2021 DATA RISK REPORT

FINANCIAL SERVICES

On average, **every employee** has access to **nearly 11 million files.**

CONTENTS

VARONIS

ABOUT THE REPORT

This is the fourth annual *Data Risk Report* — but while past reports have focused on the consolidated findings of 30+ industries, this year we've prepared separate reports for the most at-risk verticals in order to analyze industry-specific threats, trends, and solutions.

The *2021 Financial Services Data Risk Report* focuses on the data security of the financial industry: banking, insurance, and investments. It was compiled using data analysis of 4 billion files across 56 financial services organizations.

Many of our findings are further broken down by company size:

- **Small:** 0–500 employees
- **Medium:** 501–1,500 employees
- **Large:** 1,501+ employees

In addition to the key findings of past reports, this report draws meaningful correlations between the current state of the industry and the mounting threats faced by financial services. These conclusions are derived using Varonis solutions that analyze data stores in conjunction with industry benchmark reports.

Compiled using data analysis of **4 billion files** across **56 financial services organizations**

Banking

Insurance

Investments

KEY FINDINGS

2020 was an unprecedented year in IT and IT security. Organizations around the world responded to the threat of COVID-19 by implementing stay-at-home policies. This resulted in a dramatic uptick in employees collaborating using Microsoft Office 365 and other cloud-based software, while also accessing more resources through company VPNs.

The abrupt nature of this transition forced many companies to step into the cloud without proper cybersecurity preparedness, inadvertently increasing their attack surface as employees logged in through unsecured networks and home computers. The risk increases exponentially when companies have obvious gaps like passwords that never expire and folders containing sensitive data open to every employee.

On average, a financial services employee has access to nearly **11 million files the day they walk in the door.** For large organizations, the number is double: **20 million files open to all employees.** These remain prevalent issues in the industry.

Impact on the Industry

Securely transitioning to remote work and locking down exposed data to mitigate the risks stemming from remote logins were two of the highest security priorities for IT teams in financial services. Mobilizing without proper security controls exponentially increases the risk posed by insiders, malware, and ransomware attacks, and exposes companies to possible non-compliance with regulations such as SOX, GDPR, CCPA, and PCI.

VARONIS

Every employee
has access to nearly
11 million files

Nearly **two-thirds** of companies have **1,000+ sensitive files** open to **every employee**

About **60% of companies** have **500+ passwords** that **never expire**

GLOBAL FINDINGS

The Future is Automated

Exposure by company size

Financial Services company size	Avg. # of files	Avg. # of files open to everyone	Avg. % of files open to everyone
Large	134,368,022	20,427,920	15%
Medium	75,085,577	10,254,062	13%
Small	6,800,969	570,284	11%
Industry average	**74,309,255**	**10,774,940**	**13%**

Financial Services company size	Avg. # of folders	Avg. # of folders open to everyone	Avg. % of folders open to everyone
Large	9,000,369	1,383,656	15%
Medium	5,209,135	778,045	15%
Small	6,800,969	101,717	10%
Industry average	**5,204,344**	**776,943**	**13%**

Financial Services company size	Avg. # of sensitive files	Avg. # of sensitive files open to everyone	Avg. % of sensitive files open to everyone
Large	802,315	55,396	8%
Medium	344,653	37,911	18%
Small	163,435	12,550	19%
Industry average	**449,855**	**36,004**	**15%**

On average, a financial services employee has access to 13% of the company's total files. Put into perspective, this means that even employees in the smallest firms have unrestricted freedom to view, copy, move, change and delete data for over half a million files — **including almost 20% of all files containing sensitive employee and customer data.** The number of exposed files doubles as company size increases; the largest financial services organizations average over 20 million files open to every employee.

GLOBAL FINDINGS

Average State of Data Per Terabyte

Industry	Files	Folders	Exposed folders	Sensitive files	Uniquely permissioned folders	Exposed sensitive files	Stale, sensitive files	Unresolved SIDS	Folders with inconsistent permissions	Number of reports	TB Analyzed per company
Large	1,280,436	108,004	19,080	19,582	12,812	1,779	10,165	1,227	818	20	126
Medium	1,425,052	135,883	18,175	12,134	9,474	1,168	9,540	1,590	505	18	65
Small	1,090,355	131,775	20,516	35,506	12,484	2,571	20,586	1,576	1,948	18	12
Average	**1,265,822**	**124,606**	**19,251**	**22,306**	**11,634**	**1,837**	**13,314**	**1,456**	**1,081**	**56**	**70**

To compare apples to apples, we need to analyze the at-risk data per terabyte across different company sizes. The average terabyte contains 1.3 million files and approximately 2% (20,000 of those files) contains sensitive information, including financial data and PII. Assessing the risk per terabyte provides a clearer picture of the typical attack surface by company size and shows us which organizations are most vulnerable.

What we discovered is that financial services organizations average roughly 20,000 exposed folders (open to everyone[1]) per terabyte — and this remains true regardless of company size. It takes IT professionals an estimated 6–8 hours per folder to locate and manually remove global access, meaning **it would take more than 15 years to remediate these folders manually** (assuming no new folders are added… and the IT team never stops to sleep).

It's an extremely important task, **especially for small companies (<500 employees) who believe they're too small to be noticed by bad actors.** But it's impossibly tedious and time-consuming without security automation.

[1] For this report, "everyone" indicates every employee within the organization.

GLOBAL FINDINGS

Path to Least Privilege

Companies with sensitive files open to all employees via global access

Sensitive files open to everyone	% of companies
< 1,000	35.71%
1,000-10,000	25%
>10,000	39.29%

Stale sensitive data by financial services company size

Financial Services company size	Avg. # of stale sensitive files	Avg. % of sensitive files that are stale
Large	526,606	63%
Medium	208,490	74%
Small	109,152	74%
Industry average	**290,173**	**70%**

Global access groups (e.g., Everyone, Domain Users, Authenticated Users) open financial services firms up to a world of risk. Imagine one user clicking a phishing email and setting off a chain reaction. Financial services take an average of **233 days to detect and contain a data breach**[2], meaning that the industry average resolution time is **eight months** — enough time to severely damage reputation, revenue, and customer faith.

Over 64% of financial services companies have 1,000+ sensitive files open to every employee. This puts them at risk of non-compliance with regulations like the EU General Data Protection Regulation (GDPR), Sarbanes-Oxley (SOX) and California Consumer Privacy Act (CCPA) — which all require strict controls on sensitive information. Violators could face prison and (in the case of GDPR) up to €20 million or 4% of global revenues in fines.

Sensitive stale data — critical data about employees, customers, projects, clients, and proprietary business content that hasn't been touched in over 90 days — is similarly regulated. On average, **70% of all sensitive data is stale.** If this data is kept beyond a predetermined retention period, it exposes an organization to increased risk and liability.

[2] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

GLOBAL FINDINGS

Poor Active Directory Hygiene

Companies with passwords that don't expire

Passwords that don't expire	% of companies
< 500	41.07%
500-1,500	37.50%
> 1,500	21.43%

Companies with ghost users

Size of stale user account group	% of companies
< 1,000	35.71%
1,000-10,000	25.00%
> 10,000	39.29

Oftentimes, the easiest and quickest way to get into a server and move around undetected is to access user and service accounts that are inactive but enabled ("ghost users"). These, along with stale user account groups and privileged users with passwords that never expire, give hackers a window through which they can steal data or cause disruption without being detected.

Hunting down these vulnerabilities manually requires time and organized cross-team collaboration. Unfortunately, it rarely takes priority. As a result, **59% of financial services companies have over 500 passwords that never expire** and **nearly 40% have more than 10,000 ghost users**.

STATE OF THE INDUSTRY

Financial services finds itself in the strange situation of being one of the most improved in terms of security maturity, but still at incredibly high risk comparatively. It remains one of the most targeted industries by malicious attacks, due in large part to the sensitive data it collects from its customers[3]. The average cost of a data breach[4] is among the highest of any industry, at 5.85 million USD.

In 2020, financial services boasts the lowest average time to identify and contain a data breach — but remote work has the potential to significantly increase response time. The longer incident response takes, the higher the cost of the data breach is likely to be. The importance of complete visibility into network environments and fully deployed security automation cannot be overstated.

As financial services take to remote work via Office 365, having guardrails in place to enforce controls and manage the increased risk is taking priority. Proving regulatory compliance in this environment can be tricky, so clear audit trails and reporting mechanisms are must-haves.

The average cost of a financial services data breach is among the highest of any industry, at **5.85 million USD.**

[3] https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/financial-services-data-breaches/

[4] https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

CASE STUDY

PROSPECT CAPITAL

How Varonis helps Prospect Capital's CTO create compliance reports in minutes, not hours

Prospect Capital is moving its data into Microsoft's cloud. To make the move with confidence and help produce ITGC Recertifications and simplify SOX compliance, they needed more visibility into their data infrastructure and reporting mechanisms.

Find out how Varonis helps.

DOWNLOAD THE FULL CASE STUDY

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, specializing in software for data protection, threat detection and response, and compliance. Varonis protects enterprise data by analyzing data activity, perimeter telemetry, and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

Varonis is the helping hand that allows us to properly respond to our auditors and be more organized and effective in our deliverance to audit requests. Reports that used to take days to compile are now automatically prepared for us in under 10 minutes with Varonis.

AL FAELLA
CTO, Prospect Capital Management

Want to see how **your organization** stacks up?

Get a free Varonis Data Risk Assessment. Uncover hidden risks to your most important data — fast, and without adding work to your plate.

CONTACT US

Trusted by