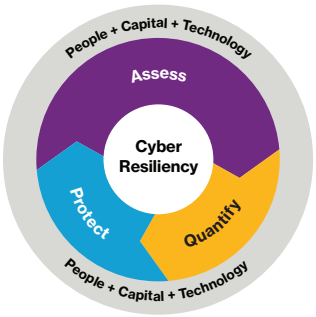


Decode risk.

Business email compromises: 365 days of vigilance

By Neeraj Sahni, Willis Towers Watson and Ankur Sheth, Ankura Consulting

The latest threat to cybersecurity isn't a new form of attack vector — it's the operational risk that can occur when using Microsoft Office 365 (O365). Research firm Gartner found that 13% of publicly listed companies around the world use Office 365 or Google Apps for email, with 8.5% using the Microsoft product compared to Google's 4.7%. As a result, O365 has a larger user population base compared to Google docs and has become a favorite target for hackers. A few best practices, if followed correctly by enterprise network management and employees, could help reduce the extent of damage should a hacker infiltrate O365.

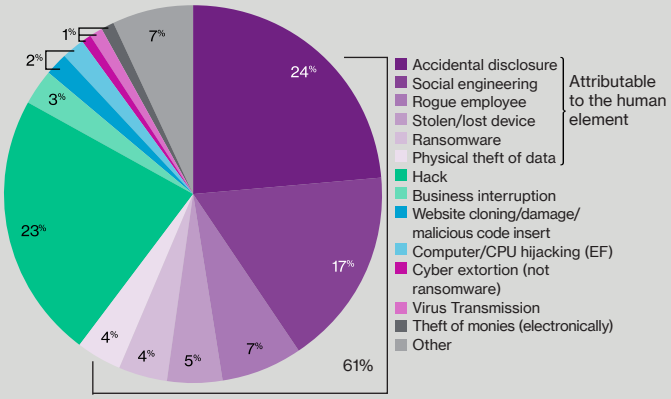
As a baseline, companies must make sure they are protected from the latest cyber threats against Office 365. The biggest pitfall of utilizing O365 is incorrect or default implementation. Many implementations of Office 365 suffer from severely under-managed and under-configured deployments. This means that the administrator doesn't fully understand how O365 works or should be deployed. Clients often assume that either Microsoft has configured Office 365 to be secured by default or that their managed service provider (MSP) or in-house support staff can deploy Office 365 in a secure configuration without specialized knowledge.

Combating this requires an organization to invest in skilled and well-trained IT staff prior to the implementation of Office 365 and vetting the MSP capability in deploying Office 365. Vetting an MSP presents its own set of parameters, which may be challenging to meet for many organizations. There is potential added cost, administrative overhead, and lack of O365 knowledge.

In fact, social engineering related claims represented 17% of the claims reported in Willis Towers Watson's 2017-18 Reported Cyber Claims Index. Moving to a cloud-based solution does not eliminate employees of a company as a target for hackers. The initial breach vector in a clear majority of incidents involving O365 are phishing emails. Individuals are still the main breach point by hackers and are therefore the first line of defense.

Phishing emails, a form of social engineering, remain the most common and effective method for O365 breaches.

Type of Loss



Source: Willis Towers Watson 2017-18 Reported Cyber Claims Index

According to a recent study conducted by ESI ThoughtLab, and sponsored by Willis Towers Watson and other organizations, 87% of 1,300 surveyed organizations with revenues ranging from under $1 billion to over $50 billion, across multiple industries spanning APAC, Europe, US/Canada

Willis Towers Watson

and Latin America, see **untrained staff as their greatest cyber risk.** Employee training remains the most effective method to defend against O365 breaches. By educating employees on how to identify phishing emails, an organization can create a bulwark of knowledge against this threat.

Every O365 implementation should follow the five guidelines below for optimal security:

1. Enable Multi Factor Authentication (MFA) for all Global Administrator accounts, because a breach of any of those accounts can lead to a breach of all the data to which that Global Administrator has been granted access. Global Administrators in O365 have elevated privileges to all facets of the software. O365 also lets organizations specify billing administrators, SharePoint administrators, and others to assist in limiting any single account area of access
2. Ensure MFA exists for all user accounts, as a breach of any of those accounts can lead to a breach of all the data to which that user has been granted access
3. Ensure Audit Data Recording for the O365 service is enabled so that you have a record of every user and administrator's interaction with the service, including Azure Active Directory, Exchange Online, and SharePoint/ OneDrive for Business. These are some of the services of O365 that can and should be actively monitored
4. Ensure mailbox auditing, which is the ability to track what actions users have taken within their O365 mailbox, for at least ninety percent of all users that have mailboxes in your tenant. By default, all non-owner access is audited, but you must enable auditing on the mailbox for owner access to also be audited. This will allow you to discover illicit access of Exchange Online activity if a user's account has been breached
5. Enable Client Rules Forwarding Blocks, as the use of client-side forwarding rules to exfiltrate data to external recipients has become an increasingly used vector by bad actors

Securing O365 is not much different from securing on-site Exchange servers. Security remains a major concern for both solutions. Whether implementing Exchange or O365, an organization must take a proactive approach to identifying and addressing security risks. A software solution, whether cloud-based or on-site can never be secure out of the box.

It will remain the responsibility of the appointed administrators and the organization to seek out and resolve potential security issues and adhere to best practices during implementation of these systems. Given the ability of hackers to continually find new ways to monetize data breaches, it is essential for an organization's enterprise risk management to evolve their protection strategies with partners who understand these evolving risks.

Contact

Neeraj Sahni
Senior Vice President, Willis Americas Administration, Inc.
FINEX Senior Broker, Cyber & Technology E&O
Willis Towers Watson
+1 212 915 8019
neeraj.sahni@willistowerswatson.com

Ankur Sheth
Senior Managing Director
Cybersecurity Leader and Proactive Services Expert
Ankura Consulting
+1 646 227 4200
ankur.sheth@ankura.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

willistowerswatson.com

Willis Towers Watson