Protecting Microsoft 365 and Google Workspace data in accordance with NCSC guidelines

Introduction

In our fast-paced digital era, data is no longer just a byproduct of operations, but the very heartbeat of modern organisations. From steering intricate educational establishments' processes and driving strategic decisions to fostering customer engagement, the importance of data cannot be overstated. Platforms like Microsoft 365 (M365) and Google Workspace (GWS) are now cornerstones of educational establishments' functions across the globe — primarily due to the ubiquity of cloud computing. Despite their widespread adoption, there exists a misconception surrounding the comprehensive protection they provide. This necessitates a deeper dive into the intricacies of data protection, the shared responsibility model, and the role of third-party backup solutions.

1. Delving deep into Microsoft 365 and Google Workspace

The range of tools

M365 and GWS offer a diverse array of cloud-based productivity tools tailored for modern educational establishments. While M365 brings to the fore tools like Outlook, Word, Excel, PowerPoint and Teams, GWS presents a suite comprising Gmail, Docs, Sheets, Slides and Drive. These tools, although user friendly and collaborative, are repositories of vast amounts of sensitive information.

The nature of stored data

From daily email exchanges and scheduled meetings to intricate data analyses, strategic educational establishments' documents and expansive customer databases, the scope of stored data is vast. In this melting pot of information, both proprietary corporate data and personal customer information coexist — making their protection paramount.

2. The shared responsibility model

Understanding the model

The shared responsibility model is a fundamental tenet of cloud computing. It demarcates the boundaries of responsibility between cloud service providers (CSPs) like Microsoft and Google, and their end users.

CSPs' role: The security of the cloud

At their end, Microsoft and Google ensure the resilience of the infrastructure supporting cloud services. This encompasses physical data center security, routine server maintenance, consistent software updates and protection against overarching threats. Their role is all about providing a stable, secure and reliable platform.

Users' role: Security in the cloud

Contrary to popular belief, users play a proactive role in this model. They're entrusted with safeguarding their specific data within these services. This extends to ensuring user account safety, data access management, and just as importantly, protecting data via backup and recovery measures.

3. Microsoft's and Google's perspectives on data protection

Service agreements

Both Microsoft's Services Agreement and Google's Terms of Service underscore service reliability. However, a closer look reveals that comprehensive data protection isn't their primary domain.

Native protection tools

While both platforms offer native protection mechanisms like versioning, trash bins and limited retention, they're often insufficient — especially when seen through the prism of stringent regulations like the GDPR or the evolving threat landscape encompassing ransomware and phishing attacks.

4. NCSC's comprehensive guidelines on data backup and protection

The imperative of regular backups

Central to National Cyber Security Centre (NCSC) guidelines is the advocacy for consistent data backups, encompassing both operational data and system configuration details. This is a testament to the fact that data integrity is as crucial as the data itself.

Comprehending third-party measures

NCSC emphasizes that educational establishments must discern their protection capabilities and understand the guarantees they should expect from third parties, be they cloud services or suppliers.

Legal responsibilities

With data breaches becoming increasingly costly, both in terms of finances and reputation, the NCSC underscores the importance of legal obligations. Guidelines specifically reference GDPR security outcomes guidance, co-developed by the Information Commissioner's Office (ICO) and the NCSC.

5. Acronis Cyber Protect: Bridging the protection gap

Aligning with NCSC's directives

Acronis for M365 and GWS aligns seamlessly with the NCSC's recommendations, offering a holistic solution that plugs the protection gaps in native features.

Data protection and compliance

With industry-standard data centres, Acronis assures data security while also offering features that champion compliance with data protection regulations.

Comprehensive backup solutions

Transcending the native backup features of M365 and GWS, Acronis offers regular, automatic backups, housed in isolated cloud storage. This siloed storage strategy is a shield against potential threats targeting primary accounts.

The '3-2-1' strategy in action

Acronis' approach embodies the NCSC's '3-2-1' rule, ensuring diverse data storage options and optimizing data availability.

Security enhancements

Acronis' offering is fortified with advanced features like multifactor authentication, role-based permissions, anti-malware functions and intuitive recovery options.

Conclusion

The evolving digital landscape mandates educational establishments stay one step ahead — not just in terms of operations, but also data protection. With the shared responsibility model underpinning cloud services like M365 and GWS, relying solely on native tools is a gamble. Acronis emerges as the much-needed safety net, perfectly aligning with the NCSC's guidelines. By adopting such robust backup solutions, educational establishments can fortify their defences, ensure regulatory compliance, and pave the way for seamless educational establishments' continuity in the face of potential threats.

In the data-centric world, the stakes are higher than ever. Reinforce your M365 and GWS data protection with **Acronis** and fortify your data security infrastructure.

Acronis

Learn more at
www.acronis.com