# Risk Assessment Report
# Arrow Leadership
2022

# Table of Contents

Executive Summary ..... 3
Background ..... 5
Analysis ..... 6
Backup ..... 6
Netstrategies or Salesforce ..... 9
Policy, Protocols and Procedure for Arrow Leaderships ..... 11
Third-Party Applications ..... 13
Recommendations ..... 14
Conclusion ..... 15
References ..... 16

## Executive Summary

The following report entails an analysis of Arrow Leadership's security state of its technological systems and applications in 2022. This report will outline the cybersecurity risks involving Arrow Leadership's backup systems, CRM system, Netstrategies, IT Protocols, and its usage of third-party applications. With the analysis focusing on these specific segments, some key factors which were used to determine if there were any risks in the segments were whether Integrity, Availability and Confidentiality of data was easily compromised through these segments. This report will also briefly provide recommendations for the company's executives to review and provide feedback on as to whether these measures are appropriate for them to commence forth.

In the Backup systems, it was discovered that Arrow Leaderships could have a potential breach in their system if staff lose their Time Capsules. Though it was informed that the staff Time Capsules were only to store their personal documents, if staff were to lose their portable storage devices, threat actors could potentially discover staff credentials or confidential information which can be linked to the company. Furthermore, it was found that due to the company not utilising any antivirus software's, data stored on the cloud could potential be breached to insecure security software's provided by the cloud service company along with ransomware or malware.

Additionaly, Netstrategies is the CRM and current website provider of Arrow Leaderships. Upon analysing Netstrategies, numerous risks were discovered. This includes the company's heavy usage of third-party applications for their company along with being unable to provide certifications and regulations of their company strategies. It is thus, recommended that Arrow Leaderships switch to using Salesforce instead of their current system as Salesforce manages its own security and protocols for clients and is able to provide the same and even more services for Arrow Leaderships than Netstrategies can provide. Upon the request of Arrow Leaderships, WordPress was evaluated on its suitability for the company, and it has been determined that because WordPress relies its security too heavily on unknown security sources, Salesforce is a more appropriate website manager for Arrow Leaderships.

Upon meeting with the company's executive, it was discovered that the company only has a Privacy Protocol, however, it does not have an IT Protocol, Firewall Policy, Anti-virus policy, constant personnel to monitor or test the company's system, and has a lack of centralized control of information flow. This poses a significant risk to not only the company's ability to secure data but also creates a huge vulnerability for its third-party partners' if a breach were to occur through Arrow Leaderships or vice versa.

With the company's usage of numerous third-party applications, Arrow Leaderships has a high risk of cyber security breaches. This is due to the vast amounts of subscriptions and servers they use. With no IT policy or staff training for handling confidential information, the company is at risk of having its employees reuse confidential credentials in numerous websites. Thus, if a breach were to occur within one of the third-party applications, cyber criminals are likely to be able to gain access to more of Arrow Leadership's accounts and potential confidential information. With numerous third-party applications in use, this could also cause complications legally as it will be difficult to determine who bears responsibility if a breach were to occur in one of the third-party applications.

As a result, the main recommendations Arrow Leaderships should strongly consider is investing more in their security system by utilising less third-party services, avoid reusing credentials, implement antivirus software's, create an IT Policy, train staff in using the online space and lastly, implementing multifactor authentication.

## Background

Cyberattacks nowadays are no longer limited to large corporations or individual scams. Companies are vulnerable to cyberattacks regardless of their size, portfolio or status. According to CNET, 1,862 data breaches were recorded in 2021. It is thereby extremely important for all organizations to get a risk assessment done and have steps taken to secure their organizations from cyber threats. These steps involve getting a look at current policy, procedure, and infrastructure of the company after which recommendations regarding the necessary actions are given with expectations that action will be taken to secure the company from vulnerabilities. This process is best done twice a year at a set time to ensure the company has installed update to date protection from evolving threats. The report will have a look at the company at all levels i.e., technical, policy wise and infrastructure wise. The current threat actors which Arrow Leaderships should consider are cyber criminals, third party applications, their employees, and malware.

# Analysis

## Backup

This risk analysis report is written for Arrow Leadership in order to look at their present backup system, analyse the risks related to it, and provide a quick summary of how to address those risks and what the best options to back up their system is.

**Cloud backup security threats:**

Although employing the cloud to back up all of Arrow Leadership's key resources is not a terrible idea, there are still certain dangers and hazards involved. Data loss is the first danger associated with utilising the cloud as a backup (Ma, J., 2022). It poses the biggest danger to data security, without a doubt. There is a lot of trust in that connection because the cloud service provider in charge of Arrow Leadership’s backup system. The contract the company have in place for the backup service provider and cloud service provider must guarantee that safeguards against unintentional deletion and unauthorised access are in place, as well as that redundancy is used to prevent data loss.

Data breaches are another concern that may emerge since Arrow Leadership's private information could be viewed by an unauthorised third party unintentionally or on purpose. If their cloud backup server is on a common platform and was not built to safeguard against multi-tenancy, tenants conducting business with Arrow Leaderships could potentially access Arrow Leaderships databases. The simplest approach to avoid this is to encrypt the company’s cloud backups, both during network transport and while they are being stored on the backup server database. Additionally, data leaking might be a problem (Ma, J., 2022). Ensuring no one from outside the business tries to access the data is a big aspect of safe data storage. Ensuring the data is not sent to anyone outside of the firm is another consideration. Since it might reveal private or business-critical data to other sources, data leaking can result in major issues. Even if we take precautions to ensure that no one in our company leaks information, the storage provider may unintentionally provide the data to the wrong person.

**Protect backups from ransomware and other security risks:**

Over the past few years, there has been a startling increase in cyberattacks. Given the increase in attack frequency and the high total cost of protection and repair, it is safe to conclude that a cyberattack is a lot more likely than a natural disaster to bring down our company (Calvancia., N. 2022). Protecting our data and backups from ransomware and other security concerns is consequently essential.

Backups are swiftly becoming into the newest popular attack method. When an organization's capacity for recovery is compromised, threat actors are still in charge of their attack. Over the past few years, it has been used in a variety of breaches, including ransomware, lateral movement, and data destruction assaults. The fact that backups are one of Arrow Leaderships' main defences against a ransomware attack is well known to cybercriminals.

Malware has been developed with the ability to precisely seek for backup storage, recognise backup files, and erase all means of a company's recovery. These scripts and executables are built to look for specific file types, leverage the APIs of backup applications, and access and destroy backups in any other way possible.

Cyberattacks that use lateral movement or moving from machine to machine while using stolen credentials, are designed to create a persistent presence on compromised endpoints and inside directory services. Malware that infiltrated the endpoint will continue to exist even after being removed thanks to endpoint persistence.

Attackers attempt to stay on your network by setting up several fictitious identities that are given membership to organisations that have access to servers, file sharing, databases, programmes, and even the directory itself. The only way to undo these kinds of alterations is to either manually undo every change that has been logged or to use backups to restore the environment's original state before the attack.

**How backup are deleted:**

Hackers have created code to automatically establish a large number of user accounts they may access later using accounts with elevated directory access. The value that destroying backups adds to ransomware campaigns is recognised by these same hackers. Therefore, it's not beyond the realm of possibility for hackers to realise that combining these two threat

activities to assure persistence on your network — even after first discovery — will only benefit their efforts.

**Portable device risks:**

Users can easily access both personal and professional data while on the go with the use of portable devices like tablets, personal audio players, and jump drives. But as their use grows, so do the risks that come with it. These devices' portability and ability to connect instantly to a variety of networks and hosts also make them susceptible to loss of physical control and network security breaches. Using portable devices can increase the risk of data loss (in the event that a physical device is lost), data exposure (in the event that private or confidential information is made available to the public or a third party without authorization), and increased vulnerability to network-based attacks to and from any systems the device is connected to (both directly and via networks over the internet) (Pennie., W. 2022).

**Risks on portable device:**

Using basic storage media might appear harmless, but it can lead to a lot of issues for a user or an organization. According to TechAdvisory.org, USB devices are now used to propagate 25% of malware (malicious programs). These USB-connected gadgets, such jump drives and music players, can contain malware that you unwittingly copy or that your computer's Autorun or Autoplay feature will automatically launch. Attacks are also becoming more advanced and difficult to detect as hackers install small circuit boards into keyboards and mice to unleash malicious code when a specific key are pushed or a certain condition is met.

Once malware has infected your computer to steal or harm your data, it may spread to more computers on your personal or professional network. Furthermore, by transmitting malware to every PCs the device is connected to, these devices make it simple for attackers to spread malware rapidly. You might not notice the infection until significant damage has been done since these storage devices can insert malware inside any firewalls set up on your computer or network. Storage devices can also give malicious insiders the chance to steal data quickly and silently because they are simple to conceal and difficult to trace.

When you download programmes or games that include malware or viruses, smart gadgets have the ability to covertly infect your PC or network. They are vulnerable to malware

assaults due to their widespread use, emphasis on usability, and lack of developed security solutions. Additionally, popular procedures for keeping sensitive data on smart devices create the risk of irreparable data disclosure or loss. Users routinely save confidential client information, such as client account numbers, on their smart devices, which may be running rogue programmes or connected to susceptible networks.

As a result, while using the cloud as a backup system has many benefits, there are drawbacks as well. However, since all of these drawbacks can be avoided, this report outlines the risks associated with using the cloud as well as some quick fixes to avoid them. Ultimately, Arrow Leadership would be much more secure after putting these fixers into place to mitigate their potential risks related to their backup system.

## Netstrategies or Salesforce

| | **Clarety (Netstrategies)** | **Salesforce** |
|---|---|---|
| **Payments' Protection** | SecurePay, Chase Paymentech, Comply with PCI DSS | Paypal, Chargent Payment, Salesforce Payments, etc. |
| **Application Security Managers (ASM)** | Utilise F5 BIG-IP, which is managed by Bulletproof. (AC3) | Support event monitor, report anomalies, measure custom application performance, and encrypt sensitive data. |
| **Email Sending Infrastructure** | Utilise SendGrid, an email marketing company | Salesforce Marketing Cloud |
| **Server Infrastructure Manager** | Utilise Bulletproof, an IT service provider, which belongs to AC3 | Salesforce manages their own server or uses AWS servers where they do not have their own data centres |

| | | |
|---|---|---|
| **Certifications, Standards and Regulations** | Cannot find enough information | A lot of compliance certifications: CS Gold Mark, GDPR, ISO 27018, etc |
| **Training** | Support training, tutoring, modelling, benchmarking | Trailhead learning website provides in-person and virtual learning |
| **Customisation** | Allow customisation in the developing phase<br><br>https://www.clarety.solutions/content/privacy-policy/gjqya0 | Provide a wide range of pre-built features that can be adjusted to fit different enterprises<br>https://www.salesforce.com/au/company/privacy/ |

Clarety is a decent provider. All of the third-party solutions utilized by Clarety are decent and reliable. However, Clarety utilizes a lot of third-party applications, which can increase the risk of a data breach with their company, thus, increasing the chances of Arrow Leadership being compromised.

Meanwhile, Salesforce is a giant provider that supports almost all the services Clarety provides, and they are all managed by Salesforce rather than third-party. For example, Slack is a popular messaging program owned by Salesforce. Using services from Salesforce will allow customers to utilize integrated applications in Salesforce's environments, which can reduce the number of third-party's applications and hence, reducing and mitigating risks of cybersecurity breaches linked by third-party applications.

**What is WordPress?**

WordPress is a tool that allows users to build a website without any programming knowledge (Price, 2021).

**Pros of WordPress:**

1. No coding skills needed
2. WordPress is free
3. Easy to build a website, edit the content of the website

4. With many pre-made themes and plugins, customers do not need to build new features from scratch
5. WordPress is very popular (Price, 2021).

**Cons of WordPress:**

1. Customers must use a lot of plugins from many third parties to customize their website. It is hard for customers to choose reliable third parties and is hard to mitigate the risks from these third parties.
2. Hard to scale up a project made from WordPress.
3. WordPress is only suitable for making small websites. It will be not appropriate to build a full-fledged web app that requires a lot of customization.
4. Customers must constantly update WordPress and the related plugins.

**Is WordPress a good option for Arrow Leaderships?**

WordPress is a good option for customers like small businesses, who want to build simple websites for advertising purposes. WordPress does not require users to have any programming language. Most of the features are acquired by using 3rd parties' solutions. For example, Jetpack is a popular tool to support the security, and performance of WordPress. However, it would be more appropriate for medium enterprises to have websites built by skilful developers or reliable companies. A website built and managed by a reliable company is a suggested option in the long run.

It is highly recommended that Arrow Leaderships switch to using Salesforce as it is a good choice for building and managing a website.

## Policy, Protocols and Procedure for Arrow Leaderships

This section of the report aims to provide the company with a list of shortcomings and areas in regard to policy and protocols where the company may be insecure. Each issue will have its own point after which the issue will be explained in detail.

### 1.1 Lack of centralized control regarding information flow

The company uses multiple software from different vendors and third-party stakeholders. As observed in the documents and conversations with the employees, it has been observed that

information is not centralized, and different parties and departments handle the information in a different manner. This can lead to discrepancies in data handling where vulnerabilities may be more easily spotted and exploited.

**1.2 Too much reliance on third party defense systems instead of establishing its own**

The organization uses too many third-party software's and none of its own to protect the company. This makes it not reliable in regard to data security. The organization does not have its own defenses that can act as a protection against any cyber-attacks or circumstances where the a third party application is breached. The company however, being the data custodian, is still legally bound to protect the data. Due to being legally bound to protect any data the customer shares and provides the company, any breach of customer data will be the responsibility of the company.

**1.3 No Firewalling Policy**

As an organization, one must have a list of rules that will be implemented across all devices and networks. The company has many different devices that may be collaborating on a network. There are no visible mentions of any rules being put that restrict the types of traffic on a network that a device may access. This leaves the devices vulnerable to malware and other types of attacks through which networks, in turn data will be compromised.

**1.4 No Anti-Virus policies**

Knowing that majority of the company's employees work remotely from home, there are no mention of standardizing of the devices' protection. There is also no mention of a standard anti-virus being implemented other than the reliance of security providing by the employee's MacBooks. This can lead to discrepancies in the protection of individual devices by which an attacker may navigate their way to client's data.

**1.5 No Mentions of constant system testing.**

There are many mentions of new systems being implemented. However, there are no mentions of testing of any software. In an ideal situation, systems are constantly tested, and documentations updated. Mock attacking is carried out and through this, vulnerabilities are discovered and addressed by means to patches being implemented. Due to constant lack of testing and no personnel to monitor their network when new software's are implemented, this means that new attack vectors or vulnerabilities which are discovered are not resolved upon

leading to the systems defenses of the company to become outdated and even more vulnerable to newer methods of cyber-attacks.

**1.6 No staff training or IT Policy**

With no basic or guidelines for their employees to follow, Arrow Leadership's have potential risks of their employees conducting malicious activities, intentionally or unintentionally. Thus, without an IT Policy, it could also be difficult for the company to take legal matters and find responsibility in employee(s) if this were to occur. By setting a standard set of rules and guidance's as to how to use the company's system safely along with security training as to how to detect malicious emails, Arrow Leadership's can reduce the chances of a cybersecurity breach occurring due to their own staff's conducts.

## Third-Party Applications

In conjunction with no IT protocol policies, utilising numerous Third-Party applications can be a significant risk towards securing confidential data and user credentials. Hence, it is important to outline the dangers of using large amounts of third-party applications and finding new ways to mitigate these risks.

With companies enhancing their guidelines to strengthen their user credentials, it can be difficult for employees to recall varying passwords they had created. This ultimately leads to employees reusing the same password from one of their accounts to other accounts hosted by different companies (Yu, X. & Liao, Q., 2016). This poses as a significant risk towards Arrow Leaderships especially since there are no IT policies for staff to follow. Staff members can be reusing the same credentials for their personal and business accounts which can make it easier for cybercriminals to infiltrate employees' business accounts if a breach were to occur within one of the third-party applications. Furthermore, majority of cybersecurity breaches occurs due to cyber criminals exploiting third-party applications by using stolen credentials to attack linked companies (Steve, S., 2018).

Arrow Leaderships are currently utilising 13 different third-party applications and subscriptions combined. These include Office 365, Clarety/Net Strategies, Mailchimp, Type

Form, Spotify, Slack, Adobe, Xero, Secure Pay, Amazon Prime, DropBox, Zoom and CCLI. Through the research of these individual companies, 6 out of 13 of these applications had experienced a data breach from 2015 to 2022. Most of these breaches consisted of hackers stealing user credentials and viewing personal information of consumers. A notable data breach case which is relevant for Arrow Leaderships to be aware of is Spotify's data breach in 2020 to early 2021. Cybercriminals were able to use credentials from Spotify's third-party applications to compromise Spotify and collect user information, ultimately infiltrating approximately 300,000 user information (Silvue., S. 2020)

With majority of the third-party applications Arrow Leaderships utilises having experienced a data breach in recent years, it is recommended that Arrow Leaderships reduces the number of third-party applications by implementing a third party which contains all the software and benefits they need. For instance, Microsoft Azure can provide the company with cloud storage, be a website provider, store consumer data etc. Not only will this reduce the chances of threat actors infiltrating Arrow Leaderships through numerous third-party applications, but it will also be cost efficient and will make it easier for the company to hold the third-party application responsibility for their data breach. In circumstances where reducing the amount of third parties is not possible, the company can implement and utilise Multi-factor authentication to prevent threat actors from accessing accounts through user credentials.

## Recommendations

To mitigate against cybersecurity breaches, it is suggested that Arrow Leaderships implement:

- Implementing encryption to data over the network
- Encrypting stored data on the cloud
- Install antivirus software's for protection againt malware
- Train safe on how to use the company's system safely along with how to detect malicious emails
- Create an IT Policy for staff to follow
- Implement Multifactor authentication
- Reduce the number of third-party subscriptions or partners by finding a company which provides all of the services such as Microsoft Azure, AWS, etc.

## Conclusion

Ultimately, through a risk assessment on Arrow Leaderships backup system, CRM system, Privacy Protocol and Third-party applications it has been concluded that Arrow Leadership's security system is extremely weak and has a high chance for threat actors to infiltrate the system. There is a high chance of their staff unknowingly contributing to malicious activities due to no training of security along with no guidelines to follow and ultimately allowing cybercriminals into the company's system. It is highly recommended that the company invest more into protecting their data and implementing a security system for their online space.

# References


Calvancia., N. 2022. *Protect backups from ransomware and other security risks*. TechTarget. Retrieved from: https://www.techtarget.com/searchdatabackup/feature/Protect-backups-from-ransomware-and-other-security-risks

Ma, Joy., 2015. Top 10 security concerns for cloud-based services. *Imperva.* Retrieved from: https://www.imperva.com/blog/top-10-cloud-security-concerns

Pennie., W. 2022. The Risks of Using Portable Devices. *United States Computer Emergency Readiness Team*. Retrieved from: http://www.am-win.com.au/pdfs/RisksOfPortableDevices.pdf

Price., S. 2021. What Is WordPress? A Beginner's Guide. Retrieved from: https://blog.hubspot.com/website/what-is-wordpress.

Sibley, L. 2022. *Top 9 Cloud Backup Data Security Threats*. Redstor. Retrieved from: https://www.redstor.com/en-us/blog/top-9-cloud-backup-data-security-threats

Silviu, S., 2020. Spotify Hit by Yet Another Data Leak. Bitdefender. Retrieved from: https://www.bitdefender.com.au/blog/hotforsecurity/spotify-hit-by-yet-another-data-leak

Steve., S. 2018. The risks of third-party app stores. Norton. Retrieved from: https://us.norton.com/internetsecurity-mobile-the-risks-of-third-party-app-stores.html#:~:text=Third%2Dparty%20app%20stores%20might,codes%20like%20ransomware%20and%20adware.

Yu, X. & Liao, Q., 2016. User password repetitive patterns analysis and visualization. *Information and computer security,* 24(1), pp.93–115.