2021 DATA RISK REPORT

MANUFACTURING

Over **6 million** files are open to every employee — a surprising blast radius that places information at risk from ransomware and insider threats.

CONTENTS

VARONIS

ABOUT THE REPORT

The *2021 Manufacturing Data Risk Report* is the third report in our annual series analyzing industry-specific threats, trends, and solutions.

This report focuses on the growing cybersecurity threats facing industrial manufacturers and engineering firms. We compiled our findings by analyzing 4 billion files across 50 organizations.

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

1. **Small:** 0–500 employees
2. **Medium:** 501–1,500 employees
3. **Large:** 1,501+ employees

This report aims to help manufacturing organizations assess the current cybersecurity landscape objectively and provide advice that companies can leverage to decrease their attack surface.

Compiled using data analysis of **4 billion files** across **50 manufacturing organizations**

Industrial Manufacturers

Engineering Firms

VARONIS

KEY FINDINGS

Threats against the manufacturing sector continue — from big game ransomware groups that steal victim's data before encrypting it, to nation-state attackers seeking technology secrets, to company insiders looking for information to grab and sell to the highest bidder. Recent news headlines show how crippling ransomware attacks can halt assembly lines and disrupt supply chains.

Overexposed information — especially sensitive data – exponentially increases risk. This exposure is your "blast radius" — think of it as all the damage an attacker can do once inside your environment. If just one employee clicks on a phishing email, an attacker can potentially access every file an employee can touch. When a company insider decides to go rogue, they can take their time and steal valuable information to exploit for personal gain.

We sought to understand the extent to which the manufacturing sector is protecting its sensitive information from these evolving threats.

We found that **every employee can access, on average, 6 million files on their first day on the job.**[1] We also found that, on average, over **27,000 sensitive files** are open to everyone in a company.

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

VARONIS

Manufacturing
Data at Risk: Key Findings

On average, every employee has access to **6 million files** — including proprietary information.

On average, **over 27,000 sensitive files** (financial + trade secrets + business plans) are open to everyone.

4 in 10 organizations have **1,000+ sensitive files** open to **every employee.**

More than half of companies have **500+ accounts with passwords that never expire.**

GLOBAL FINDINGS

Larger Companies are 2X More Exposed

Exposure by company size

Organization size	Avg. # of files	Avg. # of files open to everyone	Avg. % of files open to everyone
Large	63,571,806	12,303,704	19%
Medium	21,920,382	3,776,187	17%
Small	12,347,728	2,212,460	18%
Industry average	**33,975,882**	**6,331,523**	**18%**

Organization size	Avg. # of folders	Avg. # of folders open to everyone	Avg. % of folders open to everyone
Large	6,173,686	1,152,954	19%
Medium	1,974,167	308,329	16%
Small	1,244,511	218,620	18%
Industry average	**3,241,479**	**575,766**	**18%**

Organization size	Avg. # of sensitive files	Avg. # of sensitive files open to everyone	Avg. % of sensitive files open to everyone
Large	310,014	39,122	13%
Medium	232,305	19,958	9%
Small	166,051	23,684	14%
Industry average	**244,150**	**27,293**	**10%**

On average, every employee has access to over 6 million files — nearly one out of every five files — on their first day on the job. For large companies, that number doubles — at firms with more than 1,500 workers, employees can access over 12 million files.

One out of every ten files open to everyone in the company is sensitive. These files may include intellectual property, employee data, manufacturing and supply chain information, product development documentation, marketing plans, and more. Compared to financial services companies, manufacturing companies have fewer files open to everyone: The average employee in the financial sector can access 11 million files.

GLOBAL FINDINGS

State of Data Per Terabyte: Manufacturing

Organization size	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	1,654,486	112,973	11,772	11,558	9,460	1,739	8,506	561	375	17	86
Medium	1,073,643	103,425	26,529	21,781	8,112	2,102	12,551	1,079	250	22	19
Small	1,291,091	134,830	18,143	5,236	15,322	721	4,217	482	689	11	13
Average	**1,318,968**	**113,581**	**19,667**	**14,665**	**10,157**	**1,675**	**9,342**	**772**	**389**	**50**	**40**

Assessing risk per terabyte provides a clearer picture of the typical attack surface by company size and reveals which organizations are most vulnerable to insider and outsider threats. The average terabyte contains 1.3 million files.

We found that, per terabyte, **manufacturers average nearly 20,000 exposed folders (open to everyone)**. This number is similar to the financial services sector and significantly lower than the healthcare sector (19,251 and 29,965, respectively). It takes IT professionals an estimated 6–8 hours per folder to locate and manually remove global access, meaning it would take years to remediate and maintain these folders manually.

Manufacturers have over 1,675 exposed sensitive files per terabyte. This number is slightly lower than the healthcare sector (1,837) and about the same as the financial sector (1,646).

Our analysis revealed that manufacturing companies average **fewer overall exposed files** than other highly targeted industries like finance and healthcare. However, on average, they have **more exposed sensitive files per terabyte**. Small and mid-sized companies are especially vulnerable, as they have the most exposed sensitive files per terabyte.

GLOBAL FINDINGS

Protecting Manufacturing Data

Companies with sensitive files open to all employees via global access

Sensitive files open to everyone	% of companies
< 1,000	56%
1,000–10,000	22%
>10,000	22%

Stale sensitive data by financial services company size

Company size	Avg. # of stale sensitive files	Avg. % of sensitive files that are stale
Large	190,215	80%
Medium	131,978	74%
Small	133,957	84%
Industry average	**152,214**	**78%**

Global access groups (e.g., Everyone, Domain Users, Authenticated Users) are helpful for internal collaboration — but they also make it much easier for cybercriminals to infiltrate your environment. If a bad actor compromises one end user, they can gain a foothold that enables them to copy, share, delete and change unprotected sensitive information.

44% of manufacturing companies average 1,000+ files open to every employee — and more than one in five have 10,000 files open to every employee. For these companies with overexposed sensitive data, limiting open access by enforcing a least privilege model is a critical part of risk reduction.

Manufacturing companies store above-average amounts of stale sensitive data, which increases their attack surface and inflates storage costs unnecessarily. On average, **78% of an organization's sensitive files are stale and could be deleted or archived.**

GHOST IN THE MACHINE

Vulnerabilities in Active Directory

Companies with passwords that don't expire

Passwords that don't expire	% of companies
< 500	44%
500–1,500	32%
> 1,500	24%

Companies with ghost users

Size of stale user account group	% of companies
< 1,000	56%
1,000–10,000	36%
> 10,000	8%

Inactive user and service accounts that remain enabled long after employees leave (aka. "ghost users") provide attackers with plenty of time to brute-force their way into your environment and, once inside, move through your data stores. From there, they can quietly steal data and avoid detection before encrypting it.

Inactive, but enabled, privileged admin accounts with passwords that never expire are one of the best gifts you can give cybercriminals. These often overlooked vulnerabilities are difficult to detect and root out without proper visibility into your environment.

56% of companies have over 500 accounts with passwords that never expire and 44% of companies have more than 1,000 active "ghost user" accounts enabled.

STATE OF THE INDUSTRY

Manufacturing is the **fifth most targeted industry in 2020,** with **the average data breach costing $4.99 million. The average breach in the manufacturing sector takes 220 days to contain** — one of the longest threat lifecycles out of any industry.

Combined with our findings, there are two main takeaways:

1. The manufacturing industry's cybersecurity maturity lags behind the financial sector. Nearly half of all companies are still underprepared for a disruptive attack.
2. Manufacturers' cybersecurity preparedness is more likely to vary when compared to regulated sectors like healthcare and finance. While some companies have mature data security policies and incident response procedures, others have taken few mitigative steps.

Manufacturing companies can position themselves for success by using their deployed solutions to their full potential, removing data security blind spots by adding visibility, and reducing access to data on a least-privilege basis using automation. Reducing your blast radius will help minimize the damage attackers can do when — not if — they land on your network.

[2] IBM, Cost of a Data Breach Report 2020

The average cost of a data breach in the manufacturing sector was **4.99 million in 2020.**[2]

CASE STUDY

How Varonis Edge is Helping a U.S. Manufacturer Fortify On-Prem and Cloud Data Security

When an unauthorized user opened up an HR folder containing employee salary information, Varonis, made it possible to track down the user and review exactly what they had accessed and changed.

Read the whole story to find out how they did it.

READ THE CASE STUDY

VARONIS

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 a best-of-breed, world-class solution. It allows us to do everything from managing share permissions to locating sensitive data to securing our on-prem and cloud environments. Doing all of that from a single pane of glass saves us time in the long run.

INFRASTRUCTURE MANAGER
U.S. Manufacturer

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