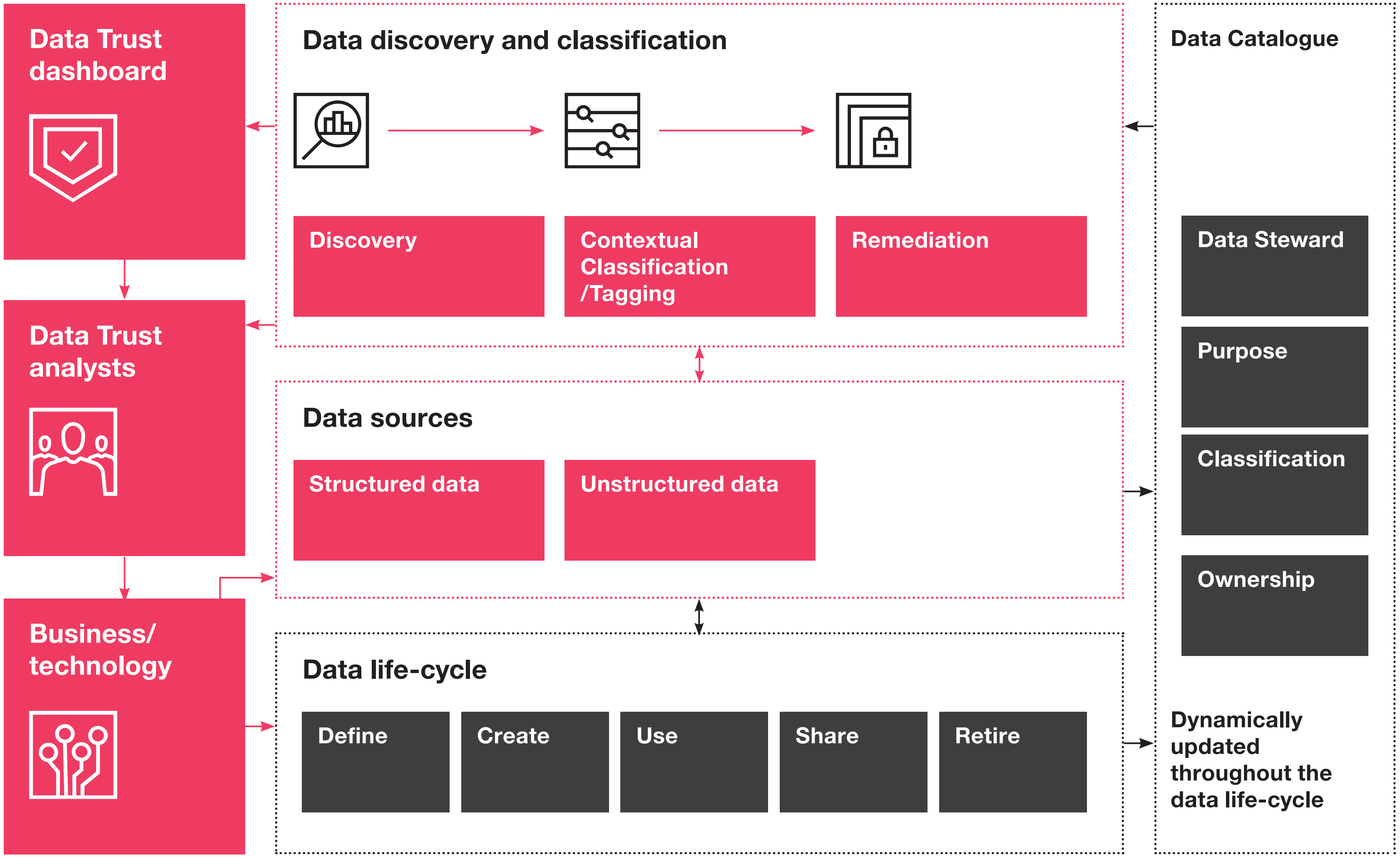
+

Chief Information Security Officer (CISO)

- Data discovery (safeguard assets) ✓
- Data inventory (crown jewels) ✓
- Data classification (data sensitivity) ✓
- Defensible security posture ✓
- Cybersecurity compliance ✓
- Data encryption ✓
- Security by design ✓
- Data de-identification and minimisation ✓
- Data breach response ✓
- 3rd party and supplier security ✓

2. Data Trust – A technical perspective

Illustrative architecture: Establishing near-real-time data visibility and data compliance



Data Trust dashboard

Data Trust analysts

Business/ technology

Data discovery and classification

Discovery

Contextual Classification /Tagging

Remediation

Data sources

Structured data

Unstructured data

Data life-cycle

Define

Create

Use

Share

Retire

Data Catalogue

Data Steward

Purpose

Classification

Ownership

Dynamically updated throughout the data life-cycle

Success factors for tooling your data trust program

- Integrated tooling
- Dedicated interaction with data owners, stewards and custodians
- Design patterns and technical specifications for data sources

Point-in-time discovery

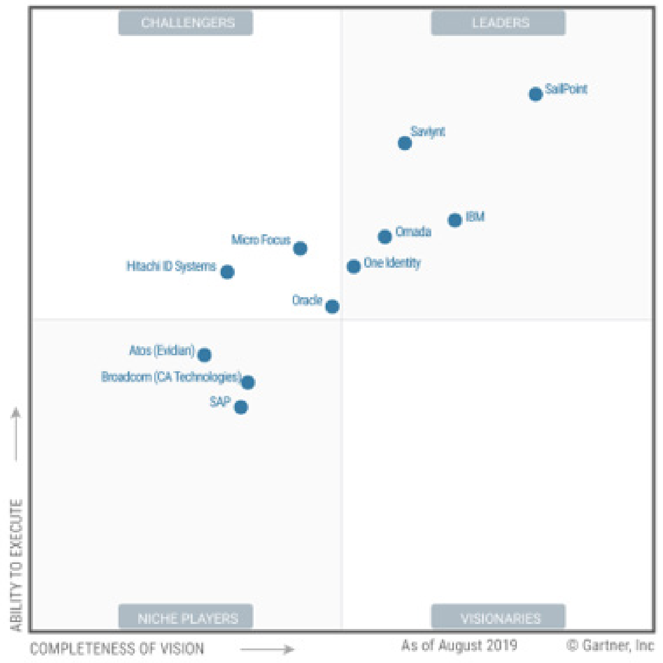
Near real-time

3. Access Management (IAM/PAM) success factors

Identity and Access Management, Privileged Access Management and Role Based Access Control (IAM/PAM/RBAC) are a significant focus for the power sector right now. PwC's estimates place the percentage of LDCs considering a major program implementation between 30-40% in the next 24 months.

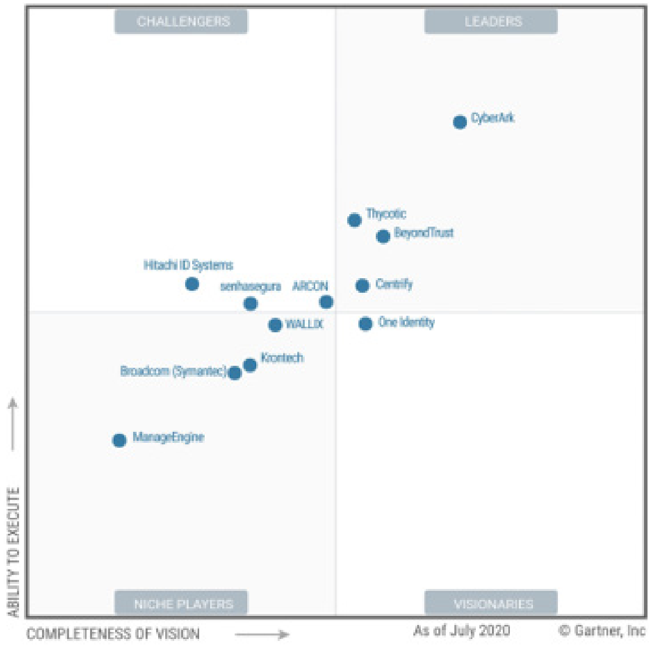
Many power companies have implemented security controls that were either foundational to their cybersecurity programs, or were 'low hanging fruit'. But our professionals have observed across many clients that IAM, PAM, and RBAC were often developed through a series of manual processes which have gone through step changes, but not wholesale upgrades until recently. The last 3 years have seen a boom of implementations to replace manual processes and disparate systems with Identity Governance and Administration (IGA) products and advanced **Privileged Access Management** (PAM) solutions.

Magic Quadrant for identity Governance and Admission



Source: Gartner (October 2019)

Magic Quadrant for Privileged Access Mangement



Source: Gartner (August 2020)

3. Access Management (IAM/PAM) success factors

Below are Success Factors for power companies to consider pre-implementation.

IAM success factors

- Senior management must understand, buy in and support the long term transformation.
- Enable streamlined decision making at the Executive level.
- Define and track Key Performance Indicators (KPIs) before and after transformation.
- Understand and track organisation interdependencies: key items (HR people/system changes, infra transformations, decommissioning).
- Clear roles and responsibilities are a transformation and end-state requirement.
- Change management to support changes to process/technology.
- Business cases are typically justified based on risk reduction and cost avoidance, but get watered down and absorbed by Line Of Business.

PAM success factors

- Spend time to define ‘privileged’ to calibrate and avoid over/under protection.
- Identify and understand data issues/gaps early: server/target inventory and account inventory are critical.
- Approach PAM by platform, not by application.
- Identify and make an individual accountable for platform access model decisions.
- Establish a platform operation model to establish sustainable operations.
- PAM solutions can be enabled to cater to NERC and non-NERC environments in parallel (including OT targets).
- Consider usability as a key adoption requirement for OT environments.
- PAM is not enabled until other access is removed.

IGA success factors

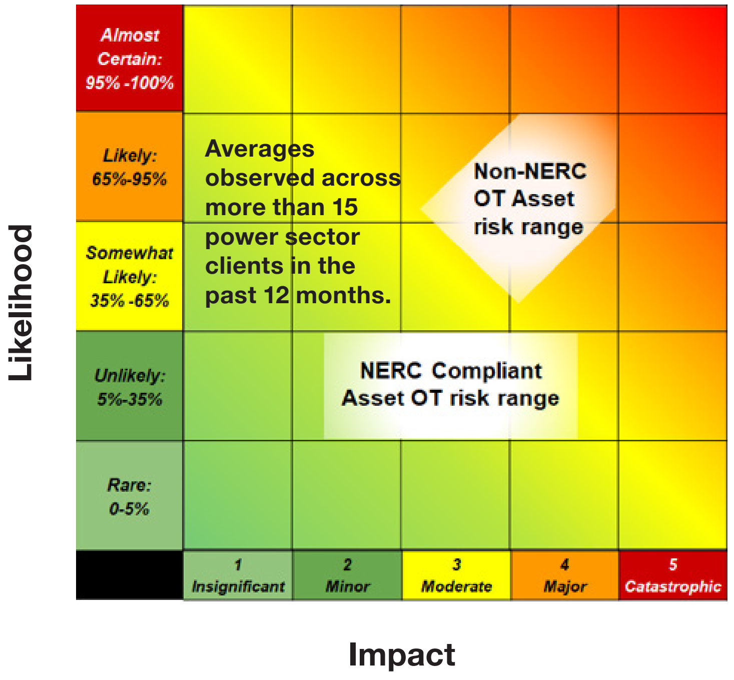
- Build a business case on efficiency or risk reduction and plan implementation roadmap based on that initial outcome.
- Identify and understand identity data issues (people/entitlement records) and begin a targeted cleanup in parallel.
- Build a thoughtful migration plan based on current state (big bang vs running migration).
- Minimise customisation but do not avoid configuration. Give and take on processes.
- IGA transformations are 70% people/process and 30% technology - effective change management is important.
- Establish an application onboarding factory
- Make application/business owners accountable for compliance.

4. Greater collaboration to secure Operational Technologies (OT)

We are observing greater pressure on power companies to reconcile the often long-standing gap between IT and OT teams. Some companies have created a single security leadership role over both areas, but we still see progress to be made with internal IT/OT collaboration across much of the sector. Boards and management teams showed increased interest for OT teams to lower security risk.

- Publicly accessible OT systems
- Insecure remote connectivity to OT networks
- Missing security updates
- Poor password practices
- Insecure firewall configuration and management
- OT systems located within corporate IT networks
- Weak protection of the corporate IT network from OT systems
- Lack of segmentation within OT networks
- Unrestricted outbound internet access from OT networks
- Insecure encryption and authentication for wireless OT networks

Where we are seeing power sector OT security risk now...



This heat map shows the ranges of Operational Technology risk in the power sector.

Examples of OT risks include:

- Failure of utility technology infrastructure
- Loss of system control data integrity
- Loss of third party service provider

The upper white shaded area reflects where risks reside, on average, for OT assets that **do not** fall under NERC regulatory requirements. OT risks are notably lower for NERC regulated assets.

4. Operational Technologies (OT) – Power Sector Initiatives

OT security tech deployment

- Automated OT asset management program (SCADA, telecom, relays, data concentrators, HMIs, IEDs).
- Secure remote access to OT (integrate with corporate remote access – MFA).
- IAM/PAM for local and remote access to assets/ systems.
- IT-OT segmentation, DMZ with jump host deployment, ICS LAN segmentation.
- OT-IT asset VM and patching program.
- ICS asset VM and patching program.
- OT secure change management and backup program.

OT monitoring and detection

- OT security monitoring tool/platform evaluation and design (assets, network, real-time threats).
- Deployment of OT security monitoring tools to assets/systems.
- OT security monitoring tool use case development and testing.
- Integration of physical security system logs in to the SIEM.
- OT cybersecurity IR plans and playbooks.

Integrated SOC

- OT security monitoring tool integration in to the SIEM.
- Full SOC visibility of OT assets and systems (monitoring tools and logs).
- Use case correlation with physical security logs.
- Use case correlation with IT logs.
- Integrated OT security, operations and engineering response team.

Glossary

- OT – Operational Technology
- HMI – Human/Machine Interface
- IED – Intelligent Electronic Device
- MFA – Multi-factor Authentication
- IAM – Identity & Access Management
- PAM – Privileged Access Management
- IR – Incident Management
- DMZ – De-Militarised Zone
- ICS – Industrial Control System
- VM – Vulnerability Management
- SIEM – Security Incident & Event Management tool

5. Evolving requirements for Managed Security Services

A significant shift in expectations of managed security service providers

At PwC we have seen a change in the needs of the power sector related to managed services. As cybersecurity, safety, reliability and data trust become increasingly intertwined, more mature power sector organisations are shifting from traditional 1.0 monitoring services, to a more advanced and integrated approach to managed security services.

Challenges that are being identified and addressed	Managed Security Services (MSS) 2.0
In-house security monitoring services that are hard-to-find, train and retain.	In-house SOCs are being moved to shared or outsourced managed security service models. Well-designed Service Level Agreements (SLAs) transfer the responsibility of service continuity and training to the security service providers.
Changing threat landscape requires a continuously evolving threat management program	2020 saw the attacks getting more sophisticated and this trend is likely to continue further. This requires a dynamic and continuous threat modelling and threat management capability.
Lack of insights in the traditional outsourced 1.0 'eyes on glass' monitoring	2021 will see a significant increase in MSS Request For Proposals (RFPs) for the power sector. Traditionally, MSS companies simply send alerts back to power companies to manage. Low context services that rely on technical routine, rather than intuitive analysis without providing meaningful insights. 1.0 providers are being replaced with new breeds of MSS companies that provide improved visibility of threats as well as insights that enable power companies to better make decisions.
Siloed or disparate managed services that are cumbersome to procure and do not effectively integrate.	A unified Cyber-as-a-Service (CaaS) capability that integrates security capabilities across IT and OT. These can include: System monitoring based upon ongoing threat intelligence, vulnerability assessments, intrusion detection, access management as-a-service, network security, endpoint detection and response, and incident response and remediation as examples. Sophisticated MSS providers will also offer a Lab environment in which to test attack scenarios and model proposed configurations
Lack of coverage in OT environments by Security Operations	A new breed of MSS provider that employs power sector OT specialists (engineering and operations) who configure passive and inline monitoring capabilities and work closely with internal OT teams to configure safely and provide custom OT monitoring capabilities.

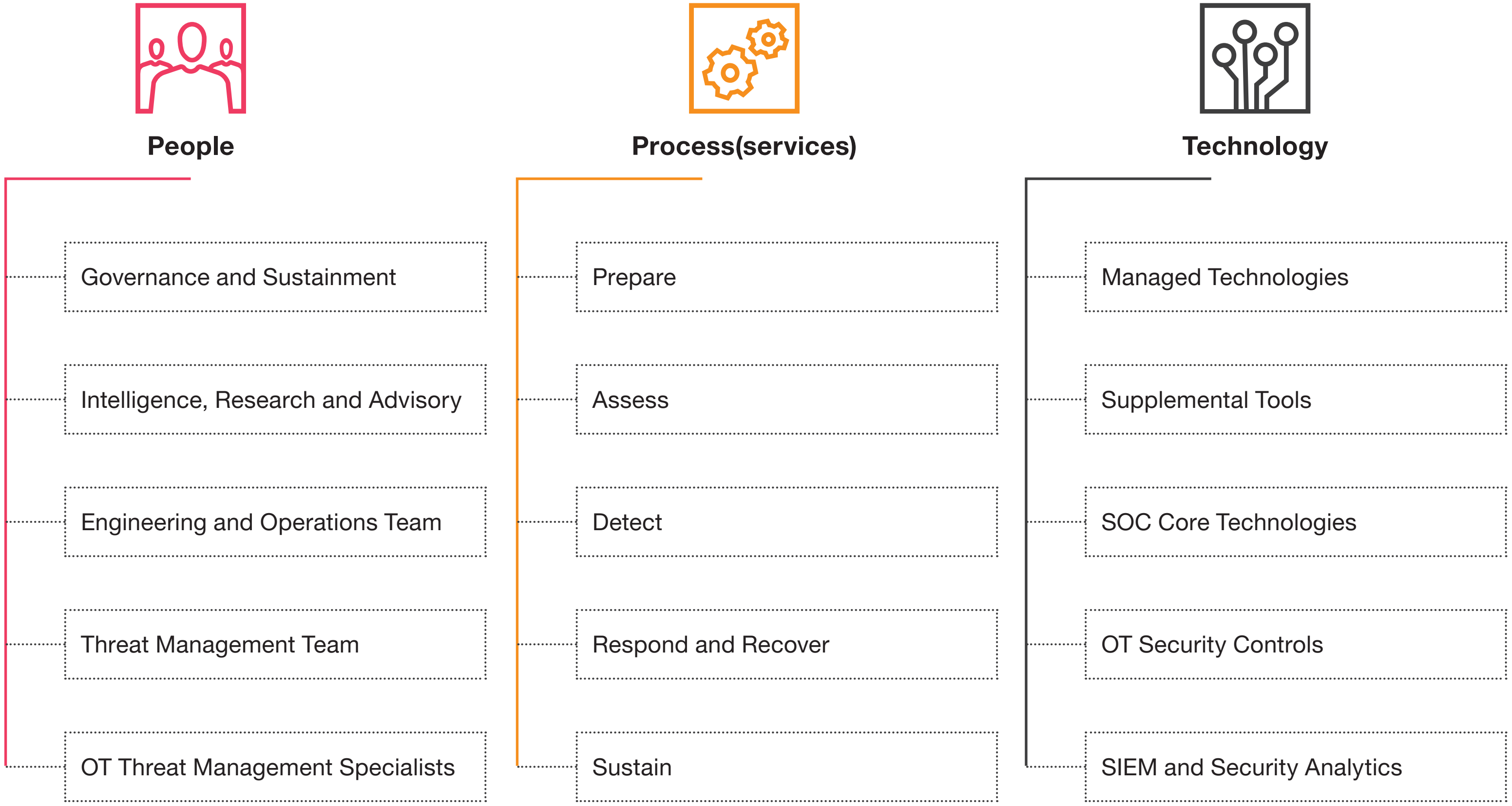
5. Managed Security Services 2.0 – Where it’s heading in 2021

The advanced security monitoring (detection and response) is a merger of capabilities across people, process and technology:

To assist with the design of a next-generation MSS, the graphic to the right lays out important components for People, Process and technologies included in an integrated MSS offering.

The important outcomes from this model include:

- An properly integrated MSS model where the left and right hands communicate effectively.
- Visibility on the range of unique skill-sets required to deliver these custom services.
- A single-architecture view of the technologies required, and an integration model for data flows between them.

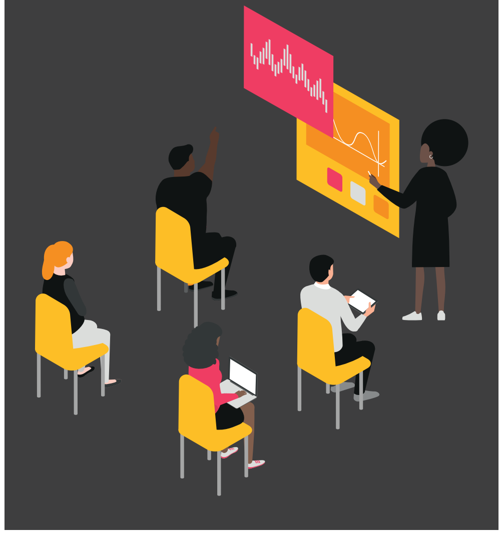


People	Process(services)	Technology
Governance and Sustainment	Prepare	Managed Technologies
Intelligence, Research and Advisory	Assess	Supplemental Tools
Engineering and Operations Team	Detect	SOC Core Technologies
Threat Management Team	Respond and Recover	OT Security Controls
OT Threat Management Specialists	Sustain	SIEM and Security Analytics

5. Advanced Security Monitoring & Managed Services 2.0

Advanced security monitoring and managed services are driven by insights led capability that would help executives make necessary decisions. These should be driven by:

PwC's OT Lab in Canada for innovation, system testing and training of OT client teams. Similar PwC labs exist in Israel and the United States.



Advanced capabilities

- Integrated security operations capability (IT/OT/Physical).
- Automation and analytics built into investigation and response.
- Advanced OT sensory capability deployed.
- Leading practices, knowledge capital, tools in the field of analytics, threat intelligence, IR.

Innovation to keep pace with emerging threats

- Constant IT and OT research and development (R&D) and threat modelling.
- Advanced cyber threat intelligence for Power Sector.
- 3rd party risk measurement for containing and remediating third party threats to the organisation.

Power industry knowledge and expertise

- You will require resources that bring an in depth experience and knowledge of power industry and threat landscape.
- Expertise to be able committed to a continued growing relationship with you.

5. MSS 2.0: MSS/MDR – A Technical Perspective*

MSS/MDR technical trends

Managed Security Services (MSS) are **40% process, 30% people and 30% technology.** Engaging an Managed Security Service Providers (MSSP) will require the right internal staffing levels and additional processes to account for the security operations and life cycle.

Over 80% of alerts generated by SIEM solutions are false positives. The key to high fidelity is feeding **organisational context** into security operations. Example user and entity profiles and behaviour.

Technical security operations staff will continue to be **hard to hire, train and retain.** Thus creating pressure on MSS 1.0 vendors and providers who focus on non-automated processes for detection and response.

MSS/MDR technology leading practices

XDR or e**X**tended **D**etection and **R**esponse has become a key requirement for gaining visibility in security operations.

Security Automation and Response are being built in many SIEM products out of the box and will also be necessary to drive automation and efficiency in security operations. MSS 2.0 vendors will offer this capability as **de-facto in their offerings**.

Managed Services 2.0 vendors are employing **threat hunting techniques as a base level service**, which is powered by XDR solutions and drives immense value in threat detection and response.

MSS/MDR technical challenges

Threat coverage will be driven by **threat vertical coverage** such as insider threats, cyber safety threats etc. Powering these capabilities will require MSS vendors to have a strategic focus as well as deep industry based technical focus.

Threat intelligence is evolving to be more **threat actor driven and strategic**, vs. only focusing on feeds and speeds. Tracking and receiving accurate threat intelligence will be one of the key factors to successful security operations.

Prioritising the high value assets, users and activities to log and monitor will be key and Security Operations will struggle to mature without a well maintained Configuration Management DataBase (CMDB).

Allow us to show you PwC's cybersecurity and privacy capabilities

PwC's cybersecurity and privacy capabilities

Our long standing power sector clients tell us...

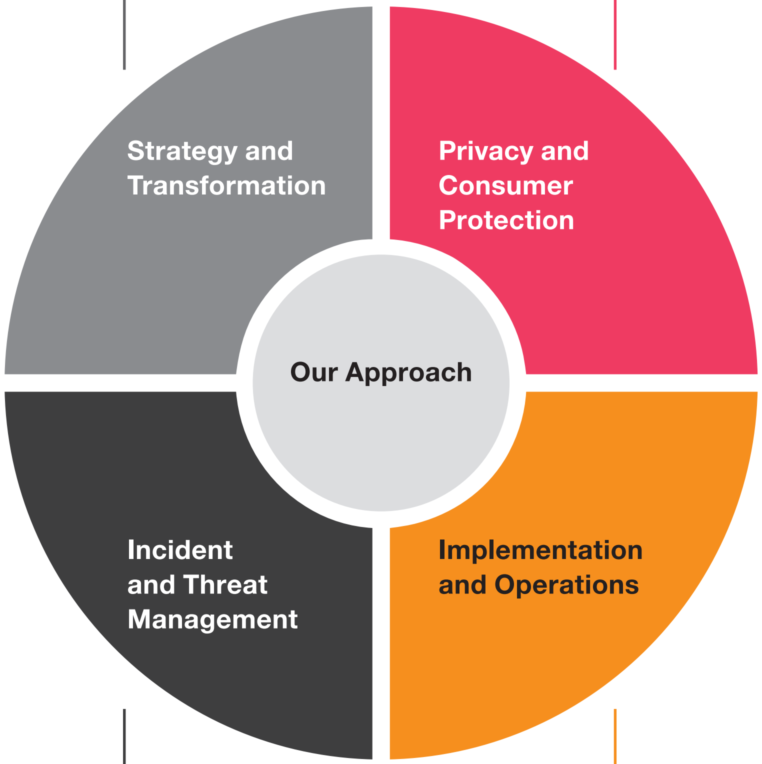
1 **PwC has a very deep technical bench (80% of our team are technical subject matter specialists), and we know power companies.**

2 **PwC knows OT. We have specialists who have built OT security systems.**

3 **PwC invests the time to know our client's needs. That's why so many of our client relationships go back 5-10 years.**

Strategy and Transformation: Growth through secure digital transformation

Develop business-focused strategies and programs that support growth and agility by making cybersecurity and privacy an enterprise-wide priority.


Strategy and Transformation
Privacy and Consumer Protection
Our Approach
Incident and Threat Management
Implementation and Operations

Privacy and Consumer Protection: Use data with confidence to create value

Design, implement and operate a privacy program that enables organisations to monetise data with confidence while promoting trust with consumers and regulators.

Incident and Threat Management: Manage impact to the business from emerging threats

Confidently prepare, identify, respond, investigate and remediate threats.

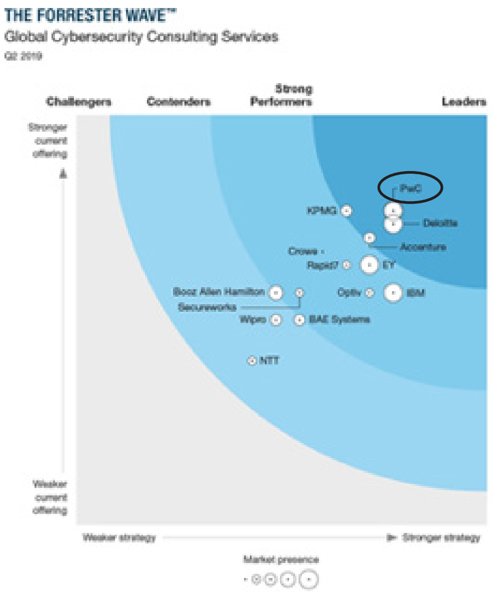
Implementation and Operations: Maximise return from cybersecurity technology investments

Design, implement, operate and enhance the use of cybersecurity technologies.

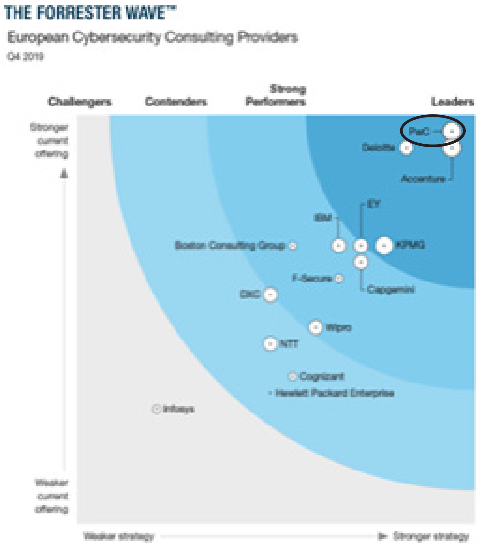
PwC's cybersecurity and privacy capabilities

Global cybersecurity and privacy leader with 4,000+ practitioners

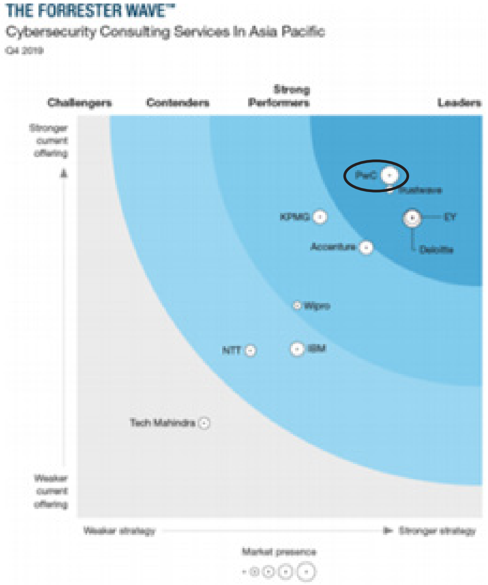
First firm to receive these three prestigious awards from Forrester Research:



Q2 2019
Global Cybersecurity Consulting
Forrester Research



Q4 2019
European Cybersecurity Consulting Providers
Forrester Research



Q4 2019
Cybersecurity Consulting Asia Pacific
Forrester Research

Analyst evaluations extending to our clients' broader digital risk management agenda.

2020 Leader
IDC Marketscape Worldwide Risk Consulting Services

2020 Leader
Gartner Magic Quadrant for Data and Analytics Service Providers

2019 Leader
ALM Vanguard of Strategic Risk Management Consulting Providers

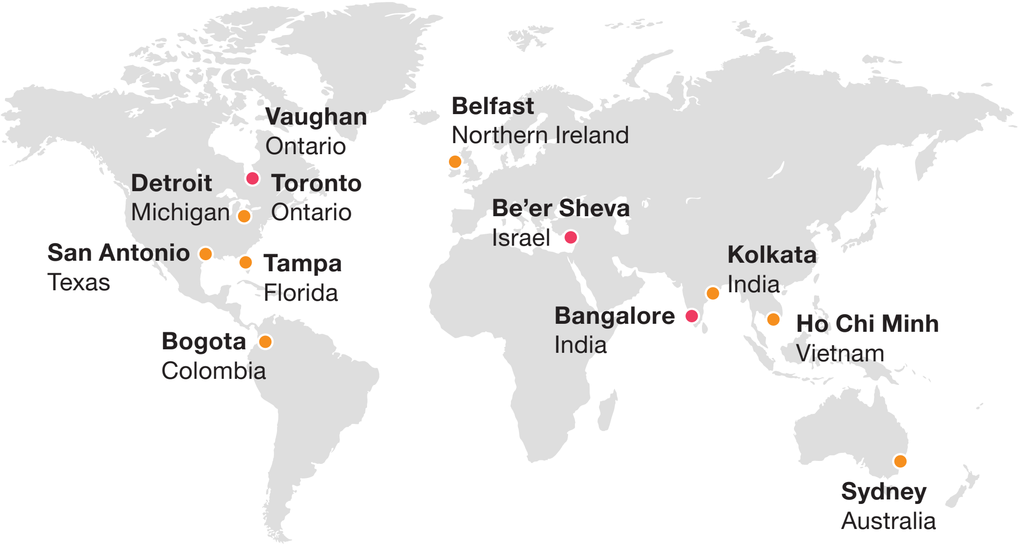
2017 Leader
Forrester Wave: Digital Forensics and Incident Response

Recognised for strong relationships, innovative intellectual property /products, diverse thought leadership, global reach with local presence and client value.

PwC's cybersecurity and privacy capabilities

PwC's global network of cyber and privacy operations centers

PwC has a global network of interconnected Security and Privacy Digital Resilience Centers (DRCs) and three Global innovation hubs for OT Security and Integrated SOC for IT and OT security monitoring. These centers are an integral part of our Global Innovation Hub for OT Security and IT/OT Security Monitoring.



● **Global innovation hubs for OT Security with Integrated SOC capability**

Innovate: We bring together power sector security teams and their relevant business units, to identify emerging security threats.

The Digital Resilience Innovation Centre is a creative space where we work with you hand in hand to ideate and co-create solutions for your digital trust and resilience challenges. You'll explore bold-play strategies through multiple lenses together with our specialists in cybersecurity, industrial systems, Internet of Things (IoT), emerging technologies, data and analytics, privacy, forensics, crisis management and human-centric design.

Experience: Cybersecurity in the power sector is hands-on. We test PwC proprietary and vendor partner solutions in a collaborative environment that mirrors our client's digital systems.

The Digital Resilience Sandbox is an immersive space where you can see, touch and experience the latest technologies, such as industrial systems, robotics, IoT, artificial intelligence (AI), 5G, cloud and mixed reality, and simulate offensive and defensive tactics on them. This will allow you to truly experience what an adverse event on your digital ecosystem would look like and test various methods to prevent, detect and react to these threats.

Operate: We provide next generation IT & OT managed services to the power sector. Our approach is a significant departure from traditional providers.

The Digital Resilience Operations Centre is a space where we can support you 24/7 as your organisation puts new solutions into operation. You'll benefit from our depth of expertise and global scale to operate your cybersecurity and privacy defenses through the entire life cycle. We can scale to sustain and mature your capabilities as your needs evolve.

PwC’s cybersecurity and privacy capabilities

PwC’s Cyber-as-a-Service (CaaS) Overview was built to fill a gap in the market

As mentioned on page 36, the power sector is struggling with traditional outsourced 1.0 ‘eyes on glass’ monitoring. We realised several years ago that the sector needed a more comprehensive service catalogue, custom solutions, and mature processes to support them.

Prepare

- Cyber strategy and development
- Cyber organisational readiness, stakeholder preparation and governance
- Cyber general controls transformation
- Cyber standards and regulatory transformation
- Cyber third party assurance
- Cyber cloud security strategy
- Policies and standards
- Security architecture and design services
- Cyber governance, risk and controls (GRC) as a service
- Cyber risk management and reporting
- Security awareness
- Cyber threat modelling and business impact as a service
- Security architecture as a service
- SDLC – Software Development Life Cycle

Assess

- Cybersecurity maturity and general control assessment
- Cybersecurity risk assessment
- Cybersecurity architecture assessment
- Penetration testing and ethical hacking
- Red and Purple teaming program
- Source Code Review
- Incident response/cyber operational effectiveness/run assessment
- Cyber kill chain and breach readiness assessment (proactive)
- Cyber kill chain and breach indicator assessment (compromise assessment)
- Attack surface determination (vulnerability assessment and testing)
- Vulnerability management for IT and OT environments
- Cyber simulation and war-gaming as a service
- Cyber attack surface reduction as a service (application security, APT testing, TVM etc.)
- Application testing, static and dynamic code reviews
- IAM Assessment and Strategy
- Role Based Access Controls
- Cyber threat modelling

Sense

- Cyber threat intelligence as a service
- Targeted intelligence, cyber surveillance, etc.
- Security fusion and intelligence
- Client-focused real-time threat content
- Human and corporate intelligence
- Actor attribution and threat tracking
- Cyber brand threat detection as a service
- Malware simulations and content
- Malware analysis and reverse engineering
- Crypto-analysis
- Private sandbox as a service
- Attack simulation as a service

Detect

- Cyber monitoring as a service
- Integrated OT security monitoring
- Use case based monitoring
- Log reviews and cyber hunting
- Advanced security analysis
- Policy, compliance and executive reporting
- Investigations and case management
- Computer Security Incident Response Team (CSIRT) front end
- Operational reporting
- Security reporting
- Cyber hunting
- Cyber analytics and data lake analysis as a service
- Traffic visibility with intel
- Data Discovery Scanning
- Data Loss Prevention (DLP)

Defend

- Managed and monitored VPN/firewall service
- Intrusion prevention and detection services (IPD)
- Managed/hosted web /URL filtering/proxy/ email
- Cloud security services
- Privacy and consumer protection
- DDoS protection
- Micro-segmentation
- Zero-Trust
- Mobile security
- Network Isolation
- Network access control (NAC)
- Application/database security
- Host/ network malware protection
- Authentication (SSO/MFA)
- Identity Governance
- Privilege Access Management
- Customer and Digital Identity
- IAM (IGA/PAM/AuthN) as a service
- Encryption/ Tokenisation /Anonymisation
- Managed Fraud solution
- Managed AML

Respond

- Advanced threat preparedness
- Digital forensic investigation
- Incident handling and management
- Tabletop exercises
- Targeted threat response
- Breach response
- Eradication and recovery
- Postmortem analysis
- Litigation support
- Incident response retainer

Check

- Security performance management and metrics
- Security governance and quality assurance
- Risk and regulatory management
- Compliance management
- Cyber operations certification
- Cyber audits

PwC’s cybersecurity and privacy capabilities

Richard Wilson

Partner, Cybersecurity and Privacy
Energy, Utilities and Resources –
Americas

E: richard.m.wilson@pwc.com

LinkedIn:
www.linkedin.com/in/richardwilson

PwC Canada

Bram van Tiel

Partner, Cybersecurity and Privacy
Energy, Utilities and Resources
– EMEA

E: bram.van.tiel@pwc.com

LinkedIn:
www.linkedin.com/in/bramvantiel

PwC Netherlands

Jason Knott

Partner, Cybersecurity and Privacy
Energy, Utilities and Resources –
AsiaPAC

E: jason.knott@pwc.com

LinkedIn:
www.linkedin.com/in/knottjason

PwC Australia

Jeroen van Hoof

Global Energy, Utilities and
Resources Leader
Global Power and Utilities Leader

E: jeroen.van.hoof@pwc.com

LinkedIn:
www.linkedin.com/in/jeroenvhoof

PwC Netherlands

PwC’s Cybersecurity and Privacy team delivers a full suite of services from strategy and transformation, to deep technical implementations, privacy, forensics, and a full suite of managed security services.

Notes

This is a proposal document and does not constitute a contract of engagement with PricewaterhouseCoopers LLP. The information set out in it is an indication of the terms on which we propose to carry out PwC power sector cybersecurity trends and insights for 2021 for you but the proposal is subject to the terms of any subsequent engagement contract that may be entered into between us. In the event that our proposal to you is successful, our acceptance of the engagement will be contingent upon the completion of all our internal engagement acceptance procedures. All information contained in this proposal document or otherwise provided or made available as part of our proposal is confidential and may not be disclosed to anyone else without our prior consent.

2021-03-31_RITM4978771