SPHERE

CASE STUDY

A Growing Bank, Exploding SharePoint Risk

Growth is great, but there are always “pains” that come along with it. This was especially true for a SPHERE customer in the banking industry that experienced substantial growth through acquisition over the previous decade. As is often the case when a large, 100+ year old banking institution absorbs other financial entities, the pace of integration has been slow, creating technological debt and a reliance on legacy systems.

Combined with the rising threat of ransomware, an expanded attack surface brought by digital transformation, and a more demanding regulatory environment, this slow transition became even riskier. Within the bank’s decade of growth, regulatory requirements for data security such as the Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), and the General Data Protection Regulation (GDPR), all developed into major concerns.

The Background

Due to a new internal audit process, it was determined that the bank needed to go deeper into the systems and tools used to collaborate within their environment. One key finding stood out: SharePoint was a specific area where access controls were exceptionally weak.

SharePoint is a popular collaboration and document management platform developed by Microsoft that can present challenges in the context of Identity and Access Management (IAM) due to its complexity and the need to manage access to sensitive information effectively.

The company was tasked with strengthening their cybersecurity measures to decrease the risk presented by SharePoint, in a heavily distributed environment across all their various subsidiaries and acquired entities. This presented unique challenges for the bank, as their information technology and security teams were called upon to implement effective controls that would simultaneously merge the assets of acquired institutions and accelerate risk reduction, while minimizing business impact.

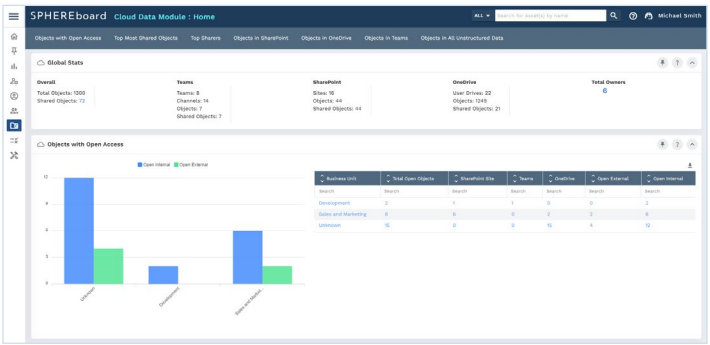
The Challenge

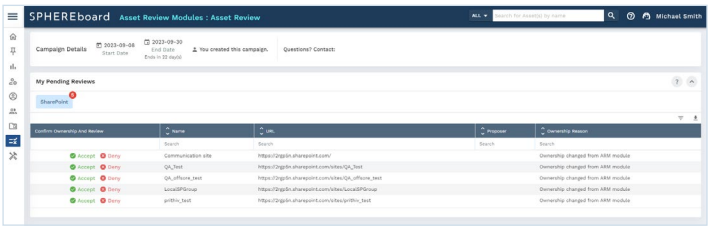
While SharePoint is an excellent tool for collaborating teams, there are some specific issues that make SharePoint a pain point in the Identity Access Management space:

- **Granular Access Control**: SharePoint allows for highly granular access control at various levels, including sites, libraries, folders, and documents, making it tough to ensure proper access governance.
- **User Roles and Groups**: SharePoint allows organizations to define custom roles and groups, but managing these while ensuring they align with organizational security policies can be complex. Without proper governance, unnecessary or inappropriate permissions may be granted.
- **Document Sharing**: SharePoint makes it easy for users to share specific documents with specific audiences, creating document-level access points which are a challenge to manage and control.
- **External Collaboration**: SharePoint often involves third-party collaboration. Managing access for external users while maintaining security can be complex and requires a robust IAM strategy.
- **Heavily nested AD Groups**: Leveraging heavily nested AD Groups in SharePoint permissions wreaks havoc on the ability to perform accurate entitlement reviews. Often, this can obfuscate the true effective membership and thereby the true entitlements to the owner.

Until this point, SharePoint had escaped the attention of the IT audit team and was not a priority for the bank's security and risk teams. The new audit schedule exposed SharePoint access issues and its lack of controls. The institution first needed to assess and present the issue, then determine action and budget to deliver a comprehensive remediation program. As SharePoint is a specialty application, the bank's security team lacked the skills to quickly perform the assessment and subsequent remediation.

The SPHERE Solution





SPHEREboard is a comprehensive Identity Hygiene platform, providing a critical identity lens to the data problem. The solution combines business intelligence, institutional knowledge, and industry best practices to reduce identity and data risk. Developed by experienced practitioners, SPHEREboard combines detailed discovery, automated remediation, seamless integration with your security ecosystem, and more.

By employing the SPHEREboard for Data platform, SPHERE successfully partnered with the organization to get these SharePoint access issues under control via a three-phase pronged approach.

Phase 1: Discovery

The first phase in the process was for SPHEREboard to identify the bank's key risks and issues. It was necessary to ensure that access controls within the SharePoint environment were effectively designed, implemented, and managed to protect sensitive data, maintain compliance, and minimize security risks. SPHEREboard was used to inventory all SharePoint sites and user access rights for sites, libraries, folders, and documents. Which users or groups have administrative privileges and superuser rights? How are internal and external documents being shared?

Access Control Lists (ACLs) and permissions inheritance were next. Reviewing the ACLs applied to SharePoint provided visibility to who has read, write, and delete permissions, not to mention their granularity and whether they aligned with data sensitivity and business requirements. By determining whether SharePoint sites and document libraries inherit permissions from parent sites or have unique permissions helped to assess the impact of breaking permission inheritance on access control.

Phase 2: Remediation

Now that most SharePoint access permissions were better understood, the next phase was to declutter data and access. By retiring stale SharePoint sites from production environments that are no longer required and cleaning up "orphaned" user accounts (inactive or terminated user accounts that haven't been promptly removed or deprovisioned), SPHEREboard provided a cleaner view of the environment.

Another crucial activity in the Remediation Phase involved flattening and "de-risking" the nested groups used across the SharePoint environment. To fully enumerate AD Groups, the group and subgroup members have to be visible. De-nesting or "flattening" the groups meant drilling into each group and providing full inventory of their members, removing redundant and unnecessary members and flattening the groups.

The team could now establish ownership and catalog the authoritative source for making decisions about who should and shouldn't have access. Owners could now be mapped to business units to understand the distribution of sites across the company, enabling the remediation of overly broad SharePoint permissions.

When changing permissions as part of Remediation, it is critical to secure access without inadvertently causing system disruption or down time. SPHEREboard provides pre- and post-change reports with simple rollback features, in the event the change needs to be reverted. Additionally, SPHEREboard integrates with Change Management solutions to ensure proper policies and procedures are adhered to and tracked as part of the remediation workflow.

Phase 3: Sustain

Once the bank's SharePoint data and access permissions were cleaned up, the final phase shifted to ongoing discovery and remediation. Resource-heavy tasks like performing regular entitlement reviews (e.g., to ensure that user permissions remain appropriate) and implementing least privileged access are now automated, and disruptive issues like breaking permission inheritance and misconfigurations are preventable with the use of the SPHEREboard platform, resulting in an evergreen state of Identity Hygiene.

Conclusion

SPHERE's partnership with the financial institution proved instrumental in tackling the significant identity and access management challenges posed by their expansive SharePoint environment. By utilizing SPHEREboard's comprehensive discovery, remediation, and sustainability processes, the bank was able to mitigate risks, streamline permissions, and establish a robust framework for ongoing governance. This proactive approach not only enhanced the bank's security posture but also ensured regulatory compliance and operational efficiency. SPHERE continues to provide critical identity hygiene solutions that help organizations protect their most sensitive assets while minimizing business disruption.

About SPHERE

SPHERE is the global leader in Identity Hygiene. We are dedicated to reshaping modern identity programs by embedding this foundational fabric, enabling organizations to quickly reduce risks. We work through an identity lens that protects an organization's accounts, data, and infrastructure. Our solutions deliver immediate time-to-value by leveraging automation to discover, remediate and secure identities, now and forever.

Driven by our core values of passion, empathy, and authenticity, our vision drives us to continually innovate, helping our clients to sleep better knowing their attack surface is drastically reduced, thwarting the plans of bad actors every single day.

We're ready to help you address your Identity Hygiene and security challenges. To find out more about SPHERE and our solutions, please visit www.sphereco.com.

