ONEDRIVE AND CLOUD STORAGE SECURITY

The remote workforce relies on cloud tools like Microsoft OneDrive to function and collaborate. To protect sensitive data, including personally identifiable information (PII), personal health information (PHI), and financial information, organizations need to take additional security measures.

Cloud storage makes it easy to reach files from any location, but it is not a backup solution. If files are accidentally deleted or attacked, they are lost. Organizations have high volumes of data, so a cloud backup service is needed to automatically copy data so it can be restored.

Storage vs Backup

Cloud storage presents data risks like data theft or loss, corrupted data, and inadvertent sharing of information. Because cloud storage provides easy access to data, it presents compliance violation risks. Establish a ransomware protection service that scans OneDrive and other services and automatically blocks attacks. In addition, optimize security for cloud storage systems like OneDrive, with strict protocols:

1. **Device security**
   Implement basic protocols for the devices, including mandatory antivirus software, firewalls, and idle-time screensaver passwords.

2. **Network security**
   Instruct employees to ensure all connections are encrypted and never open OneDrive if the link is unfamiliar. A simple way to add protection is to turn off functionality that allows the device to connect to in-range networks.

3. **Secure sharing**
   Allow access to OneDrive to only invited users (not “Everyone”). Establish outlined rules for downloading and sharing documents inside and outside the organization. Terminate OneDrive for employees who leave the organization as part of the offboarding process.

4. **Sensitive data security**
   Store sensitive payment or other data on a secure on-premises or encrypted third-party cloud backup service that is compliant with mandatory regulations (instead of storing it on cloud storage like OneDrive).

5. **Cloud backup**
   Establish a cloud-to-cloud solution with automatic daily backup.

**DESIGNING EFFECTIVE SECURITY AWARENESS**

With remote work now the norm, a healthy, secure culture that encourages positive behaviors is an important as part of organizational cybersecurity. To shake the dull, technical stigma associated with security training, Help Net Security asked for insights on security awareness training from global experts.

**Embrace diverse learning for better participation and retention rates**
- Engage positively with employees by understanding that there are diverse learning styles. Adapt to these styles with rich and varied content that is customized for the organization and multilingual, when needed.
- Consider how to capture and retain attention. If humor works within an organization’s culture, it can catch your audience’s attention and engage in a relatable way.
- Reflect real-life cyber threats for a particular audience. For example, what may be appropriate for a general audience may be too basic for an IT team.

**Provide frequent training, but keep it short**
- Engrain cybersecurity into activities. Short training sessions of five minutes or less need to be provided at least monthly.

**Test awareness, publish results, and ensure results are tangible**
- Keep staff engaged by showing security awareness training effectiveness and how it improves the security posture of the organization.

**Tailor training**
- Focus on behaviors, rather than just awareness. Experts who understand risk and know which risks to focus on are well positioned to develop your solution.
- Update training for the current landscape. As threats change, so should the training.
- Identify employees who are more phish-prone with risk scoring. Increase time and resources on employees who are most at risk, while exempting those who demonstrate understanding already.


**EMERGING CYBERSECURITY APPROACH: XDR**

The number one trend noted by Gartner, Inc. in Top 9 Security and Risk Trends for 2020 is the emergence of extended detection and response (EDR) capabilities. This new, enhanced EDR model is called “XDR”, which is able to detect attacks across endpoints, networks, software-as-a-service (SaaS) applications, cloud infrastructures, and any other network. XDR enables an organization to collect and correlate data across multiple security products to improve threat detection and provide incident response for increased accuracy and productivity.

Uri May explains in the Security Boulevard article XDR: The Cybersecurity X-Factor: “XDR lets enterprise cybersecurity teams “punch above their weight” through the integration of advanced security operations capabilities. In particular, XDR promises to address today’s snowballing threatscape by amplifying the speed, scale, and scope of attack detection, connecting the dots across sparse data sources and siloed telemetry.”

While an organization has systems like firewalls, log management, and intrusion prevention in place to detect and protect against threats, XDR threat hunting assumes that advanced threats are evading these defenses and exist within the compromised environment.


The information above is provided as a convenience, without warranties of any kind and MUFG Union Bank, N.A. disclaims all warranties, express and implied, with respect to the information. You are solely responsible for securing your systems, networks, and data. You should engage a qualified security expert to advise on your specific needs and requirements.

This Cybersecurity News contains news and information designed to help protect your company and employees.