Managing Technology Risks in the Public Sector and Regulated Industries

A Risk-Based Assessment Approach

COALITION FOR CYBERSECURITY IN ASIA-PACIFIC

Contents

Executive Summary

Today's economies shift towards digitalisation has made secure, sustainable, and resilient digital deployment a necessity. As the world digitalises, technology risk management has become a more important question for all organisations and stakeholders. This is particularly true for public sector entities and regulated industries that may have unique security requirements based on the type of data and systems they operate at scale. This report first seeks to answer common questions that policymakers have in managing technology risks in the public sector and regulated industries. These questions include how to consider Reliability, Trust and Accountability, Third-Party Risks, Resource Constraints, Data Security and Access, and more.

This report categorises policymaker concerns broadly into two primary categories, namely, risks stemming from:

1. New technologies for adoption, and
2. Existing technologies present in current systems.

In these categories, the current concerns for policymakers may revolve around two main issues: cloud computing adoption and supply chain management. The report takes a deep dive into these two issues, beginning with a primer on cloud computing, clarifying some misconceptions that may exist relating to cloud computing cybersecurity. For supply chain management, the report offers recommendations for policymakers to help bolster the resilience and security of technologies against threats arising from the technology supply chain.

The findings of the report across key concerns and best practices, cloud adoption, and supply chain management are summarised here.

Cybersecurity Concerns of Policymakers

Reliability

How to know if the technology product or system is consistently secure?

Look for products and services that comply with internationally recognised best practices, standards, and certifications. Note that:

- Cybersecurity must be tailored to the risks faced by the organisation.
- The product or service should be supported throughout its lifecycle.

Trust and Accountability

Whose technology / products / services to trust?

Trust vendors that adopt zero-trust and security-by-design approaches. Leverage mechanisms to articulate components and relevant certifications, and use cybersecurity audits or other verifiable processes that demonstrate the vendor's cybersecurity measures.

Third-Party Risks

Should outsourcing be allowed?

Yes, as third-party risks can be managed. Organisations should outsource when a third party can do a better and more efficient job. Qualified third parties can provide more proficient protection and risk management than in-house operations that may have limited expertise and resources. Outsource to credible and proficient third parties, credentialed through adherence to international standards, certifications, and incorporated in contracting requirements.

Resource Constraints

With little resources allocated to cybersecurity, where can my resources be best used?

Outsourcing helps to shift resourcing from a capital expenditure (CapEx) to an operational expenditure (OpEx) model (a shift from upfront costs to usage costs distributed over time), which can help maximise scarce resources. Also, cybersecurity can be enhanced by outsourcing IT services to vendors with better built-in cybersecurity expertise and track records.

Data Security

How to ensure that data is secure?

Leverage internationally recognised certifications and implementation of cybersecurity best practices to help select a vendor that:

- Implements data security according to the data's importance and risks
- Establishes governance mechanisms such as threat intelligence sharing networks to help strengthen cybersecurity.

Data Access

What measures should be established to ensure that authorities have legitimate access to data?

Data access can be administered through the management of encryption keys, appropriate pathways, and legal requirements for requests.

- Ensure that data owners can manage and access their own encryption keys.
- Request data from customers and not cloud service providers (CSPs).
- Establish legal mechanisms, due process, and advance notice for data access.

Important Systems

Which systems should be regulated more closely?

Prioritise "critical" systems based on impact of a security breach, and:

- Use a tiered system to align level of security or regulation with the importance of a system.
- Avoid prescriptive cybersecurity requirements to enable organisations to adopt the tools they need.
- Establish cybersecurity responsibilities for important systems using outcomes-focused, baseline cybersecurity recommendations.

Local Regulations

Should domestic cybersecurity standards or requirements be created based on geographic boundaries?

Consider carefully any localised, domestic requirements, as:

- Over-prescriptive cybersecurity regulations and regulations that deviate from international standards may create more cyber risks instead.
- Policymakers should draft guidelines that align with international best practices to foster cross-border trade in goods and services, among other benefits.
- Policymakers should ensure that entities in their markets have access to best-in-class cybersecurity products and services, and that innovators from their own markets can sell into the global market.

Large-Scale Incidents

How to address "black swan" events?

Be prepared in advance. Important IT systems should be built with resilience, service continuity, and response and recovery implementations.

Deep Dive 1

The first deep dive seeks to help policymakers manage **the risks associated with the adoption of cloud computing** by clarifying some common misconceptions. Cloud adoption has been increasingly popular and many governments in Asia are considering how cloud computing technologies can help digitalisation efforts. This section helps policymakers optimise cloud computing adoption for a secure and resilient digital economy.

Cloud Policy Misconceptions and Clarifying Considerations

1. "To enhance cybersecurity, a hybrid cloud model should be adopted for all cloud migrations."

   ...Cloud deployment models should be based on organisational needs and capabilities. ✓

2. "All cloud systems should be classified as Critical Information Infrastructures (CIIs)."

   ...Cloud computing is used across a broad variety of organisations and needs flexibility for deployment. ✓

3. "Prescriptive and specific cybersecurity requirements are needed to ensure protection."

   ...Outcome-focused and risk-based approaches enable optimisation of cybersecurity. ✓

4. "Data is safer when it is kept locally"; "using local CSPs and cloud technology suppliers is safer."

   ..."Localisation" does not provide cybersecurity. ✓

5. "Physical audits must be conducted even after migration to cloud."

   ...Physical audits should shift to logical audits. ✓

6. "Strict regulations on CSPs regarding the provision of requested data is necessary to safeguard data sovereignty."

   ...Data protection responsibility is shared between the CSP and the customer. ✓

7. "Jurisdictions must develop their own local cloud security standards and certification."

   ...More effective to align with international security standards. ✓

8. "CSPs should be required to regularly report their cybersecurity threats and events to government"

   ...Reporting should not be onerous and should be mandatory only for serious cyber incidents. ✓

9. "Subcontracting reduces security"

   ...Subcontracting can be effectively managed with clearly defined responsibilities. ✓

Deep Dive 2

The second deep dive is on **managing the cybersecurity of technology supply chains**. Policymakers are concerned with the increasing scale and prevalence of cyberattacks that exploit vulnerabilities in the technology supply chain. This deep dive explores protecting the public sector and regulated industries from supply chain cyberattacks and makes four recommendations for policymakers.

Recommendations

1. Encourage the adoption of **targeted risk management guidelines and principles**.
2. Develop or adopt **cybersecurity procedures** to assess industry supply chain partners.
3. Develop and incentivise **information-sharing mechanisms** and uphold standards of **transparency** across supply chains.
4. Work with relevant industry actors to ensure that **solutions are fit-for-purpose** and **appropriate to threat profiles** within and across supply chains.

Digitalising the Public Sector and Regulated Industries

The coronavirus disease (COVID-19) has accelerated digitalisation across all sectors of the economy as society has been forced to adapt to the need to limit physical interactions and minimise transmissions of the virus. In particular, for businesses and the public sector, the pandemic has shifted perceptions of digitalisation from a value-add to a necessity, where this digital acceleration is expected to continue even after the pandemic.[1] The world is embracing hybrid work where jobs, education, government services, entertainment, and social engagements leverage digital services more than ever. The pandemic has shown that remote work and collaboration is possible and effective and, as such, the continued use of hybrid work models is expected and would allow broader reach for those who cannot participate in person. In light of this growing reliance on digital technologies, it is critical to ensure that such technologies are deployed securely, not just for the present, but for a sustainable and resilient digital future.

To help manage technology risks and guide technology adoption in the public sector and in regulated industries, this report serves to inform policymakers by considering key concerns and highlighting best practices. The report focuses on two, top-of-mind concerns for policymakers when managing technology risks in the public sector and regulated industries—how to understand and manage the risks in cloud computing adoption and in the technology supply chain.

1 OECD (2020), Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, https://www.oecd.org/digital/digital-economy-outlook-covid.pdf
2 Anna Bjerde and Asli Demirguc-Kunt (2021) Digitalization and data can vastly improve public service delivery for citizens, https://blogs.worldbank.org/europeandcentralasia/digitalization-and-data-can-vastly-improve-public-service-delivery-citizens
3 Computer Weekly (n.d.), Essential Guide: Digital transformation in the public sector, https://www.computerweekly.com/essentialguide/Essential-Guide-Digital-transformation-in-the-public-sector
4 Joel Nichols (2019), Digital Transformation for Regulated Industries: Ask the Right Questions, https://www.cutter.com/article/digital-transformation-regulated-industries-ask-right-questions-504466
5 Planning Department (2016), Hong Kong 2030+: A Smart, Green and Resilient City Strategy, https://www.hk2030plus.hk/document/Hong%20Kong%202030+%20A%20SGR%20City%20Strategy_Eng.pdf
6 Innovation and Technology Bureau (2020), Hong Kong Smart City Blueprint 2.0, https://www.smartcity.gov.hk/modules/custom/custom_global_js_css/assets/files/HKSmartCityBlueprint(ENG)v2.pdf

Why digitalise?

Governments all around the world are making better use of data to optimise management, service delivery, and national capacity to enhance public services to citizens.[2] So too are regulated industries for their customers. This integration and adoption of digital tools, i.e. digitalisation, is a cross-cutting trend touching all types of entities and sectors. The increased use of cloud services also derives cost savings from a reduced reliance on dedicated hardware that may not be fully utilised while also leveraging the experience and expertise of cloud providers in delivering better cybersecurity support.

Benefits of digital transformation

In the public sector[3]

Transforming citizen engagement
Enabling citizens to access public services digitally and conveniently despite restricted physical access.

Transforming the bureaucracy for efficiency
Empowering public servants to access information quicker, deliver services more efficiently, and improve coordination across agencies.

Transforming the delivery of services through data-driven innovation
Facilitating greater insights and innovation where data pools are shared and integrated across public services.

In regulated industries[4]

Improved services
Helping regulated industries meet their service goals, such as safety, transparency, and equality of access through digital tools.

Innovation
Enhancing innovation, competitiveness, R&D initiatives, and efficiency in the industry through the use of smart technologies and intelligent networking under digitalisation and Industry 4.0 plans.

Access
Transforming and bridging business-customer relationships and making services more accessible.

Case example

Smart city initiatives are an excellent example of plans to embrace digital transformation across the public sector and regulated industries. For example, "Hong Kong 2030+" outlines Hong Kong's plans to leverage technologies in its infrastructure, utilities, and governmental services, among others, to make Hong Kong into an efficient, sustainable, and resilient economy.[5]

Hong Kong's smart city initiative added billions of dollars in value to their four key industries in 2018—Trade and Logistics (USD 73.2 billion), Financial Services (USD 68.4 billion), Professional Services (USD 41.4 billion), and Tourism (USD 15.5 billion).[6]

To allow public services and regulated technologies to harness the benefits of digitalisation, governments need to ensure that a variety of technologies are available for public services and regulated industries to deploy according to their needs. Streamlining the procurement and adoption of digital technologies is important to enable digitalisation, representing one of the Organisation for Economic Co-operation and Development's (OECD) Principles for Digital Government Strategies.[7] These include the use of cloud computing services that are becoming increasingly popular, affordable, and resilient. Apart from being able to outsource certain IT functions to the cloud, governments also benefit from a network of suppliers for the provision of goods and services for day-to-day operations, such as cybersecurity management, software, or platform services.

The increasing use of cloud technologies for digitalisation, coupled with third-party IT goods and service providers in the supply chain, have heightened the need to better and more comprehensively manage the associated risks.

Creating an "Enabling" Technology Risk Management Framework

Governmental frameworks can help provide regulatory clarity on the requirements to manage these risks. However, outdated or ill-informed policies may be overly restrictive or place high compliance burdens on companies and stifle digitalisation.[8] It is thus important to create frameworks and guidelines that enable technology adoption and innovation while supporting the need to manage the risks. A good way to optimise these policies is to develop these frameworks in consultation with industry and experts.

Effective digitalisation and risk management frameworks for the public sector serve as an example for the private sector to emulate. The convenience and greater accessibility of digital public services to citizens, and the secure manner in which such services are delivered, help to build confidence and familiarity in the use of digital technologies across other sectors. In turn, digitalisation helps facilitate greater productivity that can be delivered to the economy in a time of struggling growth, especially for post-pandemic economic recovery.[9]

Conversely, public trust in digital technologies can be eroded if the government or regulated industries suffer massive data breaches, have poor data handling practices, or adopt ill-formed policies that do not result in the intended purpose or effect.

Operational technology (OT) cybersecurity is also of high importance to governments due to its use in critical infrastructure and regulated industries.[10] Cyberattacks on OT can cause severe disruption to critical services and even endanger human lives. In February 2021, hackers remotely accessed the U.S. state of Florida's water treatment facility and attempted to poison the city's water supply.[11] This case highlights the need to manage all technology risks in the public sector, even technologies that are not traditionally considered as information technology (IT), to ensure that the deployment of digital capabilities is safe and resilient against disruptions and cyberattacks.[12]

7 OECD (2014), OECD Digital Government Toolkit, https://www.oecd.org/governance/digital-government/toolkit/principle11/
8 Carmelo Cennamo and D. Daniel Sokol (2021), Can the EU Regulate Platforms Without Stifling Innovation?, https://hbr.org/2021/03/can-the-eu-regulate-platforms-without-stifling-innovation
9 Landry Signe and Stephen Almond (2021), A blueprint for technology governance in the post-pandemic world, https://www.brookings.edu/research/a-blueprint-for-technology-governance-in-the-post-pandemic-world/
10 OT refers to the hardware and software platforms that interact with the physical environment, such as valve control systems in utilities or proximity detection capabilities on railway lines.
11 Peter Fretty (2021), Water Supply Cyber Breach Thwarted, https://www.industryweek.com/technology-and-iiot/article/21154622/water-supply-cyber-breach-thwarted
12 A step-by-step checklist for policymakers to protect OT from cyberattacks is available online at https://www.accesspartnership.com/cms/wp-content/uploads/2020/10/CCAPAC-Cybersecurity-for-Operational-Technologies-A-Guide-for-Governments-Digital-Report.pdf

Addressing Key Governmental Cybersecurity Concerns in the Public Sector and Regulated Industries

To help optimise risk management frameworks and promote technology-enabled efficiencies and innovation, the following is a compilation of key concerns that have been raised by the governments and businesses when navigating the process of adopting technologies. In addressing specific concerns, the improved understanding provides a baseline to encourage greater utilisation of digital technologies within the public sector and regulated industries.

Reliability

How to know if the technology product or service is consistently secure?

- Governments should use products and services that meet internationally recognised best practices, standards, and certifications. These widely adopted and vetted practices provide an indication of the level of security present in the product or service. For example, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27000 series standards for information security management may be employed to ensure reliability.[13]
- Effective cybersecurity is a risk-based activity that relies on a clear understanding of an organisation's risks, priorities, and business model balanced with its capabilities – resources, skills, and willingness to invest. It leverages security in products and services, coupled with people and process dimensions, adopting security mechanisms according to the needs and risks faced by the organisation.[14]
- Choose vendors that have processes in place to securely develop and support products throughout their lifecycle. They have a clear process to address and rectify vulnerabilities in a timely manner. Identify and prioritise vendors with these types of processes.

13 International best practices include: ISO/IEC 27001, ISO 27017, ISO/IEC 27032

14 NIST (2018), Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Trust and Accountability

Whose technology / products / services to trust?

- Adopt a zero-trust approach—that is, no component in the system should be trusted by default and that everything should be continuously verified.[15] The zero-trust approach requires every access request to be validated and all applications and network infrastructure to be secured.
- Institute mechanisms to determine what is in a product so that an informed dialogue with the vendor is possible on what security alerts and threat mitigations would be relevant to the technology acquired. For example, a software bill of materials (SBOM) from vendors can illuminate the components of the system and level of cybersecurity protections in the product. Encouraging publication of machine-readable information from vendors regarding the characteristics of the products in a standards compliant manner can also promote awareness about the cybersecurity level of a product.
- Vendors should be encouraged to adopt a security-by-default approach where the highest appropriate level of security and protection is adopted, including ensuring that security is preconfigured into the design of product, functionalities, processes, technologies, operations, architectures, and business models.
- Vendors should also be able to continuously demonstrate accountability, trustworthiness, and transparency. Where additional attention on the cybersecurity of a product is needed, a cybersecurity audit or other verifiable processes can be conducted on the product or service and the vendor's internal security practices before it is used and on a regular basis (e.g., once in three years).[16] Such audits should ensure that the product vendor's intellectual property will be protected whilst performing the audit. The audit should demonstrate the vendor's continuing commitment to security and take into account the latest technological approaches to security evaluation and monitoring.[17]
- Other factors that could provide insight into a vendor's cybersecurity practices are:
  - The vendor's own enterprise security;
  - The vendor's secure development lifecycle;
  - The vendor's supply chain security;
  - The vendor's product security vulnerability management program;
  - The vendor's adoption of tamper-resistant technologies.

Third-Party Risks

Should outsourcing be allowed?

- Organisations should outsource when the third party can do a better and more efficient job than themselves. Qualified third parties can provide more proficient protection and risk management than in-house operations that may have limited expertise and resources.
- Outsourcing can be less risky when using credible and proficient third parties. These third parties may have more expertise and experience in managing risks, invest heavily in security and have greater visibility to threats, regionally and globally.[18]
- Risks associated with outsourcing services, such as in cloud computing, can be readily managed.[19] This is explored further in the deep dive on cloud computing.

Resource Constraints

With little resources allocated to cybersecurity, where can my resources be best used?

- A good way to manage scarce resources is to allow outsourcing of IT services where possible. Outsourcing changes the billing structure from a CapEx to an OpEx model, which means that instead of upfront costs, costs can be based on the usage of computing resources and distributed over time.[20] This also helps resource-constrained entities avoid the high start-up costs in buying and maintaining IT infrastructure and pay for IT services only as they consume them. It also allows them to take advantage of lower costs and potentially better resourced security capabilities benefiting from the economies of scale realised by large CSPs. Additionally, outsourcing helps avoid the hidden costs in maintaining technologies, which may incur a security deficit that grows over time.

15 Cisco (n.d.), Cisco Zero Trust Security, https://www.cisco.com/c/en_sg/products/security/zero-trust.html
16 Solarwinds (2020), What is an IT Security Audit?, https://www.dnsstuff.com/it-security-audit
17 Other factors that could provide insight into a vendor's cybersecurity practices are: the vendor's own enterprise security; vendor's secure development lifecycle; vendor's supply chain security; vendor's product security vulnerability management program; vendor's adoption of tamper-resistant technologies.
18 AWS (n.d.), AWS Cloud Security, https://aws.amazon.com/security/
19 VMware (2020), Response To OSPAR (Outsourced Service Provider Audit Report) ABS (Association of Banks) Guidelines, https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/vmc-aws/vmware-response-to-ospar-vmware-cloud-on-aws.pdf
20 Lucy Wright (n.d.), What's driving the trend for IT outsourcing?, https://www.core.co.uk/blog/blog/driving-trend-it-outsourcing

Data Security

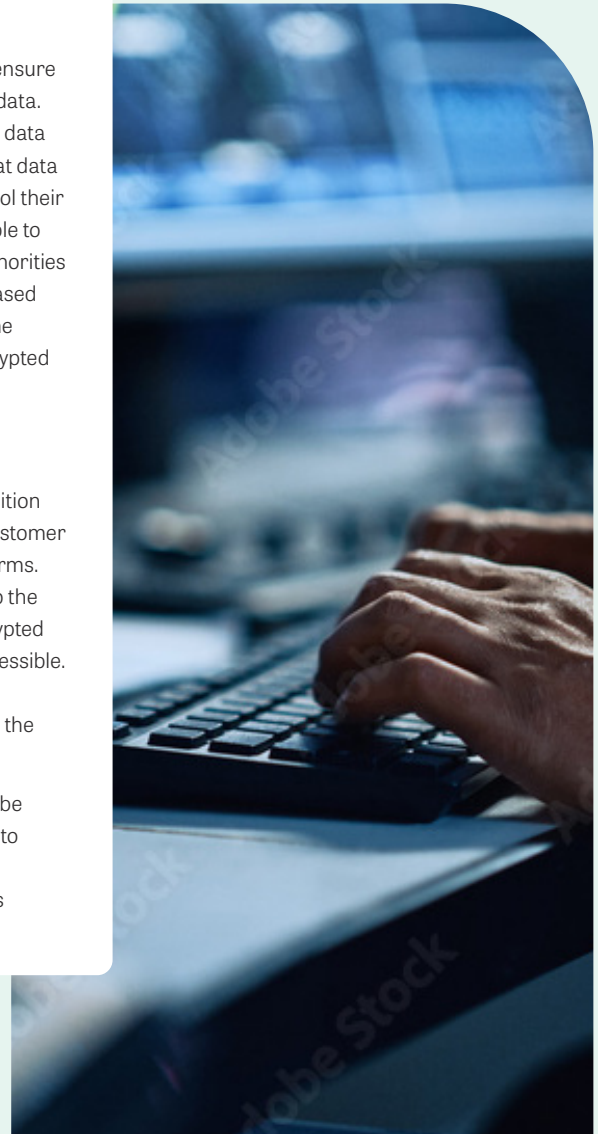
How to ensure that data is secure?

- When using cloud services, there is a division of security responsibility between the customer and the CSP. There is a need for a customer to clearly understand what it remains responsible for from a security perspective. It is important to understand how this responsibility is shared per the "shared responsibility model" explored further in the deep dive on cloud computing.
- When outsourcing IT services, ensure that the vendor is compliant with widely adopted, internationally recognised certifications and cybersecurity best practices.
- Not all data is equal—Data can be classified into several tiers, depending on its importance and potential for harm if lost. The level of cybersecurity protection should correspond with the level of importance of the data.[21]
- Government mechanisms help strengthen cybersecurity nationally. This includes establishing third-party threat intelligence sharing networks (to disseminate threat information and advisories locally and across borders), establishing a local coordinating entity for cybersecurity (Computer Emergency Response Team—CERTs),[22] and collaborating and establishing channels of communications between enterprises, regulated industries, and the government.[23]

Data Access

What measures should be established to ensure that authorities have legitimate access to data?

- Regulating to keep data in country is not required to ensure jurisdictional control over data. One effective alternative to data localisation is to ensure that data owners manage and control their encryption keys and are able to provide data access to authorities with legitimate requests based on due process. Without the encryption keys, such encrypted data will be inaccessible regardless of where they are stored.
- CSPs are often not in a position to provide access to the customer data hosted on their platforms. Even if data is accessible to the CSP, the data may be encrypted by the customer and inaccessible. Data access requests are more effective when put to the customers directly.
- Legal mechanisms should be established for authorities to access data for specific purposes with due process and advance notice.



21 NIST (2020), NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf

22 A primer and guide to CERTS is available at https://www.accesspartnership.com/access-partnerships-guide-to-computer-emergency-response-teams-certs/

23 The 9 Principles of the Paris Call (2018), https://pariscall.international/en/principles

Important Systems

Which systems should be regulated more closely?

- Prioritise critical systems based on a commensurate level of risk determined by analysis of the potential impact of a security event.[24]
- Instead of classifying entire sectors as critical and non-critical, a tiered system can be used commensurate with the level of security/regulation based on the importance of a particular system and its risks. Blanket designations can inappropriately apply high level security controls to low-risk systems and data. A clear process should be established and an agency should be designated to determine specific systems as Critical Information Infrastructure (CII).
- Even when systems are considered important, regulatory policies should avoid prescriptive cybersecurity requirements. The tools and methods used to achieve cybersecurity outcomes will vary because each organisation's risks, priorities, and systems are unique. Policies that recognise this provide companies with the flexibility to choose the appropriate approach to protect what is most important to their business and avoid shifting of resources away from securing assets to reporting and administrative requirements.[25]
- Regulations should, however, establish outcomes-focused, baseline cybersecurity requirements (also known as minimum or hygiene standards) and establish the responsibilities for important systems to implement specific cybersecurity mechanisms.[26]

Large-Scale Incidents

How to address "black swan" events?

- Large scale "black swan" events such as natural disasters can have widespread impacts for governments. Important IT systems should be built to ensure the resilience of data and systems, ability to maintain services through multiple outages, and the capability to respond to and recover from large scale events.

Local Regulations

Should domestic cybersecurity standards or requirements be created based on geographic boundaries?

- Requirements that are over-prescriptive or are developed without regard to international standards risk creating more security risks and increasing the cost of security by prescribing outdated, ineffective, or inefficient security controls. This inflexibility can unnecessarily limit business operations and significantly reduce companies' ability to respond to new threats and technologies.
- Instead of drafting a new standard independently, policymakers should prepare guidelines that follow international best practices, and align with global cybersecurity standards, to help businesses adapt to and understand the local risk landscape.[27]
- Using international standards help to reduce compliance costs and fosters cross-border trade in goods and services.[28] This also allows countries to tap into international investment in developing standards and developing training courses for implementing and overseeing them.
- Regulators leveraging and recognising compliance with existing international standards and certifications may save resources used in drafting and enforcing new policies.[28]

24 NIST Guidelines suggest designation of Critical Infrastructure as "Systems and assets, whether physical or virtual, so vital...that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters." More information is available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

25 Performance standards are requirements that state the results that should be achieved, and specifies the criteria for verifying compliance, while prescriptive standards specify the design and construction requirements and how a result should be achieved. More information is available at: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153

26 Financial Stability Board (2017), Summary Report on Financial Sector Cybersecurity Regulations Guidance and Supervisory Practices, https://www.fsb.org/wp-content/uploads/P131017-1.pdf

27 International best practices include: ISO/IEC 27001, ISO 27017, ISO/IEC 27032

28 Allan Friedman (2013), Cybersecurity and Trade: National Policies, Global and Local Consequences https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf

29 International best practices include: ISO/IEC 27001, ISO 27017, ISO/IEC 27032

Deep Dive 1

Managing Cloud Cybersecurity Risks

The use of cloud computing has been on an upwards trajectory even before the pandemic. The global cloud storage market grew in value from USD 30 billion in 2017 to USD 61 billion in 2020. With a forecasted Compound Annual Growth Rate (CAGR) of 26.2% for the 2021 to 2028 period, it is estimated to hit USD 390 billion by 2028.[30] By 2024, it is expected that cloud expenditure will rise to 40% of all overall IT spend from 27% in 2020 in the Asia Pacific, Japan, and China region.[31]

The understanding of the importance in managing cloud cybersecurity risks has grown in tandem with increasing cloud use in public sectors and regulated industries. This section of the report covers the fundamentals and benefits of cloud computing, highlighting the cybersecurity risks and considering some of the common policy misconceptions and recommended best practices around the use of cloud.

30 Fortune Business Insights (2021), Cloud Storage Market Size Regional Forecast, https://www.fortunebusinessinsights.com/cloud-storage-market-102773

31 BCG and Cisco (2021), The Future of Cloud in Asia Pacific, https://www.cisco.com/c/dam/global/en_sg/assets/pdfs/futureofcloud.pdf

32 Wayne Jansen and Timothy Grance (2011), Guidelines on Security and Privacy in Public Cloud Computing NIST Special Publication 800-144, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

What is Cloud Computing?

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[32]

Cloud computing represents a significant paradigm shift away from the traditional idea of organisations relying on their own data centres to an outsourced infrastructure that is better at facilitating cooperation and collaboration and also more efficient at allocating computing resources in a cost-effective manner. Today, cloud systems are a key part of any organisation's digitalisation and are used to offering a great variety of services including application services, data storage and management, computing resource management, web-based email services, consumer/citizen relationship management, and business intelligence systems.

Why Use the Cloud: The Benefits and Challenges

Benefits

Cloud adoption, which was already expanding rapidly before the COVID-19 pandemic, has accelerated with the onset of work-from-home and as a result of movement restrictions. In a 2021 study that surveyed 750 companies, 92% had a multi-cloud strategy and 90% expected cloud-use to exceed their plans due to the pandemic.[33] The benefits of using cloud include:

- **Increased Accessibility and Productivity** — The cloud allows users to access their data anywhere and at any time, facilitating remote-work and maximising enterprise productivity and efficiency by ensuring accessibility, even when on-the-go.
- **Enabling Collaboration —** The cloud facilitates easy sharing and collaboration amongst users across multiple locations. It also facilitates connections and data transfers across infrastructure, platforms, and tools from different vendors.
- **Cost Savings and Flexibility —** The cloud allows organisations to reduce their IT management costs in terms of both personnel and hardware. Pay-as-you-go services also provide more flexibility in managing IT costs.
- **Ease of Implementation & Scalability —** The cloud is easily scalable, allowing companies to add or subtract resources based on their needs so that their system scales easily with the demand.
- **Built-in Application Security —** Cloud services are developed with security in mind including built-in application security controls and embedding security features, wherever possible.
- **Software Currency —** CSPs can monitor, automate, and track software updates to ensure that the latest software versions are being used.
- **Data Recovery —** The cloud facilitates automatic data back-ups, making data recovery less time-consuming.

Challenges

The shift to cloud also requires users to be mindful of challenges it brings, which include:

- **Reliance on Internet Connectivity —** Public cloud systems require an Internet connection for access and some critics have highlighted that widespread Internet outages would affect operations. A different perspective on this is the flexibility that cloud provides to organisations. Users can work from *anywhere*, so long as they have an Internet connection. This is increasingly important in light of the COVID-19 pandemic and at the same time is increasingly less of a concern as digital infrastructure continues to improve around the world.[34]
- **Loss of Autonomy vs Shared Responsibility —** Another key concern is that cloud adoption leads to a loss of control and organisations are unable to handle serious issues entirely on their own. One of the key characteristics of the cloud is the shared model of responsibility where CSPs and customers work closely together to ensure security and reliability.
- **Need for Expertise —** Another challenge is the need for in-house cloud-related expertise. In a study done by the Cloud Security Alliance on organisations' top cloud security concerns, "staff lack cloud expertise" was the second most frequently selected response.[35] Cloud adoption allows organisations to focus their IT team on other tasks as they are no longer needed to perform administrative and routine tasks like updating software and installing patches. In the same survey done by the Cloud Security Alliance, 55% of enterprises were providing industry training and certification for staff and 53% were getting customer training from vendors to close this expertise gap.

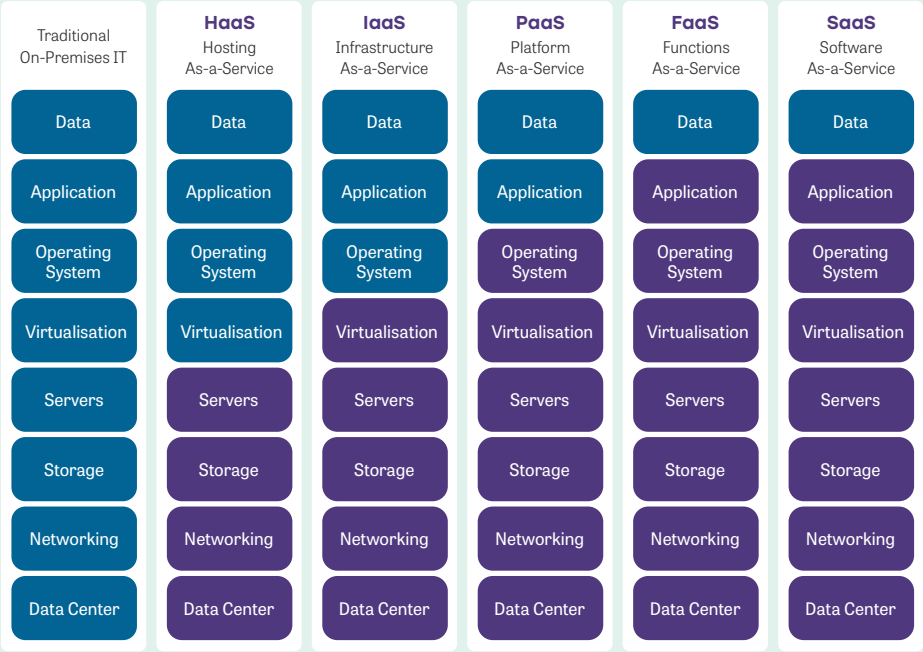
33 Flexera (2021), State of the Cloud Report, https://resources.flexera.com/web/pdf/report-cm-state-of-the-cloud-2021.pdf

34 Enhancing internet connectivity is a key priority in regional initiatives such as the One Belt One Road, the ADB, the AIIB, and the Master Plan on ASEAN Connectivity 2025.

35 Baron, Heide, Mahmud, Yeoh (2021), State of Cloud Security Concerns, Challenges, and Incidents, https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-concerns-challenges-and-incidents/

Cloud Security Fundamentals: *Is it safe?*

Cybersecurity concerns affect both traditional IT and cloud systems alike and core concerns such as unauthorised access to data and loss of oversight and control of systems are similar for both cloud and on-premise models.[36] Although the technical details can be complex, there are essentially two primary areas to protect in IT and cloud systems, and the responsibility for protecting these areas are shared between the customer and the CSP — "Security in the cloud" and "Security of the cloud". These are outlined in Figure 1 below to highlight the respective security responsibilities of the customer and the CSP:



Customer: Responsible for security 'in' the cloud
Cloud Service Provider: Responsibility for security 'of' the cloud

Figure 1: Example of the Shared Responsibility Model Across Different Cloud Services[37]

36 Redhat (2018), What is different about Cloud Security, https://www.redhat.com/en/topics/security/cloud-security
37 Adapted from AWS Cloud Security's "Shared Responsibility Model". The AWS Shared Responsibility Model is available at: https://aws.amazon.com/compliance/shared-responsibility-model/
38 Cisco (n.d.), What is Data Loss Prevention?, https://www.cisco.com/c/en_sg/products/security/email-security-appliance/data-loss-prevention-dlp.html
39 Cisco (n.d.), What Is Application Security?, https://www.cisco.com/c/en_sg/solutions/security/application-first-security/what-is-application-security.html
40 Cisco (n.d.), What Is Identity Access Management?, https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-identity-access-management.html
41 Thomas Scheibe (2020), Enhancing Business Resiliency with Data Center Cloud Networking, https://blogs.cisco.com/datacenter/enhancing-business-resiliency-with-data-center-cloud-networking
42 Baron, Heide, Mahmud, Yeoh (2021), State of Cloud Security Concerns, Challenges, and Incidents, https://cloudsecurityalliance.org/artifacts/state-of-cloud-security-concerns-challenges-and-incidents/

Regardless of whether a customer uses cloud or not, customers are responsible for protecting the data, applications, and workloads that are in the cloud ("Security in the cloud"). This includes:

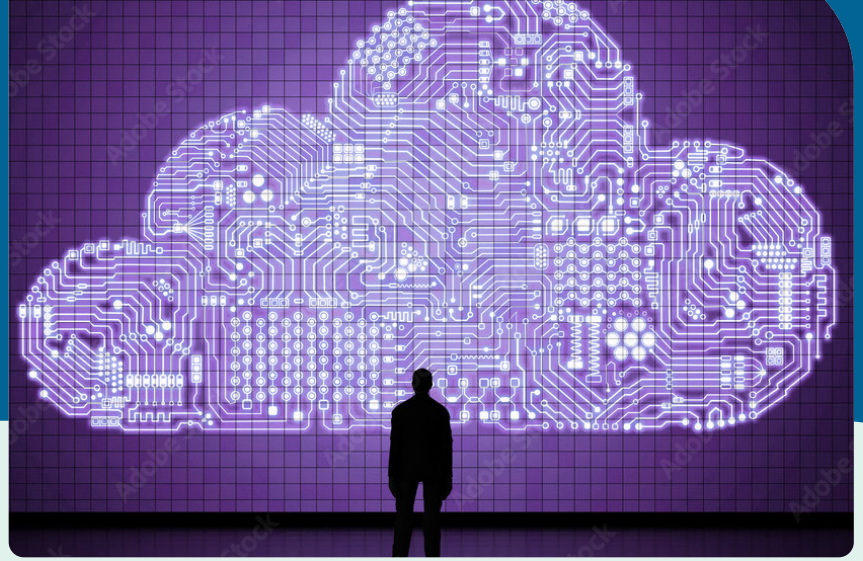
- **Data —** One way data can be protected is by encrypting the data at-rest and in-transit. A robust key management system ensures security of the encrypted data, and a Data Loss Prevention programme can be put in place to detect and classify sensitive data and identify violations of data handling policies. [38]
- **Applications and User Accounts —** Application security measures including vulnerability scanning, threat detection, and firewalling can help mitigate malware threats.[39] Implementing Identity and Access Management (IAM) and network protection measures (such as firewalls and security software) can help prevent unauthorised users from taking advantage of gaps or human error to gain access to sensitive data and internal resources.[40]

In cloud adoption, the CSP is responsible for protecting the infrastructure of the cloud service under the shared responsibility model ("Security on the cloud"). This infrastructure includes the hardware, software, networking, and facilities for the cloud.

In addition to the model described above, additional cybersecurity practices applicable to cloud adoption include:

- **Visibility —** Cloud systems give organisations full visibility of what virtual assets they are operating in the cloud and what state they are in. The ability to log activity in the cloud gives organisations the ability to see who and how data and assets are being used.
- **Continuous Security Monitoring —** Security monitoring in the cloud gives organisations the ability to know at any time one's compliance status and be aware of possible threats and anomalous behaviours.
- **Automation —** Organisations can automate security responses to prevent misconfiguration of assets, detect and mitigate vulnerabilities or respond to security and policy violations.
- **Enhanced Resilience with Backup and Recovery Procedures —** Organisations have an unprecedented ability to back up and quickly recover data and virtual infrastructure following incidents. Backups can be stored in multiple locations to make them highly resilient. Cloud technologies offer an affordable way to meet requirements for a fast recovery process with a variety of risk and disaster management solutions.[41]

While cloud security may seem like a daunting task for any organisation, under the shared-responsibility model of cloud systems, CSPs are key cybersecurity partners who can help their clients adopt the latest security innovations and best practices. CSPs have significant economic incentives to prevent incidents from happening and in facilitating quick recovery. The delivery of secure and reliable service and the ability to protect customer data is central to CSPs' brand marketing. Most reputable CSPs invest significant time, effort, and budget to develop and provide security solutions to their customers that automate security tasks to reduce human configuration errors and utilise analysis to monitor and further anticipate and mitigate threats. More organisations are also adopting CSPs' enhanced security controls, jumping from 58% in 2019 to 71% in 2021.[42]



Demystifying Cloud Policy Myths

Policymakers around the world are seeking to improve the cybersecurity of their economies through the use of legal instruments and regulatory tools, including frameworks, technical standards, ICT education initiatives, and coordinated ICT strategies. The government plays a key role in ensuring protection, assurance, and trust, and building consumer confidence in the quality of user protection and security. Despite the prevalence of cloud adoption, a 2019 survey by IDG Connect found that only 58% of end-users indicated that they trust public cloud providers' data security platforms and protocols over their own IT teams.[43] Given the dynamic and evolving nature of cloud technology, myths and misconceptions on how to keep cloud secure have arisen and entrenched themselves.

In this section, we tackle some common cloud policy misconceptions, and highlight the importance of focusing on articulable high-impact risks that are relevant to the diverse models and types of cloud service provision, instead of vague frameworks or over-prescriptive requirements that complicate compliance and increase costs with uncertain benefits.

43 IDG Connect (2019), Debunking the myths of hybrid cloud adoption, https://www.redhat.com/rhdc/managed-files/cl-debunking-hybrid-cloud-myths-analyst-paper-f17671bf-201905-en.pdf

Misconception 1

"To enhance cybersecurity, a hybrid cloud model should be adopted for all cloud migrations."

...Cloud deployment models should be based on organisational needs and capabilities. ✓

Hybrid cloud refers to an approach that mixes traditional on-premises, private infrastructure or cloud services with public cloud services. Some governments opt for a hybrid-cloud-by-default approach in their public sector agencies and regulated industries to keep selected data on-premises.

One argument for requiring a hybrid cloud adoption is the expectation that a hybrid cloud model allows for the "best of both worlds", with sensitive data being kept on-premises while other less sensitive data gets moved to the cloud. While this may be true in some cases, it does not mean that it applies to **all** cloud deployment. Organisations' decisions to choose a hybrid, public cloud, or private approach should depend on its individual business needs and security risk tolerance.

Rather than implementing a blanket hybrid cloud approach for cloud adoption, **it is more effective to first understand the needs of the organisation** and develop a cloud strategy that envisions the best role of cloud computing for the organisation. This will help answer questions regarding the model and type of cloud services needed, and consequently the appropriate cybersecurity measures and safeguards to put in place, bridging the gap between a high-level strategy and an actual cloud adoption plan.

Misconception 2

"All cloud systems should be classified as Critical Information Infrastructures (CIIs)."

...Cloud computing is used across a broad variety of organisations and need flexibility for deployment. ✓

Critical infrastructures (CIs) are services that are essential to the safety and security of a country's society, government, and economy, while critical information infrastructures (CIIs) are the information components and infrastructures that support CIs.[44] Typically, the identification and classification of critical information infrastructures (CIIs) depend on the severity of the harm if the system is compromised. For example, the Cyber Security Agency of Singapore (CSA) defines CIIs as "necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore."[45]

Cloud systems are a means to an end. An outcome-based and technology-neutral approach to defining CIIs allows for clarity and flexibility. Policymakers should evaluate and tier key information infrastructure systems on this basis rather than look to treat all cloud systems as CII. With the increasing prevalence of cloud adoption and multi-cloud strategies, defining all cloud systems as CII is also impractical to implement for a few key reasons:[46]

- First, the additional regulatory burden on small and medium-sized enterprises (SMEs) using such cloud services that are unrelated to essential services would negatively affect their ability to delicately balance between mitigating risk and growing their business.
- Second, the additional workload to supervise cloud services imposed on the regulatory authority would not be sustainable and could distract them from key cybersecurity priorities that actually affect essential services.
- Finally, most CII operators are required to submit protection plans and regular reports to regulators. If all cloud systems become CIIs, regulators will need to assess these submissions to prevent cyber threats despite being unrelated to critical or essential services.

Instead, regulators should look to the aspects of CII that leverage cloud security, the degree of dependency, and set guidelines for safe adoption, accordingly.

44 OECD (2008), OECD Recommendation of the Council on the Protection of Critical Information Infrastructures, https://www.oecd.org/sti/40825404.pdf

45 Section 7(1) of the Cybersecurity Act of Singapore, available at https://sso.agc.gov.sg/Acts-Supp/9-2018/#pr7-

46 Ariel Eli Levite and Gaurav Kalwani (2020), Cloud Governance Challenges: A Survey of Policy and Regulatory Issues, https://carnegieendowment.org/2020/11/09/cloud-governance-challenges-survey-of-policy-and-regulatory-issues-pub-83124

Misconception 3

"Prescriptive and specific cybersecurity requirements are needed to ensure protection."

...Outcome-focused and risk-based approaches enable optimisation of cybersecurity. ✓

Practical cybersecurity policies are flexible, technology-neutral, and more effective when they take a risk-based approach no matter what technology is used. The tools and methods used to achieve cybersecurity outcomes will vary because each organisation's risks, priorities, and systems are unique. Policies that recognise this provide companies with the flexibility in choosing the appropriate approach to protect what is most important to their business. Also, such policies help commit resources towards securing assets instead of committing resources to meet reporting and administrative requirements.[47]

Cloud is a flexible technology that covers a diverse spectrum of service models ranging from Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), to other new emerging services. Even within the same type of service model, the specific cloud deployment model varies and is configured by the scope of cloud users, services, and resources based on the customer's service requirements. Depending on the details of the services being provided, the commercial agreement and shared responsibility between the CSP and customers can vary greatly.

Hence, it is **critical to use an outcome-focused and risk-based approach**, rather than a fixed and prescriptive approach, which may only be practical for a minority of cases and deters CSPs from taking advantage of cutting-edge security innovations.[48] An approach that adopts appropriate measures based on target outcomes and contextual risks of the system helps to lower systematic risk.[49] It is also important for regulators to recognise the shared responsibility model, where CSPs are responsible for security on the cloud (infrastructure and software), while customers are responsible for security in the cloud (data, platforms, and network). This approach allows CSPs and customers to focus on the areas that they are best positioned to manage, thus optimising overall security.[50]

The design of a measured and fit-for-purpose approach to regulate CSPs, one that appreciates the great variety and diversity in cloud provision, would include a general set of guidance (e.g., on access control) for the generic service models, and then include additional guidelines or rules that are specific to certain sectors or higher-risk data types.

47, 48 Ascentor (n.d.), Less rules, more goals. How recent changes in regulatory approaches can enable innovation in information security, https://insights.ascentor.co.uk/blog/2019/02/less-rules-more-goals-how-recent-changes-in-regulatory-approaches-can-enable-innovation-in-information-security

49 National Grid (2013), Response to NIST: Developing a Framework to Improve Critical Infrastructure Cybersecurity, https://www.nist.gov/system/files/documents/2017/06/06/040813_national_grid.pdf

50 Radhika Mitra (2020), Understanding the Shared Responsibility Model: Securing Public Cloud Just Got Easier, https://blogs.cisco.com/security/understanding-the-shared-responsibility-model-securing-public-cloud-just-got-easier

Misconception 4

"Data is safer when it is kept locally";
"using local CSP and cloud technology suppliers is safer."
..."Localisation" does not provide cybersecurity. ✓

The physical location of data has no intrinsic bearing on the security of that data. Instead, cybersecurity comes from the security controls that are applied to protect the data regardless of its location. The preference to keep data locally rather than "abroad in the cloud" often stems from the idea that data kept inside the borders of a country is more secure or accessible. Data localisation measures may also be difficult to implement at a practical level, and without proper security processes, are ineffective as safeguards for data privacy and risk giving regulators a false sense of security.[51]

A reason why policymakers want to put in place data localisation requirements for public sector agencies and regulated industries is the lack of trust in the adequacy of privacy regimes in other jurisdictions.[52] Policymakers may also have concerns about unauthorised access by foreign governments in the name of law enforcement. However, preventing data from leaving a country is neither desirable nor always possible, and privacy regimes are constantly evolving. Frameworks such as the APEC Cross-Border Privacy Rules (CBPR) help enable cross-border flows of data by ensuring a high-level of cross-border data protection across jurisdictions even though they may have differently structured privacy regimes.

Another reason for policymakers to require data be stored locally is the concern that authorities' access to data would be more difficult if the data is stored offshore. However, considering the large economic costs of data localisation,[53] policymakers should instead consider alternatives to ensure that authorities have access to data. One such way is to enact legal mechanisms to define when and what procedures authorities may use to request data from enterprises, providing sufficient lead time to enterprises and guarantees for data privacy as well. These policies for access should be crafted in consultation with stakeholders to ensure that privacy rights are upheld and compliance is not onerous.

Some policymakers may also implement data localisation in public sector and regulated industries to prevent sensitive and important data from "leaking" into the hands of another country. However, the concern of data leaking is a concern of a lack of controls, not of localisation, and should be treated accordingly. The location, ownership or control of the servers and data centres has little to do with how secure it is.[54] Localisation does not protect data from "getting into the wrong hands", and logical and physical controls should be implemented instead. An example is to encrypt data before it is uploaded to the cloud, and for the CSP's customer to retain control over the decryption keys, thus preventing third parties and CSPs from accessing the data.

Localisation does not confer any inherent cybersecurity advantages to CSPs or cloud technology suppliers. Organisations looking to procure cloud services should select providers according to their cybersecurity practices and offerings. In addition, requirements for localisation usually involve a trade-off in terms of price, function and innovation and should be carefully considered. Requiring data residency or local operation may also mean certain features of CSPs would not be available, or support is restricted, or the service may not be offered in the specific market entirely.

51 Silvia Baur-Yazbeck (2018), 3 Myths About Data Localization, https://www.cgap.org/blog/3-myths-about-data-localization
52 John Miller and Sana Ali (2016), The Myth of Data Localization in the Name of Privacy Protection, https://www.itic.org/news-events/techwonk-blog/the-myth-of-data-localization-in-the-name-of-privacy-protection
53 Institute of International Finance (2020), Data Localization: Costs, Tradeoffs, and Impacts Across the Economy, https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf
54 Nigel Cory and Luke Dascoli (2021), How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

Misconception 5

"Physical audits must be conducted even after migration to the cloud."

...Physical audits should shift to logical audits. ✓

As new technologies disrupt traditional modes of operation, many regulators have sought to ensure that they retain their powers through existing regulatory tools as far as possible, in the hope that this will allow them to continue to fulfil their responsibilities and obligations.

The issue of physical audit requirements for the cloud is one such case where retaining previous regulatory tools are not beneficial. While a physical audit may be concerned with who can enter a building and what rooms their key card allows them to enter, **a logical audit for cloud ought to be concerned with the applications and data that users can access and the consistency and robustness of the security system used to protect it**.[55] Not only can this information be audited without entering the physical premise, but an inspection of the physical premises would not help in determining whether data can be accessed digitally since the data would not be in a human-readable form.

55 Zachary Flower (2020), What should be on your cloud audit checklist?, https://searchcloudcomputing.techtarget.com/tip/What-should-be-on-your-cloud-audit-checklist

56 Michael Peterson (2020), How Companies Simplify Data Sovereignty with the Cloud, https://gluent.com/how-companies-simplify-data-sovereignty-with-the-cloud/

57 Alex Tolsma (n.d.), GDPR and the impact on cloud computing, https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-security-privacy-gdpr-update-the-impact-on-cloud-computing.html

58 Eyal Estrin (2020), GDPR, Cloud and the Shared Responsibility Model, https://www.europeclouds.com/blog/gdpr-cloud-and-the-shared-responsibility-model

59 CloudPassage (2020), Shared Responsibility Model Explained, https://www.cloudpassage.com/articles/shared-responsibility-model-explained/

Misconception 6

"Strict regulations on CSPs on the provision of requested data is necessary to safeguard data sovereignty."

...Data protection responsibility is shared between the CSP and the customer. ✓

Data sovereignty refers to the concept that data is subject to the laws and governance structures of the nation within which it is collected.[56] Due to the distributed nature of the cloud, some policymakers are concerned that cloud adoption reduces data sovereignty.

In reality, CSPs often only function as data processors and do not have control or oversight of the personal data they process and store on behalf of their customers.[57] Under the shared responsibility model, the primary responsibility for complying with data protection laws falls on the customer. The CSP is then required to support its customer in meeting their regulatory obligations and ensuring the security of the data being processed.[58]

This allocation of responsibility makes the most sense for a few key reasons:

- The customer is the one who is most familiar with the type and purpose of the data being collected, and hence most aware of the impact and consequences of any breaches. Even in those rare cases where the CSP might have some insight into the data it is processing, it does not have a direct relationship with the data subjects being affected.[59]
- Organisations often have their own data privacy arrangements with their CSPs, and in many cases would require the data handled by the CSP to be in a non-human readable format (e.g., homogenised, encrypted, etc.), and hence are not able to "access" the data in a meaningful way. These commercial agreements also usually make the clear distinction that the customer retains data ownership, and merely gives the CSP the permission to store and process the data on their behalf.
- For regulators, it is important to establish clear lines of responsibility for data controllers (customer organisations) in the shared responsibility model. Unlike CSPs (data processors), the customer organisations will better understand the data, have a relationship with the data subjects, and are more likely to have an established local presence.

Misconception 7

"Jurisdictions must develop their own local cloud security standards and certification."

...it is more effective to align with international security standards. ✓

Cloud security is not a new idea. Global security standards, such as the ISO/IEC 27000 family of standards (ISO 27017 and 27018 are cloud-specific updates), help to create a robust and comprehensive security management framework that also ensures global applicability and interoperability.[60] Other sources of international codes of practice and standards include the NIST, the State on Standards for Attestation Engagements no. 16 (SSAE-16), and the Service Organisational Control (SOC).

Governments should recognise existing certifications of cloud computing services carried out by external assessors based on internationally recognised standards. Locally verifying existing certifications is wasteful and slows cloud adoption with no security benefits. Government certification processes should recognise equivalent international audits and certifications where possible. If local attestation is required, CSPs should be able to provide evidence prepared from previous audits by qualified auditors against internationally recognised standards rather than having to repeatedly audit services against the same controls for different customers. This evidence should be accepted in digital form and should not be required to be submitted in physical form.

It would be more effective and efficient to recognise and align to international security standards and best practices to ensure that **local requirements are globally aligned and relevant**.[61] Products and services that meet such widely adopted standards are more rigorously tested, and are more likely to be updated and patched for vulnerabilities than where requirements are specific to a market or forked from international ones. This also reduces compliance costs for international companies and companies seeking to expand overseas, while also ensuring that the standards being adopted in a jurisdiction benefit from the expertise and resources of the international community. Regulators can also consider actively participating in and collaborating with the international community to keep pace with and contribute to the latest cloud security innovations.

60 Elizabeth Gasiorowski-Denis (2015), Trust and Confidence in Cloud Privacy, https://www.iso.org/news/2015/01/Ref1921.html
61 Adam Nunn (2021), What Is ISO 27018:2019? Everything Executives Need to Know, https://auth0.com/blog/what-is-iso-27018-2019-everything-executives-need-to-know/

Misconception 8

"CSPs should be required to regularly report their cybersecurity threats and events to government"

...Reporting should not be onerous and should be mandatory only for serious cyber incidents. ✓

Cloud technology is a means to an end, and regulations pertaining to reporting requirements should adopt a technology-neutral approach. Specific requirements for CSPs or users to submit regular incident reports to governments adds regulatory burden to businesses and unnecessarily takes up the time and attention of regulators. Instead, regulators should generally encourage incident reporting where material harm has occurred,[62] and make reporting a requirement for important systems such as CIIs.

Misconception 9

"Subcontracting reduces security."

...Subcontracting can be effectively managed with clear responsibilities. ✓

CSPs subcontract a wide variety of functions (e.g., hosting, data storage, transmission, etc.) to third parties. Most, if not all major CSPs subcontract some part of their function in order to make the customer-facing service more efficient and less costly.[63]

Effective subcontracting can reduce costs for businesses, but it should not be an excuse for reductions in service quality and reliability, and subcontractors should be considered as part of the CSP. From the perspective of the regulator, the key is to ensure that the division of responsibilities, requirements, and liability between the CSP and the user organisation is clear.

62 Marnix Dekker, Dimitra Liveri, and Matina Lakka (2013), Incident Reporting for Cloud Computing, https://www.enisa.europa.eu/publications/incident-reporting-for-cloud-computing
63 Vipul N. Nishawala (2013), Subcontracting in the Cloud, https://www.sourcingspeak.com/subcontracting-in-the-cloud/

Deep Dive 2

Managing Supply Chain Cybersecurity Risks

Supply chain cyberattacks are a growing threat to organisational cybersecurity and have been the basis for some of the most catastrophic cyberattacks in recent history. Supply chain attacks notably served as the vehicle for the NotPetya virus which crippled public sector and critical infrastructure systems across the Ukraine in 2017 and shipping services globally.[64] The SolarWinds breach in late 2020 also relied on dissemination through the IT Infrastructure company's Orion monitoring software, which was (and is) widely used across both public and private sector agencies. Most recently, the Kaseya incident of July 2021 also relied on the infiltration of the company's IT management and monitoring technology products to affect further entities down the supply chain—potentially including agencies within the public sector which hold sensitive data.

This section covers what supply chain cyberattacks are, their implications on public sector and regulated industries, and recommendations for how to better manage supply chain risks. As supply chain cybersecurity has emerged as a relatively new area of concern, these recommendations offer a starting point for policymakers as they begin to consider how to address these risks.

64 Federal Reserve bank of New York (2021), Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf

What are Supply Chain Cyberattacks?

Supply chain cyberattacks are cybersecurity incidents in which attackers gain access to secured systems by compromising the software supply chains of affected organisations, instead of targeting them directly. Attackers will first compromise and infiltrate outside partners or service providers whose special access to targeted organisations is then exploited to upload malicious code. This results in cascading chains of vulnerability that potentially affect the initially compromised entity's customers. The diagram below illustrates how an organisation's own cybersecurity practices can be entirely bypassed if bad actors take advantage of vulnerabilities in vendors to compromise an organisation's software supply chain.

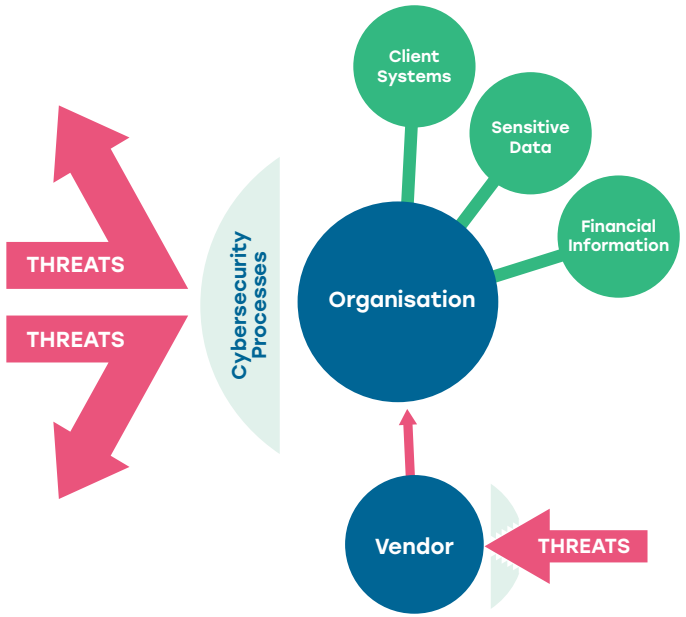


Figure 2: Cyber Threats Target Vendors to Bypass Cybersecurity Processes

Organisations typically contract with multiple vendors and, as such, attackers need only infiltrate one vendor to potentially gain access to an organisation's assets.

While not a new concept, recent events have shown that supply chain cyberattacks are growing in number and severity. Attackers have become conscious of the rising costs of penetrating well-defended organisations. A report by Accenture in late 2020 noted that four in 10 cyberattacks were thought to originate within the extended supply chain as opposed to the targeted organisation itself.[65] Perhaps even more problematically, a recent report on supply chain attacks by the European Network Information Security Agency (ENISA) notes that a 'migration' to the tactic has occurred, which it estimates will lead to a four-fold increase in such attacks across 2021.[66]

Recent incidents have prompted an industry-wide scramble to reassess network vulnerabilities in light of a cyberthreat that calls for a paradigm shift in foundational aspects of network security. Through a supply chain attack, an otherwise well-defended perimeter network can be severely compromised due to its relationship with an infiltrated partner. Organisational vulnerability to supply chain attacks is thus dependent on cybersecurity policies that take into consideration a wider awareness of where the organisation in question is positioned relative to service providers.

The challenge presented by these attacks is made even more apparent by the explosion in cloud services and managed service providers. These service offerings underpin the ability of companies to expand online operations rapidly and seamlessly and have become integral to allowing SMEs around the world to adopt digital solutions in efficient and cost-effective ways. Today, organisational networks may be connected to and reliant on hundreds of external service providers, each of which could present a significant threat to overall security if compromised.

65 Accenture (2020), Securing the supply chain, https://www.accenture.com/sg-en/insights/consulting/securing-the-supply-chain

66 ENISA (2021), Threat Landscape for Supply Chain Attacks, https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

As the diagram below illustrates, partners within the digital supply chain, and the potential vulnerabilities they bring with them, can manifest in the form of cloud-based IaaS, PaaS, and SaaS providers, industrial management, human resources management tools, or even cybersecurity suites.

This multitude of suppliers creates an extended chain of vulnerability that can functionally undermine otherwise secure networks and compromise highly sensitive data. In the aftermath of the SolarWinds breach, for example, it was immediately reported that agencies within the U.S. Treasury and Commerce Departments had been directly affected—notably, the Commerce Department's National Telecommunications and Information Administration.[67]

It later came to light that the extent of the security breach had been understated and that the State Department, the Department of Homeland Security, and the Pentagon had all been compromised, putting into peril vital information and systems of direct relevance to national security. A key factor that contributed to the attacks was the implicit trust and thus lack of scrutiny for software update patches. This could have been avoided if a zero-trust approach had been adopted where all software would be scrutinised for malware or abnormal behaviour and limited to the least privileges necessary, whether trusted or not.

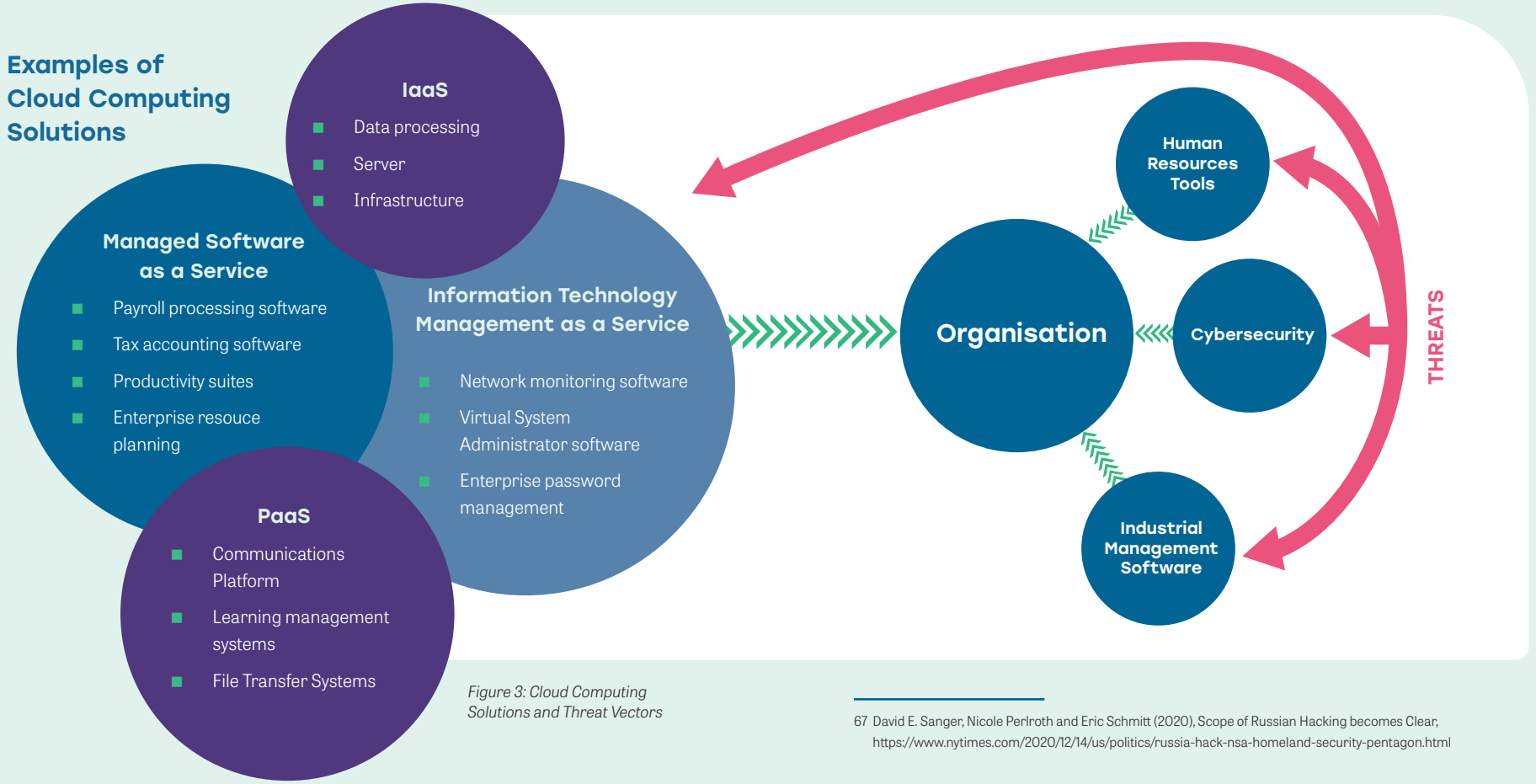


Figure 3: Cloud Computing Solutions and Threat Vectors

67 David E. Sanger, Nicole Perlroth and Eric Schmitt (2020), Scope of Russian Hacking becomes Clear, https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

Supply Chains and the Public Sector

The expansion of these software supply chains has implications on the public sector. Governments around the world are seeking to implement sweeping reforms to their administrative procedures in the wake of COVID-19 and are highlighting the importance of digital solutions to ensure the efficiency and effectiveness of public service delivery. Many of these newly inbound digital solutions may thus represent new potential vectors for supply chain attacks, which could in turn compromise sensitive public data and damage trust in the government.

The U.S. Government's response to SolarWinds focused on two key aspects. First, it stepped up its transition from perimeter-based defences that treated networks as having a trusted inside, untrusted outside, and a fixed perimeter, to an architecture that did not assume trust, i.e. a zero-trust architecture. Second, it imposed new requirements regarding how critical software is built, secured, and maintained. It introduced the approach of a SBOM with a secure build environment, vulnerability handling, and disclosure policies.

The growing threat profile of supply chain attacks thus necessitates a shift in cybersecurity practice away from a narrow, unilateral approach that emphasises shoring up internal processes and security protocols, to a wider, multilateral approach that would entail a more holistic, collaborative approach to identifying and addressing vulnerabilities. Public sector agencies should adjust their engagement with private sector service providers to improve communication and ensure that an effective working relationship is developed and maintained. This will allow for stronger oversight on security protocols and ensure that service providers are able to undertake timely, appropriate, and impactful mitigating interventions in scenarios involving security breaches.

Sharing information and building trust are some of the public sector's most effective potential assets in ensuring that service providers are appropriately equipped to understand the specific demands of public sector customers and develop relevant responses to potential threats. Guidelines, such as the ISO/IEC 27000 series of standards,[68] are an effective tool that can augment private sector efforts to pursue appropriate security policies and can take reference from internationally recognised best practice to ensure that security protocols are holistic and interoperable across jurisdictions. Government agencies can furthermore aim to thoroughly review and publish procurement supply chains while coordinating individually or directly with service providers to ensure that whole-of-government solutions are fit-for-purpose and effective for likely threat scenarios. This would help bolster understanding of the cyber risks present and the cybersecurity implementations required among the parties involved.

68 ISO (n.d.), Publicly Available Standards, https://standards.iso.org/ittf/PubliclyAvailableStandards/

Supply Chains and Regulated Industries

Compared to the public sector, regulated industries represent a much broader range and a larger number of organisations for policymakers to consider. The nature of IT adoption, cyber risks, and software and hardware supply chains also varies greatly across the regulated sectors. For example, medical device technologies may differ greatly in priorities and type of cyber risks than that of the telecommunications sector. Given this large number and broad needs, and the inherent need for access to technologies to stay competitive and effective, regulations for regulated industries need to be optimised to ensure they do not hamper innovation and yet facilitate good cybersecurity practices.

Recommendations

1. Encouraging the adoption of targeted risk management guidelines and principles

Governments may seek to assist potentially vulnerable organisations to manage vulnerabilities in their cyber supply chains by developing and promulgating guidelines which draw from industry best practices. Such guidelines can put in place standardised procedural frameworks that can be easily implemented by adopting organisations, which would both help to identify supply chain risks more efficiently and establish processes to limit potential consequences should intrusions occur. In so doing, governments would facilitate knowledge sharing across industries and encourage the development of a baseline level of resilience to supply chain attacks.

To ensure responsibility throughout the digital supply chain, risk-based rules should be encouraged to ensure adequate protection across all layers with clearly defined requirements. Confidentiality, integrity, and availability can be ensured through baseline standards that cover areas such as identity and access management, encryption, and continuous protection.[69]

Case Study

The NIST issues guidelines addressing cybersecurity and in 2013 released the NIST Cybersecurity Framework to improve cybersecurity practices of critical infrastructure providers. NIST has also produced specific guidelines aimed at supply chain risk management, called the guidelines for Cyber Supply Chain Risk Management (C-SCRM), that were formally made available in 2015.[70] Efforts to update these guidelines have been ongoing since their introduction and an overhaul of the guidelines is presently in its drafting stages under the series number SP 800-161 Rev. 1.[71]

2. Developing or adopting cybersecurity assessment procedures for industry partners

The development of guidelines for industry can help to achieve a broader overall standard of cybersecurity, but governments are growing increasingly concerned about threats posed to government systems by service providers. To address this, governments can look to implement assessment and certification regimes to ensure that potential partners are compliant with industry standards and international best practices. These certification regimes can be built on guidelines issued by government or developed and issued as separate processes—though ensuring consistency across them is advised to avoid internal contradictions. The applicability of certification regimes can be tailored to suit specific classes of service providers or even specific industries. The implementation of continuous, regular compliance assessment procedures would further enhance transparency and ensure that security standards can be updated and enforced as necessary.

While certifications play a valuable role, governments should also exercise flexibility in their use and strongly consider recognising the equivalence of existing international standards.

Particular attention should be paid to acknowledging international standards such as those promulgated by the ISO and IEC on information security and risk management. These include ISO/IEC 15408 on the evaluation criteria for IT security and standards in the ISO/IEC 27000-family such as ISO/IEC 27017 on information security processes for cloud services.

69 Charter of Trust (n.d.), Principle 2, https://www.charteroftrust.com/wp-content/uploads/2021/03/Charter-of-Trust_Principles_EN_2021-02-25.pdf
70 NIST (2015), Cyber Supply Chain Risk Management, https://csrc.nist.gov/projects/cyber-supply-chain-risk-management
71 Jon Boyens et. al. (2021), SP 800-161 Rev.1, https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/draft

3. Develop and incentivise information-sharing mechanisms and uphold standards of transparency

To more comprehensively assess risks presented by industry partners, governments should encourage service providers to maintain high standards of transparency by developing and incentivising information-sharing and, where useful, certain standards of reporting. Aside from incident reporting, which is already mandated in many cybersecurity standards, governments may seek, within the bounds of intellectual property legislation, to develop regulations allowing for greater clarity on the structure and composition of products and services acquired from service providers. Transparency in this context would allow purchasing organisations to subject products and services to independent assessments of risk and ensure that they are aware of all potential threat vectors. Aside from reducing vulnerability for purchasers, this would also mitigate the liability of service operators.

Such mechanisms should also endeavour to minimise the compliance costs in the industry, of which a good way to keep compliance costs at a minimum is to align with international standards and best practices for cross-border interoperability.[72]

Case Studies

An executive order on improving U.S. Cybersecurity was signed by U.S. President Biden in May 2021, which specifically addressed the threat posed to U.S. interests by supply chain attacks.[73] A key term re-introduced by the executive order in the context of government purchasing was the SBOM — a document which software vendors would use to enumerate software components used within a particular product. Under the executive order, NIST has been empowered to issue guidance and regulations around the generation of SBOMs, which may become necessary for service providers wishing to sell certain "critical software" products to the U.S. federal government. This initiative would allow government agencies to gain oversight on specific elements in software products they use, improving their capacity to monitor and address vulnerabilities these components might introduce.

Separately, Singapore's CSA is introducing a CII Supply Chain Programme to enhance the security and resilience of Singapore's CII sectors.[74] Transparency and accountability are noted to be core objectives of CII Supply Chain Programme, and work is underway to implement guidelines which will both require and empower CII Operators to gain a more holistic understanding of the services they use. Through such information gathering exercises, the CSA hopes to enable CII Operators to comprehensively map service providers and software components to rank them according to their cybersecurity posture, and hold them accountable for their actions.

4. Working with relevant industry actors to ensure that solutions are fit-for-purpose and appropriate to threat profiles

Governments should additionally ensure that channels to the private sector remain open to allow for a robust exchange of knowledge and ideas. Technical expertise on cybersecurity topics can be difficult to understand, while skilled labour is often in high demand and concentrated in the private sector. While training and developing organic capabilities is a fundamental long-term objective, governments can make up for shortfalls in relevant digital skills by remaining engaged with the private sector on initiatives that can be replicated to good effect in the public sector. Innovative applications and platforms developed by the public sector can furthermore aid in the enhancement of supply chain security in the public sector.

Case Study

In May 2021, U.K.'s Department for Digital, Culture, Media and Sport issued a call for views on cyber security in supply chains and managed providers to better understand how organisations manage supply chain risks and to gather input on a proposed framework.[75] Gathering views and input by holding such consultations are key for policymakers to understand the local context of cybersecurity, the solutions currently implemented and available in the industry, and the support and policies that would help organisations mitigate cyber risks. Also, consultations on frameworks help optimise policies by incorporating suggestions and addressing the concerns of stakeholders.

To manage risks across supply chains, Singapore's CII Supply Chain Programme recommends processes and sound practices for stakeholders to manage supply chain risks.[76] The programme brings together CSA, CII owners, and vendors to help Singapore improve policies on supply chain risks. The approach by Singapore differs slightly from the U.K., but the premise of gathering stakeholders to contribute to supply chain cybersecurity is the same. Of note, Singapore's approach focuses on supply chain cybersecurity as it relates to CIIs.

72 Examples of international standards and best practices for reporting include ISO/IEC 27010:2015 and NIST Special Publication 800-150,
73 The White House (2021), Executive Order on Improving the Nation's Cybersecurity, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
74 Kenny Chee (2021), Push to better manage cyber-security risks in critical infrastructure, https://www.straitstimes.com/singapore/push-to-better-manage-cyber-security-risks-in-critical-infrastructure
75 Gov.uk (2021), Call for views on cyber security in supply chains and managed service providers, https://www.gov.uk/government/publications/call-for-views-on-supply-chain-cyber-security/call-for-views-on-cyber-security-in-supply-chains-and-managed-service-providers#open-call-for-views
76 Ahmad Zhaki Abdullah (2021), New initiative to help manage cybersecurity risks in Singapore's critical information infrastructure, https://www.channelnewsasia.com/singapore/cybersecurity-risk-singapore-critical-information-infrastructure-252136

Conclusion: Cybersecurity Policies Enable the Digital Economy

In today's digitalised world, technology risk management is a complex task for organisations of any type or size. Public sector agencies and regulated industries face special challenges based on the technologies they employ to deliver everything from citizen services to transportation, and telecommunications to healthcare.

Cybersecurity policy regimes can be crafted to support technology risk management for these sectors in ways that help ensure sustainable and resilient digital economies. Policymakers should optimise cybersecurity policies in ways that leverage internationally recognised standards and certifications, encourage uptake of zero-trust approaches, utilise outsourcing (where appropriate) to manage costs, prioritise critical systems based on risk, carefully consider local mandates, and support preparations for major cyber events.

Cybersecurity regimes should also seek to address pertinent questions arising for public sector and regulated industries as they consider new technologies to adopt while also adapting their existing systems and supply chains to an evolving array of cyber threats.

In the adoption of new technologies like the cloud, policymakers should ensure technology risk managers can employ diverse models and types of cloud services based on unique organisational requirements. This includes limiting overly prescriptive or localised mandates, as well as notification requirements for low-risk breaches, while encouraging logical audits, data sharing between CSPs and their customers, uptake of international standards, and effective sub-contracting to manage costs.

For existing systems and supply chains, cybersecurity regimes should encourage adoption of targeted risk management guidelines and principles, support uptake of cybersecurity assessment procedures, incentivise information-sharing and transparency, and promote close consultation between government and industry partners to ensure supply chain security requirements are fit-for-purpose.

These recommendations lie at the heart of a risk-based assessment approach to technology risk management. Public sector and regulated industries, often at the vanguard of entities grappling with how to manage today's rapidly shifting technology risk environment, have an opportunity to pave the way for an improved approach to managing risk across every sector of the digital economy. Good policy will lay the groundwork to help them seize it.

COALITION FOR CYBERSECURITY IN ASIA-PACIFIC

The Coalition for Cybersecurity in Asia-Pacific comprises Amazon Web Services, Becton Dickinson, Cisco Systems, MasterCard, and VMware. We are a group of dedicated industry stakeholders who are working to positively shape the cybersecurity environment in Asia through policy analysis, engagement, and capacity building.

Access Partnership

We lead countries to fair tech.

Access Partnership is the world's leading public policy firm that provides market access for technology. Our team uniquely mixes policy and technical expertise to optimise outcomes for companies operating at the intersection of technology, data, and connectivity.

singapore@accesspartnership.com

www.accesspartnership.com