Top Data Security Trends

300+ IT leaders detail must-have tools for their data security toolkit.

Contents

Executive Summary

To stay competitive in a digital-first world, organizations must be able to innovate anywhere, automate anything, scale everything, and most importantly, empower everyone. But doing so requires IT governance at scale and the highest levels of IT security and compliance.

How are IT leaders juggling these demands in the new hybrid workplace? Pulse and Salesforce surveyed 300 InfoSec and IT executives to find out. Get the key findings and data security best practices in this summary and the pages that follow.

01 Security Takes on the Distributed-Team Challenge

Ninety percent of surveyed IT leaders say that their organization supports a distributed workforce. But they note major compliance, vendor management, and data security difficulties in doing so. Despite these challenges, the majority report high levels of international data compliance.

02 Three Security Threats to Get Ahead Of

With the average cost of a data breach standing at 9.44M USD, loss of revenue is the cyberattack outcome that worries IT leaders most. And they see phishing, ransomware, and DOS/DDOS attacks as the top threats to stay ahead of. However, respondents across the software, manufacturing, and professional services sectors note insider breaches among their top three concerns

03 Three Must-Have Tools for Your Data Security Toolkit

IT leaders frequently use employees as the first line of defense against attacks. In addition to employee vigilance, **77% report multifactor authentication as a top security tactic**. Identity access management is a close second, with 72% reporting it as a best practice. Surprisingly, there's **one glaring gap in the IT leaders' security arsenal: backup and restore solutions**. Only 41% say it's a core component of their security strategy.

04 Look Ahead: The Top Data Security Tactics for 2022

Most predict that threats will continue to rage on this year. IT leaders across the board expect the finance, government, and healthcare sectors to be targeted the most by cyberattacks. However, qualitative feedback indicates hope for more and better tools to predict and eliminate threats.

01 Security Takes on the Distributed-Team Challenge

A global pandemic brought the future of work to the business world – sooner than anyone had ever imagined. **Ninety percent of executives say that their organization supports a distributed workforce**, thanks, in part, to accelerated digital transformation.

But new ways of working have also brought new challenges. Chief among them are data security and governance, as pictured here.

In the last 18 months, what have been your top three pain points in managing data security?

> “I think as more people and companies move to a work-from-anywhere model, endpoint security and breaches will be at the top of the risk register.”
>
> **VP, SOFTWARE INDUSTRY (5,000–10,000 EMPLOYEES)**

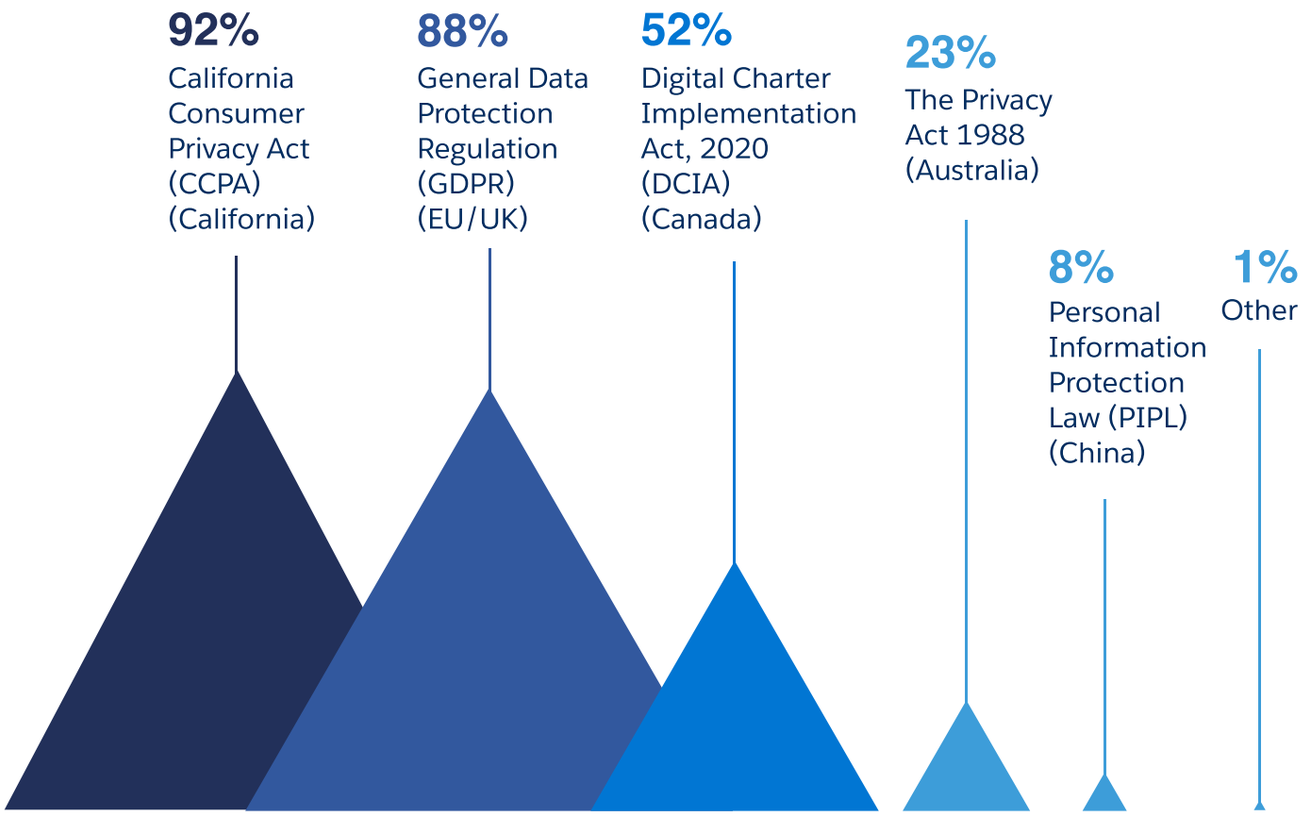
01

Compliance Drives Secure Remote Work

Topping the list of data security challenges are third-party security management and compliance. Interestingly, despite the reported compliance-management headaches, leaders from across industries are stepping up to the plate – with the majority indicating high levels of international data compliance. This, in turn, is also supporting secure remote work.

> “I see more security and privacy legislation coming down the pipe.”
>
> C–SUITE, PROFESSIONAL SERVICES (10,001+ EMPLOYEES)

Which of the following international privacy laws is your organization compliant with?

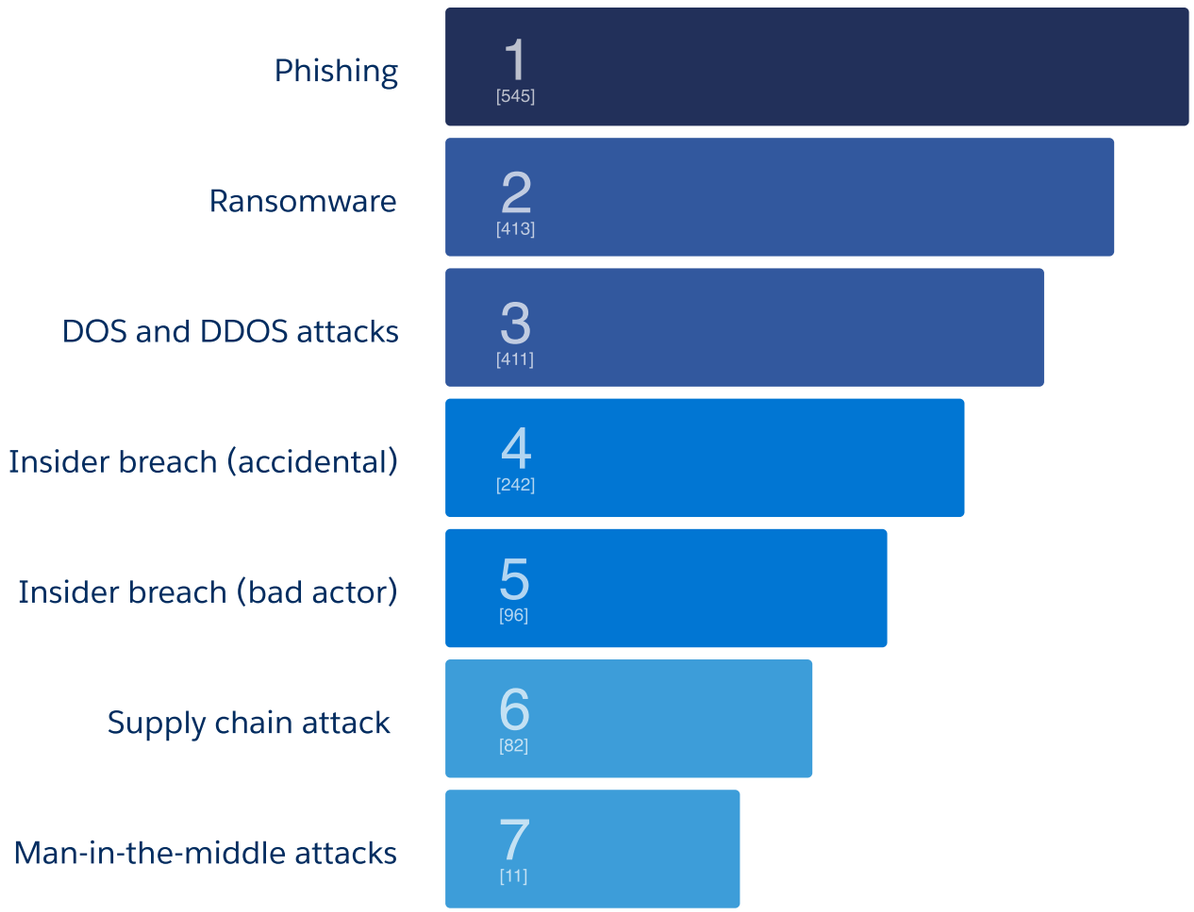


02 Three Security Threats to Get Ahead Of

Bad actors have a bigger terrain than ever before to wreak their havoc due to our reliance on digital. 2021 was a record-breaking year for data compromises, with nearly 1,300 data breaches – 17% more than in 2020.[1]

Given these trends, it's not surprising that **phishing, ransomware, and DOS and DDOS** attacks topped the list of security concerns among the IT leaders we surveyed.

What are your top three IT security concerns?
(top = highest level of concern, bottom = lower level of concern)



> "More investment will need to be made to catch up to adversaries who are well ahead of the good guys."
>
> VP, MANUFACTURING
> (1,001–5,000 EMPLOYEES)

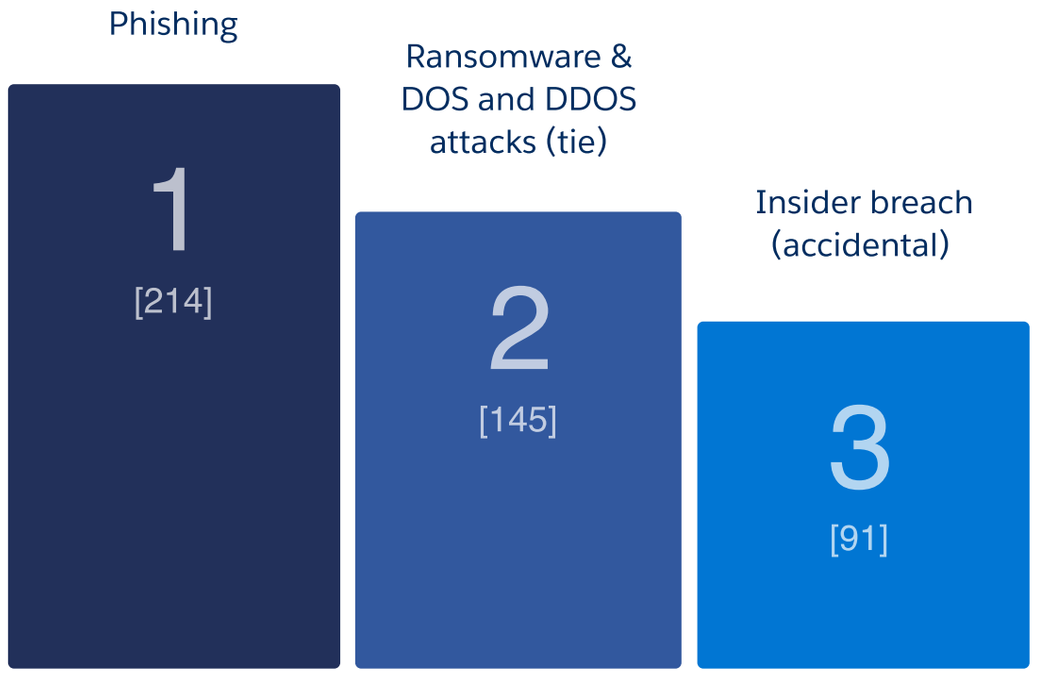
02

Insider Breaches: A Major Concern for Nonregulated Industries

While security concerns are consistent across industries, there's a key difference for the software, manufacturing, and professional services sectors. These nonregulated industries – which manage volumes of sensitive data – note **accidental insider breaches** in their top three security concerns (n=107).

> "I think we will see data security and privacy evolve together, and we'll have solutions to address both out of the box."
>
> **VP, MANUFACTURING (5,001–10,000 EMPLOYEES)**

What are your top three IT security concerns? (top = highest level of concern, bottom = lower level of concern)



02

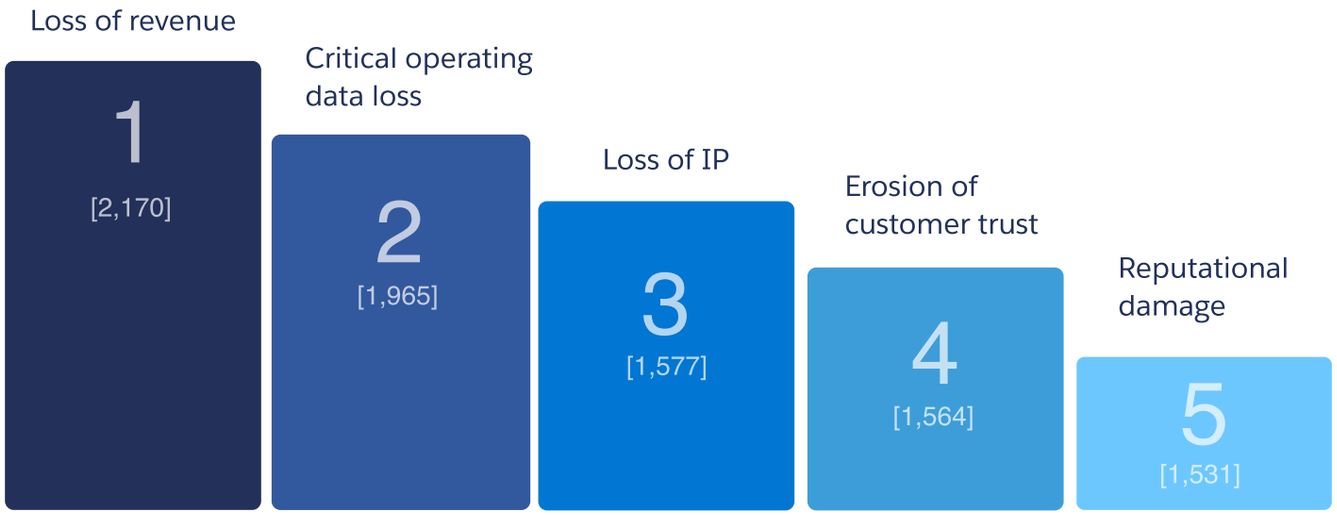
The Three Outcomes IT Leaders Worry About Most

A data breach in the US costs a staggering 9.44 M USD -- more than twice the global average of $4.35M.[2] It's no wonder **loss of revenue** is the cyberattack outcome that worries IT leaders most. Additionally, they express significant concerns over **losing critical operating data and intellectual property.**

However, respondents in regulated industries – such as finance, banking and insurance, educational services, healthcare services – are more concerned about reputational damage and loss of trust.

This, understandably, reflects the catastrophic compliance and customer-privacy risks of losing the highly sensitive data these sectors manage.

What potential cyberattack outcomes are you most concerned about? (top = highest level of concern, bottom = lower level of concern)



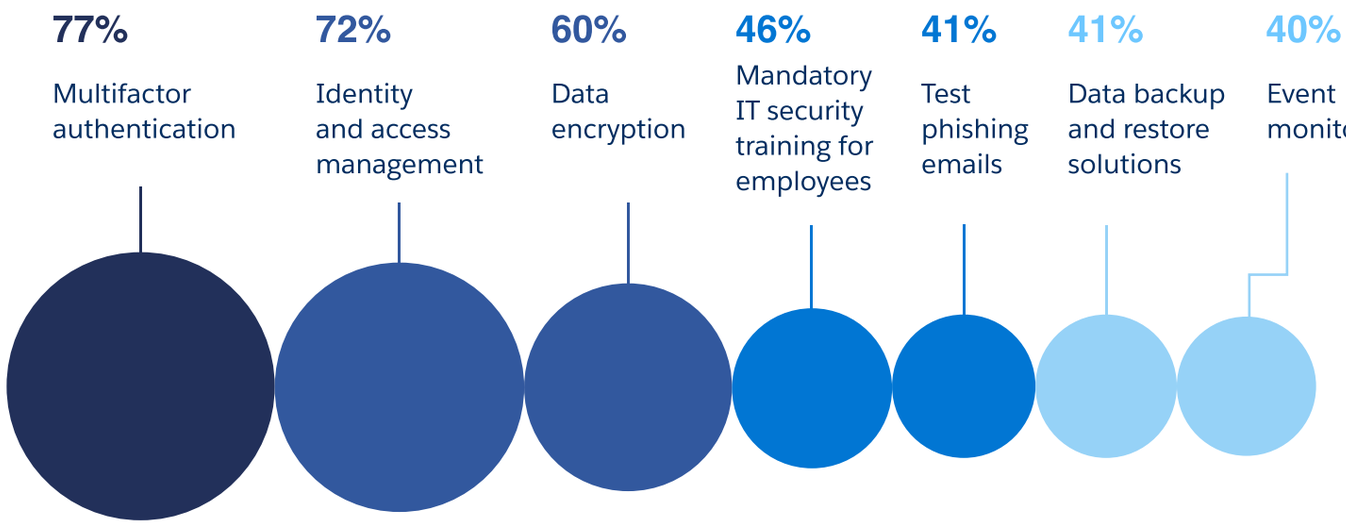
6 Operational outages [1,390]
7 Lawsuit(s) [1,261]
8 Data corruption [1,063]
9 Downtime and recovery time [979]

03 Three Must-Have Tools for Your Data Security Toolkit

What are the most powerful weapons in the IT leader's security arsenal? According to our findings, they're **data encryption, identity and access management**, and **multifactor authentication**. But there are some key industry nuances.

Industry Insight: Multifactor authentication is especially important for large enterprises and highly regulated industries that deal with sensitive data. **Eighty-nine percent of IT leaders in the finance, banking, and insurance industries say multifactor authentication is a key part of their security strategy.**

What strategies have been most effective in defending your organization against security attacks?



> "I think we're going to start to see some of the outcome from companies using freeware or other solutions for collaboration without adequate consideration of security implications or privacy impact."
>
> **VP, SOFTWARE INDUSTRY (10,000+ EMPLOYEES)**

03

Employee Vigilance Is a Key Defense

Employees are a huge part of the data-security solution. And that's why the majority of leaders are empowering employees to be a first line of defense against cyberattacks. **Eighty-four percent of leaders say that they are more frequently training employees on IT security tactics** to drive adoption of security measures.

> “I see more and more attacks. I hope to see more employees take data and privacy more seriously.”
>
> C–SUITE, EDUCATION
> (1,001–5,000 EMPLOYEES)

What are you doing to encourage employee adoption of IT security measures?

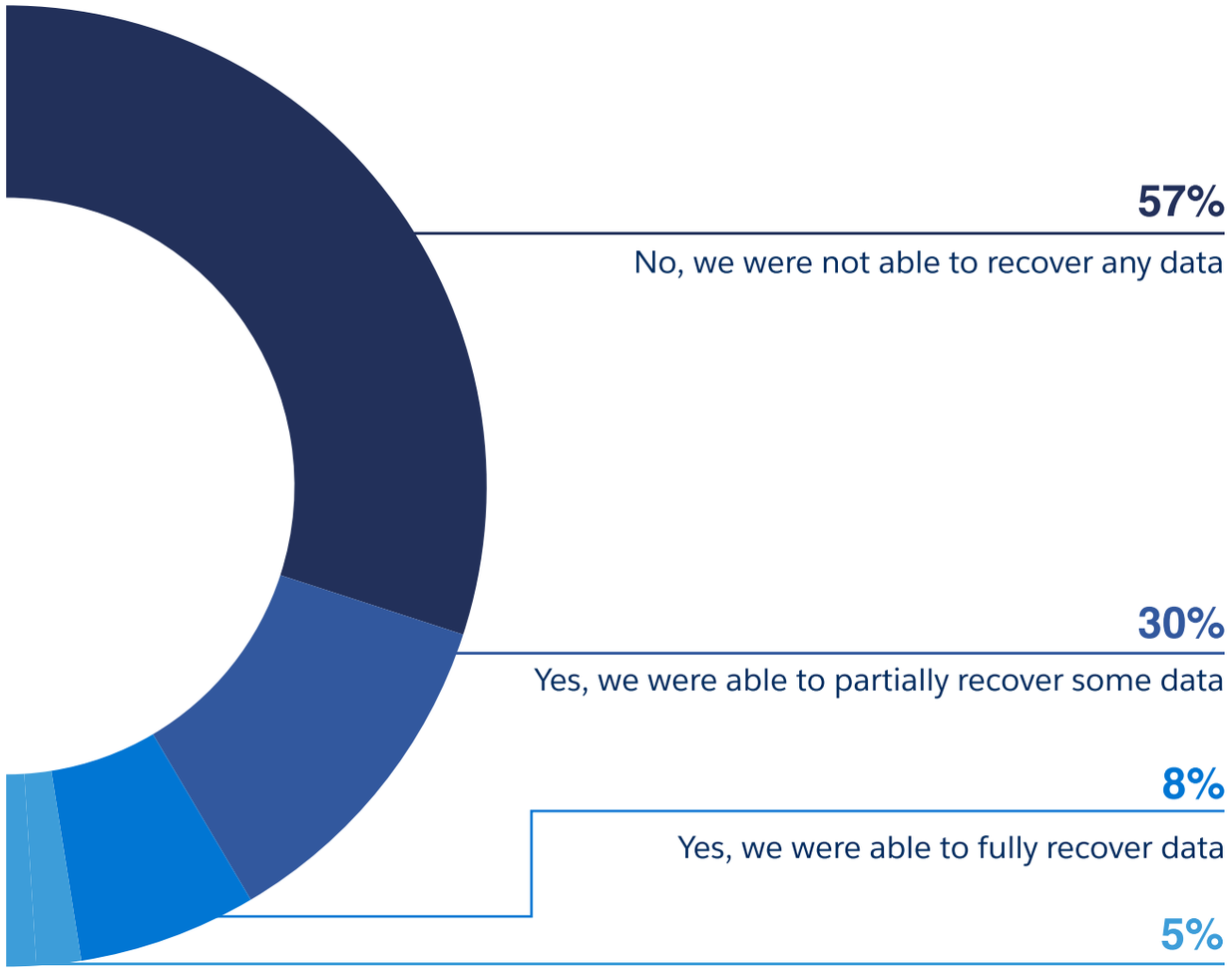
03

Cyberattacks Expose a Security Gap: Data Recovery

More than a third (38%) of surveyed security leaders reported experiencing a security breach last year – despite their best efforts. Of those who experienced a breach, 57% were not able to recover any data. And only **8% were able to fully recover lost data**, highlighting the need for robust data recovery solutions.

Quick Tip: Identity and access management is worth the investment. Of those who **did not** experience a breach in 2021, the majority (79%) used both an identity and access management solution and multifactor authentication (n=142).

If you experienced a security breach in 2021, were you able to recover data lost or corrupted during the breach? (n=121)



04 Look Ahead: The Top Data Security Tactics for 2022

As was the case last year, IT leaders will remain on high alert for increased ransomware, phishing, and DOS and DDOS attacks. And they expect regulated industries to be at the highest risk. In fact, **20% of surveyed respondents expect an increase in the volume and complexity of attacks for these industries.**

Here are four foolproof ways to fortify your defenses this year and beyond, according to our survey findings:

- **Ensure you have the right toolkit:** Data encryption, identity and access management, and multifactor authentication are a must.
- **Keep employees vigilant:** The more employees know about data security, the less likely they are to let bad actors through your firewalls.
- **Back up your data:** Data loss could be catastrophic to your business. So, protect your data with robust data backup and recovery solutions. And prioritize this as a core part of your security strategy.
- **Invest in emerging technology:** Tools, like AI/machine learning, can help you more efficiently identify existing risks and predict new ones. Many surveyed respondents expressed optimism about the effectiveness of these and other breakthrough technologies to remediate threats.

Please rank the top five industries you think are at the highest risk of experiencing a cybersecurity attack within the next 12 months. (top = highest risk, bottom = lower risk)

1	2	3	4	5
[1,142]	[808]	[794]	[465]	[227]
Finance, banking & insurance	Healthcare	Government	Educational services	Agriculture

> “I think threats will continue to increase and expand while breadth of coverage options will become more diverse and sophisticated.”
>
> VP, MANUFACTURING
> (1,001–5,000 EMPLOYEES)

Data Sources & Research Methodology

The Salesforce Data Security Study

Salesforce ran a study on trends in data security in Pulse's community of verified technology decision makers. The 300 respondents – surveyed between November 8 and December 15, 2021 – included VPs and C–Suite Infosec and IT executives in North America. The executives worked for organizations with more than 1,000 employees.

More About Pulse

Pulse is a social research platform trusted by technology leaders around the world. These leaders rely on the community to make connections, share knowledge, get advice, and stay on top of current trends in the technology space.

The questions, polls, and surveys posted in Pulse's platform are curated into insight reports that reflect what matters most to technology leaders right now. Learn more about Pulse at pulse.qa or reach out to hello@pulse.qa