Cloud Security TABA

*Note: Sub-titles are not captured in Xplore and should not be used

Simon Lowry
x21168938
MSCCYBE_JANOL_O
National College of Ireland

I. Question 1

Disaster recovery plans are a necessity for most organisations to sustain the high availability and security of their services & data and ensuring the organisation remains resilient. Natural disasters such as floods, earthquakes, wars or even volcanic eruptions can partially or completely incapacitated data centres. A good example of this is the Northeast Blackout of 2003, which led to over 50 million people in the United States covering 8 US states and one Canadian province. [30] As such, careful consideration and planning must go into implementing the disaster recovery plan in order to be able to respond effectively. No major business can do without one these days to ensure major reputational and financial damage doesn't occur from not having one. The disaster recovery plans for this report will be centered around the RPO and RTO provided as a baseline of expected requirements. The fact that the service level agreements are looking to hit targets of 15 minutes and 1 hour implies that the company is looking to be aggressive on maintaining high availability and ability to recover extremely fast to maintain resiliency.

This is required not only for mission critical applications but also for non-critical applications. Usually it would only be for the mission critical applications getting greater priority and needing a faster recovery but in this case, this will require a lot of investment from the company to match these goals. This would effectively require a hot site for the RPO aspects and perhaps a warm to site approach for the relevant components to the RTO. Having a 15 minute indicates that the company has a low tolerance for losing data and having as close to up to date as possible may well be central to their functioning as an organisation. Requiring a recovery time objective of only 1 hour shows that the company does not want to have their applications and systems back up and running in an hour again highlights that the company can't afford to be down. This may well be a fear of losing revenue, customer trust and damaging reputation. As mentioned this will be both resource intensive and expensive.

While this RPO and RTO doesn't include indications on how regular this hour of outage occurs. Looking for a cloud provider who can match either 3 or 4 9's of uptime (99.99% or 99.999%) would escalate high availability into the upper echelons of what's possible. Some cloud providers which include 3 9's (99.9% uptime) are Amazon, Google and Microsoft. Offerings such as AWS provide multi-site active/active disaster recovery. This would be the maximal kind of offering a single cloud provider seems to have available. It contends that there would be zero downtime, near zero data loss, and mission critical services sustaining their availability. As mentioned this could be extremely costly over time. In order to mitigate against this particular potentially excessive operational expenditure, other options could also be in their active/passive category. Their warm standby is always running but smaller in terms of environments. It's recovery is deemed to be in minutes

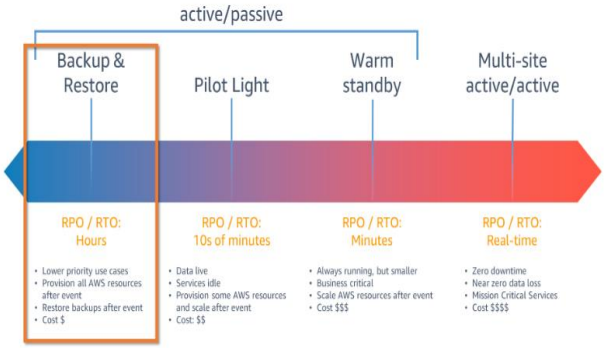


Figure 1. DR strategies

[31] The other alternative gets everything back up and running within 10's of minutes and is called Pilot Light. The Warm Standby option may well be the most appropriate here to hit the 15 minutes RPO and 1 hour RPO objectives and still save some cash relative to the multi-site active/active approach.

In the event that the RPO is not 0 minutes, having data which is out of date potentially by 15 minutes (if our aims are achieved), could result in some modifications, insertions and deletion of data being out of sync with the actual reality prior to the disaster. This may well come at the cost of the integrity of such data being diminished and customer grievances as a result of this and have a knock on effect on them. This may well be not acceptable to customers if this is data related to financial transactions for example which involve large quantities of cash and could lose customers.

As such, the frequency of backups would need to be highly frequent for databases and having a warm running databases ought to be of high priority. Backups ought to be stored in multiple regions as well to increase availability. Differential backups ought to be in operation and occurring frequently. These are smaller and quicker than the full backup options, only backing up what has changed since the last backup. They are good for our scenario where downtime is aimed to be minimal and rapid restores vital. It's also good for data loss protections as well. [32] The shift from replication mode to failover mode would need to be as seamless as possible. A secondary benefit of having these backups in place is also in the event of ransomware attacks occurring. Having backups in place can return the operations to running states and neutralise this kind of threat. Replication latency is an important consideration here as the Round Trip Time (RTT) ought to

again that into account our main objectives for RPO and RTO. Selecting the wrong setup could render this not possible. [33]

The use of Synchronized replication here may be the way to achieve our aims here as it increases the likelihood of meeting our RPO and RTO requirements. The drawback here is that it again would cost more and may have some impact on performance. The alternative asynchronous replication would cost less but would not meet our goals and thus would not be the optimal solution here.

On top of this, the company ought to be using a secondary cloud provider as well. In the event that renders a cloud provider unable to perform its duties due to a fatal disaster, failovers. This kind of failure can create a lack of redundancy and be an issue for sole reliance on a single CSP. Mitigations ought to be able to get to an active setup on another cloud provider. Contractual agreements would want to be in place, and have the tools, networks, and identity and access management infrastructure in place for such an occurrence. Data management will be an important consideration in terms of transferring it from CSP to another. It ought to be done securely with TLS and its latest version and the ability of the alternative CSP to be able to handle the data types is also a consideration that must be taken into account. Valid certificates must be checked to ensure the CSP is who they claim they are. The data formats must be able to coexist with each other or a transformation ought to occur to meet the other data types of the secondary CSP. The time taken for this transformation still needs to be in line with meeting our objectives otherwise this would not be a suitable CSP for our purposes. Integrity checks of data transported and translated must also take place to ensure the data's integrity has been sustained. Failure to adequately protect data and take the proper precautions can result in GDPR fines depending on the location of that data. Data must be encrypted at rest as well by both CSPs with industry standard cryptographic algorithms and using effective key management solutions.

For IAM, the use of federated identity management can be helpful for disaster recovery. Trust can be established and configured for multiple domains. It may well include setting this up to operate over separate CSPs as well. The identity information can be stored in a non-centralized location and independent of the cloud environments meaning in the event of a particular data centres going down or even CSPs, the same credentials could be sustained as a means of authentication and not be affected by the outage. This is due to the identity information being stored by separate individual organisations, this may be the customers storing them, themselves or other setups like using azure active directory or some company like Daimler for example as the sign on, for example. Here protocols such as OAuth can come into play and the identity provider can verify the identity of credentials and provide a federated token in exchange. These can be encrypted with digital signatures to ensure they have not been tampered with and contain both identity information and also authorisation privileges as well. This can help to ensure authentication and authorisation is sustained across multiple sites, and multiple CSPs and thus an important facet of security maintained in the event of a disaster occurring.

Another consideration is that staff ought to be trained on both CSPs systems and capable of making that shift over. Especially in this case where there is little room for any downtime or loss of data, there would otherwise be no time to perform that training after the fact and could otherwise lead to increased risk of not meeting the SLAs. Some security principles ought to be applied to the staff like separation of duties to prevent any individual from having too much power and least privilege which enforces that a given employee only has the necessary privileges to perform their duties and no more. Access to backups as well as live data, ought not to be allowed, the same for particular assets like data and servers. The ability to perform those backups and view them with read only permissions and without deletion could be set up.

Another aspect of this disaster recovery plan is the detection of the disaster occurring. This can be done through logging and alerting. Detection of these disasters is crucial to achieving our RTO and RPO objectives. Ensuring that there is enough logging and tools in place that trigger events and alarms based on those events occurring. Tools from AWS can help here like CloudWatch which can trigger alarms when specific thresholds have been hit. This may well be configuring alarms for multiple systems going down, automation should kick this into switching to other regions and multi-regions setups ought to be employed in general on each cloud provider as well. These events being triggered could launch some automation in place to begin the full operations of the secondary cloud provider and can allow staff to know what's happening and at this point they can follow a playbook for how these changeovers would occur. Personal Health Dashboard of AWS can also help to show alerts which could be impacting on us as well. [31] Networking also must be sustained across the backup site as well. This includes subnets, firewalls, IDS/IPS systems, application firewalls, load balancers and all the rest of the networking apparatus required for the operation of the environment and maintaining it's security. The necessary compute power as well as storage space must be available. On top of that the structures and applications that are required to keep those in operations whether it be Devop pipelines or Key management systems.

Testing of the disaster recovery plan in action ought to take place as well. This could potentially first occur in a dry run phase on test systems to get some practice in for the team and have some muscle memory built up for how they need to act in those situations. Then moving onto fake triggering of the alerts on production systems and carrying out all actions to try and restore the systems to the original state while ensuring that the backup options are functioning as expected and the level of performance is meeting required standards.

II. Question 2

This report is considering and comparing the capabilities of AWS's Key Management Service and CloudHSM versus Microsoft's Key Vault. Confidentiality is one part of the CIA triad of security, and encryption is a core aspect of how this is performed in modern systems and applications. To paraphrase Kerckoff's principle a cryptosystem should be secure if everything about the system, except the key, is public knowledge. Protecting the keys for the full lifecycle of their use and destruction is paramount to protecting the data they have helped secure. Applying secure algorithms which are industry standard matters and so does the protection of the keys throughout their lifecycle. Even with the most advanced cryptographic algorithms being applied, if the key is found that very sophistication may well be undone. Key management solutions are also a single point of failure so they

need to be robust enough to be highly available and also secure.

AWS KMS allows you to create, manage and control cryptographic keys throughout your applications and services that you operate in AWS. They can be used for cryptographic operations such as encrypting and decrypting data, singing and verifying, generating and exporting of data keys and also for the generation and verification of MACs and also to generate random numbers for cryptographic applications. KMS is integrated with Amazon EC2, Amazon S3 and Amazon EBS to name a few services. It offers automated monitoring via AWS Cloud Trail and Amazon Cloudwatch so that we're able to see what individual used which keys, and on what resources as well as when this has happened. These can also trigger alerts as well at our discretion and selection.

KMS keys rely on a spread of FIPS 140-2 Security Level-2-validated hardware security modules(HSMs). Each of these HSMS has their hardware appliance Some of the more advanced features include multi region keys can pose as the same key in different AWS regions. They can also go and place the KMS keys in AWS CloudHSM key store or in an external key store. AWS KMS can also be connected to via a private endpoint in your VPC offering protection for it. It offers fine grained policies as well on accessing the various keys. AWS key management service is part of a variety of AWS compliance programs and these include HIPAA, PCI SOC and FedRamp. [23]

Some of the main features of Microsoft's Key Vault is that they can create and import encryption keys in minutes, they can increase security and control over keys, passwords, tokens, certificates and API keys. Applications do not have any access directly to the keys. They use both FIPS-2 Level 2 hardware security modules. They can help for automating tasks for SSL/TLS certificates and reduce latency with cloud scale and global redundancy. [24] Key vault only provides support for Elliptic Curve keys and RSA. [25] It also offers logging and monitoring and IAM authentication for users and groups.

One of the most common uses cases in Azure is building IaaS infrastructure. virtual machines with disks. disks will contain operating systems and application data. All of the information on the disk is encrypted in case the event occurs whereby someone were to get access to the disk and this prevents it from being obtained. Typically this is done with an Azure VM key. All disks in Azure are encrypted by default. the users can provide their own keys to both encrypt and decrypt the virtual drives. Another example for when data is stored with Keyvault is when you have an application which is connecting to a database. The data that is from the config file like the database address, the database username and password being used by the application, this kind of information is typically application secrets and this kind of data can help with storing and secure management of those secrets for our applications. They allow you to integrate Azure Key Vault without a single line of code. Certificates can be used for securing encrypted traffic and for authentication for a given site. As mentioned Key Vault can also store these.

Both Amazon and Microsoft, you have the principle of a master key. They are protected by the key management service and never exposed outside of this. in aws kms, these are symmetric keys, aes 256 bit keys, meaning they are encrypted and decrypted with the same key. In Microsoft Azure in contrast the master key are a set of asymmetric keys. The private key is used to do the decryption and the public key is used to encrypt. These master keys in both azure and aws are used to encrypt the data keys whether it be used in a software application or in an IaaS Vm. The AWS KMS generates the keys for the users or a system. They will automatically also rotate the keys for you periodically.

With KeyVault, in contrast, you generate your own data key, encrypt your data with it and then you encrypt your data key with a public key which has been provided by azure KeyVault. Azure has no knowledge of which data keys have been encrypted or decrypted. This means of managing keys falls on the user or service and the rotation, deletion and lifecycle as well is not carried out by KeyVault. You can do asymmetric encryption with digital signatures on KMS but it's not the primary way they encrypt keys. You can't do asymmetric encryption with KeyVault but you can, as mentioned store individual secrets there. This ought to be considered for which use case matches the given scenario best and how valuable this for the organisation and possibly in relation to some compliance frameworks they are looking to meet or adhere to. On top of that it ought to be considered how much you want to be in control of this key management process, are there going to be a lot of keys to manage, does it make sense to handle that ourselves or to have that taken care of by the key management service.

Some pros of AWS KMS is it's reliability through it's availability citing it's uptime as an important factor for managing their data security. It's robust with key rotation occurring, and less maintenance required therefore when it is setup. No missed dates of changing keys which decreases the window of opportunity for attackers. The data in KMS is also protected well with it also being encrypted itself. Easily able to make changes to whom has access to certain keys reducing the likelihood of too much privilege being afforded. Some drawbacks of KMS is that it can have a steep learning curve for a beginner and it's not intuitive and may require a number of video tutorials to get up to speed. This also brings with it some security risk, as efforts to rush this process could lead to inadvertent exposures and misconfigurations. Many users also were dissatisfied with the per key pricing model which didn't work that well for larger companies. Some found the API's were cumbersome to use, in particular with the Python SDKS. [26] Another downside would be less control over the key management process which may be important for certain compliance programs as mentioned.

Some pros of Azure Key Vault is that it's seen as simple and easy to use as one of it's best features. It provides customers with efficient key management and high volume data storage. It doesn't require a vast amount of technical knowledge to get value from it. It's security features were also seen as a plus with no accidental leakages as well as effective IAM and role based access control applied. The level of encryption and API support, as well as version control was seen as really positive. It's also seen as having high availability, being cost effective and scalable. Some cons observed where the lack of search function and not the most intuitive UI experience. The authentication process can also be a bit more hectic and complicated in particular with certificate authentication. It also lacks features like certificate expiry notifications or versioning. [27]

In conclusion, both offer an array of functionality which are similar on some aspects like with logging, auditing, high availability. Key Vault appears to have the edge when it comes to being easier to setup and require less technical knowledge whereas KMS has the benefits of not requiring the management of keys or key rotation. It seems to have more features than Key Vault overall. So ultimately, the right choice would be constrained to the best use case for a given scenario and ought to be considered in relation to the requirements and capacities of the individuals who will be both setting them up and managing them and the use cases where they will be applied.

III. QUESITON 3

Before you begin to format your paper, first write and save the content as a separate text file. Complete all content and organizational editing before formatting. Please note sections A-D below for more information on proofreading, spelling and grammar.

The three cyber security attacks that will be discussed in this section involve Medibank and their ransomware attack, the supply chain attack aimed at Veeam and finally, Twitter's breach. Medibank is a health insurance giant originally stemming from Australia and incurred a major cyberscurity breach recently. Medibank was hit initially with a ransomware attack that subsequently led to multiple releases of sensitive information being posted. The initial breach date is not known but Medibank did eventually geta security alert on the 11th of October 2022. They then looked to close down the attackers persistence and subsequently they believe there has been no further action taken since the 12th of October 2022. [13]

The attackers were looking for a $10 million dollar ransom which was later reduced to $9.7 million dollars which represented $1 dollar for every customer they had stolen data for. The means of getting into Medibank was via the stolen credentials of a high level access individual within the company. They may have been stolen via phishing or spear phishing, the exact method the credentials were obtained is unknown at this point. These were deemed to be a third party IT service provider according to Medibank. [13] Those credentials were subsequently put up for sale on a Russian language cybercrime forum. The individual who obtained them was acting as a credential broker who purchased them and used them to establish two backdoors within the company which gave them enhanced persistence in the organisation in case one of them was discovered. [14] They were using a variant of REvils file-encrypting malware.

The attackers themselves which are believed to be linked to the ransomware group known as REvil posted an entry to their blog which is located on the Dark Web and said "Happy Cyber Security Day!! Added folder full. Case closed.". The folder contained six zipped files containing customer data. It was at a total of 6 gigabytes in size and contained 9.7 million customers personal details and health claims. This included PHI (Protected/Personal Health Information) & PII (Personal Identifiable information) data related to abortions, alcohol related illnesses and passport numbers, names, dates of birth. This is the kind of information that is very distressing for customers to have revealed online and is protected in different countries by data protection laws. Some examples of such laws include the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and GDPR in europe. This regulation requires that the data is created, collected, transmitted and maintained in a secure manner and the failure to do so can result in fines.

The attackers themselves who have not been formally identified as of yet but have already moved onto more victims with a New York based medical group and the Kenosha Unified School District becoming the latest victims to be placed on their blog.[15] Medibank could face major financial penalties as the Australian government had recently passed legislation which can lead to up to $50 million dollars in fines for serious or repeated data breaches. They are also now facing a class action lawsuit from the law firm Baker McKenzie with up to 10 million customers details being posted onto the dark web. It's attempted to give the affected individuals "an avenue for redress and compensation for the loss and distress caused by Medibank Private's alleged failings".

[16] Bloomberg intelligence claims that the compensation could end up reaching $700 million for the humiliation and distress caused. [17] A second class action lawsuit has been also filed by US law firm Quinn Emanuel Urquhart & Sullivan where they are asserting that Medibank breached disclosure obligations by failing to reveal information relevant to alleged deficiencies in its cyber security systems. [18] We can see here the monumental cost of not adequately protecting customer data and not having sufficient detection tools in place to identify attackers on their networks.

This attack highlights the encumbered weight which is placed on organisations which contain sensitive information such as PHI and PII data. All of these organisations are faced now with the necessity of expanding their capabilities to include a level of security which was prior to this considered unnecessary and a waste of cash. One silver lining is that hopefully other organisations in the same industry will see this occurrence and more protectively put in place more protections and defences to protect the data which they have. It can almost become a required but toxic asset housing this data. It would likely increase their investment and attention paid to security concerns with a loss of customers, reputational damage, revenue loss and potential fines and lawsuits all in motion currently.

The attackers were able to move around their networks and obtain the sensitive information without being detected highlighting a lack of security controls in place. The sensitive data itself appears to not have been encrypted and thus making it more vulnerable for attacks like this. It's unknown how long the attackers were in the network which could have been months and it may well be indicative of a lack of proper monitoring and detection capabilities within the organization. It appears as if this data may have been not been on the cloud and if it was, they were not leveraging the full capabilities of what's on offer from cloud organizations.

Mediation & Fixes:

- **Move their data to the cloud**

Opting for cloud could be particularly helpful for an organization which is not centred around tech as their main purpose and thus they can leverage the compliance and capabilities afforded to them by a cloud offering. Most cloud offerings like AWS & IBM are rigorously setup for meeting compliance requirements and could have been an asset to Medibank. Cloud storage can have the added benefit of being

monitored by security operations teams and can easily be encrypted and protected with additional security controls in place. They could also setup alerting for the databases which could help detect anomalous activity and put data loss prevention mechanism in place. Data loss prevention tools can also monitor for data being exfiltrated from an organisation.

- **Network segmentation**

Within a cloud offering Medibank could easily have setup network segmentation with restricted private subnets separating out different networks from each other. This could have protected against lateral movement and made it more difficult for the attackers to access the database. Network access control lists could also have been configured further restricting the access.

- **Intrusion detection and intrusion prevention systems**

Intrusion detection and prevention systems in a cloud environment could have helped to detect the attempt moves of the attacker as they looked to navigate through the networks.

- **Email filtering**

Email filtering could also have helped to increase the detection of phishing attacks and other kinds of malicious attachments here.

- **Effective user training**

It's theorised that the credentials may have been compromised through phishing. Security training and best practices ought to be mandatory for individuals within the organisation. This can help reduce the likelihood of individuals using weak credentials, failing for a phishing email or any other poor security practices.

- **Regular Internal phishing campaigns**

Internal phishing campaigns can be run by security staff within medibank or by a third party security provider to increase the learning returns and highlight those employees who need additional training.

- **Employ least privilege**

The attackers obtained a high privileged account to access. Assessments ought to be put in place to ensure that the individuals are only having the necessary privileges to perform their duties and no more. Role based access control setup in a cloud environment could also help here for assigning permissions and making it easier to maintain for operators.

Veeam Breach

Veeam backup and recovery (VBR) software is currently used by over 450,000 customers across the globe and this includes 82% of Fortune 500 companies and also 72% of Global 2000 companies. While Veeam does cater to a lot of big companies at this point, it's still an SME itself (Small and medium enterprises). 43% of cyber attacks occur on SME's according to a study conducted by Accenture so the fact that they were exploited does not come as a surprise. [1] There is a fallacy among SME's that goes "it will never happen to us" and as a result of this mindset (and also a lower budget for security as well for some with tighter profit margins), this can no longer continue. Attackers are often looking to go for the lowering hanging fruit exploits where it's feasible to expend less effort and resources to gain their goals. They know that these SME's can have less to very limited security practices in place which lowers the barrier of entry for even unsophisticated attackers to make gains.

Veeam suffered intrusions because of their software since March 28th, less than a week than a high severity vulnerability CVE-2023-27532 became available in Veeam backup and replication software (VBR). [3] The software vulnerability was initially identified by a security researcher known as Shanigan and it affects all versions of the of the software. The vulnerability exposes encrypted credentials stored in the vbr configuration to unauthenticated users in the backup infrastructure. This could be used to access backup infrastructure hosts through other APIs available and thus gaining plaintext credentials. [2] Veeam fixed the issue on march 7th and provided workaround instructions.

What we can see here is another example of a Supply Chain Attack. The risk posed by the third party tools, software and dependencies in the supply chain has never been greater. There has been an increase of 300% of Supply Chain Attacks over the last few years according to Argon Security. [4] Malware is usually considered to be a centre of most cyberattacks, however in 2022, supply chain attacks went beyond attacks based on malware by 40%. [19] These corporate giants may well have rigorous security measures in place for their own systems and networks and then can be undone by poor security practices and vulnerabilities brought into their organisation by the third party software they use. Attackers are able to exploit the established trust of these applications and exploit the vulnerabilities of those applications as a way to get into what could otherwise be secure networks. As noted, since Veeam is used by so many fortune 500 companies, it becomes a vehicle to exploit so many of these companies as well.

This is similar to what happened with Notpetya, one of the most dangerous pieces of malware which caused billions in damage and devastation across entire countries like Ukraine. The attackers made their way into various companies by exploiting a Supply Chain Attack. They got into an update server of an SME Linkos Group and subsequently gained entry into all of their customers and execute their goals from there which included deploying Notpetya and bricking thousands of systems.

Weaknesses Which Facilitated the Attack

There are APIs available from Veeam which can be directly accessed by unauthenticated users. These exposed api demonstrate not operating with deny by default access, too liberal access creating an easy means for attackers to gain sensitive information. It's also a weakness in Authorisation to be able to perform an action like this which would go under the Broken Access Control of OWASP. [5] On top of that, attackers were able to unencrypt their data from their configuration which would come into the category of Crytographic failures by OWASP categorization. [6] The Veeam solution prior to transmitting data decrypts the credentials which attackers can take advantage of and gain cleartext credentials. [7]

We see the danger of sending credentials unencrypted here as well and some bad cryptographic choices in the architecture of the solution. So there's a number of issues here, exposed APIs which don't require authentication to use and do not appear to have employed authorisation checks. Another issue is that there are APIs available which return credentials in encrypted form. What use case could adequately explain why credentials including passwords would be returned from any user API? It's feasible to understand how maybe a username but to have the password returned as well is beyond comprehension as a software developer. Thirdly, those credentials are also decrypted before being sent in another API call and can thus be dumped and extracted. It's a lot of weaknesses around a very sensitive set of APIs and shows a lack of effective security mechanisms in place. It's hard to imagine that there was much threat modeling or secure design practices or principles being put in place for these APIs.

Suspected attackers and motivation of attack:

The threat group Fin7 are deemed to be responsible for the attack. Fin7 is known for conducting software supply chain attacks with extensive backdoors, distributing malicious USB sticks and more recently moving into ransomware as well. Their primary motivation tends to centre around stealing financial information and also other sensitive information to sell on the darkweb and also to use for upcoming ransomware attacks.

[8] There was a huge overlap between the TTPs (tactics, techniques and practices) which included a lot of the same code in DiceLoader, as well as a powershell script which is capable of performing similar activities to a DNS which resolving IPs for hostnames and also a reconnaissance tool which can be deployed in the stage of looking to move laterally in a given network were also associated with FIN7. [9]

IBM noted in a report published recently that FIN7 have been ganging up with form members of the malware group Conti to spread a new kind of malware. [10] This included a backdoor onto systems called Domino and Cobalt strike which is also used in establishing persistence on a system. The malware Domino acts as a loader in the first stage of an attack and then further downloads an information stealing form of malware known as Project Nemesis. This is capable of obtaining credentials which have been stored in applications such as Discord, Steam, Telegram, cryptowallets, VPNS, as well as browsers & browser history too. It's suspected that they were looking to at least leverage the credentials stolen and use them for further exploits, potentially acquiring more sensitive information or to eventually deploy ransomware. There has been no reports as of yet that they were successful in deploying the ransomware as of yet. [11]

Mitigations for Veeam:

- **Veeam services ought not to be exposed to the internet directly:**

Limiting exposure to allowlists by default with deny by default access in place would reduce the attack surface for threat actors trying to access Veeam software.

- **All API's ought to require a user with a valid session**

Unauthenticated users ought to have no privileges beyond reaching a login page. It ought to be again, deny by default for any other APIs.

- **Employ least privilege for API access**

Authenticated users ought to be only able to perform actions necessary for their role and no more.

- **Perform Threat modeling and secure design review of APIs**

Why there is an API which not only returns password information but also goes and unencrpts it before transmission is very bad security practice. It's hard to understand what valid use case this could have come under. It highlights a lack of security requirements, threat modeling, secure code reviews needing to be adhered to more vigorously. Functionality such as this which exposes passwords and decrypts ought to be considered to be removed and replaced with something more secure. This is clearly an example of insecure design (A04 Insecure Design, OWASP TOP 10). [12]

- **MFA:** MFA could also be required to increase the burden on attackers who even if they compromise some credentials may not be able to get authenticated with the second means of authentication.

- **Faster processes for public addressing of issue through a CVE:**

It took close to a month from when the security researcher found the vulnerablity and posted about it online to the company getting a CVE out and a fix in place. This is too long and leaves a big room of opportunity for attackers to get in there and exploit it. Application Security engineers and the rest of the cybersecurity staff ought to be vigilant for findings such as this online and through communications with the company. They need to be subscribed to security bulletins and newsletters from major establishments. Resources need to be allocated to investigated them and following a clearly laid out plan for dealing with major vulnerabilities like this across all departments ought to be implemented.

- **Hire more staff and expand security training:** it's clear that more security training could be a help for the developers and architects at Veeam to enhance their ability to see some of the flaws in the functionality that led to this vulnerability. They may also benefit from an increased number of application security engineers that are involved in the software

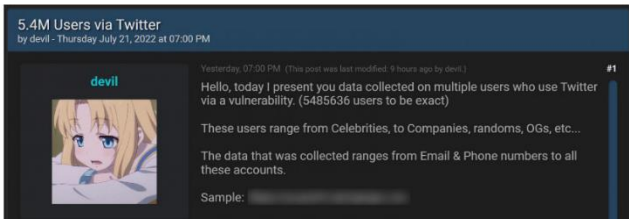
development lifecycle with a shift left mindset. Meaning they are employing security concerns right from the get go and throughout the lifecycle.

- **Expose the Veeam Systems to periodic Penetration testing:** Performing this with capable penetration testers can provide a simulated effort which would be similar to attackers. It could have highlighted these gaping holes in the security of the APIs and given some useful insight as to where they are lacking in their security posture.

More rigorous risk analysis of third party tools & software: This breach again highlights that a company could be doing very well in a lot of ways with their security mechanism but still be breached through their third party software. A lot of consideration ought to be placed in the risk of introducing or continuing all of the third party software. Of course it's a necessity but it ought to be placed under a lot of scrutiny and the practices of the company which are selling the software need to be thoroughly investigated and risk analysis performed on them. Questions worth considering: how much do these companies invest in their security of their software? Is security a priority for them? Do they include security heavily in the SDLC? Do they respond to security vulnerabilities in a timely manner? Failure to perform the necessary due diligence with third party software on an ongoing basis is a necessity to keep the perimeter of the organization secure from supply chain attacks. Methods to quickly revoke access to third party software on a full spread of all systems across the organisation ought to be considered as well for major breaches where the software has been deemed unfit for purpose.

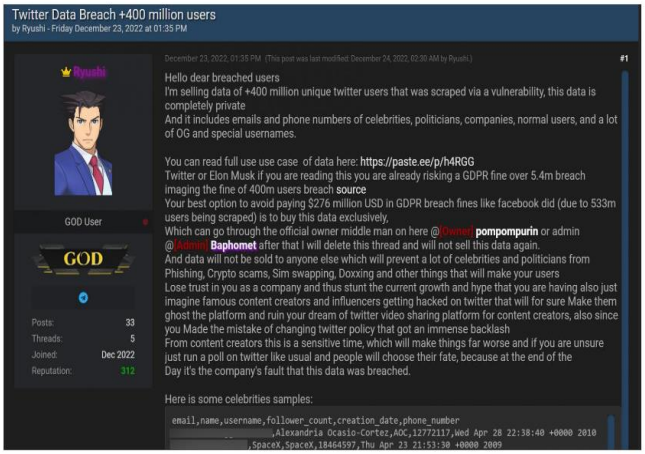
Twitter Breach

In December and November of 2022, Twitter incurred a number of security breaches whereby attackers were able to gain significant amounts of user data. The attack in December claims to have gained 400 million user records and another was claiming to have obtained 5.4 million user records. [19] The data breach for the November attack gained data including private phone numbers, email addresses. This threat actor was selling the data for $30,000 and claim that interested parties were already in contact with them. The threat actor was named Devil and is clearly financially motivated looking to obtain cash for the data:



[20]

The next breach in December was looking for even more money. The attacker named "Ryush" then tried to extort money from Elon Musk directly himself and/or Twitter.



They were looking to obtain $200,000 for this sale and promising to remove the data and post immediately after the sales's completion. This was on the Breached hacking forum. The date was placed in a pastebin and was accessible via a link included in the image above. [21] Again, it's clear that the attacker's motivation is to obtain a payment for the sale of the data.

In order to motivate the sale, he also lists a number of ways this data could be exploited including SIM Swaps, Crypto scams, BEC scams, Phishings accounts or crypto users as well. The attacker mentioned GDPR fines in relation to Facebook's fine for leaking 533 million users also as a way to try and incentivize the sale.

They were not wrong in making this kind of suggestion related to GDPR. Twitter are currently under investigation by the EU privacy watchdog which is the Irish Data Protection Commission (DPC) in relation to this breach. They had already been fined 450,000 euro for failing to notify the DPC of a breach within the 72 hour timeframe as required by GDPR and for providing inadequate documentation of the breach. [22]

The vulnerability itself allowed a given individual to send phone numbers as well as email addresses into an exposed and publicly facing Twitter API and gain a user id from that. The attacker could then build out a profile of the data of that user comprising of both public and private data. The attacker claims that this API was part of the API login flow which revealed the user id. Then combining that data with another publicly available API they were able to gain usernames and other private information about the given user. Thus, making up a given profile of both private and public data. This vulnerability was accessible even in the events where the user had prohibited the action in the privacy settings.

Twitter had received notification of this vulnerability through their bug bounty program and the disclosure was from a security researcher named Zhirinovsky. Twitter had claimed that this vulnerability was fixed, however the legitimate data which has been checked, would suggest otherwise.

Mitigation

- **authorisation issues in relation to APIs**

APIs ought to be deny by default and only those with the necessary permissions while authenticated may be able to access them. It must be clear also that they are not revealing any sensitive information to attackers as was the case in this

situation even in the event of users having privacy settings selected breaching expected authorization security controls.

- **Employ least privilege for API access**

As before, authenticated users ought to be only able to perform actions necessary for their role and no more.

- **perform regression testing on vulnerabilities that are fixed**

Ensure that vulnerabilities have been properly fixed with regression testing and looking for extraneous possibilities and potentially performing some attacker like use cases in the testing to uncover any more weaknesses in the given security controls or APIs.

- **treat GDPR responsibilities more seriously**

It's no longer acceptable to create, collect, maintain, deletion & store user data without adequate safeguards in place to protect that data. This includes using effective and industry standard cryptographic algorithms for storing the data at transit, transferring it across secure networks with the latest version of TLS as well. Any interactions with sensitive data ought to be logged and auditable and the same applied for any attempts to tamper with that data as well.

- **contact DPC in the event of a breach within 72 hours**

A few times now Twitter has failed to reach it's responsibility to notify the DPC of breaches which has resulted in significant fines. Hiding from this responsibility will not help them and only make things worse, as they fines have been shown to do. They would only compound the future potential cost for the breach incurred by GDPR as well.

- **ensure that security is embedded throughout the security lifecycle**

Operating with a shift left mindset looking to find security vulnerabilities from the design phase can massively help to reduce the likelihood of vulnerabilities making their way to production and having costly fixes later or costly breaches in this case. Security ought to be included a variety of ways with security requirements, threat modelling, security testing, DevSecOp pipelines with automated SAST and DAST tools, secure code reviews. This is an imperative for companies like Twitter which have vast quantities of customer data and can stop that data from being an asset in terms of advertisement, to a toxic asset, when breaches like the couple that have happened in the last few years, occur. Employing enough application security engineers and other security folk to perform these duties could have saved them a lot of money here.

One interesting thing to note in the overall picture of procuring information about these different security breaches is that there is drastically less information being made available about these breaches from the companies that are experiencing. This was noted in the Identity Theft Resource Centre's yearly data breach report that the attack details and victim information have dropped by 50% since 2019. No victim public response sums this up better than AT&T's who suffered a massive breach where 28 million records were released impacting on 22 million people. Their response was that it was data from AT&T but they didn't have a breach and instead "may be tied to a previous incident at another" company. [19] These companies appear to become growing more paranoid about owning up to a breach which may potentially make them liable to lawsuits, loss of revenue and exposes the deficiencies in their security posture and where exactly that may lie. This is a worrying trend and shows the importance of organisations like the Data Protection Commission and GDPR regulation which requires that these companies report a breach within 72 hours and detail what has happened.

This level of denial won't actually help these companies as the data could be relatively easily traced back to them. It poses a risk to the privacy of individuals who have trusted these companies with their data to take that responsibility seriously. The consequences of not adhering to the requirements of GDPR ought to be enforced vehemently especially with not reporting a breach and its details within 72 hours. Otherwise this trend will continue. Security researchers and other companies would also not be able to gain insight from these attacks to help protect others and the overall community at large from cyber criminals. The TTPs obtained can help to prevent other attacks in the future. There may need to be an increase in the fines for not adequately reporting breeches and protecting data and requiring it to be paid within a short period of time which could force these companies to take their security responsibilities and their responsibilities to the customers who they have been entrusted with more seriously. An interesting very recent development on this front is the sentencing of ex-Uber CISO to 3 years probation and 200 hours of community service for covering up Uber's cybersecurity data breach. [27] It seems that the law is going to start holding individuals as these companies accountable for these kinds of coverups in future. Perhaps with their own skin in the game, and this level of accountability held to the individuals it may lead to better practices around security and breaches.

IV. Question 4

Structure & title for paper:

This is a highly complex title that seems fairly ambiguous. The abstract shows that they are looking to propose a new encryption model for cloud platforms. They may be performing analysis throughout the paper but this title does not reflect what is the true purpose. That is: proposing a new encryption approach for cloud systems. The information about analysis appears to be superfluous and redundant. There is the formal structure of including an introduction, lit review, results analysis and conclusion. However, it separates the research gap into it's own section where it actually just contains the lit review. This section 4 ought to be scrapped and it should just be part of section 3, the lit review. There is also no discussion section, instead this seems to be condensed into the results section which can happen in computer science papers.

Abstract:

It takes too long to get to the actual purpose of the paper. This ought to be in the first line or two. The abstract contains results and acronyms which are likely well known to the paper writers but not to others like TPR, FPR and CCR. These ought to be in plaintext. A reader ought not to need to read the actual paper or do a google search to find out what acronyms on the abstract mean. There's a lot of bloat at the start which is not relevant to what the paper is actually analyzing. It read more

like an introduction to a paper about cloud computing generally as opposed to an abstract about a very specific area that was target within. The first three lines could be cut and instead move directly to the problem statement. This is background information about Cloud computing instead of being background information about the problem area that the paper being focused on here. The lines up to "Although the area is frequently being analyzed and reformed…." could all be cut. Even that line could do with this section in quotes removed as it doesn't give the reader any information about the paper. It's just announcing that there are already papers in the area which doesn't have a place on a research paper. The problem, objectives of the paper, results and significance of those results could be expanded upon to have more value here. More precision on where the problem lies could be helpful as well.

• Introduction

Again, the beginning paragraphs of this section gives us no background information about the problem. They give us generic background information about cloud computing. It discusses things such as the value of cloud computing and apparent issues with cloud computing data transfers. This may well lose the interest of readers. The paper only gets to what its trying to achieve in parts of 1.2 and covers actual more relevant background information to the area in parts of 1.1. In section 1.1 we're getting some of the more broad context of the area and problem. The paper could benefit from having section 1.2 as the opening paragraph of the paper and remove all that's prior to 1.1 section. By doing this we get straight to the point of the objectives of the paper and the methods that will be applied to achieve the end results. Then expanding into some more relevant contextual information for the problem at the hand after.

Some of the introduction makes claims which are not followed by evidence or references to support those claims. For example, the author makes claims the "risk of data compromise is increasing" and provides no actual evidence of this mentioning cloud storage has a lack of access and security concerns and mentions some security principles. Another example of this is: "Due to the quick development of information technology, there is a significant amount of data outsourcing to cloud servers, and multiple attacks will jeopardize the secrecy of cloud data". This appears to be a justification on why this problem area is important but it offers no examples of such attacks that are relevant to the area of encryption. It's again a baseless claim on the reasoning for data being outsourced to the cloud and not all that relevant. If this instead provided some attacks that have occurred that are relevant to encryption and data breaches and the area of focus, with references, it could be more beneficial. Another example would be:

"Despite the many advantages of cloud computing, the most crucial area of concern is privacy and security."

The author is not giving justifications as to why this is an area of concern and instead follows up with listing some deemed important areas of cloud security. They could here bring in some financial figures of actual breaches that have occurred and perhaps some cases where companies were forced to shut down as a result of severe reputational damage to emphasise this point. Instead it makes the assertion baseless.

"certain standard network and storage security technology are no longer fully relevant in cloud storage environments. For instance, message digital signatures are employed in traditional storage technology to confirm file integrity, but with cloud storage, the data is stored on a remote server, making it impossible to periodically retrieve the data and validate the signature to ensure data integrity. "

Here the author claims message digital signatures are not possible in cloud storage environments. This is factually incorrect. AWS for example offers four supported checksum algorithms for upload and download requests in S3 and has even claimed to have improved those integrity checks by up to 90% [29] However, after skimming that paper it shows that there is possibly even some evidence of plagiarism from this paper. That paper from the Pakistani researched is only referenced for this part. However there is a couple of lines taken from this paper directly like:

"As a result, the risk of data compromise is increasing, and it may be classified into two categories: vital data and archival material. Important information is information that a subscriber needs at any given time and would be irritated by any halt or disappearance. Furthermore, archival data is data that is extremely rare in its entirety, and typically in a non-critical moment. As a result, a gap in it won't be able to be regarded as a major issue."

There are other examples of this as well. The information needs to be properly cited and credit given directly to the researchers who have written these words. Their information ought to be paraphrased and not effectively almost completely copied in this paper. [34]

There's a throughline here of not being able to actually show with evidence weakness in current cloud security of data. We're not seeing why this problem is important (too much). We don't get much information on the different architectures that will be looked at. It lacks clarity on how the hypothesis is going to be evaluated and why their approach is a good one. There is no brief and concise summary of the research conducted in the area.

• Graphical abstracts and/or highlights

The paper has some graphical images as well as a number of tables. Some of those include a neural network image. While the image is clear, there was no explanation as to what was happening within the image, only that four inputs enter this algorithm. This renders it fairly ineffective and could be improved by explaining a bit of how the ANN algorithm works and what it may produce to the benefit of the paper. Some of the graphs were well chosen and appropriate for the context like the use of the bar chart. It effectively displays the comparison of CCR across the different algorithms. However, other tables like Table 4 were very complex and did convey the message well. It could have been two separate line graphs instead and this is expanded upon in the results section. The formulas used as images in the methodology section are just planted in again with little detail of why they are necessary and what part they play in the overall scheme of things. It could have been better to show clearly what part they play and put more detail to give more connective tissue between the constituent parts of this section. The work flow of the proposed algorithm (Fig 2.) is an effective graphic but more in depth context ought to be given

here to accompany it. It shoulders too much responsibility on it's own leaving the reader with a lot of questions and ambiguities about the approach.

• Methodology

The methodology sections begins with the following introduction:

"The primary goal of this research is to provide a methodology for document or query encryption that encrypts data in the cloud. The document is given a keyword, and during decryption, ANN is used to rank and extract the best appropriate document based on the keyword. Certain parameters are computed to determine whether a document is approved or denied for a certain keyword."

This paragraph doesn't really explain what's happened in the experiments. For example, on what basis are keywords applied to documents? Are they used as an identifier? Why is one keyword selected over another? Query encryption is mentioned as well but it's not outlined what this actually means or represents in this section or previous sections. The remaining pages of the methodology are sparse on details and disjointed.

There's a description then of the HAC index, Neural Index and Search index with some mathematical formulas & diagrams. There's no indication of why these are applied or selected. What are they going to provide individually and collectively? Why were they selected over other algorithms? Why are these indexes performed in the order they are performed? What's the significance of using them? How will they give us the results the researchers are after and be useful for the area the experiments are taking place in? There's no examination of where previous literature has come into play and what novel aspects are being applied here and what the hopes or expectations were in applying this algorithm. How is this going to meet the identified research gap? There's no explanation as to why SVM and naive bayes are selected as the comparison. There is no evidence given to support that these are algorithms which would serve as a benchmark for what's the industry standard for this kind of encryption in the cloud either. They are not mentioned here at all.

The methodology section does make use of a number of diagrams, some of which are explained, others are not. Fig 1 is of a neural network and we're told that it receives some input: P1, P2, P3, P4. We're not told anything else about this particular neural network, how it works, why it was selected, what value it could and would provide in this case. It's treated completely as a black box. Fig 2 shows a work flow of the proposed algorithm with no explanation at all for the bigger picture of how this all works. We have an upper boundary and lower boundary provided for the Search Index, both are set to 30%. Why not 80% or 20%? There is no reasoning or evidence or explanation as to why those values are selected or why they might yield significant results. We don't get much information on the different architectures that will be looked at as well. This section lacks clarity on how the hypothesis is going to be evaluated as well as what measures will be applied to detect. These ought to have been in place here.

Expanding into answering some of the questions posed above could have yielded greater clarity on what's happening in the approach taken, why it's been selected, it's significance and why it might yield positive results. None of this seems to be apparent in this section. It's not clear that the researchers have a great understanding of the area in question from this.

• Results

The results section is a bit confusing. It starts with a section about keywords "that are mentioned for the search word". It's unclear what this means. How has this selection of data been acquired? Why this amount of words and how was the data collected? Is it a representative subset acquired? We then find out that these are keywords from tweets, likely from the social media site Twitter. There has been no mention of Twitter or tweets at all in the entire paper preceding this. Why are we suddenly seeing data acquired from tweets? Table 3 on the following page is a block of numbers which are the results for the recommendation. There's no explanation of what's gained from these results and what they may mean. The reader is left to their own devices to read and interpret the results.

This is the first time in the entire paper we are introduced to the algorithms being compared against: Naive Bayes and SVM. Naive bayes has not been mentioned in any way at all throughout the paper prior to this. SVM got a brief mention in the literature review in relation to another paper using it. These ought to have been included in the methodology section and why their selection as a means of comparison is used. This is the same for false positives, true positives and the cost computation ratio. Why have these been selected as evaluation metrics and what value do they bring to our objectives? It's just mentioned what they are instead and that they have been applied. It seems like a lot of this information ought to have been placed in the methodology section along with the explanation of where the data was coming from, Twitter and how that was performed. It's likely this was done with some Twitter APIs or perhaps some Kaggle data set containing tweets but the reader should not be put in the position to have to guess this and only hear about all of these things in the results section.

Table 4 then gives a title of classified results. Classified results of what? Again, the reader is left to figure this out from themselves. The results contained the true positives for multi class SVM, naive bayes, the proposed solution as well as false positives for all of the above over different ranges of searches. This is again a big block of numbers with too much information. It puts the onus on the reader to make the comparison through a whole host of numbers and columns. It may have been better to break this down into two separate line graphs instead of the table. One graph showing the true positive comparison and the other false positive comparison of each algorithm. This would demonstrate the performance of each of the algorithms selected and leave the reader to just visually see that represented in a clearer format. This table does at least have a discussion section after where there is some explanation of the results and their significance. The claim that the algorithms selected are state of the art though however, is false and that will be expanded upon more later. There is a better graph selected for CCR comparison with a bar chart. It shows the performance differences well between each selected algorithm. However, we don't get the significance of where this value matters to the overall final results and why it's valuable. We then, finally, get a comparison of the true positive results versus two other papers Zhang et al 2022 & Wang et al 2016 in a small table. This lacks context and raises doubt about the legitimacy of the comparison. It's not noted for example whether the data was constant between the papers. We have very limited

information about the data in this paper as it is & this may well skew the results and make them not all that meaningful or relevant.

Computation Cost Ratio (CCR) is a performance measure and has less relevance to being applied in this context of security. It's debatable as to whether it's an appropriate measure to have applied here. False positives and true positives are more effective measures selected in relation to asserting security.

• Conclusion/Discussion

In this section we can see that the proposed solutions perform better than some other less sophisticated machine learning algorithms naive bayes and SVM. While we are given some implications of the results in relation to those algorithms it doesn't show whether this is going to improve cloud encryption. Those are not state of the art algorithms when it comes to encryption despite the author claiming them to be in the results section. There has been no evidence provided to prove this. These results of the method chosen would likely hold more weight if it was performing comparisons to those state of the art methods with the correct metrics to evaluate that. Those state of the art methods may well be found in cloud computing environments like AWS, Azure, Google etc. Basic machine learning models do not equate to that. There are also no limitations provided on the paper in the conclusion or any other part. The future research suggests another machine learning approach with a fuzzy data model. There is no further information on why this could or would be an appropriate model to employ or how it give better results or a different perspective. This forces the reader to only speculate on where it may have been applied and doesn't provide much benefit for other researchers as to why this may be an area to further expand into. It appears that this research may have gone in a different direction based on the literature findings. The researchers could have opted to find a way to solve the issue of why there is data leakage which appears to be a commonly occurring problem in Symmetric Searchable Encryption, the area the research is based. This is flagged in the literature review as a failing in the area and it's consistently been found in multiple papers. It could have also have been noted as a future area of research. Instead this research does not appear to be providing anything novel with employing machine learning against one another. It may have been more prudent to consider this work as a proof of concept for further expansion.

• Language

The language contains a lot of unnecessary bloat with tangents about cloud computing and it's features in the introduction. A lot of this content is not relevant and ought to be cut out and replaced with an introduction containing relevant content to the problem at hand. There's also the use of three abbreviations TPR, FPR and CCR in the abstract which have not been explained. A number of claims made by the authors are not followed up with actual evidence as mentioned previously. Sections of the paper lack cohesion and appear disjointed. This is particularly the case in the methodology section where it's unclear what is happening in the overall workflow and algorithm. There's an algorithm given at the end and a lack of descriptions missing for context of what each part is doing and why it matters. It's also lacking in detail and important relevant information like the comparison algorithms and measures of evaluating the results. These are only introduced in the results section for the first time. There is undue effort on proclaiming the height of what is being achieved in the paper as mentioned in the conclusion section. There may also have been some plagiarism in the paper. Overall, it's a confusing paper to read which leaves a lot of work on the part of the reader to discern what the author is trying to convey.

• Previous Research

The literature review looks to be one of the more effective parts of the paper in terms of it's structure. The author does go through a whole host of different papers, explores what encryption architectures were used and the pros and cons of each. This is done in a tabular format. It seems like the author has done their research properly here and has at least identified a whole host of different approaches to explore. They have presented a survey of preceding literature on the topic. This does demonstrate some scholarly rigour for this section and gives the author the footing for furthering their own research and exploiting the research gap identified. They have critically analyzed the literature and found the advantages and disadvantages of each and then tied them all together based on different architectures at the end to present what each brings and where it falls down. This has likely helped set the authors up for the methodology, experiments and testing they would then conduct themselves.

REFERENCES

[1] L. Irwin, 'Cyber Security Statistics for 2022', February 2022, Available: https://www.itgovernance.eu/blog/en/20-cyber-security-statistics-for-2022#:~:text=1)%2043%25%20of%20cyber%20attacks,data%20breaches%20occur%20at%20SMEs

[2] S. Gatlan, 'Veeam Fixes Bug that lets Hackers Breach Backup Infrastructure', *Bleeping Computer*, March 2023, Available at: https://www.bleepingcomputer.com/news/security/veeam-fixes-bug-that-lets-hackers-breach-backup-infrastructure/

[3] NIST. 'CVE-2023-27532'. 2023. Available: https://nvd.nist.gov/vuln/detail/CVE-2023-27532

[4] V. Davies, 'Software supply chain attacks tripled in 2021 says Argon', *Cyber*., January 2022, Available: https://cybermagazine.com/cyber-security/software-supply-chain-attacks-tripled-2021-says-argon

[5] OWASP. 'A01 2021 Broken Access Control'. Available: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

[6] OWASP. 'A02 2021 Crytographic Failures'. Available: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

[7] M. Stueck, 'Veeam BAackup & Replication Vulnerability Exposes Stored Credentials', *Kudelski Security*, March 2023, Available: https://research.kudelskisecurity.com/2023/03/10/cve-2023-27532-veeam-backup-amp-replication-vulnerability-exposes-stored-credentials-no-auth-necessary/

[8] -Prodaft. 'Fin7 Unveiled'. 2022. Available: https://www.prodaft.com/m/reports/FIN7_TLPCLEAR.pdf

[9] B. Toulas, 'Hackers Target Vulnerable Veeam Backup Servers Exposed Online', *Bleeping Computer*, April 2023, Available: https://www.bleepingcomputer.com/news/security/hackers-target-vulnerable-veeam-backup-servers-exposed-online/

[10] C. Hammond, 'Ex-Conti Members and Fin-7 Actors Collaborate with New Backdoor', *Security Intelligence*, April 2023, Available at: https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-backdoor/

[11] L. Abrams, 'Ex-Conti Members and Fin-7 devs team up to push New Domino Malware', *Bleeping Computer*, 17 April 2023, Available at:

https://www.bleepingcomputer.com/news/security/ex-conti-members-and-fin7-devs-team-up-to-push-new-domino-malware/

[12] OWASP. ‘A04 Insecure Design’.
Available: https://owasp.org/Top10/A04_2021-Insecure_Design/

[13] Medibank. ‘Cyber Security timeline’.
Available: https://www.medibank.com.au/health-insurance/info/cyber-security/timeline/

[14] J. Taylor, ‘Medibank Hack Started with Theft of Staff Members Credentials’, *The Guardian*, 24 October 2022, Available at: https://www.theguardian.com/technology/2022/oct/24/medibank-hack-started-with-theft-of-staff-members-credentials-investigation-suggests

[15] C. Page, ‘Medibank hackers declare case closed as trove of stolen data released’, *Tech Crunch*, December 2022, Available at: https://techcrunch.com/2022/12/01/medibank-case-closed-stolen-data-released/

[16] J. Taylor, ‘Medbank class action launched after massive hack put private information of millions on dark web’, *The Guardian,* February 2023, Available at: https://www.theguardian.com/australia-news/2023/feb/16/medibank-class-action-launched-data-breach-private-information-dark-web

[17] C. Kruger, ‘Medibank hack victims compensation in limbo due to unexpected hurdle’, *The Sydney Morning Herald*, April 2023, Available at: https://www.smh.com.au/business/companies/medibank-hack-victims-compensation-in-limbo-due-to-unexpected-hurdle-20230414-p5d0gx.html

[18] M. Or, ‘Medibank hit by second class action lawsuit for cyber breach’, *Insurance Business*, May 2023, Available at: https://www.insurancebusinessmag.com/au/news/cyber/medibank-hit-by-second-classaction-lawsuit-for-cyber-breach-441147.aspx

[19] IdTheftCenter, ‘2022 Data Breach Report’, Available at: https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf

[20] L. Abrams, ‘54 million twitter users stolen data leaked online’, *Bleeping Computer*, November 2022, Available at: https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/

[21] L. Abrams, ‘Hackers claims to be selling twitter data of 400 million users’, *Bleeping Computer*, 26 December 2022, Available at: https://www.bleepingcomputer.com/news/security/hacker-claims-to-be-selling-twitter-data-of-400-million-users/

[22] S. Gatlan, ‘Twitter fined by EU protection watchdog for GDPR breach’, December 2022, Available at: https://www.bleepingcomputer.com/news/technology/twitter-fined-by-eu-data-protection-watchdog-for-gdpr-breach/

[23] Amazon. ‘KMS Compliance’. Available: https://docs.aws.amazon.com/kms/latest/developerguide/kms-compliance.html

[24] ExpertInsights, ‘AWS secrets management vs Microsoft Azure Key Vault’, Available at: https://expertinsights.com/reviews/microsoft-azure-key-vault?utm_source=AWS%20Secrets%20Manager-vs-Microsoft%20Azure%20Key%20Vault

[25] Puneet, ‘AWS vs Azure KMS’, *Encryption Consulting*, October 2018, Available at: https://www.encryptionconsulting.com/the-debate-for-key-management-service-by-aws-or-azure/

[26] E. Shanks, ‘Pros and Cons of Amazon’s Key Management Service’, *The IT Hollow*, February 2017, Available: https://theithollow.com/2017/02/13/pros-cons-amazons-key-management-service/

[27] TrustRadius, ‘Azure Key Vault, Available at: https://www.trustradius.com/products/microsoft-azure-key-vault/reviews?qs=pros-and-cons

[28] S. Sabin, ‘Ex-Uber security chief gets probation for concealing 2016 data breach’, *Axios*, May 2023, Available: https://www.axios.com/2023/05/04/uber-joe-sullivan-sentencing

[29] Amazon, ‘Amazon S3 accelerates integrity checking requests by 90%’, Available: https://aws.amazon.com/about-aws/whats-new/2022/02/amazon-s3-integrity-checking-requests-90-percent/

[30] IBM. ‘Disaster Recovery’. Available: https://www.ibm.com/docs/en/configurepricequote/10.0?topic=availability-disaster-recovery

[31] Amazon. ‘Disaster Recovery Architecture on AWS part ii’. Available: https://aws.amazon.com/blogs/architecture/disaster-recovery-dr-architecture-on-aws-part-ii-backup-and-restore-with-rapid-recovery/

[32] Microsoft. ‘Differential Backups on SQL Server’. Available: https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/differential-backups-sql-server?view=sql-server-ver16

[33] M. M. Alshammari, A. A. Alwan, A. Nordin and I. F. Al-Shaikhli, "Disaster recovery in single-cloud and multi-cloud environments: Issues and challenges," 2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS), Salmabad, Bahrain, 2017, pp. 1-7, doi: 10.1109/ICETAS.2017.8277868, 2017, Available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8277868

[34] Zulifqar, Anayat, Kharal, “A Review of Data Security Challenges and their Solutions in Cloud Computing.” International Journal of Information Engineering & Electronic Business, 13(3): 32-41., 2021 Available at: https://www.sciencedirect.com/science/article/pii/S1877050915006808