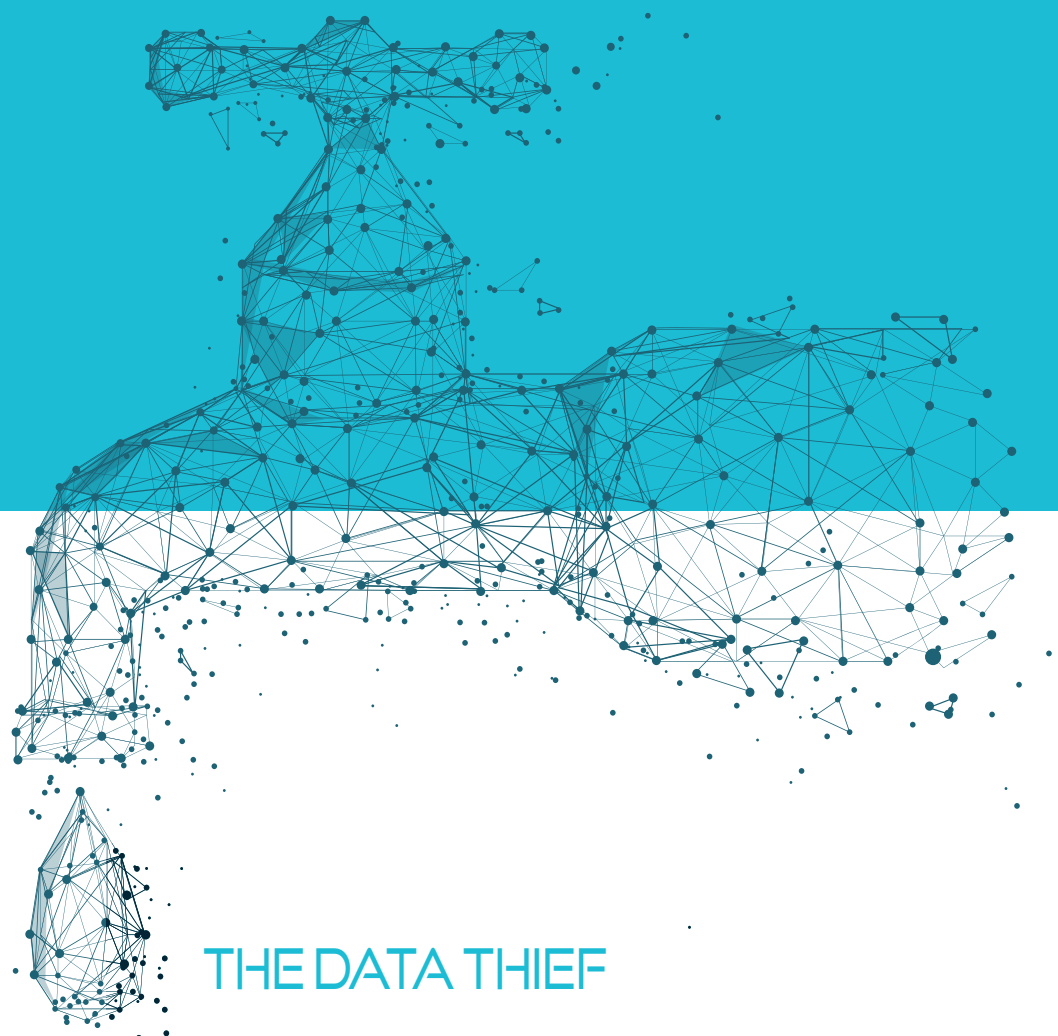
IDENTIFYING THE TOP INSIDER THREATS TO DATA SECURITY



The best thing and worst thing about collaboration tools is you can put anything in them and share it. They present a multitude of ways to collaborate, but without the proper data-centric security controls also open the door for insider threats from data misuse, to malicious theft and those dreaded 'whoops!' moments.

We've identified the insiders found in every organization who are inadvertently (and some deliberately) putting your organization at risk bypassing governance and training, misusing privileges, stealing IP, sharing confidential data with unauthorized parties, and making innocent mistakes.

The insiders we uncovered might surprise you.

THE ANONYMOUS ADMIN

Andy likes to log into SharePoint Sites as the farm account admin and browse libraries and documents that otherwise are not shared with him. Site and document access are regularly audited, but Andy knows multiple people have access to the farm account and thought his actions were untraceable. Unfortunately, Andy was busy browsing over the holidays when he was the only admin on site and subsequently caught.

1/3 of IT administrators or somebody they know with admin rights have read documents hosted in Microsoft's collaboration tools that they are not meant to read.

92% of admins said they realized their actions made the material less secure.

30% of admins were not bothered because taking the information had helped them get their job done.

34% of IT admins admit to sneaking a peak at documents they were not authorized to view including employee details and salary information.

74% of data breaches involve privileged credential abuse.

THE DATA THIEF

Dave just accepted a job offer with a competitor that pays better and has a shorter commute. He'll be moving on in two weeks, but not until he makes copies of his client contacts, internal communications on planned product improvements, and anything else that will help him succeed at his new company.

$600 BILLION in annual losses to the U.S. economy due to theft of American intellectual property.

69% of organizations say that they have suffered significant data or knowledge loss resulting from employees who took information resources with them when they left the business.

50% of data breaches come from within a company, not from external threats as many think.

68% of breaches took months or longer to discover – especially when they involved legitimate access.

THE FOLDER FIEND

Fran creates sub-folder after sub-folder within her document libraries. She sometimes buries them 6, 8 or even 10 layers deep, creating unique permissions which make them hard for others to find and collaborate. She even uploads files to folders on Dropbox to share them with others instead of going through the hassle of asking IT to adjust sharing permissions or provision a new third party user.

71% of enterprises struggle to manage and protect unstructured data.

4 OF 5 organizations don't know where their sensitive data is located, nor how to secure it.

77% of all businesses experience rogue clouds;

40% saw confidential data exposed there.

THE CLUELESS UPLOADER

Cher inadvertently emailed the wrong recipient, a third party, an unsecured file with all her company's employee social security information and other PII (personally identifiable information). An innocent mistake that's now opened up the company to privacy violations and fines.

50% of breaches had significant insider element;

22% of breaches involved employee negligence.

$3.86 MILLION average cost of a data breach.

$148 average cost for each lost or stolen record containing sensitive and confidential information.

THE REPEAT OFFENDER

Phil repeatedly snoops on patient data and shares PHI (protected health information) with unauthorized parties. His actions are the cause of chronic data breaches exposing his organization to costly HIPAA violations and fines.

28% of healthcare breaches are caused by insiders;

2.8 MILLION patient records breached in 139 insider related incidents.

4 PER 1,000 nearly four healthcare employees breaching patient privacy per every 1,000 employees.

51% of healthcare privacy violations were caused by repeat offenders.

4 WAYS TO PREVENT INSIDER BREACHES

1 Find & Audit Your Data

- Identify where all your data currently exists within the various data repositories and tools used to store it.
- Scan content at rest and in motion in collaboration systems including Office 365, SharePoint, files shares, Dropbox, email, enterprise social platforms, BOTs, etc. for sensitive data including personally identifiable information (PII), cardholder data, protected healthcare data (PHI), IP or corporate confidential information.
- Track all access to sensitive data as well as what actions that have been taken with it to provide a full audit trail.

2 Classify & Secure Data

- Classify documents automatically based on the presence of sensitive data and provide options for users to classify data as it's created.
- Set business rules with your classifications to restrict actions that can be taken with classified documents such as print, email or save as to prevent data leakage.
- Ensure that documents accessed on the mobile devices like iPads have the same security restrictions and prevent back door access to documents

3 Address Changing Risk Profiles

- Look at data on a continuous basis to account for how information and its associated access attributes and user context change over time, then adjust its security accordingly.
- Assess the risk profile associated with the data and its use cases, then consider the security that should be applied in each scenario.

4 Balance Collaboration with Security

- Keep the right balance between what users want from a collaboration perspective and what the organization demands from a security perspective.
- Go too far in either direction and you can make your situation worse. Too lax and your data can be shared far too freely. Too stringent and your users find an alternative way to share and collaborate. In either situation you lose visibility and control of your sensitive data.

McKinsey review of VERIS Community Database - 2018 , 2018 Cost of a Data Breach Study, Ponemon Institute & IBM, Symantec: Avoiding the Hidden Costs of the Cloud, SailPoint's 2017 Market Pulse Survey, 2017 State of Cybersecurity Metrics Annual Report from Thycotic, Protenus 2019 Breach Barometer, https://www.cio.com/article/3192842/sensitive-data-often-follows-former-employees-out-the-door.html, https://www.theregister.co.uk/2012/01/23/sharepoint_leaky_security/

NUCLEUS CYBER

www.nucleuscyber.com