E-book

The Rackspace Technology guide to protecting your business with Microsoft 365

Microsoft 365

rackspace technology

You must continuously protect your organization against a multitude of potentially costly cyberattacks — originating from both inside and outside your company. Fortunately, Microsoft 365 provides the policies and tools you need to strengthen your company's defenses. And Rackspace Technology is here to help you make the most of this powerful technology.

Every business is a target — regardless of size

In today's hyper-connected world — made even more complex due to the COVID-19 pandemic — protecting your business from internal and external cybersecurity threats is a never-ending battle. Cybercriminals, nation-states and other bad actors continue to exploit holes in technology, software and company processes to obtain personal and confidential information, regardless of business size.

Small and midsize businesses

Small and midsize businesses are particularly vulnerable because they lack the budget, resources and expertise to adequately defend themselves. Once cybercriminals have breached a company's defenses, their goal is to steal financial data — usually draining its checking account or stealing from its customers. They also take advantage of the company's business relationships with larger organizations, either as a customer or a service provider, and are exploited as an illicit entry point into the bigger company.

For many of these businesses, cyberattacks are fatal. Up to 60% of small and midsize businesses go out of business within six months of a successful cyberattack, according to a study by the National Cyber Security Alliance. Yet, according to Keeper Security's 2019 SMB Cyberthreat Study, 66% of senior decision-makers at small businesses still believe they aren't likely to become targets of cybercriminal activity. In addition, 6 in 10 businesses have no digital defense strategy in place. These businesses underestimate the severity of these threats, at their own peril.

The average cost of a breach for small and medium sized businesses is $77,000, whereas for large and enterprise businesses it's $612,000.

Source: Hiscox Cyber Readiness Report 2019

Enterprises

When large corporations are under attack, it impacts everyone — employees, customers, suppliers and business partners. Intellectual property is stolen, money is demanded (or taken), employees lose productivity and the company's reputation is tarnished. The list goes on and, unfortunately, the attack vector of large corporations is far too big and lucrative for cybercriminals to pass up. The more data cybercriminals can extract, the more money they'll make selling it on the dark web.

And just as small businesses leave the door open to larger businesses, corporations that pursue mergers and acquisitions inherit increased risk for cybersecurity threats. According to Forescout Technologies' study on The Role of Cybersecurity in M&A Diligence, 49% of IT decision-makers and business decision-makers encountered unknown or undisclosed cybersecurity incidents, issues or risks when integrating the acquired company's information and technology. Furthermore, only 37% agreed that their IT team had the skills necessary to conduct a cybersecurity assessment.

Insider Threats

In a recent survey conducted by Microsoft, 73% of CISOs indicate that their organization has encountered leaks of sensitive data and data spillage in the last 12 months, and that they plan to spend more on insider risk technology due to the COVID-19 pandemic (Microsoft Digital Defense Report, September 2020).

Fortunately, one technology you can leverage to prevent insider threats or to lessen their impact is Microsoft 365. Here are three ways Microsoft 365 protects you from insider threats:

Secure your data

One of the best tools for protecting your company's data is OneDrive for Business. You can set OneDrive's controls so its data can be encrypted and shared only with approved devices, like a company-owned computer or phone, thereby significantly decreasing the chance that any unauthorized user can access it. Likewise, you can also limit external sharing permissions for specific users, to help prevent your contractors' unauthorized employees from gaining access to your confidential business documents.

$307,111

The average cost to resolve a security incident caused by an employee or contractor's carelessness or negligence.

Source: Ponemon Institute, 2020

One all-too-common way that employees accidently expose business or customer data is when they send company documents via their personal email account or use a consumer storage service like Dropbox. With OneDrive, the data remains inside your network, and your employees can use it to easily share files with others, both inside and outside your organization, just as they would with Dropbox.

Prevent data loss

Employees send various types of business and customer information outside of your company every day via email. Some of this information warrants protection because it contains sensitive business information or personally identifiable information such as account, credit card or Social Security numbers. You can configure Exchange Online Plan 2 and E3 so that specified types of data, or certain attachments, can't be emailed by unauthorized users. You can also protect this information with Exchange Online Protection Message Encryption, which encrypts these sensitive emails so only their intended recipient can read them. This typically works through a one-time passcode, which is needed to access the sent email.

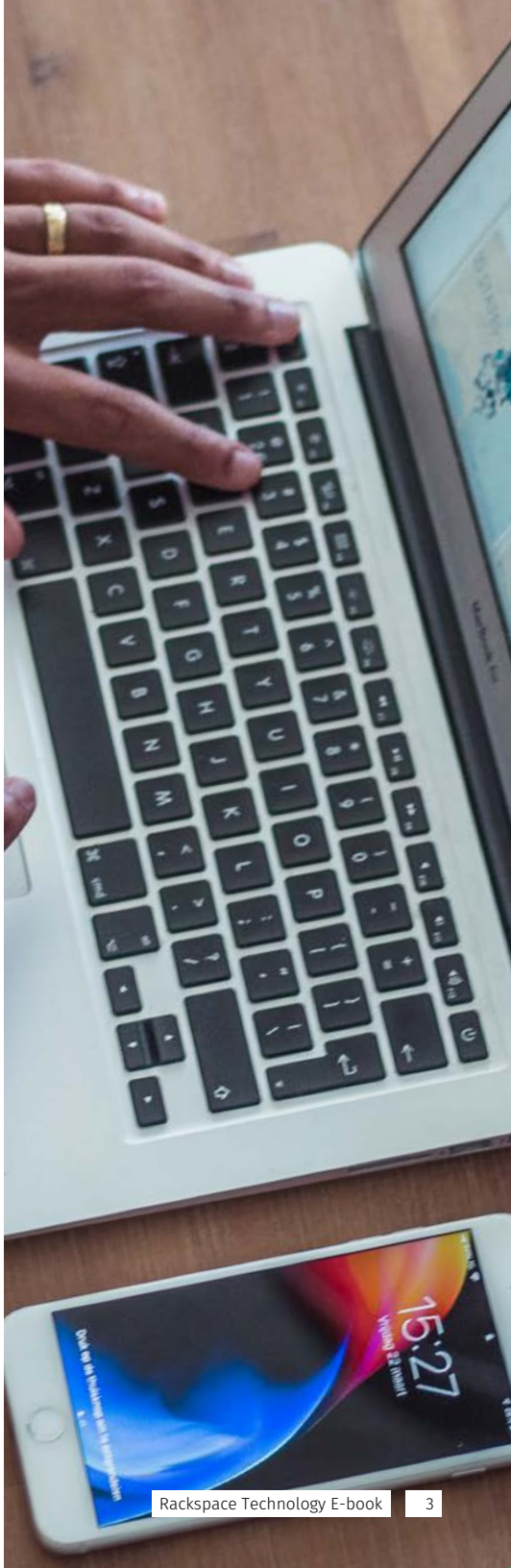
You can also safeguard sensitive business information by setting up a data loss prevention policy in the Microsoft 365 Security & Compliance Center. This enables you to identify, monitor and automatically protect sensitive information across Microsoft 365, including Exchange Online, SharePoint® Online and OneDrive for Business. For instance, you can identify any document or email containing a health record that's shared with people outside your organization and automatically block access to that document or block the email from being sent.

Restrict data access

Information rights management is a set of technologies that enables you to tightly control who can access specified files and emails — even after they leave your company's network. With Azure Rights Management, you can set authorization, encryption and identity policies — which work with computers, tablets and phones — so documents and emails can be read by only the intended recipient. Azure Rights Management also offers information rights management capabilities like Do Not Forward and Company Confidential, which protect documents from being shared with unauthorized users.

Lost or stolen devices

While lost or stolen devices aren't the major cause of security incidents, they resulted in 4% of breaches last year, according to a recent Verizon report. While these incidents can take place in various locations, they primarily happen from personal vehicles and victim-owned areas. In other words, practice good home security and lock your home and car doors.



Microsoft 365 helps businesses defend against these and other security incidents with the following tools and policies, among others:

Mobile Device Management for Microsoft 365
With Mobile Device Management for Microsoft 365, you can set access rules and security policies for iPhones, iPads, and Android and Windows phones used by your company's licensed Microsoft 365 users. Not only can you safeguard your company's emails, documents, Outlook contacts and more, but if a mobile device is lost or stolen, you can selectively or fully wipe the device.

Exchange ActiveSync
Exchange ActiveSync also provides some of the same device and data protection as Mobile Device Management, such as wiping a misplaced or stolen device, but it also enables you to configure mailbox policies, such as requiring an employee to use a password with their smartphone.

Azure Rights Management
Microsoft 365 protects data on lost or stolen devices through Azure Rights Management. As discussed in the first chapter, this Microsoft 365 add-on uses encryption, identity and authorization policies to protect the data stored on a smartphone, tablet and laptop so only authorized persons can access the data — not a team of thieves working the busy curbside of an international airport.

Phishing emails, ransomware, spam and other malware

In 2019, Microsoft blocked over 13 billion malicious and suspicious emails, 1 billion of which were URL-based phishing threats (Microsoft Digital Defense Report, September 2020). Up until a few years ago, cybercriminals focused their efforts on malware attacks because they provided the greatest ROI. Not until recently have they shifted to phishing attacks with the goal of harvesting user credentials.

Microsoft recognizes that these advanced persistent threats are a fact of life for every internet-connected company and has outfitted Microsoft 365 with an arsenal of malware-killing tools and policies.

Exchange Online Protection
One of the best tools for guarding your employees' email inboxes in real time is Exchange Online Protection, which protects against malware, viruses and spam. Exchange Online Protection scans both inbound and outbound emails, plus their attachments, for known and unknown (i.e., suspicious) malware. It not only scans zipped files for malware but also scans multiple layers of zipped files within zipped files.

SafeLinks
Microsoft Defender for Office 365 provides further protection with its SafeLinks and SafeAttachments features. Cybercriminals will hide malicious URLs within seemingly safe links that are redirected to dangerous sites by a forwarding service after a message is received. SafeLinks proactively protects your employees if they click on one of these links by dynamically blocking the malicious links.

SafeAttachments
SafeAttachments will examine all email, Teams, and SharePoint file attachments and uploads to detect known malware and will execute any unfamiliar attachments in controlled Azure detonation chambers. Microsoft Defender for Office 365 can also be used to understand who in your company is being targeted and what type of attacks are being launched so you can be informed and proactive.

Data breaches and compliance

Broadly speaking, a data breach is an incident in which sensitive, confidential or proprietary information has been viewed, used or stolen by an unauthorized individual. Data breaches typically involve business secrets, intellectual property, personally identifiable information like credit card and Social Security numbers, and personal health information like a patient's medical records.

Data breaches can be caused by malicious or accidental insider threats, lost or stolen devices, and malware like phishing emails, but for the purposes of this chapter, we'll focus on a different security risk: intruders inside your network. And because this chapter involves sensitive data, we'll also discuss key considerations when working to ensure compliance with regulations like FINRA, PCI DSS, PII and SOX.

Preventing data breaches

Earlier, we discussed using Encrypted Exchange Online to encrypt emails, encrypting files in OneDrive for Business and setting up information rights policies to monitor and protect sensitive information across Microsoft 365. All of these actions are also must-dos to stymie intruders.

Another security must-do is monitoring and restricting your administrators' Microsoft 365 access and privileges. Bad actors specifically target administrators because of their unrestricted or nearly unrestricted network access. With Microsoft 365, you can audit and restrict your administrators' access and actions, which not only locks down data access but also helps you determine if an administrator's user account has been taken over by an attacker.

Ensuring compliance and enabling eDiscovery

The Microsoft 365 Discovery Center lets your compliance officer or HR staff conduct compliance and eDiscovery tasks without burdening your IT staff. Using Microsoft 365 eDiscovery, they can retrieve data from Exchange Online, SharePoint Online (which includes OneDrive for Business) and elsewhere. Microsoft 365 eDiscovery also lets compliance officers create a single experience for hunting down and preserving email, documents and mailboxes.

Another powerful compliance and eDiscovery tool is Rackspace Email Archiving, which searches your employees' message text, attachments and metadata so you're able to quickly respond to audits and discovery requests. It provides unlimited storage and retention for your employees' emails so that you can store and access all of your sensitive and critical IP, communications and documents without limit. This helps with business continuity in order to meet compliance requirements, protect against malicious employee behavior or employee churn, and respond to legal inquiries. Rackspace Email Archiving can reduce your IT costs and workloads by removing the need for in-house email server management and archiving. It also enables your employees to recover files themselves, so your IT staff doesn't have to.

Fanatical Support for Microsoft 365

Since 2001, Rackspace Technology and Microsoft have worked together to cultivate a global relationship, focused on helping businesses make the most of Microsoft technologies. They do this through innovative product delivery and unmatched service and support across the Microsoft portfolio.

As a five-time Microsoft Hosting Partner of the Year, with over 150 Microsoft Certified Professionals, Rackspace Technology works together with Microsoft to create solutions that address the transformational needs of today's businesses. You can trust Rackspace Technology to provide the expertise you need, for the Microsoft technologies your business relies on.

When you purchase Microsoft 365 through Rackspace Technology, you'll gain access to Microsoft's arsenal of state-of-the-art security tools to strengthen your business's defenses against today's leading cyberthreats. Additional benefits include:

- **Access to experts:** The Microsoft Certified Professionals at Rackspace Technology configure and support your solution to help you get the most out of your investment. They'll even help with migrating to Microsoft 365, configuring data and email encryption, access and user identity management, and other security settings.
- **A perfect fit:** Rackspace Technology can help you make sure you're purchasing the right Office 365 or Microsoft 365 licenses for your business needs.
- **Premium admin portal:** Simplify administrative tasks using a control panel built for easy and efficient management.
- **Expert 24x7x365 support:** Day or night, you'll have around-the-clock access to our award-winning support, with unlimited requests and no per-incident charges.

Rackspace Secure 365 Assessment & Implementation Services

Security configuration is the most critical area of your Microsoft 365 environment. With the pace of innovation on the Microsoft 365 platform at an all-time high, properly securing your environment can be overwhelming. The best strategy is a baseline assessment, followed by structured and deliberate implementation of your security protocols, and a final assessment once implementation is complete. With Rackspace Secure 365, you get an assessment powered by industry-leading cybersecurity technology from QS solutions, and implementation guidance and execution by a seasoned team of Microsoft professionals.

Get started today

Whether your organization is large or small, Rackspace Technology has the experts to help you assess your current business needs and security posture and can recommend and support the appropriate solution to make sure your business is protected. If your business currently uses Microsoft 365 or plans to migrate to it, our experts can help you secure and protect your data, identities, email and mobile access by employing security features that include encryption, data loss prevention, anti-spam and anti-malware protection.

Take the first step toward protecting your business. Fill out our quick online form at the bottom of our Microsoft 365 product page or speak with a specialist using our Live Chat feature.

Learn more

About Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their business challenges, designing solutions that scale, building and managing those solutions, and optimizing returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences. Named a best place to work, year after year according to Fortune, Forbes, and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers' success — our Fanatical Experience™ — so they can work faster, smarter and stay ahead of what's next.

Learn more at www.rackspace.com or call 1-800-961-2888.

Rackspace-Ebook-Rackspace-Guide-to-Protecting-your-Business-w-M365-MST-TSK-3620 :: January 6, 2021