2020

DATA EXPOSURE REPORT

ON INSIDER THREAT

CODE42

Table of contents

Executive summary

Today's corporate race for ideas has given way to a new collaboration era. We are living in a time when data is being created and shared every second of every day from everywhere. Powered by the latest technologies, employees are emailing, airdropping, messaging and slacking 24/7 from laptops, mobile devices, at customer sites and in coffee shops. And while these hallmarks of the modern workforce yield critical innovation, they're also a breeding ground for dangerous data security risks — more specifically insider threats.

Yes, technology has made it easy for employees to legitimately share files via personal email and the cloud. However, it also has made it easier for them to exfiltrate — or even infiltrate — data like product ideas, source code and customer lists. All it takes is one employee to intentionally take or accidentally leak data, and an organization could be on the hook for millions of dollars in lost revenue, fines for non-compliance, a loss of intellectual property and damage to the brand.

The ease in which data can be accessed, moved and shared across an organization is not the only factor contributing to the rise in insider threat incidents today. Workforce turnover also plays a major role. Employees are changing jobs at a record pace — and, the fact is, when they leave, they often take data with them. Absent or underdeveloped insider threat programs are only making the situation worse — leaving corporate data vulnerable and wide open for the taking.

The 2020 Code42 Data Exposure Report on insider threat is based on a survey of 4,505 knowledge workers in the U.S., U.K. and Germany, Austria and Switzerland. The report examines the growing role that cloud-based collaboration tools, workforce turnover and absent or underdeveloped insider threat programs play in the rise of data loss, leak and theft in today's digital workplace.

Key findings

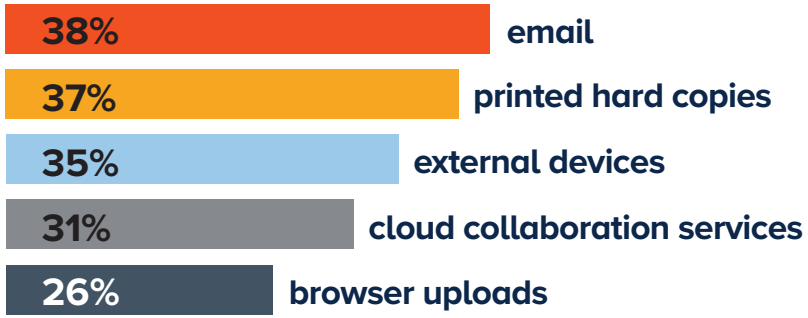
36%

of workers believe that the increased emphasis on sharing and collaboration has made them more complacent about data security

51%

of workers are calling on companies to reassess their insider threat programs

The tools workers use to collaborate are the very tools they use to exfiltrate data



87% of employees say companies failed to verify if they had taken data when they left the organization

THE COLLABORATION ERA

Collaboration tools are changing the nature of work

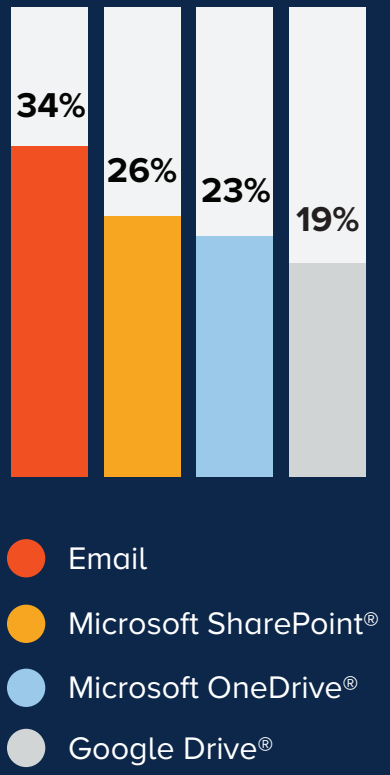
Data has never been more portable. In today's open and collaborative work environments, employees can upload files to the web, sync data to personal cloud accounts, email file attachments and even share files publicly from corporate cloud storage accounts. As part of their daily routines, colleagues separated by a few feet or thousands of miles can work on the same document concurrently, share data and workshop a complex problem — all in real time.

The unintended consequences of using collaboration tools

While great for productivity, collaboration tools also serve to decentralize corporate data that has traditionally been created, stored, secured and backed up in the data center. The reality is instead of residing behind a firewall, data now lives and moves among servers in multi-tenant data centers spread across the world. The end result? For security teams, it means a lack of visibility to where company data is stored, who has access to it, and when and what data leaves. And without visibility to all data, a business remains vulnerable to insider threats. For employees, the modern collaborative workplace creates a sense of complacency, which only exacerbates the risk of a data breach.

36% of workers believe that the increased emphasis on sharing has made them more complacent about data security.

According to respondents of Code42's Data Exposure Report, the leading corporate standards for file sharing and collaboration include email, Microsoft SharePoint®, Microsoft OneDrive® and Google Drive®.



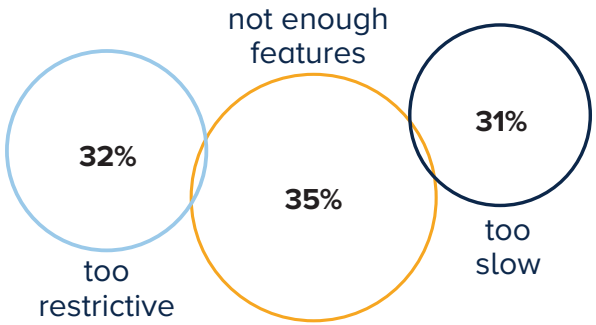
Workers opt for unsanctioned collaboration tools to share company files

Data loss detection, investigation and response is complicated enough on corporate-sanctioned cloud platforms and applications. Unfortunately, employees are just as likely to use unauthorized cloud-based platforms in the course of their daily work routines. According to our survey, workers are increasingly relying on unauthorized tools, such as WhatsApp®, Google Drive®, Facebook® and personal email to share files with colleagues. They sidestep sanctioned tools because they believe they are too restrictive and slow — or don't have enough features to accomplish regular tasks. When comparing generational demographics, the younger the employee, the more likely they are to use unsanctioned applications to collaborate.

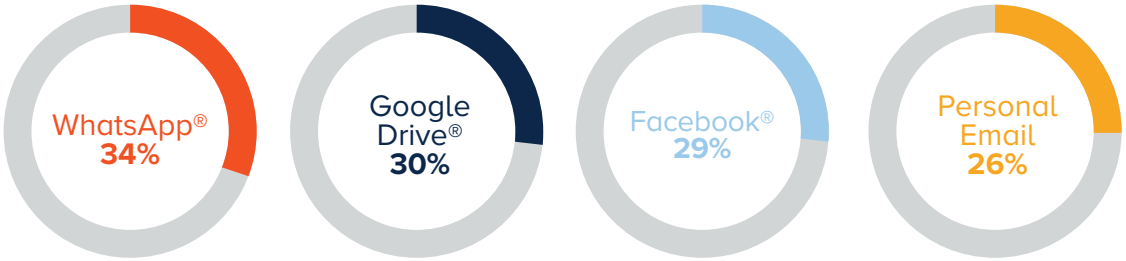
37%
of workers use unauthorized apps daily, while

26%
use them weekly to share files with colleagues

REASONS TO NOT USE AUTHORIZED TOOLS



MOST COMMONLY-USED UNAUTHORIZED PLATFORMS FOR SHARING FILES WITH COLLEAGUES



THE YOUNGER THE EMPLOYEE, THE MORE THEY USE UNSANCTIONED SOLUTIONS TO COLLABORATE

Do you have visibility into how your employees are sharing data?

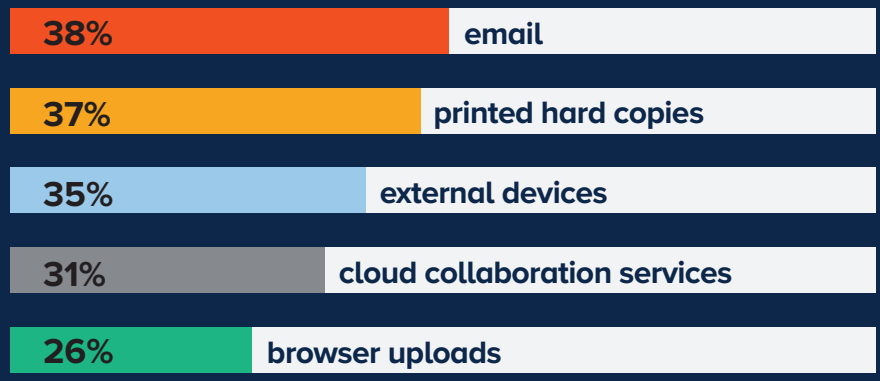
THE RISK OF DATA EXFILTRATION

Cloud-based collaboration tools rated among top vectors for data exfiltration

Companies are empowering their employees to use collaboration tools to store, share and send data inside and outside their organizations without the proper security programs and controls in place. The inability to detect, investigate and respond to potential insider threats has heightened the risk companies face. Nearly three-fourths (73%) of employees report they have access to data they didn't create, 69% can view data they didn't contribute to and 59% can see data from other departments.

The risks to data security are further multiplied because the very tools that workers use to collaborate have become some of the most popular vectors for moving data from one organization to another. Personal email, printed documents and external devices are the data exfiltration tools of choice, followed closely by cloud collaboration services and browser uploads.

WORKERS EXFILTRATE DATA USING:



How do you walk the line between empowering employees to collaborate and securing corporate data?

WORKFORCE TURNOVER

Workforce turnover is a constant factor in insider threat

According to the U.S. Bureau of Labor Statistics, turnover in the U.S. is at an all-time high. The Code42 Data Exposure Report found that people are changing jobs as a way to advance their career, increase earning power, move to a new location or simply as a change of pace. And who can blame them? Technology coupled with more progressive remote working policies are opening up new opportunities in markets that many workers simply couldn't pursue due to geography.

Departing employees shouldn't mean departing data

Turnover creates risk. The simple act of changing jobs can tempt employees to take company data. Well intentioned employees might simply be trying to make their next job easier. Other employees believe the files belong to them because, after all, it's their work. More nefarious employees might use sensitive data as leverage when negotiating a new job offer.

Regardless of the motivation, two-thirds (63%) of employees who admit to taking data with them to a new job are repeat offenders. The consequences of this behavior is even more damaging to a business when workers take data from a former employer and go to work for a competitor. Three in five (59%) departing employees move to a company in the same industry, and more than half (52%) land a similar job in the same department within their new company.

63% of employees who admit to taking data with them to a new job are repeat offenders

59% of departing workers move to a job in the same industry

52% stay in the same department within a new company

Do you know when AND what data is leaving your organization?

INSIDER THREAT

Insider threat programs earn a failing mark

Insider threat continues to be an unsolved problem. Absent or underdeveloped insider threat programs offer little to no deterrent for departing employees. Nearly nine in ten workers say that no one ever approached them from their former employer to verify they hadn't taken data with them when they left. Three quarters of workers said their new employer didn't ask them if they brought data with them. In fact, one third of workers who had exfiltrated data said they were encouraged by their new employers to share it with their new colleagues.

It's clear that insider threats are a much more serious issue than companies realize. Just ask the front-line workers who have access to and use corporate information on a daily basis. In fact, more than half (51%) surveyed say that they believe the risk to corporate data when employees depart is bigger than organizations think.

87%

of employees report that no one ever approached them from their former employer to verify that they hadn't taken data

75%

say that their new employer did not ask them if they brought data from their previous employer

32%

of respondents who had infiltrated data were encouraged by their new employers to share it with new colleagues

Shouldn’t you listen when your employees are the ones telling you it’s time to invest in an insider threat program?

Conclusion

A new approach to data security

The results of the Code42 Data Exposure Report are a wake-up call for security teams that have traditionally relied on prevention-based security strategies for blocking when the rest of their organizations are busy sharing. Instead, companies today require insider threat programs that promise complete data visibility, easy investigation and rapid response when insider threats strike. Backed by this kind of data security strategy, security teams can take action before employees walk out the door with trade secrets and the damage is done.

The collaboration culture in the digital workplace is unavoidable. Are you investing enough in the right insider threat solutions to protect your data?

Summary

So, what does all of this mean?

Insider threat is real. Regardless of whether worker actions are malicious or unintentional, the end result is the same: Data is leaving organizations everyday.

Security teams can't protect what they can't see. The heavy use of cloud-based collaboration tools has moved data outside traditional security perimeters and created security blindspots, leaving company data vulnerable.

It's time for a new approach to data security. Insider threat programs have failed to keep pace with collaborative work environments and workforce turnover. Traditional prevention-based data security solutions are no longer enough.

Speed matters. Security teams need to invest in insider threat programs that give them the right tools to quickly detect, investigate and respond to data loss, leak and theft.

Never compromise the safety of data. There are new and better strategies for securing the collaboration culture.

Methodology

The research for this report was conducted by Sapio Research, an independent research consultancy based in the United Kingdom. The survey was completed by 4,505 knowledge workers with more than 1,000 employees, via online response, during December 2019.

The respondent breakdown is as follows:

2,003
US

1,501
UK

1,001
Germany, Austria and Switzerland

About Code42

Code42 is the leader in insider threat detection, investigation and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider threat solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. For more information, visit code42.com, read Code42's blog or follow the company on Twitter.

Contact Us

Code42.com

US: +1 844 333 4242
UK: +44 808 178 3042

twitter.com/Code42

linkedin.com/company/code-42-software-inc

code42.com