5 DATA SECURITY CHALLENGES & TIPS FOR SECURE COLLABORATION

How to Balance Security and Collaboration Needs

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Team collaboration within the workplace has been evolving steadily for several years. From the early days of email attachments and network shares to the cloud-based document centric tools that are available today. In parallel, the data security and protection needs have also changed as collaboration has moved data beyond fixed office locations and corporate firewalls, cybersecurity threats have increased and new data protection regulations have come into effect. This paper will explore the underlying factors driving how people now use and share information and the impact that has had on how organizations need to protect their sensitive data. It will examine how the competing needs of users, IT Security and Information Security can result in serious data security risk within an organization and some of the considerations for mitigating that risk.

Collaboration in the Modern Workplace

Today the options for sharing and collaborating on content are more plentiful than they have been at any other point in time. The tools have also evolved to the stage where collaborating in real time on a single piece of content through dual editing or conversing with team members in the same user interface that the content resides is rapidly becoming commonplace.

Initially driven by collaboration platforms such as SharePoint, OneDrive, Box and Dropbox and now with tools like Slack and Microsoft Teams enjoying rapid adoption and favorable feedback from end users with their flexible content and user centric approach to collaboration. From the IT perspective many challenges remain as administrators and information security professionals attempt to maintain control of sensitive business data while also trying to keep users happy.

The resulting dynamic nature of how information is created and shared within the modern workplace coupled with the variety of security threats now present in the world requires enterprises to adopt new processes and technologies that will appropriately protect their sensitive data assets.

5 SECURITY CHALLENGES IN THE MODERN WORKPLACE

THE GROWING THREAT FROM WITHIN

Breaches or leaks where an inside element is either wholly or partly responsible is on the rise. McKinsey reports that almost 50% of breaches now fall into this category.

Sadly, there are no shortage of references for data breaches in the world today. Breaches and leaks are now headline news and their effect on an organization of any size can be devastating. The accidentally leaked Doctor Who scripts from the BBC and the huge Marriott data breach which exposed a large range of personally identifiable information including passport numbers are just two of the high-profile incidents in recent times. These two cases illustrated the two main categories of breaches that organizations face – those originating from external parties and those from inside threats.

Historically IT security has focused on protecting from threats outside the firewall. Perimeter defences, anti-malware and intrusion detection systems are just some of the tools that organizations deploy to protect their networks. However, when it comes to the nature of information collaboration and its associated security a different approach is needed in order to appropriately protect data within the modern workplace.

Traditional information security approaches for collaboration tools have relied upon authentication and permissions to secure access in order to protect to the data. Today data is almost constantly in motion, often traveling outside firewalls or organizational boundaries, therefore location-based controls are no longer enough. Protection must also extend to other elements of modern collaboration such as the social exchanges as sensitive content no longer just takes the form of documents and files.

1. The Increasing Threat from the Inside

Most cybersecurity reports will show that the largest number of attacks still originate from external parties attempting to infiltrate an organization's network through a variety of different means. However, breaches or leaks where an inside element is either wholly or partly responsible is on the rise. McKinsey reports that almost 50% of breaches now fall into this category. When it comes to insiders being completely responsible the figure for accidental leaks alone is 22%.[1] As a result, many organizations are rethinking their approach to protecting sensitive data as traditional location-based security of restricting access to where data is at rest does not adequately protect data that is nowadays in an almost perpetual state of motion and change.

2. Balancing IT and User Requirements

When there is disconnect between the needs of the business users and the responsibilities of IT for securing sensitive data the result is often increased data security risks from the use of rogue or shadow IT solutions. In the modern workplace the challenge is greater than ever due to increased cybersecurity threats and increasingly tech-savvy users that are happy to obtain their own tools in order to get their work done.

What Users Expect

Users expect a seamless experience for most of the technology that they use as part of their working life, in particular collaboration tools. Today's users want access to their data from any location and on any device. They want to share information with colleagues or external parties with only a few clicks. At the same time, users are more aware of the part that they are expected to play in protecting sensitive company data due to the heightened threat of data breaches - many of which have impacted individual's personal lives.

[1] McKinsey, Insider threat: The human element of cyberrisk: https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk

However, users still demand that enterprise tools fit their collaboration needs while also providing the built-in protection that sensitive data requires – a difficult balancing act for IT. If the tools do not, then despite knowing that they are breaking the rules, users will circumvent the IT provided tools. This behaviour contributes to the 22% of data breaches that involve accidental leakage of data.

What IT and Information Security Expects

Despite IT's investment in technologies that provide a better fit for both data security and user needs, there will likely still be conflicts between IT requirements and user desires. In organizations that have a distinct Information Security function the potential for conflict can be particularly high. Typically, when it comes to security, IT will focus on adaptability, technical features, and efficiency; information security professionals' priorities include confidentiality, integrity, and availability with user priorities often straddling somewhere in between the two.[2]

As IT tries to simplify sharing capabilities or improve collaboration with social tools to enable users to get their work done this will likely add risk to the confidentiality and integrity of information. Conversely running any information security requested audits on access rights or scanning for device vulnerabilities can frustrate both users and IT alike as they cause resource constraints for IT and system performance or uptime challenges for users.

3. Enterprise Collaboration Tools

The latest breed of collaboration tools like Slack and Microsoft Teams incorporate in-context comments and messaging to surround documents and files in a single user experience presenting a new challenge for IT. Slack and Teams have enjoyed rapid adoption and growth, clearly pleasing users with their collaboration capabilities. However, most organizations will likely not be prepared to provide the required level of data security across all elements of these tools. The single location to freely share files and other data with both colleagues from within an organization and users from outside clearly demonstrates one of the areas of conflict for users, IT and Information Security. Not only does this present a single platform to attack for external threats but the possibility for accidentally leaking sensitive content is also increased. This risk is made worse by the nature of the where the sensitive data is captured – both within files and the associated social interactions.

4. Collaborating on Any Device from Any Location

Users can now carry out their work from almost any location and from any device. In response, IT has employed Bring Your Own Device (BYOD) protection and management technologies. While this type of approach certainly improves data protection, e.g. remote wipe capabilities for lost or stolen mobile devices, they fail to take into account the context of both the data in question and the person trying to access and use it. The static or binary nature of typical BYOD or mobile workforce controls – either allowing or denying a device or an individual access to content falls short of what is truly required.

REGULATIONS DRIVING CHANGE

It should come as no surprise that regulatory bodies have acted due to the increase in the number of high-profile and large-scale breaches that have occurred. New EU regulations have had a domino effect on other controls that were historically in place driving regulations that have implications for almost every enterprise on the planet that handles sensitive data.

Although the definition of sensitive data within these regulations applies to consumers or individuals, the policies and controls that result, such as "privacy by design", can also be applied to other sensitive data types. For example, the systems and process used to protect an organization's intellectual property or any other sensitive proprietary data type.

1. **European Union General Data Protection (GDPR) i**s a law that is directly binding and applicable with heavy fines being imposed on those who are found to have not met the data protection requirements. Large companies are already under investigation by the European Regulators. The recent Facebook data breach could carry a fine of up to $1.63 Billion under GDPR and Marriott could also be fined a large amount due to their massive data breach.
2. **EU-US Privacy Shield** is a framework for regulating the transatlantic exchange of sensitive data for commercial purposes between the European Union and the United States. It is designed to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens.
3. **At present there is no US equivalent of GDPR** but there are signs that US government agencies are in the process of considering how they should adapt their policies. In September of 2018 the National Telecommunications and Information Administration announced a request for comment on a new approach for consumer data privacy. In parallel, the Commerce Department's National Institute of Standards and Technology and the International Trade Administration are working on new initiatives. The former is working on a framework to assist organizations manage data privacy risks and the latter is working to increase global regulatory harmony.

[2] Dark Reading https://www.darkreading.com/vulnerabilities---threats/rip-it-security/a/d-id/1333236?_mc=sm_iwfs_editor_kellysheridan

ON DEMAND COLLABORATION

Users can now carry out their work from almost any location and from any device. The almost constant in-transit and dynamic nature of collaboration results in an ever-changing data risk profile. It might be perfectly acceptable for an individual to access 99% of content from both within their office location and their local coffee shop but restrict access or usage rights to the most sensitive 1% of documents.

The almost constant in-transit and dynamic nature of collaboration results in an ever-changing data risk profile. It might be perfectly acceptable for an individual to access 99% of content from both within their office location and their local coffee shop but restrict access or usage rights to the most sensitive 1% of documents. A data location-based approach to data security for a mobile workforce would require a different data container in order to enable protection in this scenario.

There are many challenges associated with this approach. First the sensitive data must be located and then the multiple data containers with their multiple permissions must be administered over time for all the sensitive data within the organization. Multiple data containers often break collaboration and make it difficult for users to find the data that they need. If this approach is to be successful it relies on the sensitive data remaining within the original locations or that other files outside the protected containers do not gain sensitive data later. Typically, this is not a viable approach therefore organizations have to choose between overly restrictive permissions or much more open access thus increasing their risk.

5. Retaining Control of Sensitive Data

Even if securing access to sensitive data in modern collaboration is achieved in a way that satisfies both IT and users this only solves part of the overall challenge. In order to fully protect data organizations need to be able to control what happens after the sensitive data is accessed. The container-based security approach fails to consider usage rights for the data across all scenarios e.g. perhaps there is a need for a user to access data from a remote location but restrict them to a secure viewer with a watermark applied to the data. Another common scenario when sharing between organizations is restricting the ability for the user to additionally share the information with another user within their own organization or perhaps automatically expire access to that content after a period.

The additional reason for applying a more layered approach to securing the data relates to a data point earlier in this paper – namely that 50% of breaches involve an insider element. In breaches that involve compromised credentials accessing data a more sophisticated approach that recognises the context of a user using properties such as location of the user or typical hours of access can mitigate the risk of an external party obtaining sensitive data. The ability to dynamically apply access and usage rights based on the context of both the content and the user is necessary in order to match the capabilities of modern collaboration tools and the types of security risks that organizations face.

Data security within modern collaboration needs to learn the lessons that the collaboration tools themselves learned. An effective security model must take a balanced user and content centric approach to protecting sensitive data. The collaboration tools themselves cannot take center stage with the security mechanisms but instead must work in tandem with technologies that maintain security long after the data has left the confines of the collaboration repository.

To do this successfully organizations need to take a 5-step approach to build their security for modern collaboration.

5 TIPS FOR BALANCING SECURITY AND COLLABORATION NEEDS

1. Start with the Data Locations

The first step is to identify where all the organization's data currently exists within the various data repositories and the various tools used to store it. With 70% of organizations still suffering from data in rogue clouds it is critical to correctly identify where this is happening.[3] The assumption that an enterprises data resides solely in IT provided collaboration environments is likely to be mistaken. To achieve this Cloud Access Security Broker (CASB) tools should be considered in order to detect where Shadow IT exists within your organization.

2. Classify Data

Once the locations of all the data have been identified there should be an attempt to classify the data. It should be noted that it will be almost impossible to accurately classify every piece of data within an organization and this should not be the goal. A successful strategy will classify data on a continuous basis to account for how information and its associated attributes changes over time therefore accurate classification of data will increase over time. The tools typically employed for this task form part of a Data Loss Prevention solution although this capability is sometimes available as a standalone offering. These solutions usually rely on standard sensitive data types, such as PII like Social Security Numbers, and mechanisms to detect data of this type. The limitations of detection and classification mechanisms is why it is difficult to strive for a very high percentage of classification accuracy. Newer tools have begun to incorporate elements of Artificial Intelligence, in particular Machine Learning, to improve how they identify and classify information.

3. Audit User Interactions with Data

Users are obviously going to be central to the success of any solution therefore it is important to analyse how users are currently creating and interacting with the data. Is there a group of users or department that handles a high volume of sensitive data? Who has access to key intellectual property assets or who has been accessing this type of content? Where is there a need to share and collaborate externally? Which users tend to work remotely?

These are just some of the questions that should be asked when building a picture of user interactions with the sensitive data. As it is likely that current protection mechanisms will rely on access and permissions-based controls an audit of said controls should be conducted. The results of these audits should only form part of the picture and content owner and user interviews should also be carried out to establish what should be happening. Current permissions-based security likely offers too much or not enough access to individuals in certain scenarios. An audit alone will not reveal where this is the case. This stage will also identify where the access and usage rights should change based on the content and context of the user.

4. Identify Governance Requirements

The most obvious requirements are to identify any data protection regulations that must be followed. The EU GDPR has far reaching implications including for organizations not based within the EU's borders. Even enterprises without any physical location within Europe should not assume that the regulations do not apply to them. Secondly, the data security needs specific to your organization should be considered. What intellectual property assets within the organization must be protected and what other information if leaked would be catastrophic? Within the organization itself what are the departmental boundaries that must be respected? Segregating access and use of HR content or securing financially sensitive data for securities regulatory compliance is commonplace. For example, mergers and acquisitions often have their own set of data protection and usage requirements.

5. Enlist the Right Technology

Just as the collaboration tools have evolved, so have the available technologies for protecting sensitive data within modern collaboration environments. New capabilities have emerged, and some existing technologies have undergone change to the point where they are enjoying a rebirth within the data security market. CASB, Data Classification tools and DLP solutions form key components of data security and protection within modern collaboration as indicated in earlier sections. Two key technologies that warrant additional attention are data-centric security and Rights Management.

Data-Centric Security

A data-centric approach goes beyond the information at rest security scenarios in your collaboration tools and associated repositories that traditional access controls and permissions provide. When you consider the data itself rather than the container in which it resides and how it will be created, how it will change, be used and shared across its lifetime you quickly realize that security and protection must be extended to more than just the collaboration repository. It also greatly mitigates against breaches caused by insider threats, whether that is due to compromised credentials, a deliberate leak by a disgruntled employee or a user accidentally exposing information.

[3] Symantec: Avoiding the Hidden Costs of the Cloud https://www.symantec.com/connect/blogs/avoiding-hidden-costs-cloud

A data-centric mindset also fits better with how people within and between organizations collaborate by using a variety of different tools. An approach of this type will apply regardless of where the data moves and the tools and platforms that it moves through.

Rights Management

Although Rights Management has been available as a technology for many years, Microsoft's version was first released in 2003, it has struggled to gain a foothold outside of the field of digital rights management for protecting media assets. However, this technology is key to providing the flexible control on the access and usage rights needed to enable the protection that modern collaboration scenarios require.

Data-centric next gen DLP solutions will provide contextual classification and protection policies but Rights Management will be needed to enforce those policies particularly in scenarios that require dynamic protection based on the content and user context as discussed previously. It is also required to provide the same security and protection to sensitive data when it is shared outside the collaboration repository.

PUTTING THE PIECES TOGETHER

While modern collaboration has provided many benefits to the enterprise, its next iteration needs to also incorporate intelligence to help combat the risks. IT and information security practitioners need to evolve to an intelligent workplace that is secure, where users are free to be as dynamic as they need to be with the protection businesses require.

Nucleus Cyber provides a way to leverage AI-driven data security that dynamically provides granular control over your organization's IP and information without restricting the collaboration freedom that your users demand or risking the high cost of being too open with your sensitive data.

5 TIPS FOR BALANCING SECURITY & COLLABORATION

1. Start with Data Locations
2. Classify Data
3. Audit User Interactions with Data
4. Identify Governance Requirements
5. Enlist the Right Technology

CONTACT US TO LEARN MORE.

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS.com | info@archtis.com

Australia | United States | United Kingdom