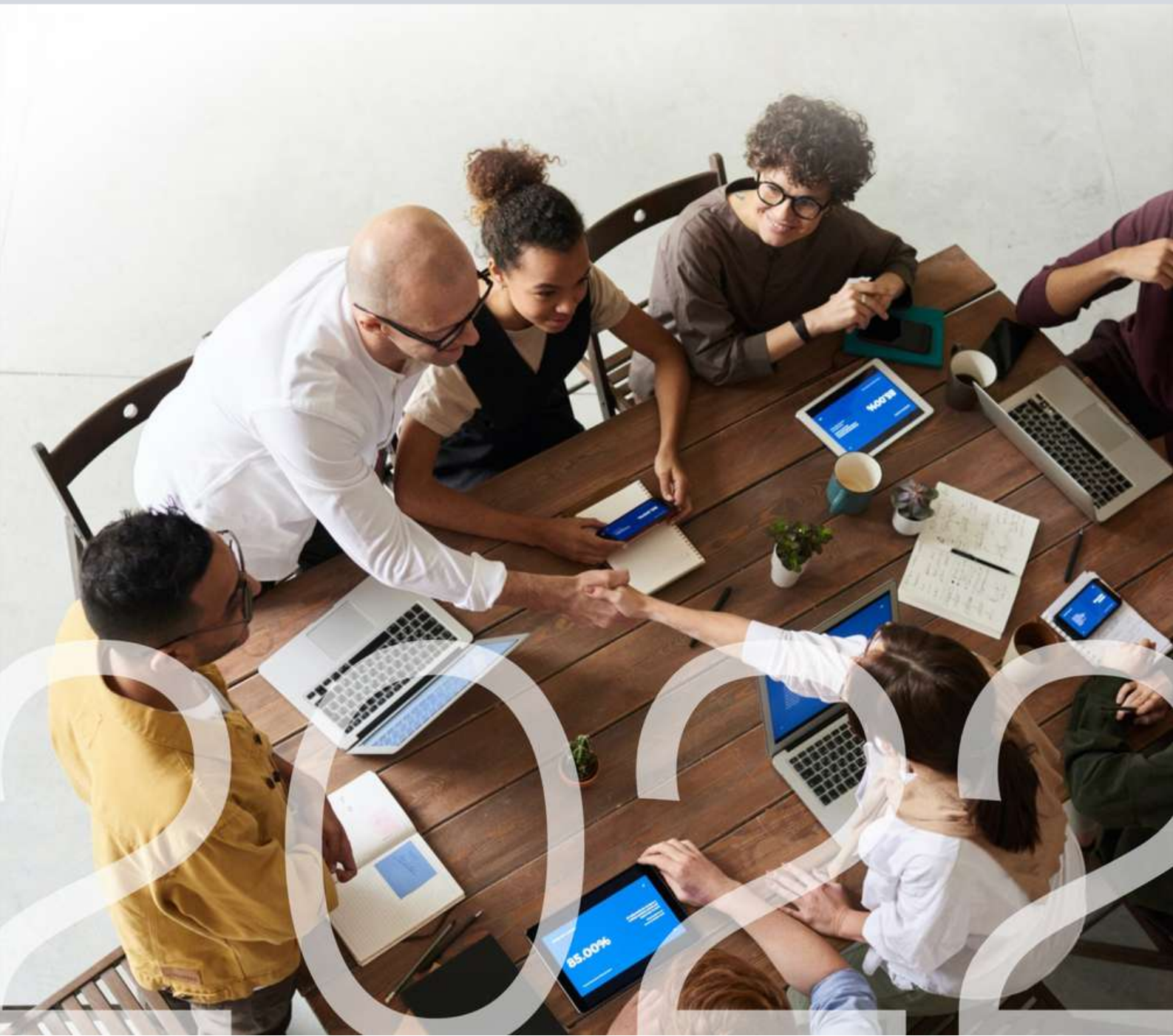
MyRepublic Ignite

BLACKPANDA

Building a successful

Cloud Security Strategy



Contents

About Us

MyRepublic has grown at a compound annual growth rate of 26% over the past four years, and currently has more than 270,000 subscribers across Singapore, Australia and New Zealand.

MyRepublic is one of the fastest-growing telecom operators in the Asia-Pacific, with operations across Singapore, New Zealand and Australia, and plans to expand further into the region.

MyRepublic's values lie in the future of connectivity, the next opportunity to disrupt, and innovations that will make a real difference. The provider's priority is to redefine broadband and mobile connectivity and empower customers to understand what a true modern connectivity experience can be.

Introduction

Cloud security is one of the most important issues to consider when moving to the cloud. Despite the many benefits of cloud computing, security concerns remain a top inhibitor of adoption. To help organisations overcome these concerns and develop a successful cloud security strategy, this paper will outline the key steps to consider.

The cloud is becoming an increasingly important topic for businesses as our world gets more digital. Organisations may accomplish more with less by utilising cloud technology. Advanced business intelligence, remote working, and the Internet of Things are all made possible by the cloud.

However, cloud adoption comes with several risks. Every organisation needs to understand cloud security best practices so that they can integrate crucial processes and safeguard their assets.

Cloud Security Strategy

Today's security landscape is complicated. Accepting that your systems will be breached at some point is necessary for protecting your organisation. To protect your data and applications in the cloud, you need to have an effective security plan in place. The five components of an effective cloud security plan are:

01

Identity and Access Management (IAM)

IAM systems manage access control for the users of your cloud infrastructure. They provide different levels of control, for example, to ensure that only authorised users can access sensitive data. IAM systems are essential for protecting your data from unauthorised access or theft.

02

Data Loss Prevention (DLP)

DLP solutions are also instrumental in the prevention of unauthorised access or data theft. They can help you comply with regulations such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS). DLP solutions scan all data traffic for sensitive information and block or quarantine any data that is found to be in violation of your security policies.

03

Security Monitoring and Attack Detection

Security monitoring solutions track all activity in the cloud environment and identify any unusual or malicious behavior. This helps you quickly detect any attacks or intrusions in your system. Attack detection solutions use various techniques such as behavioral analysis and machine learning to identify malicious activity.

04

Cloud Access Security Brokers (CASBs)

CASBs provide visibility and control over how users access the cloud. They can help you enforce security policies for both sanctioned and unsanctioned cloud services. CASBs can also help you with data loss prevention and compliance reporting.

05

Encryption

Encryption is one of the most important tools for protecting data in the cloud. It helps ensure that even if your data is stolen, it cannot be read without the proper encryption key. Encryption can be used at rest (i.e. when your data is stored on disk) or in transit (i.e. when it is being transmitted over the network).

Steps and Guide

Your cloud journey is guided by your cloud security plan. Creating a plan gives your company the opportunity to set its cloud security program on track, address risks and achieve its corporate goals.

It is assumed that you already have a thorough security plan in place, of which the cloud security plan is a subset, that addresses the risks posed by the entire business. Your strategy should take into account areas both inside and outside of the cloud where you can have a significant impact and reduce risk unless you are a native cloud shop or have already migrated all of your workloads to the cloud.

Define your organisation's needs

Before you can begin to create a cloud security policy, you need to understand your organisation's needs. What data do you need to protect? What are your biggest concerns when it comes to cloud security? Understanding these things will help you determine the best way to protect your data.

Assess the risks

Once you understand your organisation's needs, you need to assess the risks associated with using the cloud. What are the potential threats? What could go wrong? Understanding the risks will help you determine what measures need to be taken to protect your data.

Create a plan

Once you understand the risks, you need to create a plan on how to address them. This plan should include specific steps that need to be taken and should be tailored to your organisation's needs.

> And I hope I don't have to emphasise the importance of security professionals being involved in the DEV cycle; "security that is built-in, not bolted-on" has literally been the motto of every single industry event I've attended in recent years, and we've all been bombarded with buzzwords like "DEVSECOPS" for quite some time now.
>
> -Andy Jassy, CEO of Amazon

The primary goal of a security strategy is to address risks; therefore, keep the risk-based approach at the forefront of your program and constantly re-evaluate your priorities.

Implement the plan

Once the plan is created, it needs to be implemented. This means putting into place all of the measures that have been outlined in order to protect your data.

Monitor and adjust as needed

Security is never static - it needs to be constantly monitored and adjusted as needed. The cloud is constantly evolving, so your security strategy must evolve with it. This means regularly evaluating your policy and making changes as needed.

Educate employees

One of the most important components of any security strategy is education. Employees must be made aware of the dangers associated with using the cloud and what they can do to help protect the organisation's data.

Cloud security is a joint effort between you and your cloud provider. To create a cloud security strategy that will protect your organisation, you must first understand where the provider's responsibility ends and yours begins.

How to Strengthen Workload Security

Implement a strong identity foundation

Implement a centralised identity and access management system based on the principles of least privilege and separation of duties to eliminate reliance on long-term static credentials.

Allow for traceability

Enable real-time monitoring and alerting of critical actions and changes in your environment. Use systems that integrate log and metric collection to investigate and act automatically.

Implement security at all levels

Apply a defence-in-depth approach with multiple security controls. Use on all layers such as the edge of the network, Virtual Private Cloud (VPC),load balancing, every instance and compute service, operating system, application and code.

Automate security best practices

Software-based security mechanisms that are automated improve your ability to securely scale more quickly and cost-effectively.

Safeguard data in transit

Sort your data into sensitivity levels and use mechanisms like encryption, tokenisation and access control as needed.

Keep data away from people

Use mechanisms and tools (also known as "infrastructure as code") to reduce or eliminate the need for direct data access or manual data processing.

Prepare for security incidents

Prepare for an incident by establishing incident management and investigation policies and processes that are in line with your organisation's needs.

Protect the cloud by using cloud encryption

Cloud encryption is a technology that helps keep data safe when it is stored in the cloud. It works by encrypting the data before it is uploaded to the cloud and then decrypting it when it is needed. This helps to protect it from unauthorised access and makes it difficult for anyone to hack into.

Cloud encryption is particularly important for businesses that store confidential information in the cloud. By encrypting data, businesses can protect against data breaches and deter hackers from gaining access to sensitive information. In addition, cloud encryption can help businesses meet compliance requirements, such as Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA).

There are many different encryption algorithms available, but Advanced Encryption Standard (AES) is a good choice for encrypting data in the cloud. AES is a strong encryption algorithm that is widely used and supported. It can be used to encrypt data at rest (stored in the cloud) or in transit (sent over the network).

Investment in training

The shift to cloud infrastructure providers is unsurprising given the advantages of increased scalability and flexibility of deployment, as well as a more appealing pay-as-you-go pricing model versus on-premises deployments. As a result, businesses are increasingly looking for employees who can manage and secure this new type of infrastructure. There are many companies that provide training in this sector and Amazon Web Services (AWS) is one of them. AWS offers a comprehensive set of training courses to help you stay up to date on the latest threats and vulnerabilities.

The AWS Security Training and Certification provides you with the skills and knowledge you need to protect your data and applications in the cloud. The courses cover a wide range of topics, from identity and access management to data encryption. You'll learn how to secure your AWS infrastructure, identify and prevent attacks, and respond effectively to security incidents.

Practice makes perfect

The way you respond to security incidents is perhaps the most important aspect of your cloud security strategy. Run incident response simulations and use automated tools to improve the speed of detection, investigation and recovery. Your preparation has a significant impact on your team's ability to operate effectively during an incident, isolate and contain issues, and restore operations to a known good state. Having the tools and access in place before a security incident, and then routinely practising incident response through game days, helps ensure that you can recover while minimising business disruption.

AWS privacy

AWS Privacy Training helps you understand the regulations surrounding data privacy, including the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). In this training you'll learn how to comply with these laws, as well as how to protect your customers' data. The courses cover topics such as data classification, data retention and incident response.

How to Protect Businesses from Threats

Methods	Solutions and benefits
Role-based access control	Provides granular control over who has access to what data and applications. This means that businesses can restrict access to only those individuals who need it, making it much more difficult for unauthorised individuals to gain access to sensitive data.
Network security groups	Allows businesses to create groups of virtual machines (VMs) that can communicate with each other, making it easy to segment networks and isolate potential threats.
Storage encryption	Utilise storage encryption for both data at rest and data in transit, helping to protect information from being accessed by unauthorised individuals.
Application gateway application firewall	The web application firewall helps protect web applications from various attacks, including Structured Query Language (SQL) injection and cross-site scripting (XSS).
DDoS protection	Using a Distributed Denial of Service (DDoS) protection service helps protect against attacks that seek to overload systems with traffic in an attempt to disable them.
Threat management	Using threat management services helps identify and mitigate threats before they can do damage. The service uses a variety of techniques, including machine learning, behavioural analytics and telemetry analysis.
Regular updates	Regularly update your security features in response to new threats and customer feedback. This means that you can be confident that your environment is always up to date with the latest security protections.

Challenges SMEs face with their Cloud Security Strategy

In addition to traditional cyber security threats, COVID-19 has introduced some fresh problems over the past few years. For many SMEs, 2022 has been a particularly disruptive year due to the widespread adoption of permanent hybrid and remote work arrangements, as well as rapid infrastructure development. Here are the top five security issues that SMEs have had to deal with in 2022 as we draw to a close.

01

Inadequate staff training and awareness

Staff members are frequently a small business' greatest asset, but they may also be its weakest defence. This is hardly surprising considering the difficulties SMEs have had in implementing efficient security training. Since most successful attacks use social engineering, the transition to remote working has further underlined the urgent need for SMEs to train personnel in secure home-working practices. In 2023 and beyond, SMEs are anticipated to continue to fall short in terms of giving staff members access to sufficient security training materials.

BLACKPANDA

According to Blackpanda, less than 30% of SMEs indicated that they offer data safety and best practices training, proving that promoting security training and awareness continues to be difficult for SMEs.

02

Rise in sophisticated ransomware attacks

This year, the encryption-based software known as ransomware continued to terrorise businesses, and attacks are expected to rise even further in 2022. Smaller firms are also more likely than larger firms to pay ransoms to have their data decrypted because they often do not back up their data. However, Ransomware 2.0, as it has been dubbed, has rendered the backup of data useless because it not only encrypts the data but also threatens to make it public if the ransom is not paid. Although it's unclear whether the prevalence of Ransomware 2.0 attacks will change the willingness of companies to pay, protecting against this kind of attack should be a top priority for all SMEs.

According to Blackpanda, ransomware continues to be a particular problem for smaller businesses compared to their larger counterparts, with 60% of assaults occurring against organisations with fewer than 100 employees.

03

Lack of dedicated resources

While COVID-19 has tightened spending for many companies, a Kaspersky analysis [2] shows that since 2021, the average SME's IT budget has seen a small 3% growth in security spending. Blackpanda has witnessed this, with organisations increasingly willing to invest more to enhance their security level by purchasing firewalls, Endpoint Detection Response (EDR) solutions, email gateways, and so on.

However, the rising demand for cybersecurity professionals, who are in short supply and are commanding commensurate salaries, may mean that this is insufficient.

Many SMEs simply lack the funds necessary to recruit personnel for specific cyber security jobs. In Blackpanda's experience, less than 5% of SMEs have a full-time cyber security employee. Smaller companies are still at a disadvantage as a result, making them easy prey for cybercriminals who are well aware of the issues SMEs frequently encounter.

kaspersky

A Kaspersky analysis shows that since 2021, the average SME's IT budget has seen a small 3% growth in security spending.

04

Device administration shortcomings

Bring your own device (BYOD) is becoming more popular, and in some situations, remote workers are being compelled to switch to personal devices, which has made device administration a complete mess. Many SMEs have chosen cloud-based endpoint management solutions to fill the gap; nevertheless, endpoint management systems have inherent limits when remotely managing devices with different operating systems.

The protection provided by their corporate network to office-based personnel has also been taken away by remote working, leaving them dependent on the fundamental security measures of their home office network. Many employees won't have access to sophisticated firewalls and web proxy tools, leaving them more vulnerable to outside threats while using their devices in an office setting. We are likely to observe that many SMEs have not yet implemented a successful remote administration plan as 2023 approaches.

05

Absent information management framework

The implementation of GDPR in 2021 ushered in a period of increased data awareness. The EU Commission did, however, say in a study [3] released in July that "implementation of the GDPR is problematic, especially for small and medium-sized firms." The International Organization for Standardization (ISO) 27001 standard for information management and security, which is often regarded as the gold standard, is still out of reach for many smaller firms.

SMEs are confronted with significant challenges when implementing an information management strategy, including trying to identify information assets efficiently and keeping track of personnel access levels. Alternative programmes, such as the Information Assurance for Small and Medium Enterprises Consortium (IASME) Governance programme in the UK, have been developed to aid SMEs in improving their information management processes.

Despite this, as we approach 2023, many SMEs will still face difficulties with information management and security.

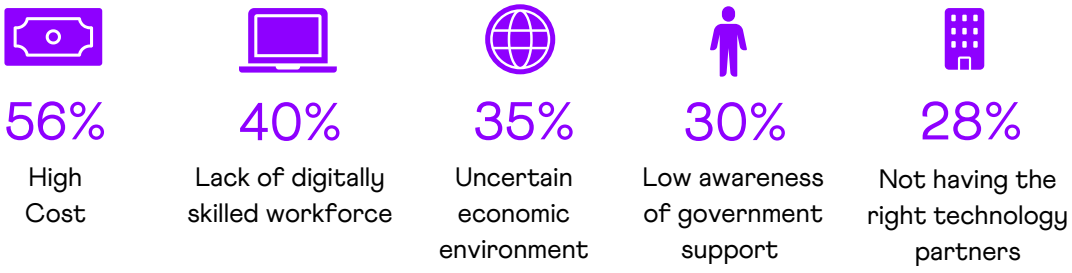
A study released in July says that "implementation of the GDPR is problematic, especially for small and medium-sized firms."

Local stats about SMEs in relation to Cloud

Even though 83% of Singapore's SMEs had digital transformation strategies in place, more than half (54%) said that COVID-19 delays had an impact on their digitalisation efforts. Additionally, just 2 in 5 SMEs believe their efforts to implement digital transformation have been successful, despite the greater adoption rate.

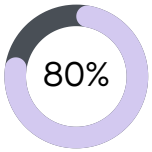
In a separate research [4] released by Microsoft and International Data Corporation (IDC) Asia Pacific, it was found that 73% of Singapore organisations, both mid-sized and large-sized, have sped up their digitalisation in reaction to the pandemic. In contrast, the Association of Small & Medium Enterprises (ASME)-Microsoft study discovered that only 30% of SMEs claimed that COVID-19 forced them to digitalise, with the majority citing delays in their plans. Additionally, more than 80% of SMEs said that COVID-19's global border control restrictions have caused them to postpone their plans for internationalisation (overseas expansion).

SMEs have had their digitalisation and internationalisation plans delayed by COVID-19 [5]

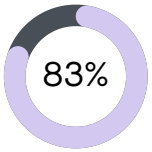


Barriers faced by SMEs in their digital transformation journeys are exacerbated by COVID-19

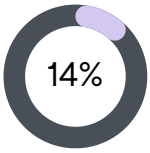
The study found that most participants were unaware of government programmes and initiatives that are accessible to SMEs, including the Productivity Solutions Grant [6] and the Start Digital Pack [7]. Nevertheless, it was discovered that more than 3 in 5 SMEs would be eager to make use of these subsidies and schemes to assist digital transformation in the upcoming year, despite the low levels of knowledge of such initiatives. Larger enterprises also frequently benefit from current government assistance, with medium and medium-large corporations reporting [8] that they are more likely to find government assistance valuable (60% and 73% respectively).



Aware of digital transformation



Now have strategies in place for digital transformation



Increase in adoption of more advanced technologies

But only

2 out of 5

companies perceive their efforts to be successful

Awareness and adoption of digital transformation have increased significantly among SMEs [9]

When the pandemic struck, many SMEs in Singapore struggled to stay afloat as their businesses took a hit. Survival became a priority for these smaller companies as they grappled with rising costs and falling revenue, and naturally, digital transformation may have taken a backseat. When providing support to businesses impacted by COVID-19, it is important to consider the unique challenges faced by SMEs in order to identify areas where the government, corporates, or industry associations can support them in digitally transforming during this time.

- Mr Vivek Chatrath
Small, Medium and Corporate Lead
Microsoft Singapore

It is encouraging to see that majority of Singapore SMEs are aware of digital transformation and have adopted some form of digital technology since 2018. However, digital transformation calls for more than just updating technology or adopting a new platform – it is never about tech for tech's sake. Success and value derived from digital transformation can only be achieved if these strategies are clearly aligned with SMEs' business objectives. Factors such as workforce skills also play a pivotal role in ensuring the success of digital initiatives in any firm, hence the need for SMEs to build competencies in areas such as data analytics. As data from the study suggests, more guidance can be offered to SMEs to help them strategise, upskill and properly leverage government grants to harness the full suite of benefits from digital transformation.

- Ms Irene Boey
Vice President
Membership & Training, ASME.

Cloud Incident Response

Over 85% of organisations will adopt a cloud-first principle [10] by 2025 and cannot fully execute their digital strategies without it. By 2025, over 95% of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021.

Since the transition from on-premises to cloud computing over a decade ago, incident response has changed drastically.

Nowadays, business networks typically consist of a combined cloud infrastructure from a number of cloud providers, including SaaS and PaaS. There are many challenges related to this, including data volume, accessibility, and the rapid evolution of threats.

This year alone, 27% of businesses experienced a cyber attack on their cloud environment, according to CheckPoint [11]. In order to stay in business, organisations that adopt a cloud-first approach need to keep themselves prepared in case of critical, service-disrupting incidents. With cyber attackers increasingly targeting the cloud, organisations should prepare themselves to respond to this type of cyber breaches.

Cloud Ransomware

Cloud ransomware, which was previously extremely rare, is now growing in frequency.

Traditional ransomware cannot attack Application Programming Interface (API)-based cloud storage systems, as these do not have access to file systems. As a result, threat actors are developing new Tactics, Techniques, and Procedures (TTPs) to launch ransomware attacks more easily in cloud environments. These are highly challenging to predict, which is why only the most experienced incident responders are able to anticipate what these TTPs might entail in order to best prepare for and respond to them.

In order to encrypt persistent data in cloud resources, cloud ransomware actors are likely to use cloud APIs to find and access cloud resources that contain persistent data.

A threat actor may target specific cloud services based on the APIs for accessing them, or they may develop different payloads for each targeted service (just like some traditional ransomware actors have previously developed different payloads targeting different operating systems).

> Last year, the average ransomware demand was USD 2.2 million, according to Palo Alto Networks [12], and as attackers start targeting the cloud, this is only predicted to rise.

Cloud Incident Response Process

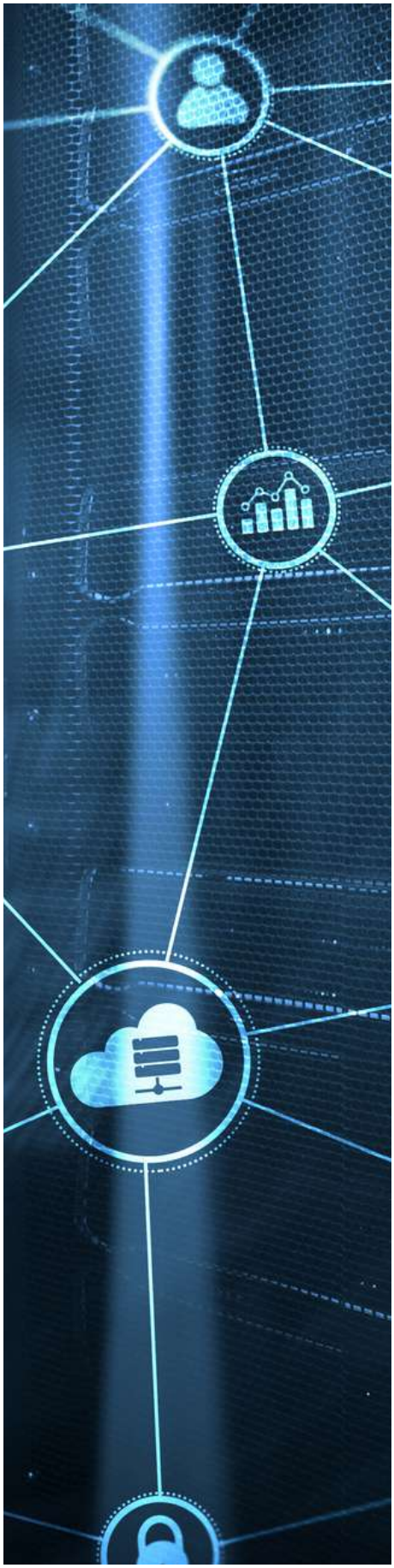
As cloud workloads rapidly evolve, organisations require specialised incident responders, who have a deep understanding of cloud security, investigations, and specialised tools and processes.

By engaging an experienced team of cloud incident responders, organisations can cut down the dwell time of cyber attacks – that is the time between the start of an attack and when it is eradicated, comply with legal requirements, ensure business continuity, and limit the damages that such breaches may cause. This way, having a cloud incident response strategy helps organisations deliver their cloud-based services and products reliably and efficiently.

Cloud incident response involves the alignment of critical resources, operations, and services necessary to manage incidents within a cloud infrastructure. Knowing who to contact in case of a cloud cyber attack, and having a comprehensive cloud incident response plan allow cloud technicians to quickly restore the operations of a downed service.

Conducting frequent compromise assessments is also vital to ensuring cloud cyber security. By detecting and containing malware through proactive threat hunting, organisations can limit their impact on electronic data and valuable networks, and eradicate cyber incidents prior to their escalation into full-blown cyber crises.

Key Attack on a Cloud Infrastructure



Here is a Blackpanda case study of a possible cloud cyber attack, whereby a cyber criminal creates a master key that allows them to access cloud accounts.

Using the Communications Service Provider (CSP)'s key management services, an attacker creates a master key that is controlled by the attacker if data encryption is done in the public cloud. Depending on the situation, the key can be created in the victim's cloud environment or in the attacker's cloud environment. To access cloud resources in one account from another, an attacker must also have "cross-account" permission.

The attacker then attempts to encrypt the victim's cloud resources using the attacker-controlled key. Once a cloud resource has been created, an attacker can change the encryption keys for data at rest, and the existing data will automatically be re-encrypted. In some cases, however, it may not be possible to change data-at-rest encryption keys after cloud resources have been created.

In this case, the attacker would encrypt the data using the key controlled by them and overwrite the original data with the decrypted dump, including snapshots.

Lastly, the attacker hides the keys from the victims or the CSP. The raw key material can be then used by the attacker to reconstruct encryption keys, and these might be removed from cloud environments by an attacker and stored locally.

A solid cloud incident response strategy should cover preparation, identification, containment, eradication, recovery, and lessons learnt.

Cloud Incident Response Strategy

01

Preparation

This stage is critical, and much effort should be put in to ensure the organisation is as prepared as possible.

Some (non-exhaustive) questions to consider:

- What elements comprise your security infrastructure?
- Who is in your response team?
- Who are the decision-makers?
- Do you need experts in Media, Legal, Human Resources (HR), or Information Technology (IT) Systems?
- Do you have reporting obligations to external authorities? If so, who will liaise with them and when?
- Do you have adequate internal skills or do you need trusted partners to assist?
- Are you capable of capturing evidence for use in potential criminal or civil proceedings?

When developing incident response plans in cloud environments, a key first step that the incident response team works on is asset prioritisation. This includes listing not just critical assets but also systems, networks, servers, and applications. Then, the responders start observing the traffic patterns for these assets with the help of Endpoint Detection and Response (EDR). This helps in determining the norm and being aware of any discrepancies.

As with traditional incident response, the next step is to set up appropriate policies and standards to follow in different situations such as network access, login guidelines, use of strong passwords, file sharing, as well as email and other platform access.

Strategising on how to manage the different types of cases and incidents involves ranking each possible event based on priority, severity, and organisational impact; providing notes on each event, specifying how it can be solved, what steps to take to remediate it, and what tools to use if any.

Setting up a communication plan among all stakeholders involved is also important. This involves assigning responsibilities among individual contact persons, what form of communication to use, when they should be contacted and during which kinds of incidents.

02 Identification

A cloud environment will host millions of “events”, such as system log-ons, software updates, network connections established, and more. Most of these events will be normal behaviour for your environment.

It is important to be able to identify the events that are unauthorised or have an adverse impact on your systems and business. These are what we commonly call incidents.

In order to prevent incidents from happening, regular and strict monitoring must be observed. This helps in detecting and reporting any anomalies or potential security risks. Monitoring security events include a constant review of log files, error messages, intrusion detection systems and firewalls.

At the onset of an attack, identifying the root cause of the breach is and should be the main objective. This includes finding out who, what, when, where, and how it happened. Check from different entry points and indicators including user accounts, system administrators, network administrators, Security Information and Event Management (SIEM), and logs.

Alert and report the incident to the proper authority by submitting an incident ticket. Classify the incident based on the provided incident types. Analyse and record the extent of the event, especially its damage/s to the systems.

03 Containment

The essential focus of incident response is to contain the damage, eradicate all threats and restore all systems back online.

Part of containing the damage is to ensure that the incident will not escalate further. This includes isolating the infected accounts, servers, or networks from the rest of the environment; backing up files and systems, and temporarily repairing any damaged material. Aside from these, it is important to keep all evidence safe from destruction.

Note that managing containment can be tricky as many stakeholders may be affected and certain efforts may even tip off the attackers that you are aware of their actions. As such, decision-makers need to be informed and empowered. Consideration must be given to balancing the risk of continuing normal operations with the actions required to mitigate the threat.

04 Eradication

Following Identification and Containment, there should be enough information to determine the root cause of the incident and how to best disrupt the attacker and remove them from your environment.

The priority is to neutralise and remove all threats, including malicious activities and contents. Consider conducting a complete reimaging of the system's hard drive to safeguard it from subsequent attacks.

05 Recovery

Any affected cloud systems or platforms will need to be restored to proper working order following an incident. Examine any connected or related systems to ensure they are operating as normal with no signs of compromise.

Security professionals must coordinate these efforts with the business and operations teams to minimise disruption and maximise efficiency. Lastly, recovery requires establishing more sophisticated monitoring and detection techniques for combating future threats.

06 Lesson learnt/post-incident activity

This final step involves the assessment of the entire incident, from how it was prepared for, managed, and addressed. While many firms regrettably skip this process, it is absolutely essential to recognise your victories and failures during the entire process.

Systematic reflection highlights areas for sustainment and improvement for the future. This final step will serve as training, from which you are able to update your current incident response plan and the list of incidents you have already encountered.

What did the organisation and stakeholders learn from this incident? Could the incident have been prevented? Was it handled correctly? Do we have the right people and resources to detect and manage such incidents in the future?

During this step, incident responders prepare briefings for the board, shareholders, and reporting agencies where required, and suggest ways to train employees to be more cyber aware.

In Conclusion

Fighting fires is not a strategy.

A well-defined cloud security strategy can help your organisation avoid overspending or underspending on cloud security controls.

Is it possible to be secure without a security strategy?

Sure, but your security activities may not be aligned with your organisation's strategic business outcomes, requiring a significant amount of time and money to rectify.

Resources

[1] 3 million cybersecurity
https://cybersecurityventures.com/jobs/

[2] Kaspersky analysis
https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_IT%20Security%20Economics%202020_Executive%20Summary.pdf

[3] Study
https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf

[4] Research
https://news.microsoft.com/en-sg/2020/09/10/culture-of-innovation/

[5] Digitalisation and internationalisation plans delayed by COVID-19
https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever

[6] Productivity Solutions Grant
https://govassist.gobusiness.gov.sg/productivity-solutions-grant/

[7] Start Digital Pack
https://www.imda.gov.sg/programme-listing/smes-go-digital/start-digital-pack

[8] Reporting
https://news.microsoft.com/en-sg/2020/10/22/over-80-of-singapore-smes-embrace-digital-transformation-more-than-half-report-slowdowns-due-to-covid-19-asme-microsoft-study-2020/#_ftn2

[9] Microsoft's SME Digital Transformation Study
https://news.microsoft.com/wp-content/uploads/prod/sites/439/2020/10/2020-SME-Digital-Transformation-Study-by-Microsoft-and-ASME-Infographic.pdf

[10] Cloud-computing adoption
https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

[11] Checkpoint
https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/the-biggest-cloud-security-challenges-in-2022/

[12] Palo Alto Networks
https://unit42.paloaltonetworks.com/ransomware-in-public-clouds/