February 2023

The risk of ransomware to Microsoft 365 data

A case for backups

Barracuda

The ransomware threat landscape

Ransomware attacks have consistently hit the headlines in recent years, causing serious reputational and financial losses for organizations in every industry. Ransomware attackers ruthlessly seize data from compromised companies, encrypt the data taking systems offline, extort payouts to restore access and blackmail companies to prevent stolen data from being publicly exposed.

The average ransomware payment is increasing year upon year: according to the Coveware Quarterly Ransomware Report, the average payment reached $258,143 in Q3 22 — the highest yet, up 13.2% from the previous quarter. It's the cost of recovering from a ransomware attack that is the real issue, though. Recovery costs rose to an average of $1.85 million in 2021. Results for 2022 are not available yet, but are expected to reveal even higher figures.

Microsoft 365 accounts prove an attractive target for ransomware

While it's clear that ransomware has a financial effect on businesses that are compromised, what may be an even bigger concern is the potential of data loss. This risk is particularly high for organizations using Microsoft 365 in their daily operations. Approximately 54% of attacks are initiated via email, and with over 354 million licensed Microsoft 365 users, this makes corporate Outlook accounts attractive targets. Phishing attacks — in which the attacker delivers, for example, a fake login page to an email account in the hope of gaining that account's credentials — are hitting corporate inboxes daily.

On top of this, researchers recently discovered a potential loophole that could allow attackers to encrypt files stored on SharePoint and OneDrive, rendering them completely unrecoverable without a decryption key. With multiple vulnerabilities within Microsoft 365 accounts, attackers can use a variety of tactics to penetrate the network and encrypt confidential data to hold it for ransom. Organizations are then faced with the decision to either pay the ransom or face the consequences. The best way to mitigate this risk is with a secure backup, which allows you to restore your Microsoft 365 data without paying a significant ransom.

Ransomware is a major reason why it's crucial for a company to back up all its data, and to regularly test backups to ensure that the vital information is available, and operations can be restored, even in the event of an attack. But a strong backup solution can also help protect you against other types of malware, everyday lost files, accidental data deletion that can cause disruption or worse for the IT staff.

Third-party backup is critical for Microsoft 365

Despite the clear risk of ransomware attacks and the devastating effect on corporate data, 67% of IT managers believe that they can rely on Microsoft to back up their Microsoft 365 data and have no formal — or even informal — backup procedure in place. These organizations misunderstand Microsoft's default retention policies by assuming that their data is being backed up by Microsoft. Microsoft is not backing up your data. Microsoft explicitly states that it is not liable for any disruption or data loss in the event of an outage. This lack of backup is a huge risk that many organizations are not aware of.

While Microsoft 365 does have a series of data retention policies, the maximum default retention policy is just 90 days, and it is not a failsafe option as noted in the agreement. Microsoft recommends using a third-party service to back up your data – their default

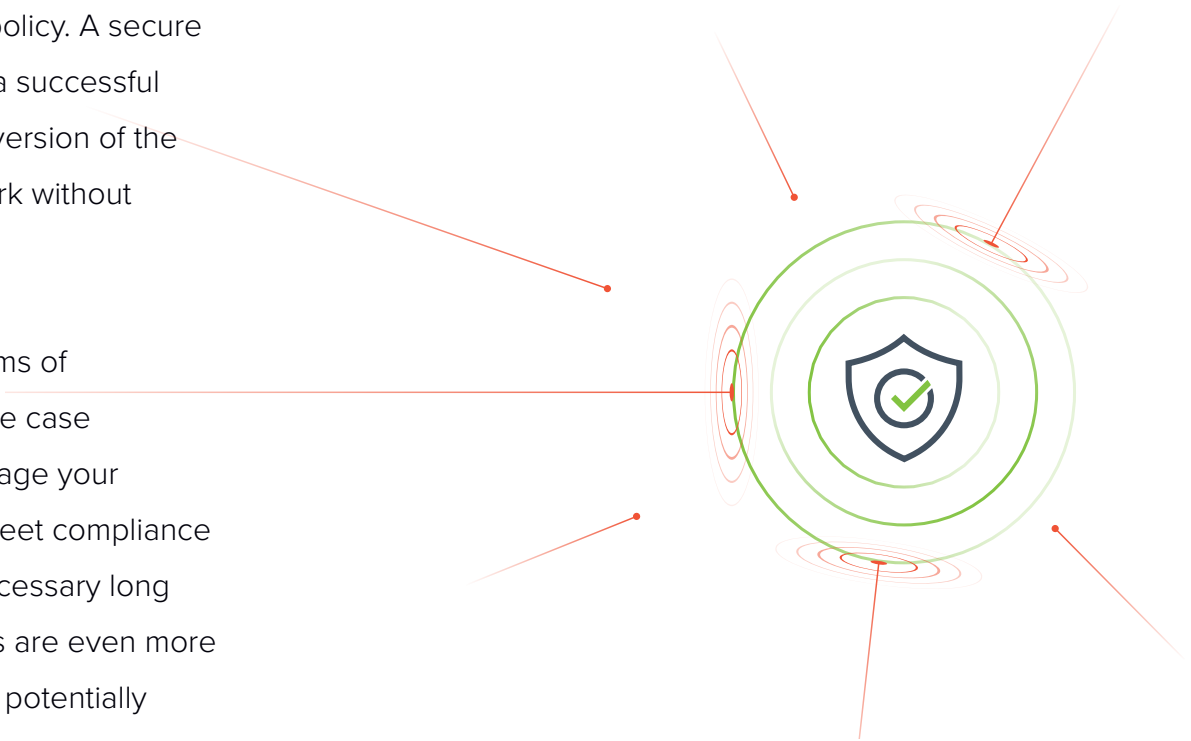
Microsoft's Services Agreement reads:

We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve your content or data that you've stored. We recommend that you regularly backup your content and data that you store on the Services or store using Third-Party Apps and Services.

retention policy is not a backup and is not designed to restore large volumes of data for production use.

A true backup is your safest bet to protecting your organization's data from ransomware attacks. Companies must invest in a third-party backup solution as a ransomware insurance policy. A secure backup will help ensure that you can recover after a successful ransomware attack as you can roll back to a clean version of the data, restore, and get your organization back to work without paying the ransom.

That's not to say that backups are only useful in terms of ransomware: backups are a basic IT necessity. In the case of Microsoft 365, a good backup can help you manage your licenses, cross-restore users, and data as well as meet compliance requirements. Backup procedures were already necessary long before ransomware entered the arena, but backups are even more crucial now that ransomware is such a looming and potentially devastating threat.



Protecting your Microsoft 365 users and data from ransomware attacks

In addition to a secure backup, it's important to have Microsoft 365 email protection in place to prevent ransomware from being successful in the first place. Good email protection will block spam and malware, include account takeover protection, and include incident response capabilities.

Regular awareness training for your staff is essential. Staff should be trained on how to identify a potential phishing email that could introduce ransomware and how to respond, including who to report it to. In many cases, breaches happen due to a lack of education or understanding of how to identify suspicious emails and what the latest attacks involve. This training must be a key pillar of your cybersecurity strategy. Educating your staff on things like password hygiene is important, but be aware that the sheer number of data breaches mean that credentials are likely to have been stolen so implementing additional security such as multi-factor authentication and zero trust access are increasingly important.

Unfortunately, preventing a ransomware attack is not enough by itself. It is still vital that you implement a strong and secure third-party backup solution that you regularly test to make sure you can access your data in the event of a ransomware attack. The backup you choose should include features such as such as full-scale encryption, multi-factor authentication, role-based access control, immutable data, and delayed purging as your backup is your last line of defense against having to pay a ransom.

Barracuda Cloud-to-Cloud Backup

Flexible, easy to use Microsoft 365 protection

Back up your Teams, Exchange, SharePoint, and OneDrive data, and find and recover the exact data you want quickly and easily with advanced search.

Ransomware protection

Your final defense against ransomware and other cyber-threats is your backup, so you need a secure backup that offers role-based access control, encryption, and multiple copies of the data.

Cloud native

Your Microsoft 365 data is already in the cloud — saving secure, encrypted backups in the same network means better performance and instant scalability.

Find out more about Barracuda Cloud-to-Cloud Backup and try it for free with no obligation.

Barracuda

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organizations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.

Barracuda

Subscribe to the Barracuda blog for the latest insights from our monthly Threat Spotlight.