**Risk analysis report**

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

<https://www.techtarget.com/searchdatabackup/feature/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. 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, the bad guys 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 your organization's 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:**

[**http://www.am-win.com.au/pdfs/RisksOfPortableDevices.pdf**](http://www.am-win.com.au/pdfs/RisksOfPortableDevices.pdf)

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).

**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 tiny circuit boards into keyboards and mice to unleash malicious code when a specific key is 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.

**Cloud backup security threats:**

<https://www.redstor.com/en-us/blog/top-9-cloud-backup-data-security-threats/>