2019

DATA EXPOSURE REPORT

CODE42

Table of Contents

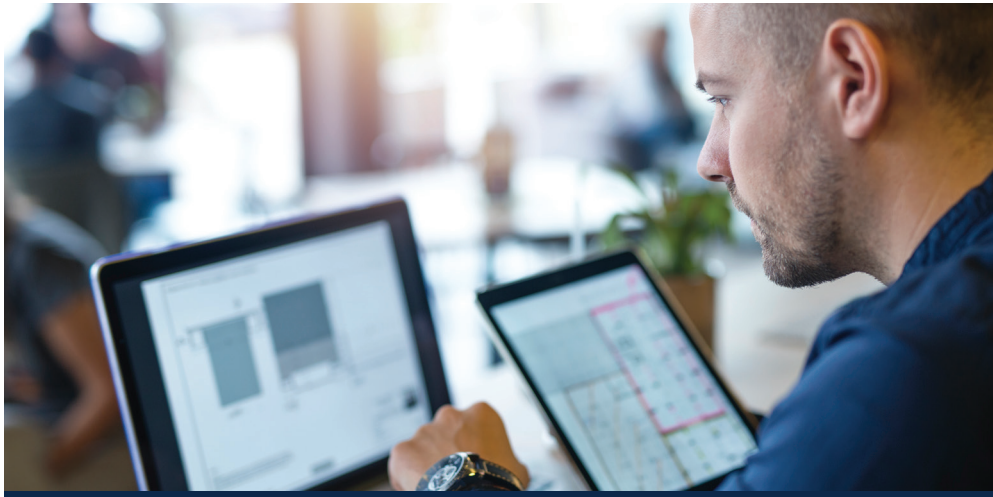
Executive summary

Most organizations have some kind of data loss prevention strategy in place. However, that strategy typically ignores one of the greatest threats to data: the threat posed by employees.

In today's progressive workplaces, people and data are on the move like never before. Job tenure is declining and people are switching jobs far more frequently. At the same time, leaders want to empower employees to be creative, innovative and collaborative. To do this, they are granting their employees access to easy-to-use data-sharing platforms and mechanisms known for speeding productivity. The challenge is, these tools perhaps make it too easy to move data around. In a matter of seconds, valuable data can be transferred to a private cloud or removable media and whisked out the door.

The brutal truth? Employees take data – especially when they quit. Although many companies have traditional prevention tools in place, data loss, leak and theft — particularly from insiders — continues to happen at an alarming pace. That's why information security teams need to find new ways to secure data. Without urgent action, insider threats will become increasingly disruptive.

The 2019 Data Exposure Report is based on our survey of 1,028 information security leaders, as well as 615 business decision-makers, all with budgetary decision-making power. The report examines the role of employee actions in causing insider threat, organizational attitudes toward intellectual property and the ability of legacy data loss prevention technologies to stem insider threats.



Key findings include:

- Employees are one of the biggest threats to organizations' data security.
- Employee actions were the primary reason for half of the intellectual property breaches occurring in the last 18 months.
- Even information security leaders are guilty of careless behavior when handling sensitive data.
- Traditional data loss prevention solutions are not effective for protecting data from insider threats.

INSIDER THREATS

The brutal truth: employees are the biggest internal threat to data.

Employees are the power behind any organization. To improve employees' productivity, executive leadership and IT have made sharing corporate information easier than ever. Unfortunately, organizations have not put in appropriate detection and response data security controls and instead trust employees to keep data safe. However, this trust is frequently abused. Between employee negligence, malicious acts and general ignorance around data security best practices, security organizations need to recognize and plan for insider threats.

The data shows that employees take more risks with data than employers think they do, which leaves organizations open to insider threat.

Risky business on personal platforms

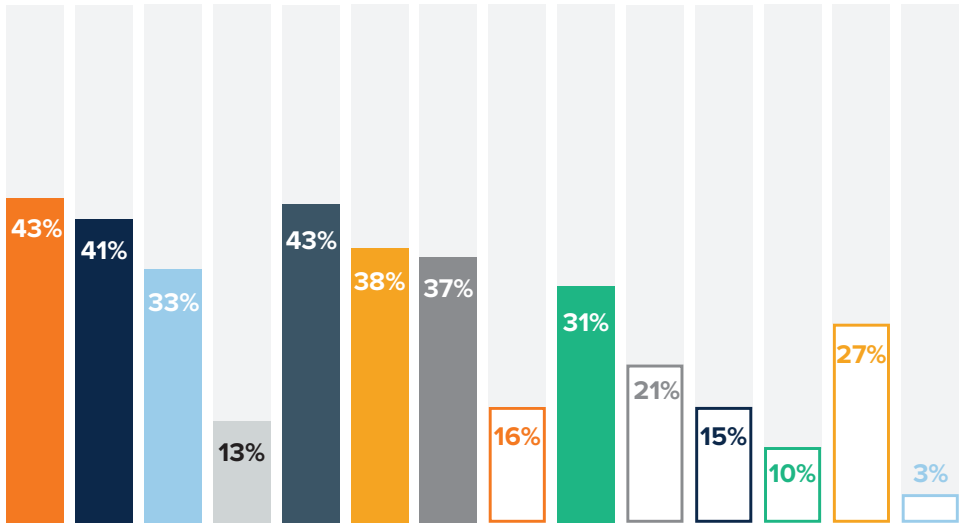
Think Microsoft OneDrive, Google Drive and Box are equally secure file-sharing platforms? Think again. While these platforms are typically company-sanctioned, employees often use their personal accounts to share company data.

When data is moved outside of company-sanctioned applications and platforms, employees create a personal copy of company intellectual property that they could take with them when they leave the organization. Information security teams are powerless to stop this outbound flow of data.

While convenient, file-sharing and social media platforms present dangerous vulnerabilities for data security when used to send files and collaborate. That's because information security teams lose visibility to data and thus their ability to protect it. Rather than sticking to company-provided file-sharing and collaboration tools, one in three (31%) business decision-makers also use social media platforms, such as Twitter, Facebook or LinkedIn, 37% use WhatsApp and 43% use personal email to send files and collaborate with their colleagues.

Question: Which applications or tools, other than company-provided email, do you use today to collaborate and share files with peers?

BUSINESS DECISION-MAKERS:



- Microsoft OneDrive
- Google Drive
- Dropbox
- Slack
- Social media platforms (LinkedIn, Facebook, Twitter, etc.)
- Ticketing or project management system (Jira, Basecamp, Trello, Microsoft Project, etc.)
- External devices (hard drives, removable media, such as flash drives)
- FTP clients
- Other (please specify)
- Personal email
- iCloud
- WhatsApp
- Chat clients
- Box

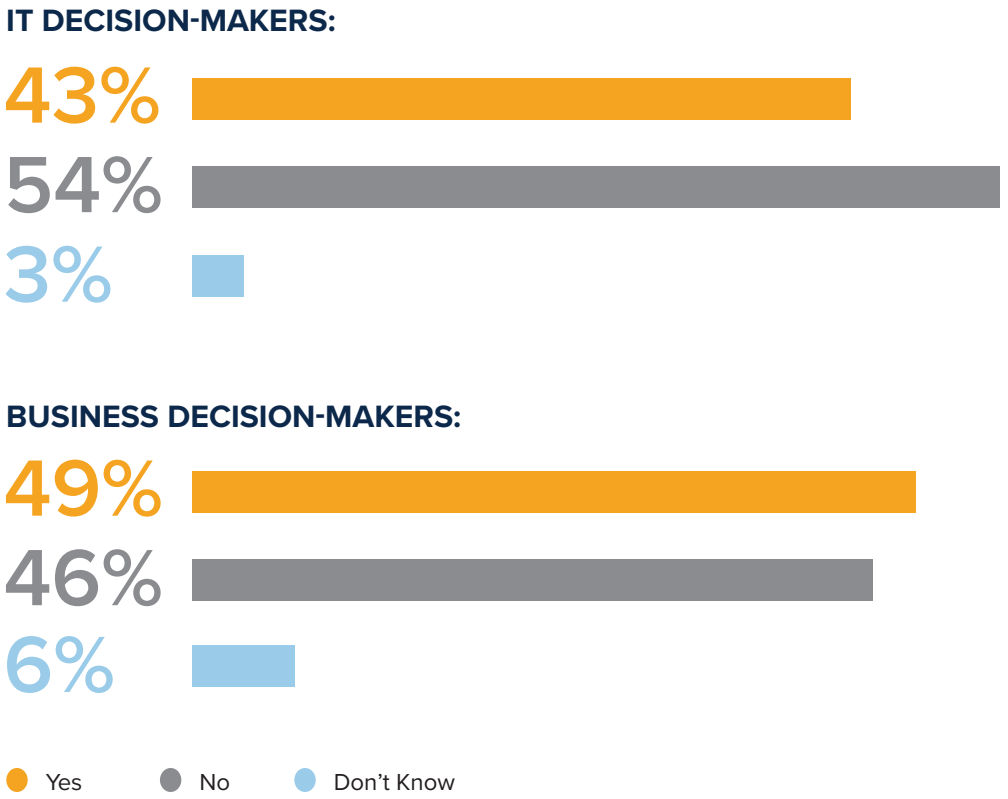
Bad behavior

Go Phish: No level of employee is immune to lapses in judgment when it comes to cybersecurity – even though they're in the C-suite.

Over three-quarters admit to clicking on a link they should not have.

This is a troubling statistic, considering the role of the CSO is to protect company data and set a strong infosecurity example for the organization.

Question: Have you ever personally clicked on a link you shouldn't have/didn't intend to?



Wake-up call

Organizations erroneously believe employees are an effective front-line defense against data security incidents. However, employees often abuse their privileges to collaborate and share data, leaving their organizations at a heightened level of risk for data loss and breach.

Of the 38% of companies that admitted to experiencing a data breach in the previous 18 months, half cited employee actions as the cause,

according to both information security leaders and business decision-makers (50% and 53%, respectively). This figure should serve as a wake-up call. Insider threat is a real danger to your data and your business.

Another finding that's disconcerting, but not necessarily surprising: employees tend to operate however they please to best get their jobs done. Seventy-seven percent of information security leaders agree that the most significant risk to an organization is employees doing their jobs however they want, with no regard to data security protocols or rules.

Question: If your company experienced a data breach in the last 18 months, what was the cause of the data breach?

INFORMATION SECURITY LEADERS:

BUSINESS DECISION-MAKERS:

If insider threat data loss is not top of mind for your organization, it should be.

DEPARTING EMPLOYEES

Employees who quit pose a high data security risk

Chances are, people in your organization are job-hunting. In 2018, 40 million employees in the U.S. quit their jobs, and the number continues to rise. Unlike past generations of American workers who stayed at jobs for decades, today half of the labor force is looking for a new job. A similar trend can be seen in parts of western Europe where voluntary turnover rates are two- to three-times those of involuntary turnover rates.

It's no secret among information security leaders that employees are a threat to company data. In fact, half of business decision-makers agree that employees are the single biggest threat to their company's intellectual property. Further, 86% of information security leaders know that employee behavior will always impact their ability to protect corporate data.

Yet, employee off-boarding protocols at most companies include exit interviews and procedures for passing along projects and collecting laptops, but not measures to protect valuable data. The reality is, departing employees take much more than staplers when they quit.

Taking data to go

Chances are your employees have brought data from past employers into your business. Nearly two-thirds (63%) of all survey respondents and 65% of information security leaders admit to doing so – more than other employees in the business (59%).

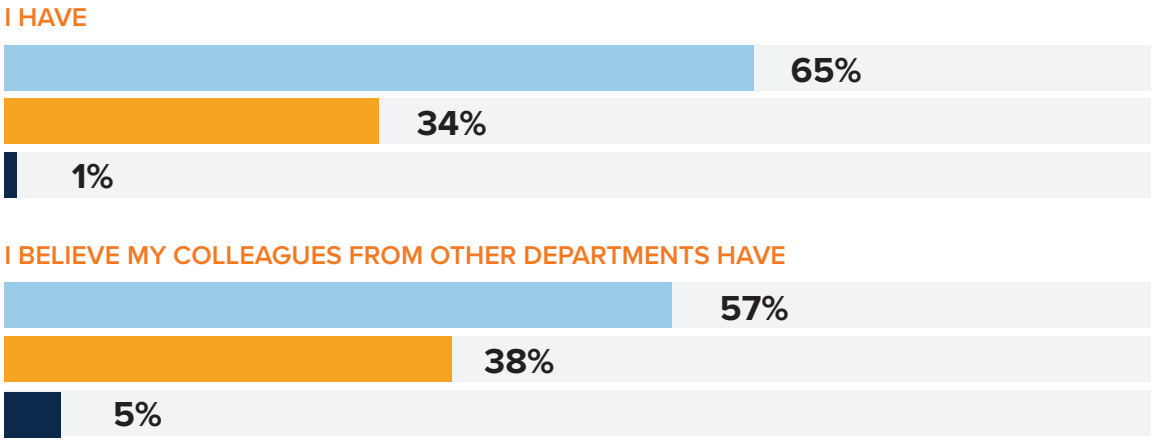
Moreover, just over a quarter (27%) of information security leaders do not monitor the data that new employees bring into their organizations.

Today, more than half (57%) of information security leaders and 51% of business decision-makers say that their colleagues have infiltrated data, which puts their current organization at risk of lawsuits and reputational damage.

If employees are bringing data from their former employers to your company, what's to stop them from taking your data when they leave for their next job?

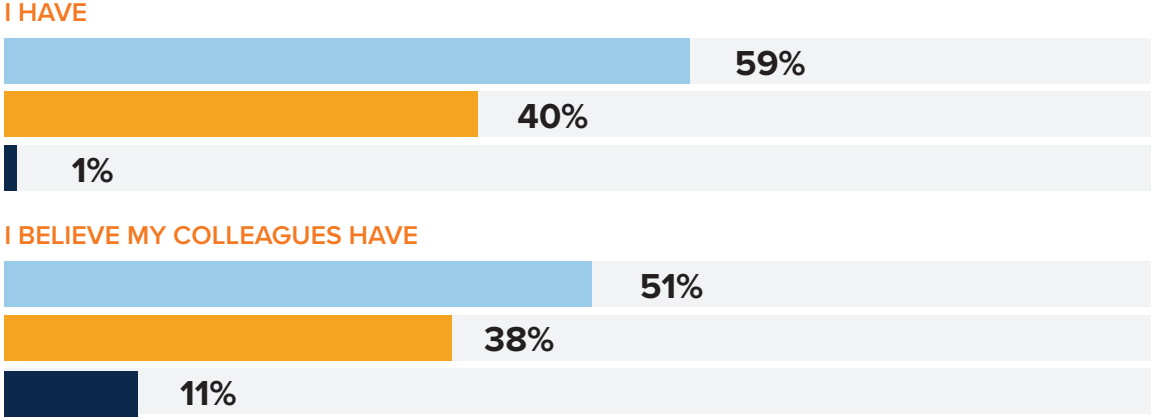
INFORMATION SECURITY LEADERS:

Question: Have you, or do you believe your colleagues from other departments, brought information/ideas/intellectual property/data with you/them from a previous employer to use in your current organization?



BUSINESS DECISION-MAKERS:

Question: Have you, or do you believe your colleagues, brought information/ ideas/intellectual property/data with you/them from a previous employer to use in your current organization?



Yes
No
Don't Know

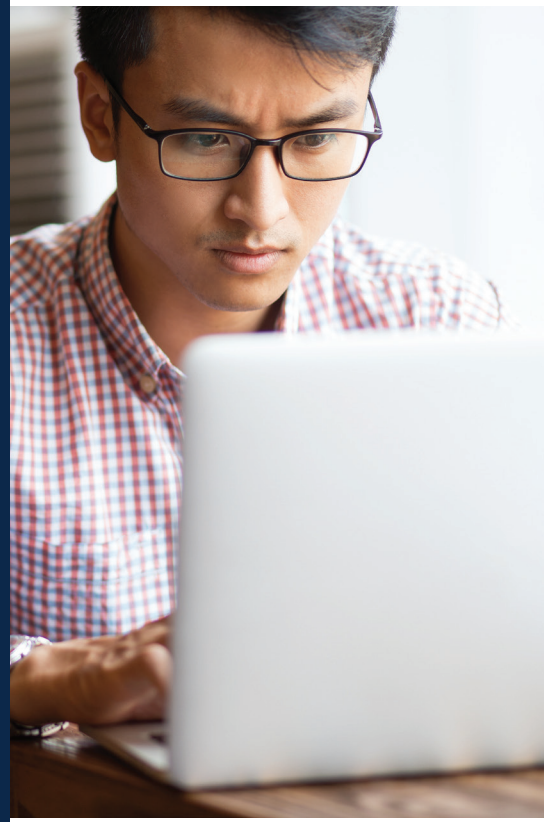
Yours, mine, ours

Why would employees feel entitled to take data with them when they quit? The question should be, why wouldn't they? For one thing, data has never been more portable and taking it never easier. Employees can store hundreds of gigabytes on their mobile devices, put 1TB or more of data on removable media, or quickly transfer data to personal cloud storage services.

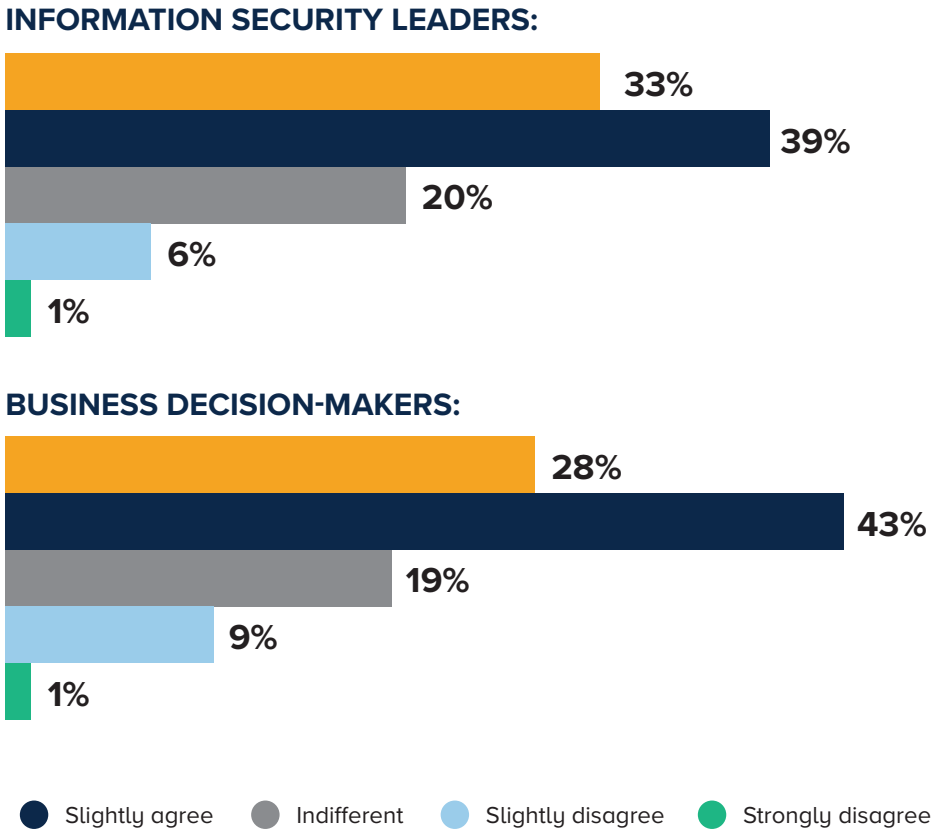
What's more, many employees today feel entitled to personal ownership over their work. In fact, a large majority of information security and business decision-makers

72% and 71%

respectively, agree, "It's not just corporate data, it's my work – and my ideas."



It's not just 'corporate data,' it's my work — and my ideas.



When employees leave, be aware of what they're stuffing in their pockets and stashing in their cloud.

PREVENTION-ONLY SOLUTIONS

aren’t enough to stop insider threat

It's an inside job

The numbers don't lie – over a third (38%) of information security leaders admit that their company suffered a breach of intellectual property in the last 18 months.

While 45% of information security leaders believe that data loss prevention is effective for keeping tabs on data as it moves throughout the organization, these prevention solutions don't make the grade when it comes to stopping employees from exfiltrating valuable data, such as customer lists and source code.

69% **Over two-thirds of organizations say they were breached due to an insider threat and confirm they did have a prevention solution in place at the time of their breach.**

The upshot: traditional data loss prevention solutions are not preventing data loss from insider threats.

Prevention was never the complete solution

Over three-quarters (78%) of information security leaders believe that prevention strategies and solutions are not enough to stop insider threat – including those with traditional data loss prevention (DLP) tools in place.

When asked how they might be able to achieve a higher level of data security, survey respondents agreed on one strategy. Nearly three quarters (73%) of information security leaders and business decision-makers said that the only way to keep their organization's data safe is to lock down devices and access. Though it may be widely regarded as the best way to keep data safe, it's also widely regarded as exceedingly impractical now and in the future.

As pressures mount, investments suffer

Information security leaders know their data is at risk. However, they are increasingly under pressure and distracted by a combination of endless alerts from their security tools and relentless media exposure about data breaches. This noise is prompting information security leaders to under-invest or delay investments in data security solutions or make misguided investments in tools that don't stop data loss.

More than two-thirds (69%) of information security leaders agree that a lack of coordinated security planning is putting their organizations at risk.

However, **89%** of CSOs admit to feeling desensitized toward potential cybersecurity threats due to over-exaggeration and exposure to the media.

Just under a third (30%) of information security leaders believe that the constant alerts and media coverage of data breaches results in their colleagues feeling desensitized toward potential risks. A quarter of business decision-makers similary admit to growing apathetic due to increased media coverage around data breaches.

Security teams must act now

The workforce is making a marked shift to partially and fully remote teams, and rarely reflects a once standard nine-to-five work day. It's become a greater challenge for information security teams to protect sensitive information in this age of different access points, devices and exfiltration vectors.

When not within the walls of the traditional office, employees may feel more emboldened to make corporate data as mobile as they are. Business decision-makers on average spend 23% of their working week outside the office, at meetings, and 19% of the week working from home. Both business and information security leaders noted that the 18- to 24-year-old group is more likely to work remotely or in co-working spaces compared to other age ranges, a trend that will only continue as this age group moves forward in the workforce.

By and large, security teams' data security investments and strategies are failing to evolve alongside recent changes in the workforce. Eighty-nine percent of CSOs believe the fast-paced cultural model of their business puts their company at greater risk of data security threats. Security teams must act now and find a new way to safeguard their organization's valuable intellectual property.

The workforce is changing and pressures are mounting. Are you investing enough and in the right solutions to protect your data?

Summary

Insider threat is an unsolved problem plaguing organizations worldwide. To stop data loss, leak and theft, security teams primarily rely on their employees and technology solutions to safeguard data. The reality is, they are being let down on both fronts. Traditional prevention solutions are no match for stopping data loss from insider threats. Furthermore, employees take more risks in how they handle sensitive data, like source code and customer lists, than employers think they do. What's worse, employees who quit often take data with them from their previous employers to their new companies.

The shifting workplace culture in the modern-day office only adds to this challenge. Employees are increasingly likely to be on the go – working from home or remote locations. Security teams need to find a new way to keep data safe as it becomes more mobile and the number of exfiltration vectors expand.

So, what does all of this mean?

Security teams must evolve their data loss protection strategies and think beyond prevention – prevention solutions aren't enough to stop insider threat.

When prevention methods fail, security teams must detect, investigate and respond to data leak, loss and theft as quickly as possible.

Focus on the data – it's imperative to know what data leaves when so that security teams can protect it across endpoints and cloud.

Invest in a next-gen data loss protection solution. This is the only way to truly mitigate the growing and evolving impact of insider threats.

Methodology

The research for this report was conducted by Sapio Research, an independent research consultancy based in the United Kingdom. The survey was completed, via online response, during May 2019.

The respondent breakdown is as follows:

Information Security Leaders:

375
USA

377
UK

276
Germany, Austria and Switzerland

Almost a quarter (21%) of the information security audience are representative of the C-suite, including CISOs, CSOs, CIOs and CTOs.

Business Decision-Makers:

200
USA

200
UK

215
Germany, Austria and Switzerland

Thirty percent of the business audience is representative of the C-suite.

The research surveyed 1,028 information security leaders, as well as 615 business decision-makers, all with decision-making powers, or influence over, the provisioning of security solutions, products and services.

About Code42

Code42, the leader in data loss protection, secures the ideas of more than 50,000 organizations worldwide, including the most recognized brands in business and education.

Native to the cloud, the Code42® Next-Gen Data Loss Protection solution rapidly detects insider threats, helps satisfy regulatory compliance requirements and speeds incident response – all without lengthy deployments, complex policy management or blocking user productivity. Because the solution collects and indexes every version of every file, it offers total visibility and recovery of data – wherever it lives and moves. Security, IT and compliance professionals can protect endpoint and cloud data from loss, leak and theft while maintaining an open and collaborative culture for employees.

Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners.

Contact Us

Code42.com

USA: +1 844 333 4242
UK: +44 808 178 3042
Germany: +49 89 416 1169 40

twitter.com/Code42

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

blog.code42.com