imprivata®

Ponemon INSTITUTE

PONEMON REPORT

Unlocking the cost of chaos: The state of enterprise mobility in life- and mission-critical industries

Sponsored by **Imprivata**
Independently conducted by Ponemon Institute LLC
Publication date: March 2024

Ponemon Institute© Research Report

PONEMON REPORT

A letter from Imprivata CEO Fran Rosch

Our personal smartphones and tablets have become indispensable tools, allowing us to efficiently communicate, collaborate, and improve our quality of life. But as modern businesses implement enterprise-owned mobile devices for their workforce, many experience significant security, financial, and operational consequences before reaping the benefits these devices were meant to enable.

28% of IT and IT security practitioners believe their organizations' strategies can secure mobile devices and access to sensitive or confidential data

54% have experienced a data breach due to unauthorized access of these devices

Although well-intentioned executives typically make the decision to implement mobile tools, the responsibility to correct any problems often falls on IT teams. Despite the broader security and operational impacts of mobile devices, organizations lack cross-functional alignment when deploying them, and it's taking a widespread toll.

Replacing lost mobile devices has a significant financial and operational impact, with organizations paying out an average of **$5.45 million** annually on devices alone. This figure doesn't account for the costs of IT security and help desk support or diminished productivity and idle time, tacking on an additional $1.4 million, on average. Moreover, replacing them diverts time away from other IT and security obligations, potentially leaving more gaps in an organization's security posture.

At the same time, employees using these devices bear the brunt of usability issues with just 31% citing that it's easy to access applications and data on shared devices. Repetitive, manual authentication is a common challenge, underscored by less than half (42%) citing satisfaction with the access experience.

These findings, among others, depict a costly reality: enterprise-owned mobile devices have great potential, but businesses are struggling to harness it and need effective solutions to do so. While all organizations are vulnerable to breaches that not only disrupt workflows and can lead to significant financial loss, those in life- and mission-critical industries often result in dire consequences for patients and consumers who rely on critical goods and services.

This report offers a deep dive into the challenges these organizations experience, making one thing clear: the stakes are too high to implement enterprise-owned mobile devices without an effective security and access management strategy.

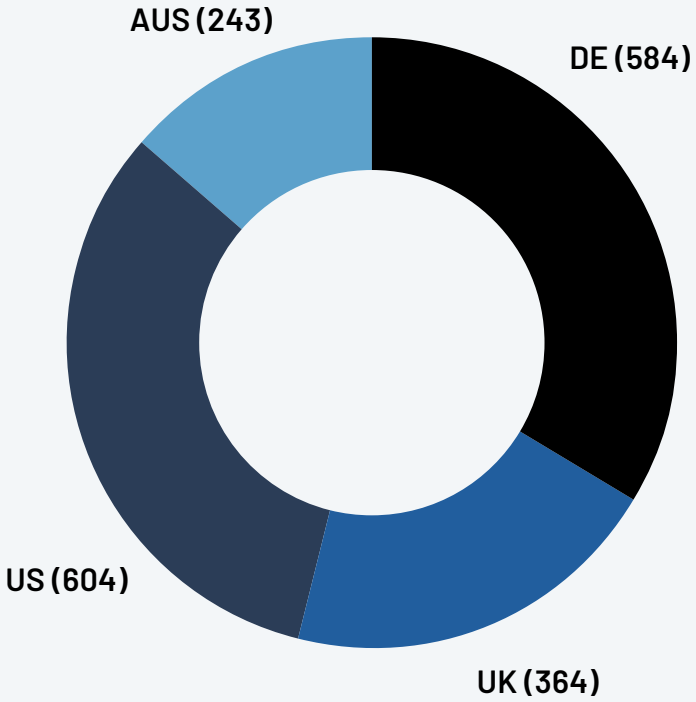
01

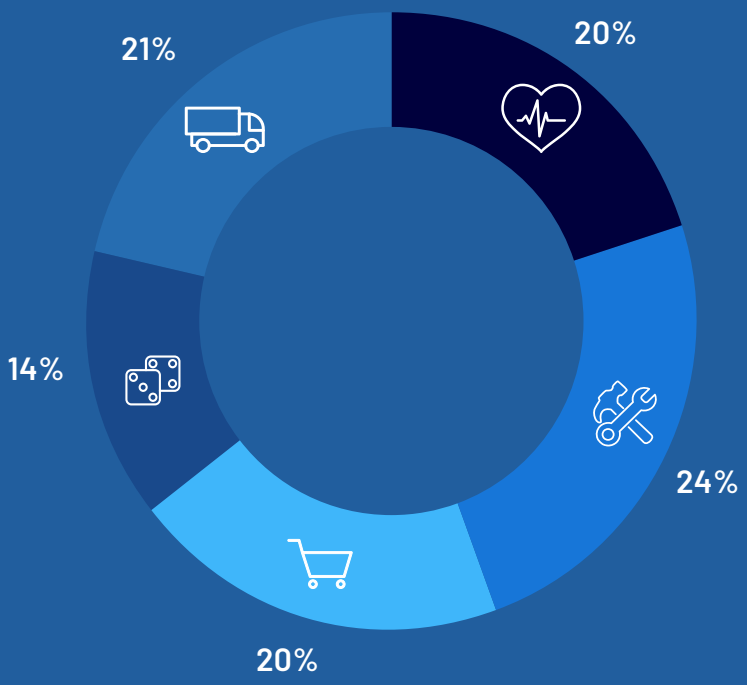
INTRODUCTION

The financial sustainability of organizations in life- and mission-critical industries is dependent upon a productive workforce that is securely and efficiently connected through their mobile devices. As shown in this research, employee productivity understandably declines when mobile devices are lost or unusable. In fact, an average of **872 hours are lost each week** due to unplanned downtime from problems with mobile devices.

For those in high-stakes organizations, this can mean the inability to provide efficient patient care, ensure timely production of goods and services, and facilitate positive customer experiences. At the same time, IT and security staff are commonly forced to delay or stop other responsibilities, which may make organizations vulnerable to cyberattacks. The findings also confirm that the inability to control access to mobile devices — especially shared devices — may result in a data breach.

The purpose of this research is to understand the state of enterprises' management of employees' mobile devices and the ability to protect access to applications without disrupting workflows or impacting productivity. Ponemon Institute surveyed 1,795 IT and IT security practitioners in the United States (604), the United Kingdom (364), Germany (584), and Australia (243) who are familiar with their organizations' strategy for mobile workflow requirements and security practices.





The industry sectors represented are **healthcare (20%)**, **manufacturing (24%)**, **retail (20%)**, **gaming (14%)**, and **transportation and logistics (21%)**.

The research focuses on the use of enterprise-provided mobile devices. These include **enterprise-owned 1:1 (38% of respondents)**, **shared enterprise-owned mobile devices (33% of respondents)**, and **both enterprise-owned 1:1 and shared enterprise-owned mobile devices (29% of respondents)**.

More than half of organizations (54%) had a data breach due to inappropriate access of employees' mobile devices and its sensitive and confidential information. The average costliest breach in the organizations represented in this research was $2.2 million.

Table 1 provides a breakdown of four costs incurred from the one data breach that averaged

$2.2 million

23% of the cost was based on the value of the data or device compromise

25% came from the loss of reputation and customer goodwill

25% was due to cost of non-compliance or regulatory violations

27% of costs were related to detecting, containing, and remediating the data breach

Table 1. Costs incurred from an average data breach	Cost
The value of the data or device compromised (23%)	$510,597
The cost of non-compliance or regulatory violations (25%)	$554,801
The cost of lost reputation and customer goodwill (25%)	$554,801
Other costs incurred related to detecting, containing, and remediating the data breach (27%)	$590,855
Total	**$2.2 million**

02

KEY FINDINGS

In this section, we provide a deeper dive into the research findings. The complete audited findings are presented in the Appendix of this report. We have organized the report according to the following:

- IT and IT security staff lose valuable time when dealing with lost devices
- Shared devices have security challenges which can lead to unsatisfactory user experiences
- Strategies used to deal with enterprise-provided mobile device security risks
- Country and industry differences

IT and IT security staff lose valuable time when dealing with lost devices

The IT and IT security teams' involvement in dealing with lost mobile devices is costly. Respondents were asked to estimate the different costs incurred when devices are lost. Table 2 presents the average annual cost of IT help desk support, IT security support, and diminished productivity or idle time when dealing with lost devices. At $716,411 annually, IT security support is the most expensive, with the total average annual cost being $1,384,660.

An average of

39,439

mobile devices are used by employees in organizations represented in this research

and an average of 16% or

6,310

of these are typically lost each year.

The average replacement cost for a single mobile device is

$864

On average, replacing lost devices costs organizations

$5.45 mil

annually (6,310 x $864).

Table 2. The average annual cost of dealing with lost mobile devices	Cost
IT help desk support	$140,000
IT security support	$716,411
Diminished productivity or idle time	$668,249
Total	**$1,384,660**

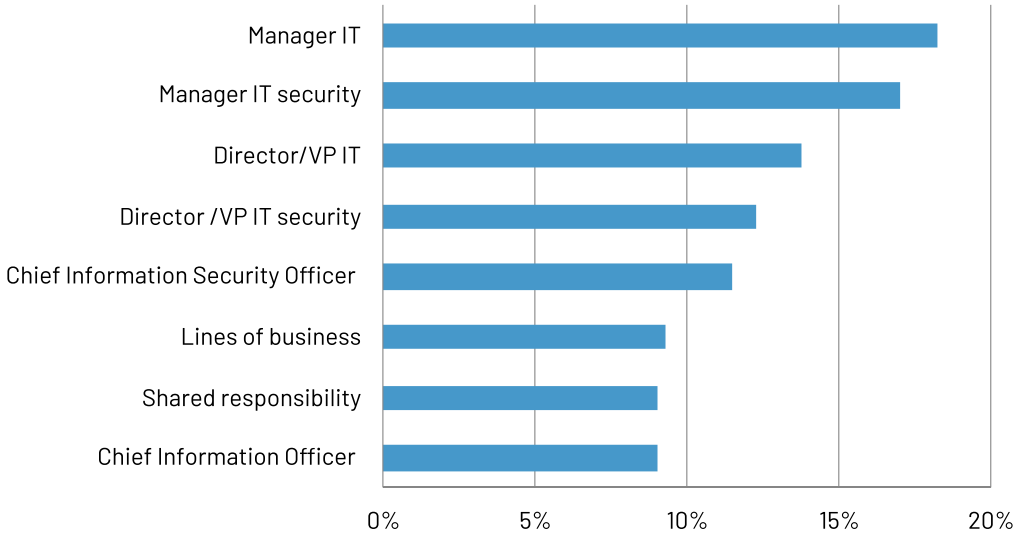
In addition to being costly, the productivity of IT, IT security, and other employees decreases as a result of device loss. Diverting time away from their other IT and IT security duties can increase workplace stress and potentially leave gaps in an organization's security posture. Respondents estimated that **203 hours are spent annually to replace lost devices.**

In addition to estimating the hours spent annually to replace lost devices, we asked respondents to estimate how much time is spent each week to manage, maintain, track, and monitor mobile devices as well as downtime caused by devices that are not useable due to loss, as shown in Table 3. The average total weekly hours spent on these activities and downtime is 1,062 hours.

Table 3. Average hours spent each week finding lost devices and managing, maintaining, tracking, and monitoring all mobile devices and employee downtime	Hours
Hours spent each week finding lost devices by the IT team and frontline workers	78
Hours spent each week managing, maintaining, tracking, and monitoring mobile devices	112
Downtime due to devices that are not useable	872
Total hours spent weekly	1,062

IT and IT security managers bear the financial burden of lost mobile devices. According to Figure 1, the roles least financially responsible are lines of business and chief information officers.

Figure 1. Roles that are financially responsible for replacing lost mobile devices



User productivity would improve if maintaining and managing mobile devices could be done remotely.

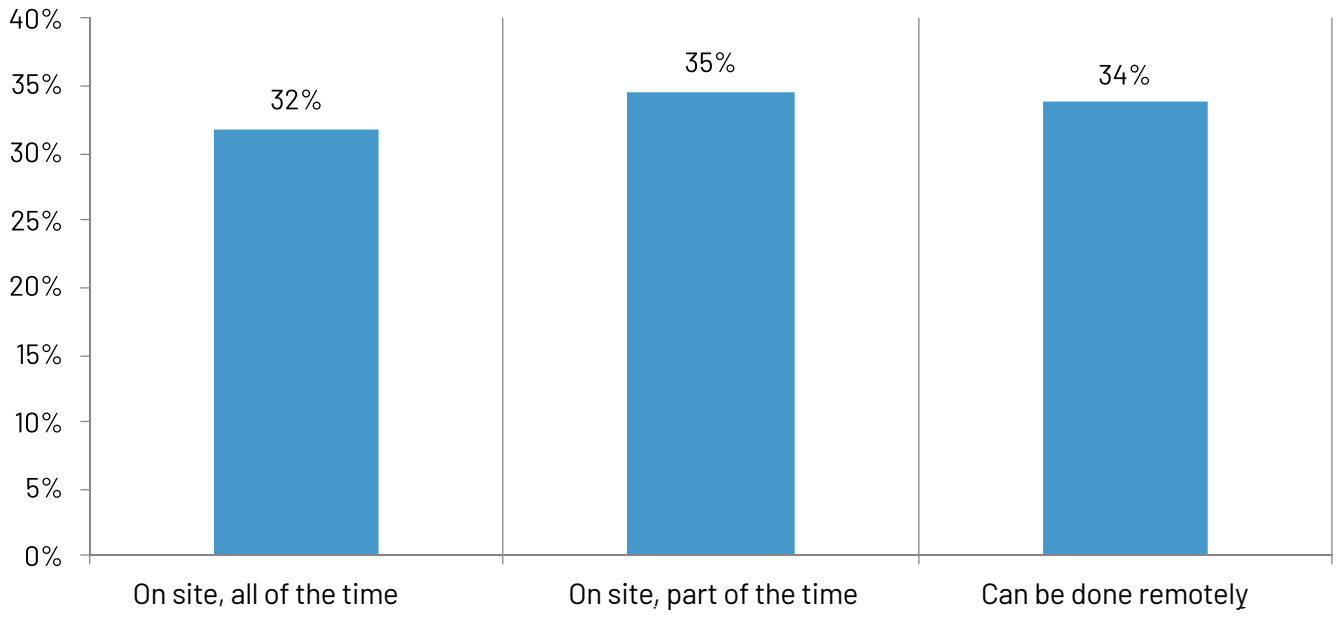
52%

More than half (52%) of respondents cite that user productivity is significantly impacted if the organization cannot maintain and manage mobile devices remotely.

67%

Nearly seven in ten respondents say they maintain and manage mobile devices onsite, all or part of the time.

Figure 2. Percentage of respondents who maintain and manage mobile devices onsite or remotely



At the same time, organizations are struggling with manual processes, with less than half citing that the mobile device management is fully automated.

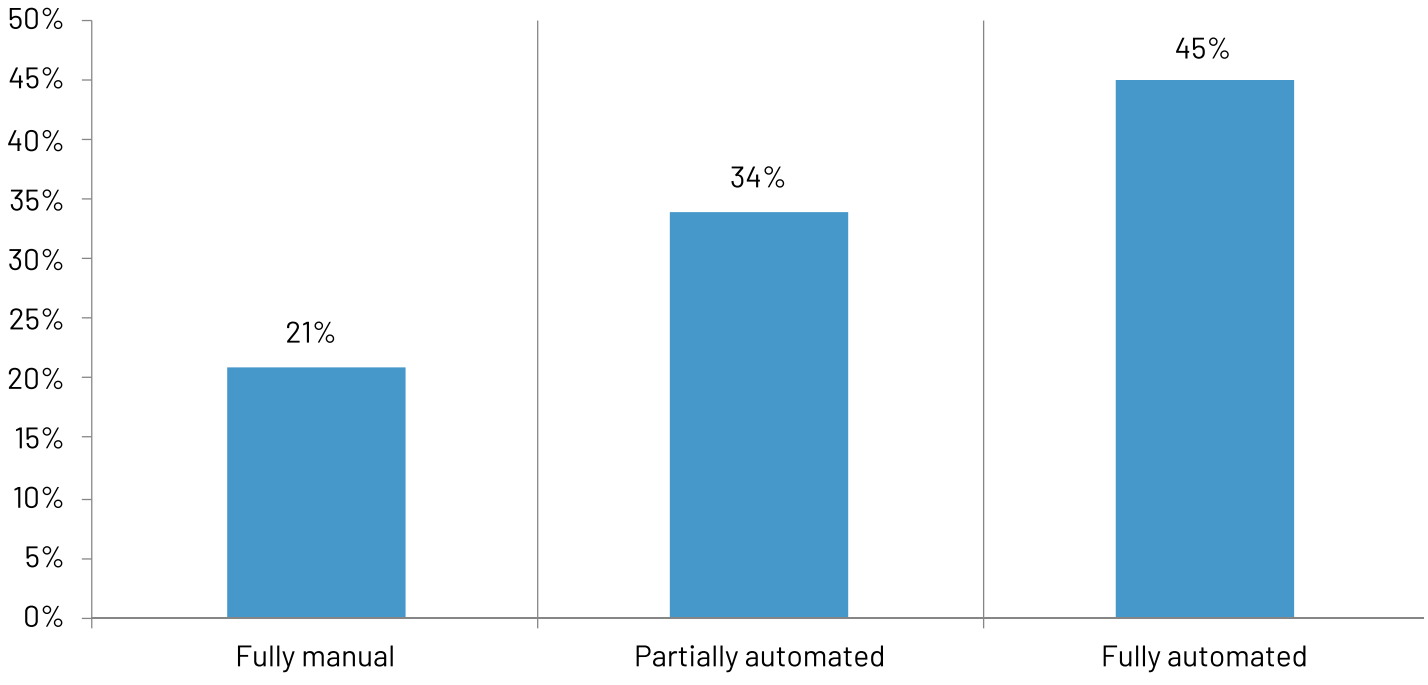
34%

Mobile device management is partially automated

21%

Mobile device management is fully manual

Figure 3. Process for maintaining and managing mobile devices

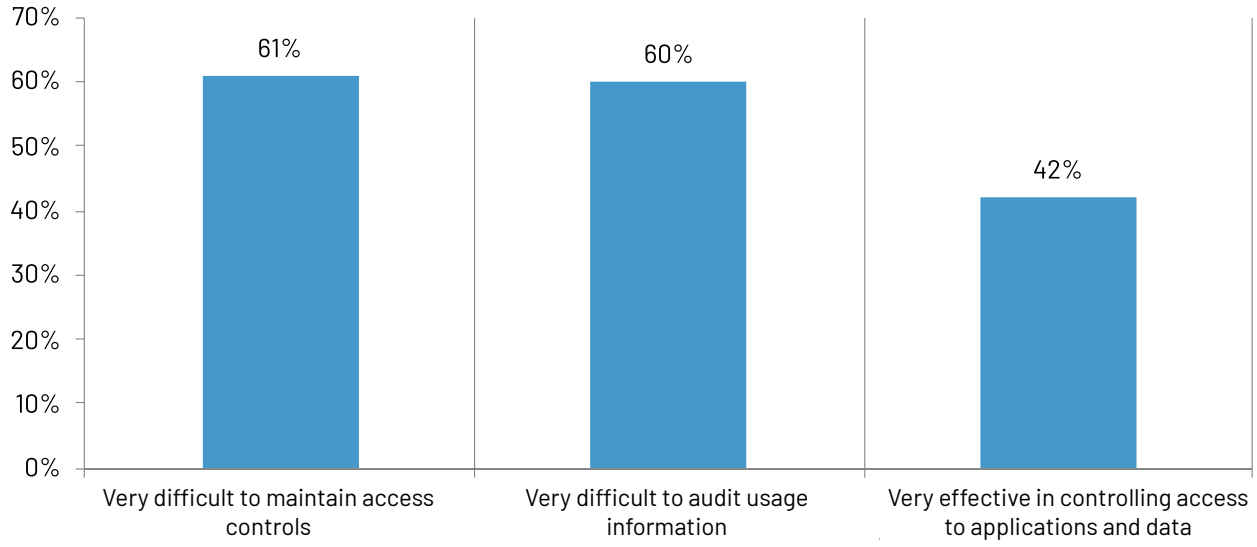


THE SECURITY CHALLENGES OF SHARED DEVICES CAN LEAD TO UNSATISFACTORY USER EXPERIENCES

Sixty-two percent of respondents say their enterprise-provided mobile devices are shared. As shown in Figure 4, organizations find it very difficult to maintain access controls on shared devices (61% of respondents) and to audit usage information on shared devices (60% of respondents). Only 42% of respondents say their organizations are very effective in controlling access to applications and data on shared mobile devices.

Figure 4. Challenges with maintaining access controls, audit usage information, and access to applications and data

Data represents percentage of respondents who ranked themselves as 7+ on a scale from 1 = not difficult/not effective to 10 = very difficult/very effective



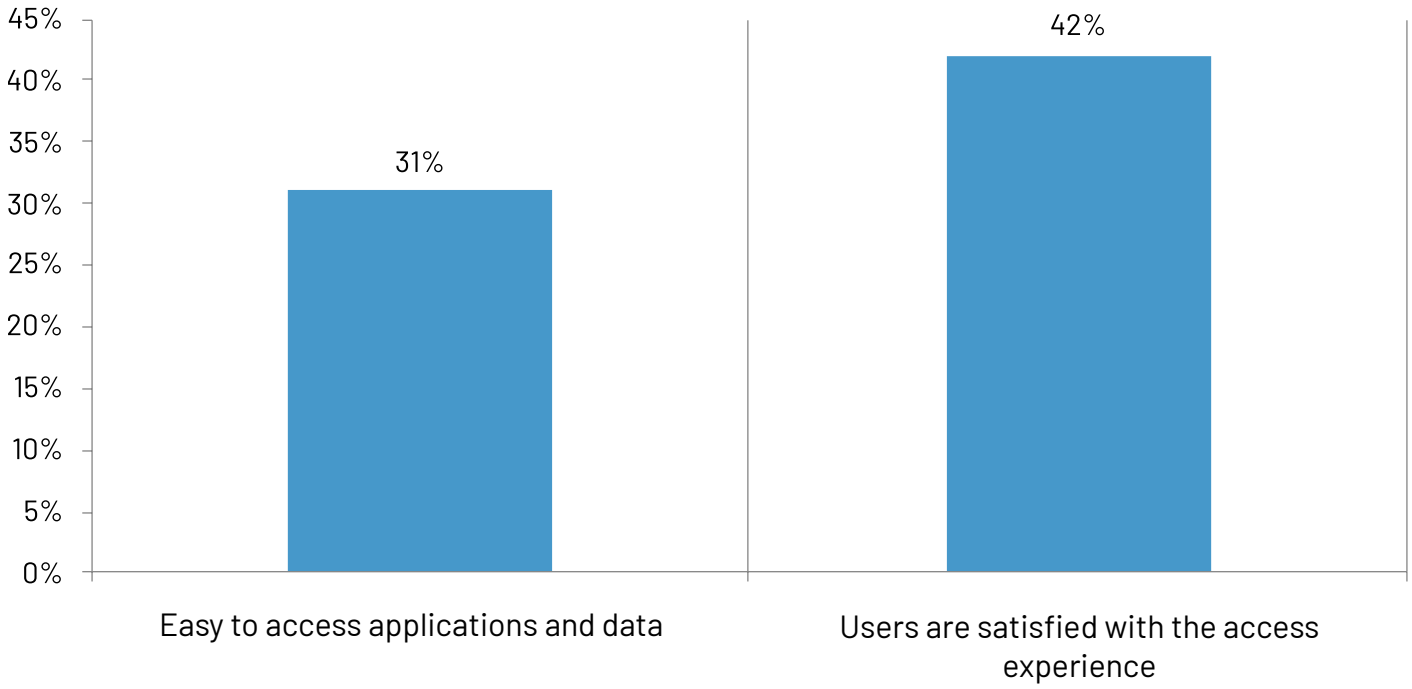
42%

Less than half (42%) say users are satisfied with the access experience on shared mobile devices.

Difficult access workflows on shared mobile devices affect user productivity.

According to Figure 5, while there are security issues, users also have challenges with accessing applications and data on shared devices. Only 31% of respondents say it is very easy for users to have access and only 42% say users are satisfied with the access experience.

Figure 5. User satisifcation with accessing applications

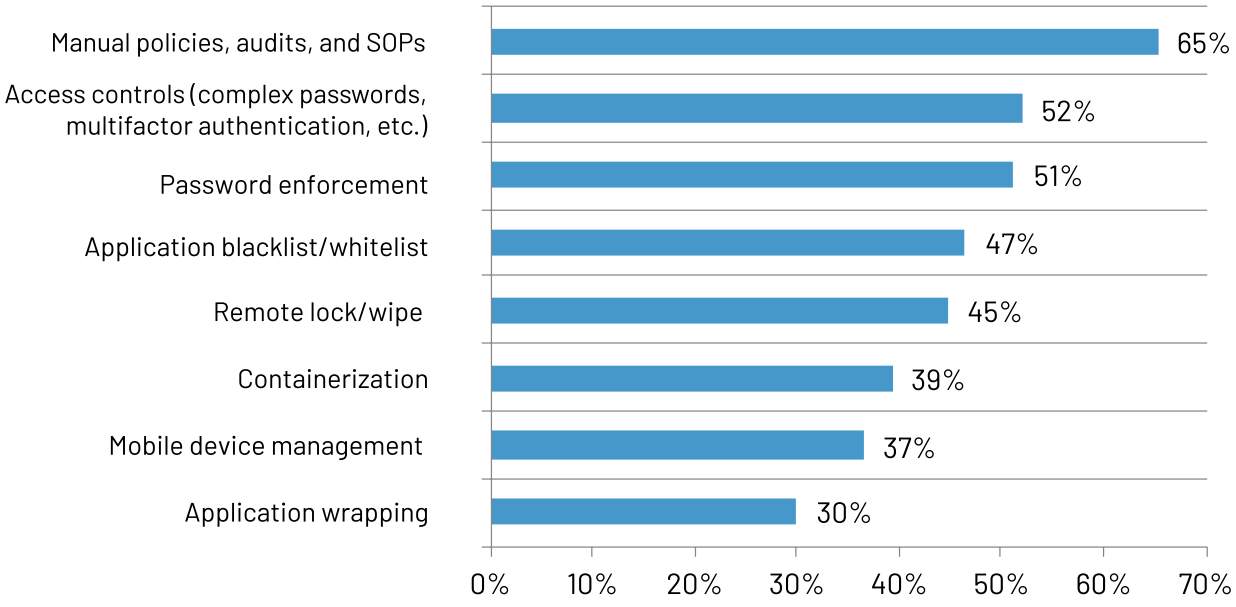


Strategies used to deal with enterprise-provided mobile device security risks

Most organizations use manual policies, audits, and SOPs to manage data accessible on mobile devices. On average, four staff are dedicated to the security and management of mobile devices.

For 65% of respondents, manual policies, audits, and SOPs are the top measures taken to manage data accessible on mobile devices.

Figure 6. Measures taken to manage data accessible on mobile devices
More than one response permitted

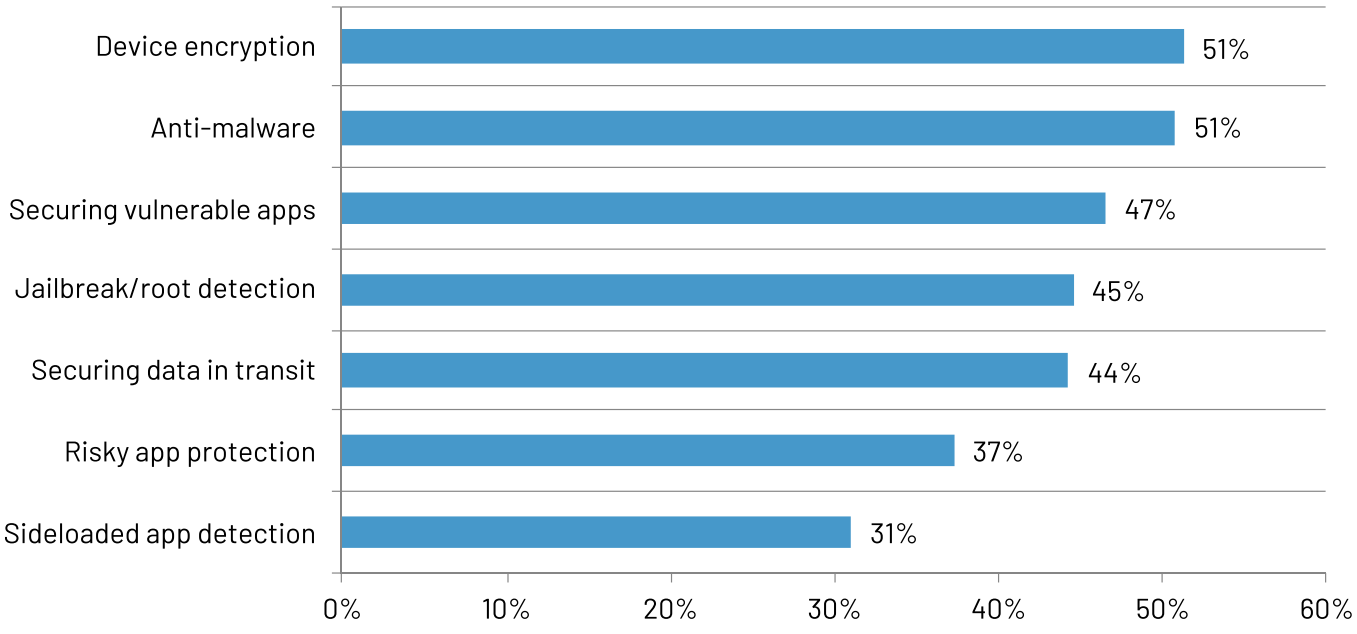


51%

Slightly more than half (51% of respondents) say their programs or strategies can maintain control over who has access to what devices and when they are accessed.

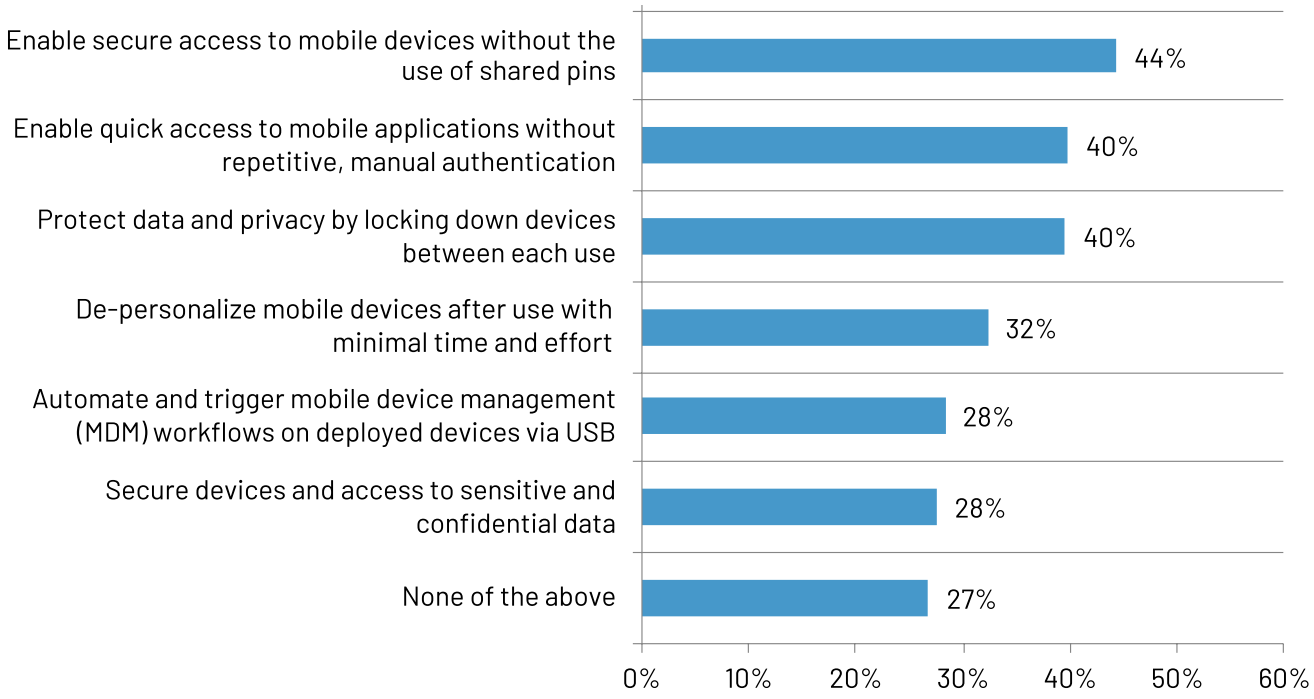
Sensitive data on mobile devices is vulnerable and organizations need to increase measures used to secure access. As shown in Figure 7, slightly more than half (51% of respondents) encrypt devices. Only 47% are securing vulnerable apps and only 44% are securing data in transit.

Figure 7. Measures taken to secure data accessible on enterprise-owned mobile devices
More than one response permitted



Many organizations' mobile device programs or strategies are failing to secure devices and access. The CIO and CTO are most responsible for their organizations' mobile device strategies and programs. As shown in Figure 8, only **28% of respondents say their programs and strategies can both secure devices and secure access to sensitive and confidential data. At the same time, just 40% of respondents say their programs enable quick access to mobile applications without repetitive, manual authentication and only 40% can ensure data privacy by locking down devices between each use.**

Figure 8. Mobile device programs or strageties currently enable the following



Mobile device programs or strategies often do not include much needed requirements to reduce the financial and productivity consequences caused by unsecured mobile devices.

Figure 9 presents what organizations include in their mobile device programs or strategies. While significant time is spent tracking devices, only 40%of respondents say their organizations are making the delivery of an auditable trail of user access as devices change hands part of their strategies.

44%

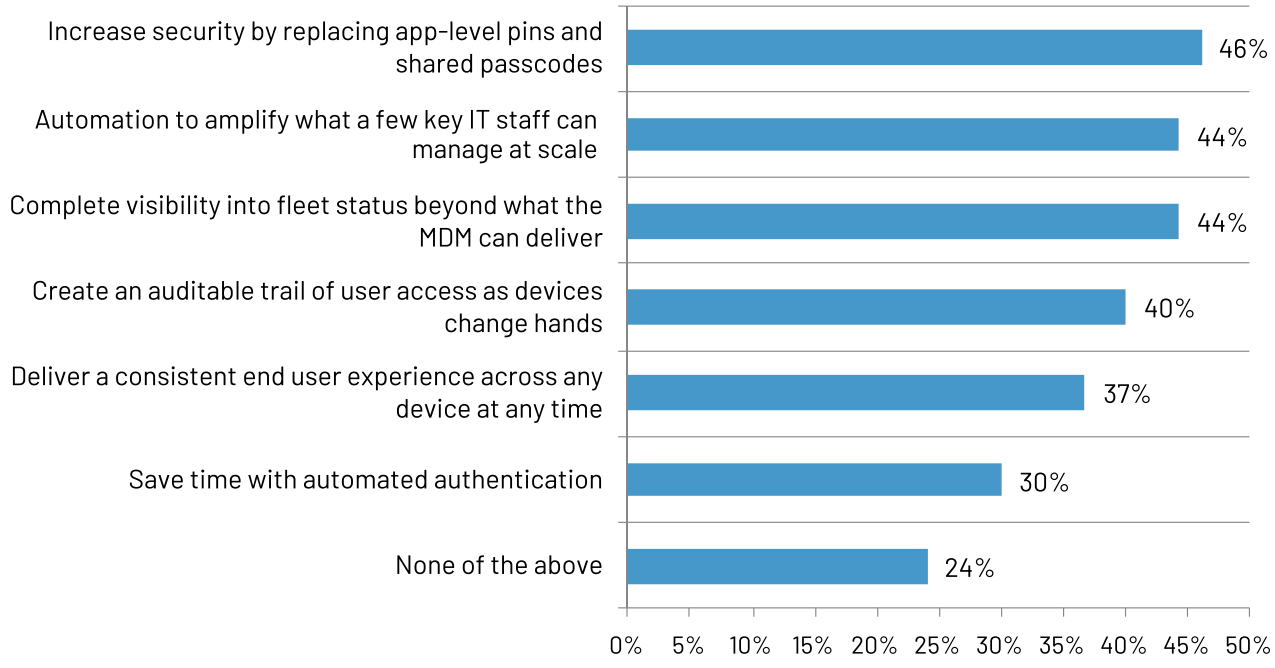
IT and IT security spend a significant amount of time managing devices, with less than half (44%) of respondents saying their strategy includes automation to amplify what a few key IT staff can manage at scale.

37%

Only 37% of respondents say their organizations include the requirement to deliver a consistent end user experience across any device at any time.

Figure 9. Requirements included in current mobile device programs or strategies

More than one response permitted



03 COUNTRY AND INDUSTRY DIFFERENCES

Country differences

In this section, we present the most interesting differences among the countries represented in the research: US (604 respondents), UK (364 respondents), Germany (584 respondents), and Australia (243 respondents).

Germany is most effective in protecting sensitive or confidential data on lost devices. Figure 10 shows the very effective findings (7 or higher on a scale of 10) in safeguarding data on lost devices. The highest in effectiveness is Germany (51%) and the lowest is the UK (40%).

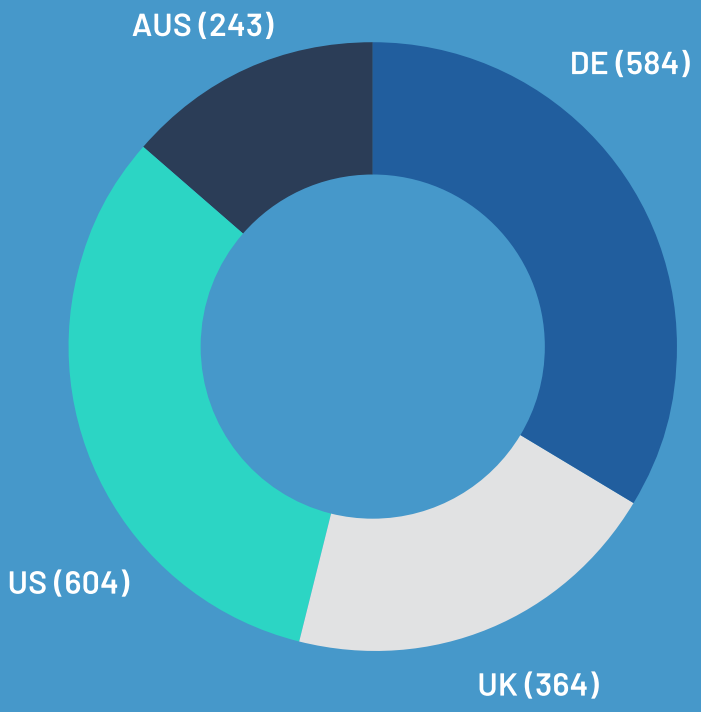
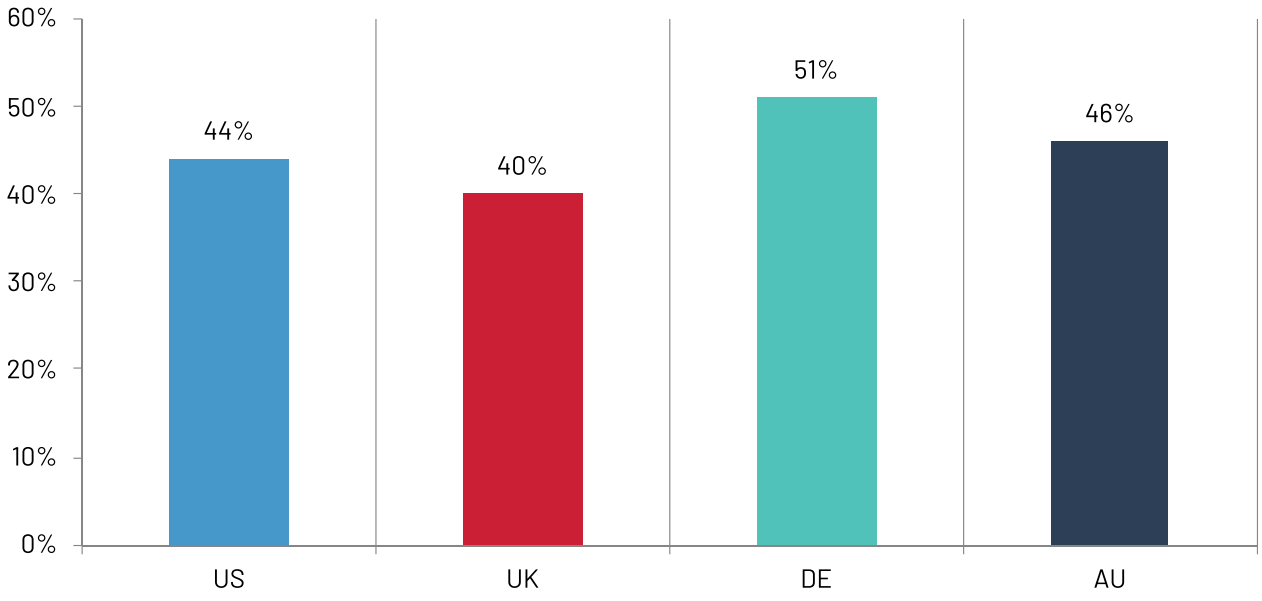


Figure 10. Effectiveness of protecting sensitive or confidental data on lost devices

Data represents percentage of respondents who ranked their effectiveness as 7+ on a scale of 1 = not effective to 10 = very effective



All countries consider it very difficult to maintain access controls on shared devices. Respondents were asked to rate the difficulty in maintaining access controls on shared devices. Figure 11 shows the very difficult responses. Australian respondents are more likely to say it is very difficult to protect access on shared devices (64%).

Figure 11. Percentage of organizations that find it very difficult to maintain access controls on shared devices

Data represents percentage of respondents who ranked their difficulty as a 7+ on a scale of 1 = not difficult to 10 = very difficult

The US is by far the most effective in controlling access to applications and data on shared mobile devices. Respondents were asked to rate the effectiveness of their ability to control access to applications and data on shared mobile devices. Figure 12 presents the highly effective responses.

Figure 12. Percentage of organizations that are highly effective at controlling access to applications and data on shared mobile devices

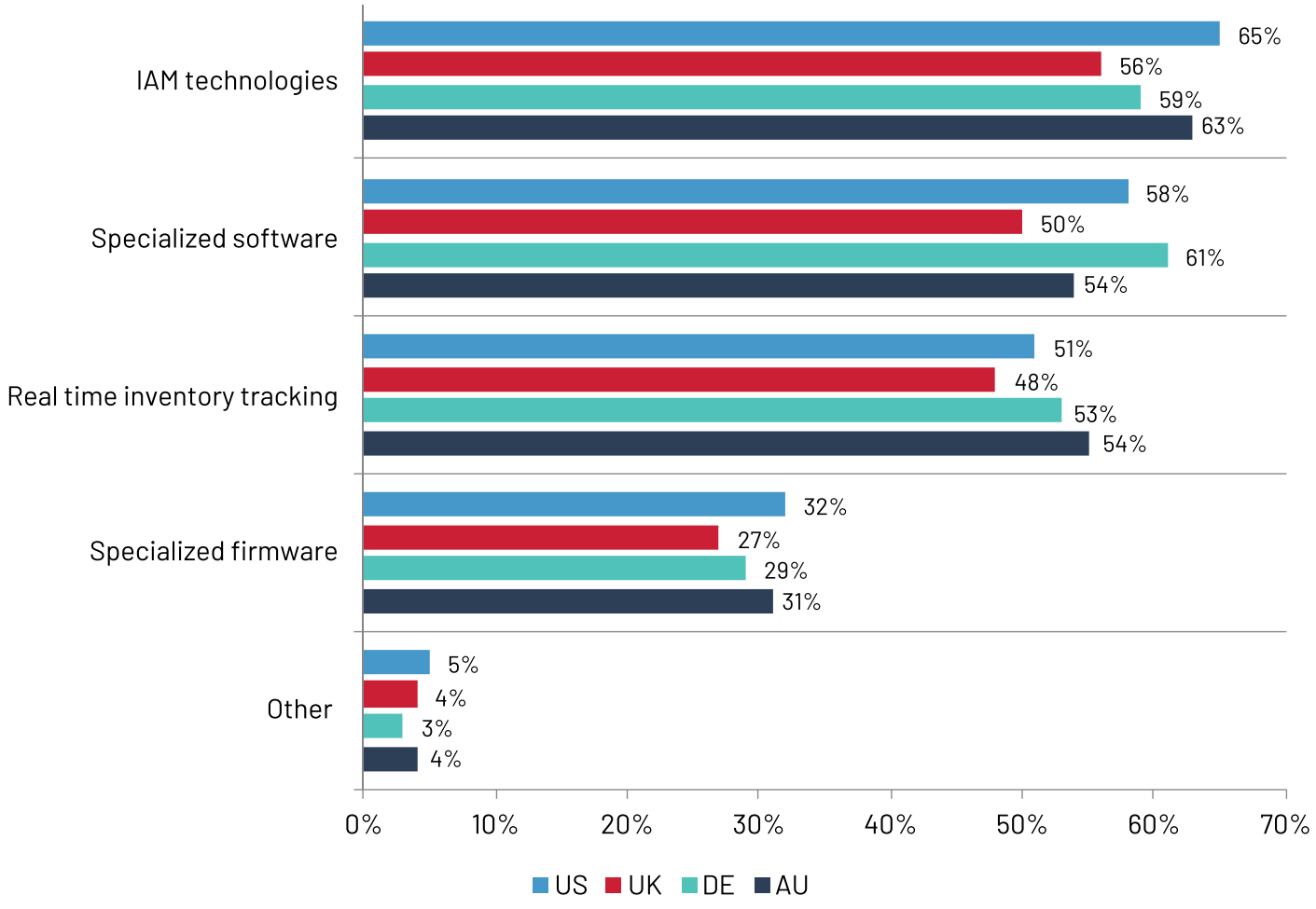
Data represents percentage of respondents who ranked their effectiveness as a 7+ on a scale of 1 = not effective to 10 = highly effective

Most countries are using identity and access management (IAM) when managing assets as they move throughout the organization.

According to Figure 13, 65% of US respondents say their organizations use IAM to support asset tracking. Germany is most likely to use specialized software.

Figure 13. Methods used to support asset tracking as devices move throughout facilities

More than one response permitted



04 INDUSTRY DIFFERENCES

In this section, we present the most interesting differences among the industries represented in this research: healthcare (20%), manufacturing (24%), and retail (20%).

The highest replacement cost, as shown in Figure 14, is in manufacturing at

$901 per device.

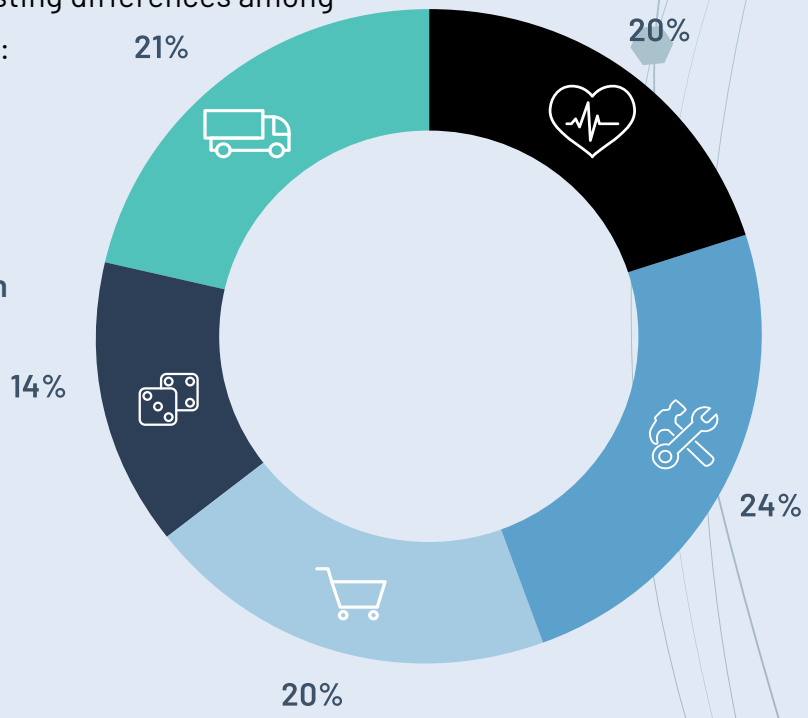
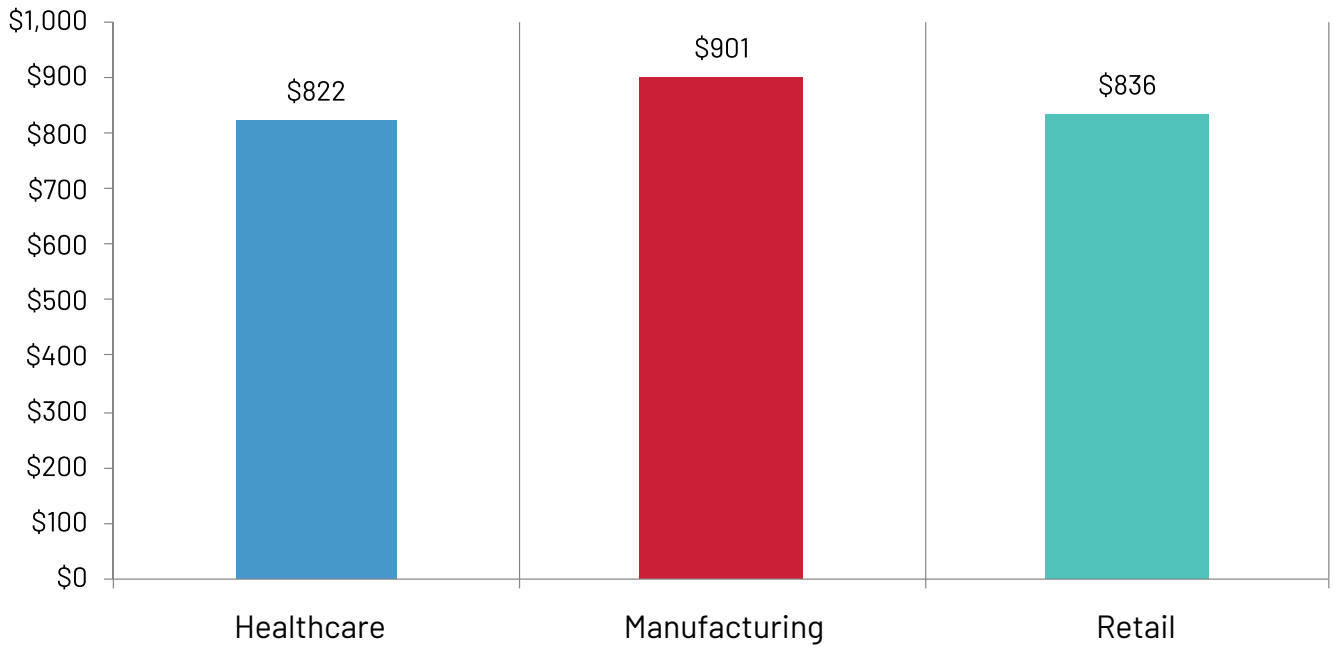


Figure 14. Average replacement cost of one mobile device

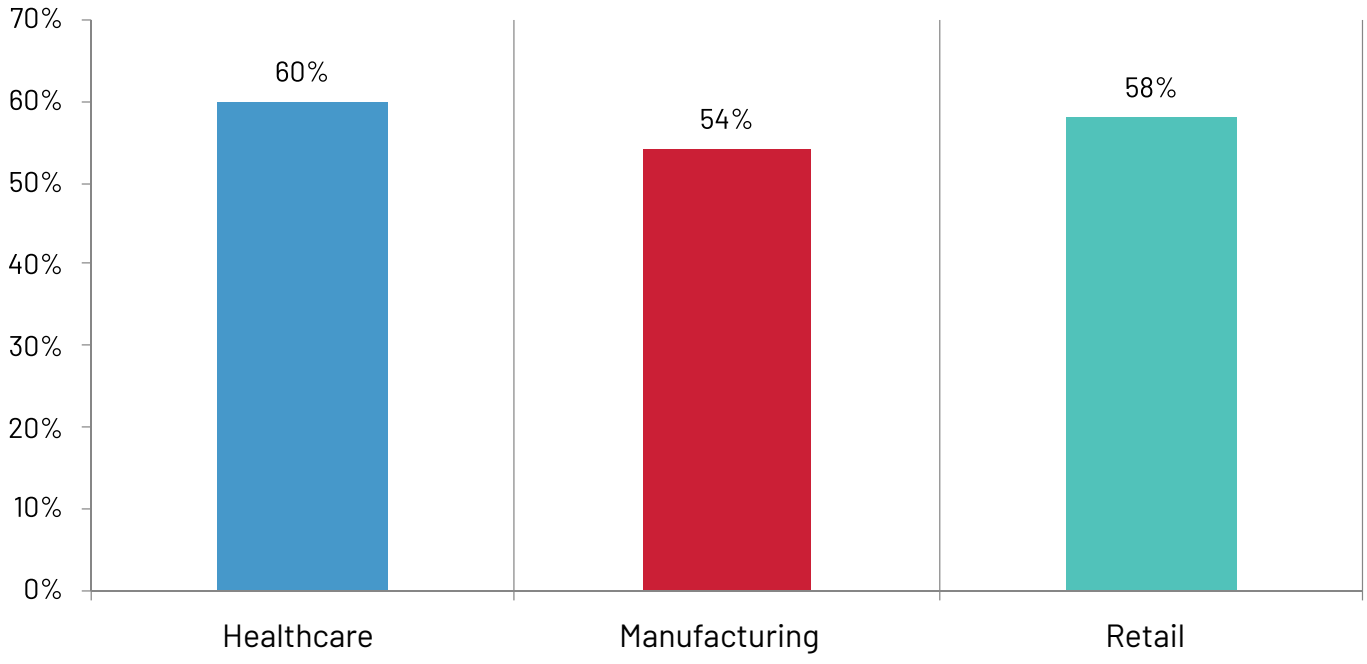
Extrapolated average presented



Respondents were asked to rate the difficulty of auditing usage information on shared devices on a scale from 1 = not difficult to 10 = very difficult. Figure 15 shows the very difficult responses. While very difficult in all industries, more healthcare organizations rate auditing usage information as very difficult.

Figure 15. Percentage of organizations that find it very difficult to audit usage information on shared devices

Data represents percentage of respondents who ranked their difficulty as a 7+ on a scale of 1 = not difficult to 10 = very difficult



Healthcare organizations are most likely to maintain control over who has access to what devices and when, at 55% of respondents.

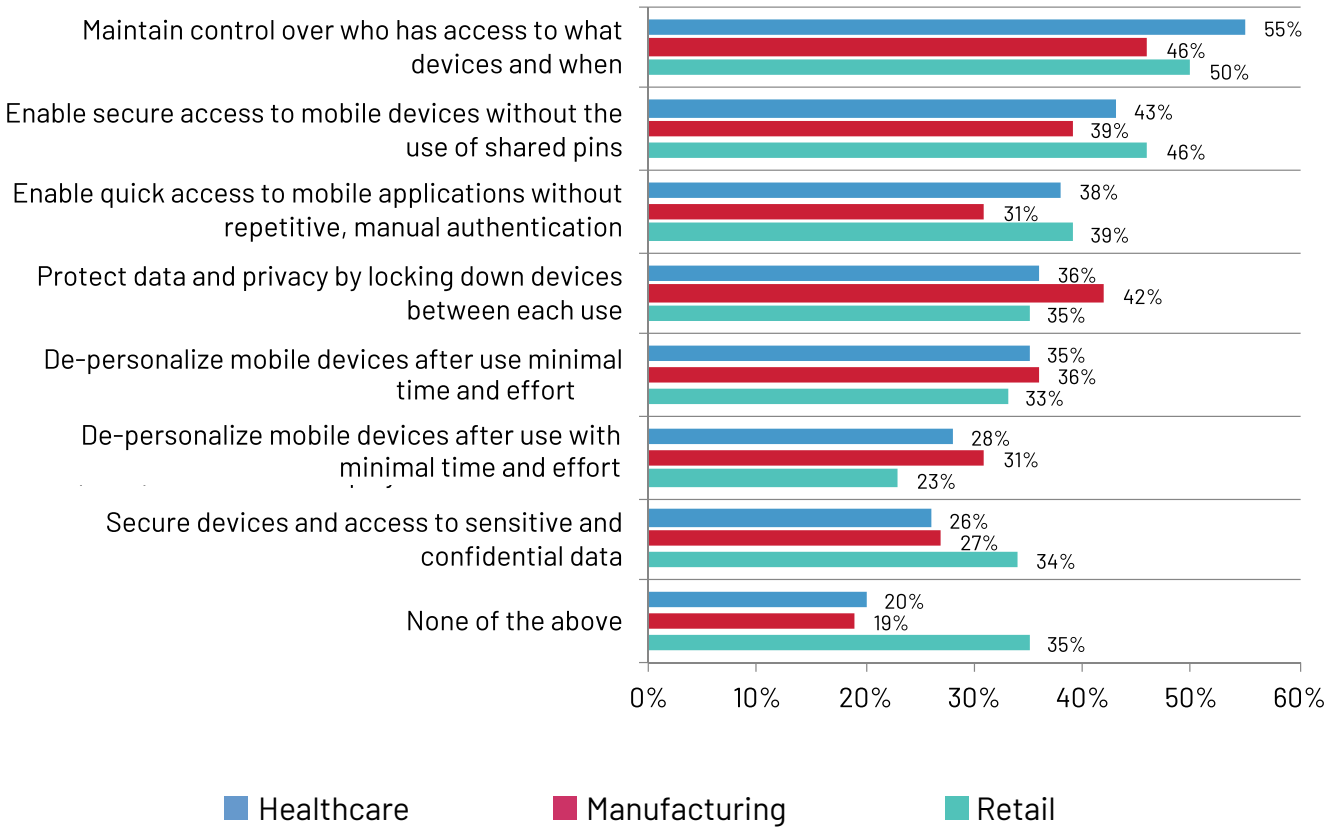
42%

Manufacturing is most likely to protect data and privacy by locking down devices between each use at 42% of respondents.

34%

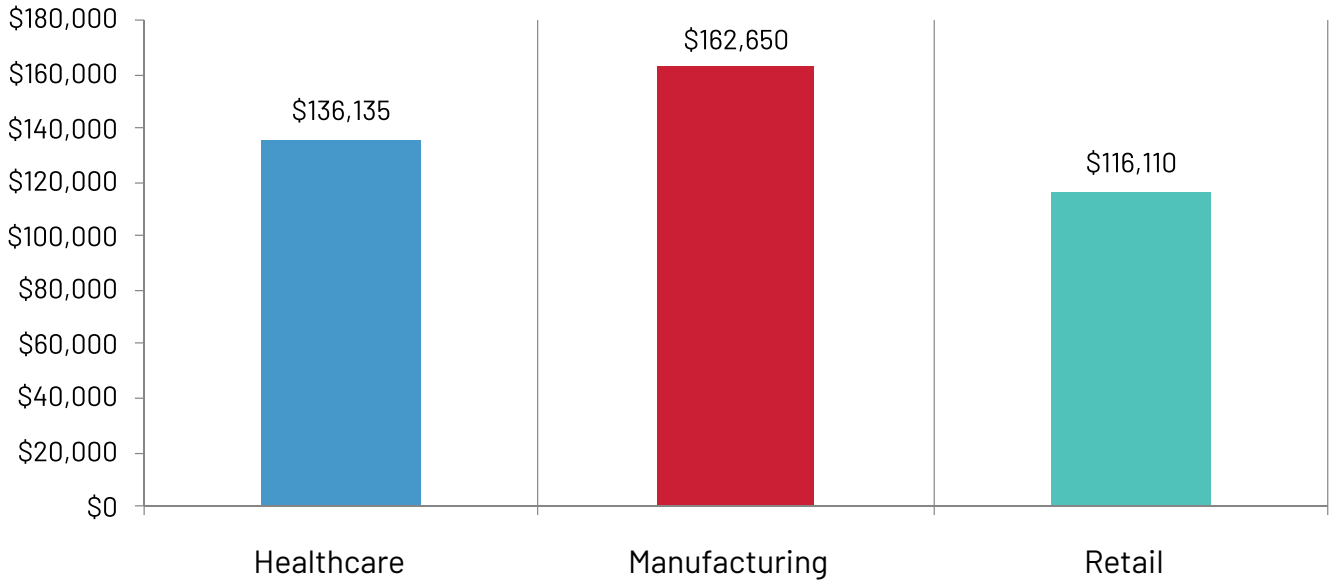
Retail is most likely to be able to secure devices and access to sensitive and confidential data at 34% of respondents.

Figure 16. Percentage of mobile device programs or strategies that enable the following



Manufacturing spends significantly more on IT help desk support due to lost mobile devices at $162,650, as shown in Figure 17. Retail spends the least at $116,110.

Figure 17. Annual spend on IT help desk support due to lost mobile devices



As shown in Figure 18, there are significant differences among the industries in what was spent on IT security support.

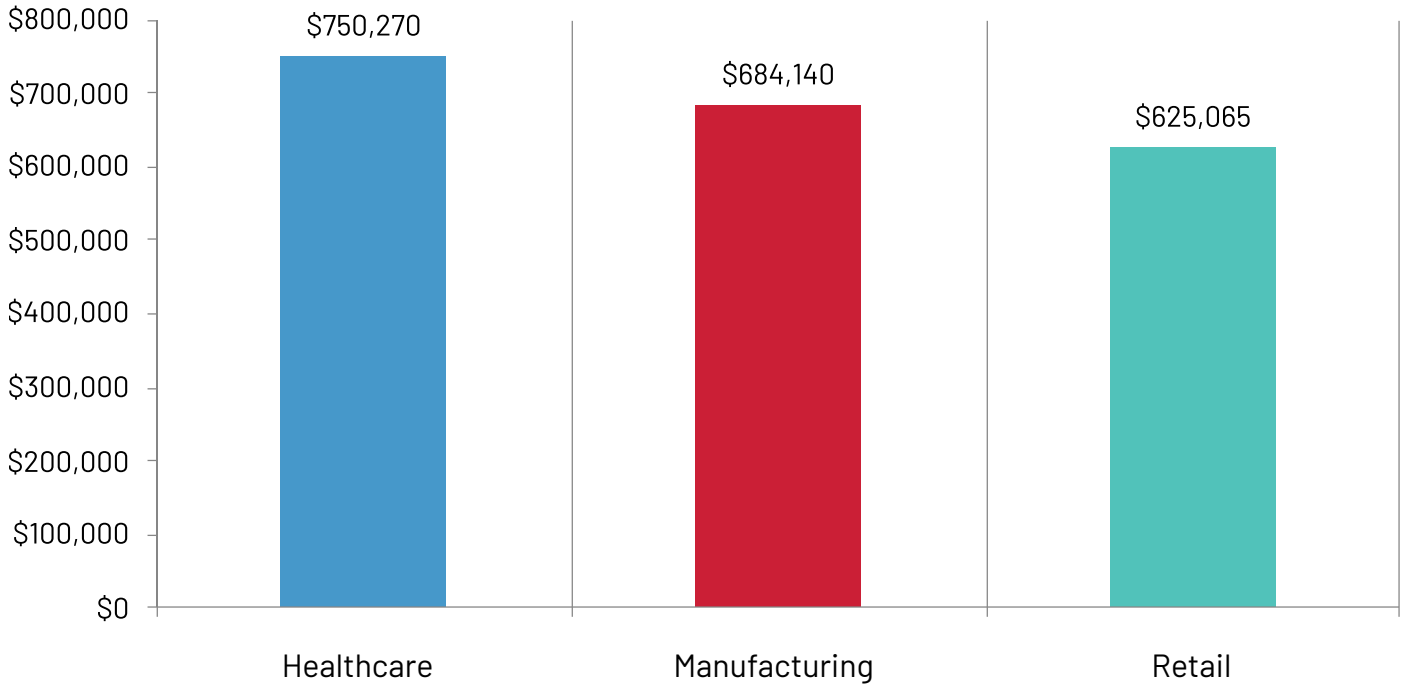
Healthcare spends the most on IT security support at

$750,270

Retail spends the least at

$625,065

Figure 18. Amount spent annually on IT security support (including investigation and forensics) due to lost mobile devices



Healthcare organizations are also more severely impacted by diminished productivity or idle time when mobile devices are lost.

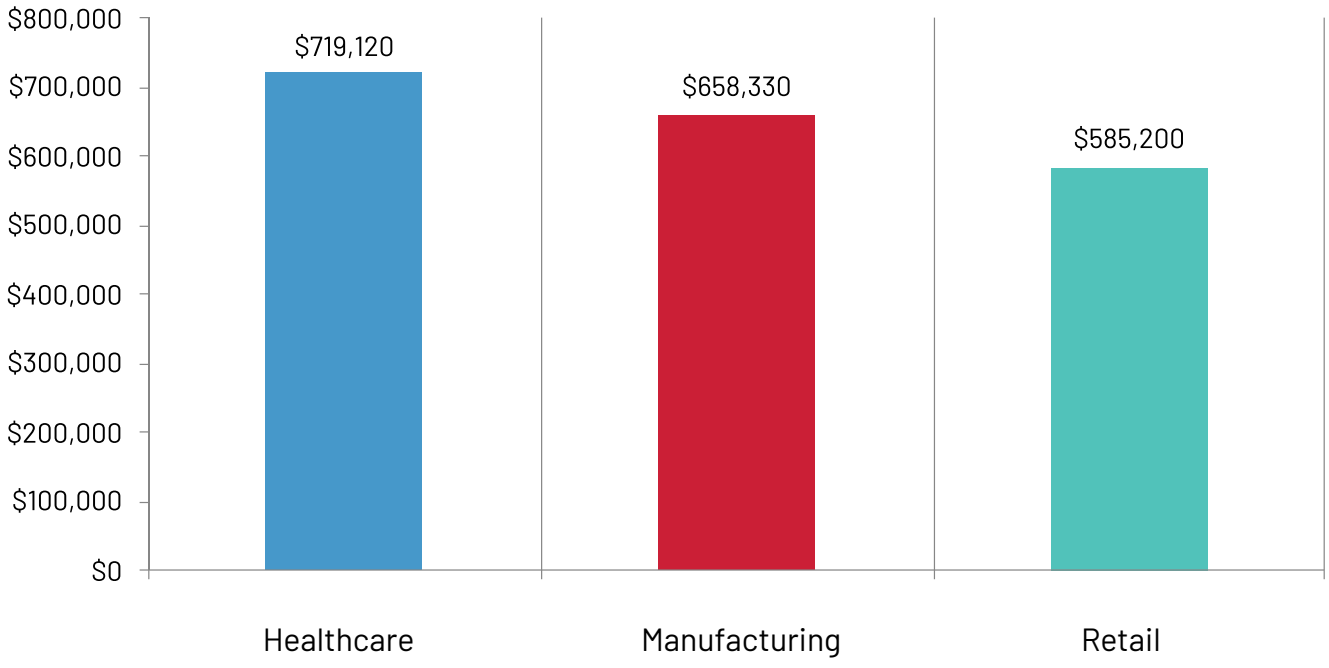
The average cost of diminished productivity due to lost mobile devices in healthcare is

$719,120

Retail is not as severely impacted at

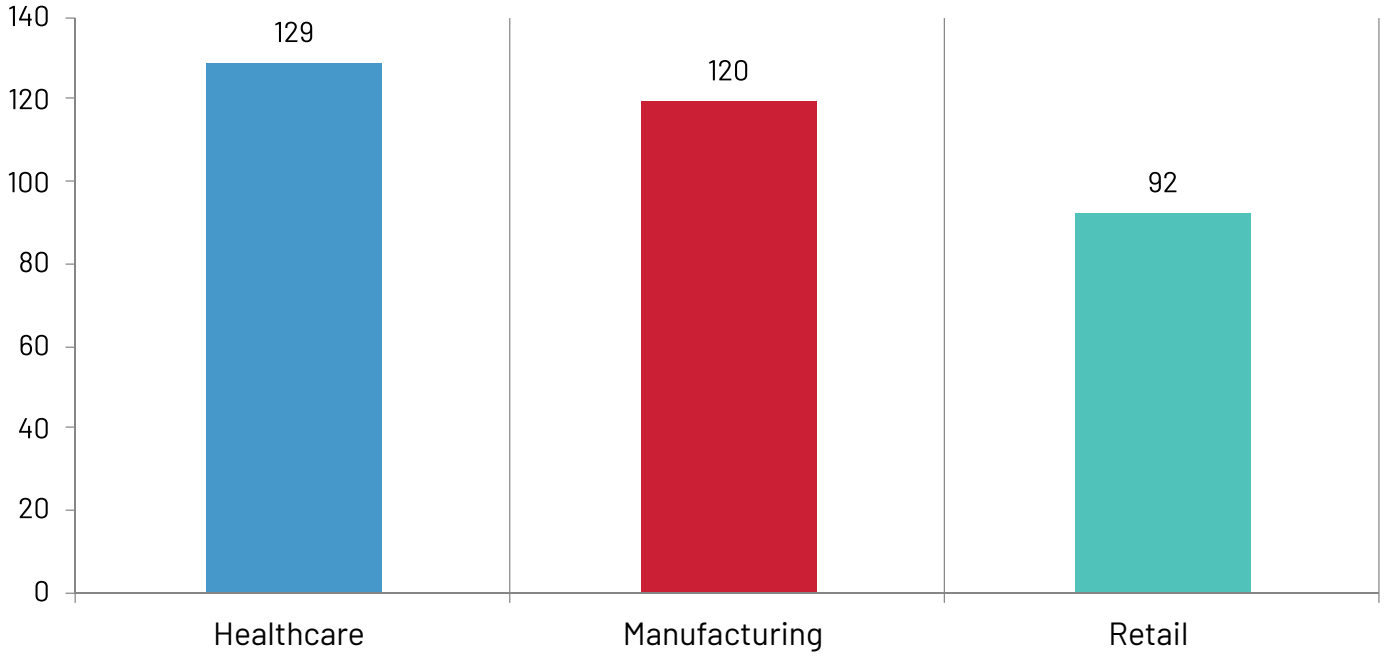
$585,200

Figure 19. Annual cost of diminished productivity or idle time due to lost mobile devices



Healthcare and manufacturing are spending the the most time each week on managing, maintaining, tracking, and monitoring mobile devices. As shown in Figure 20, healthcare spends an average of 129 hours per week and manufacturing spends an average of 120 hours per week on activities related to mobile devices.

Figure 20. Approximate hours spent each week managing, maintaining, tracking, and monitoring mobile devices



The user access experience on shared mobile devices is poor in every industry.

Respondents were asked to rate the user experience accessing applications and data on a scale of 1 = not satisfied to 10 = highly satisfied. Figure 21 presents the highly satisfied responses (7+ on a 10-point scale).

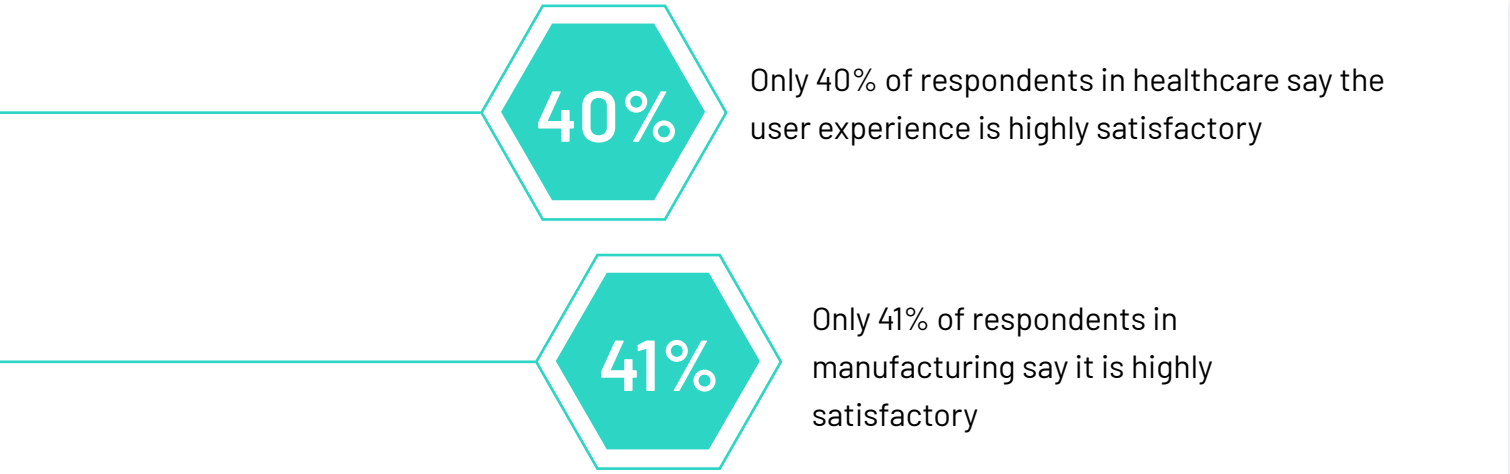
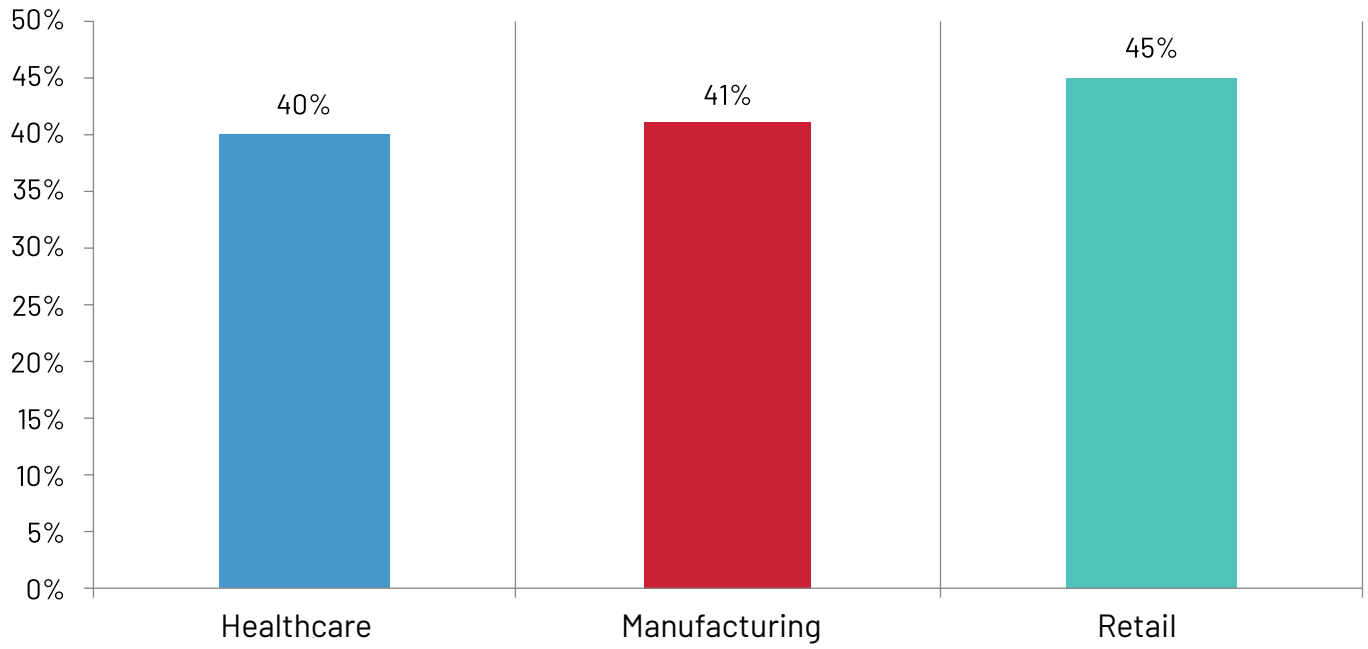


Figure 21. Percentage of respondents that are highly satisfied with the user access experience
Data represents percentage of respondents who ranked their satisfaction as a 7+ on a scale of 1 = not satisfied to 10 = very satisfied.

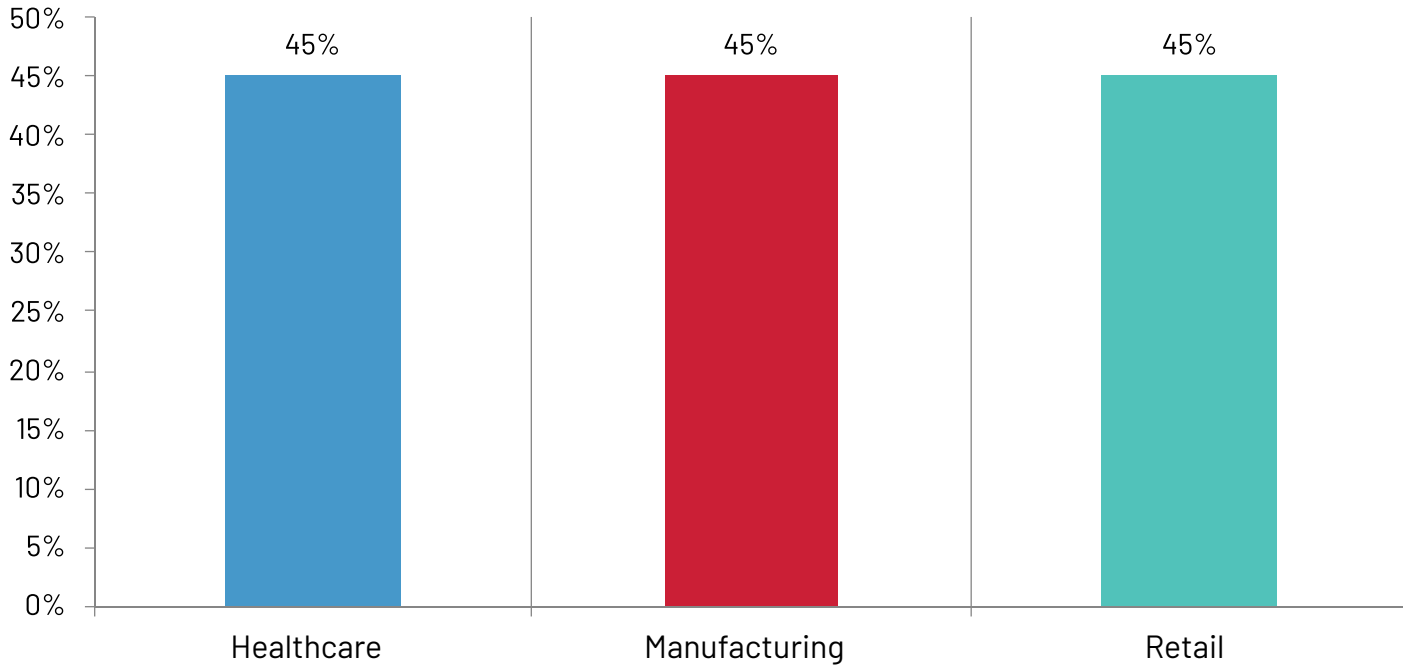


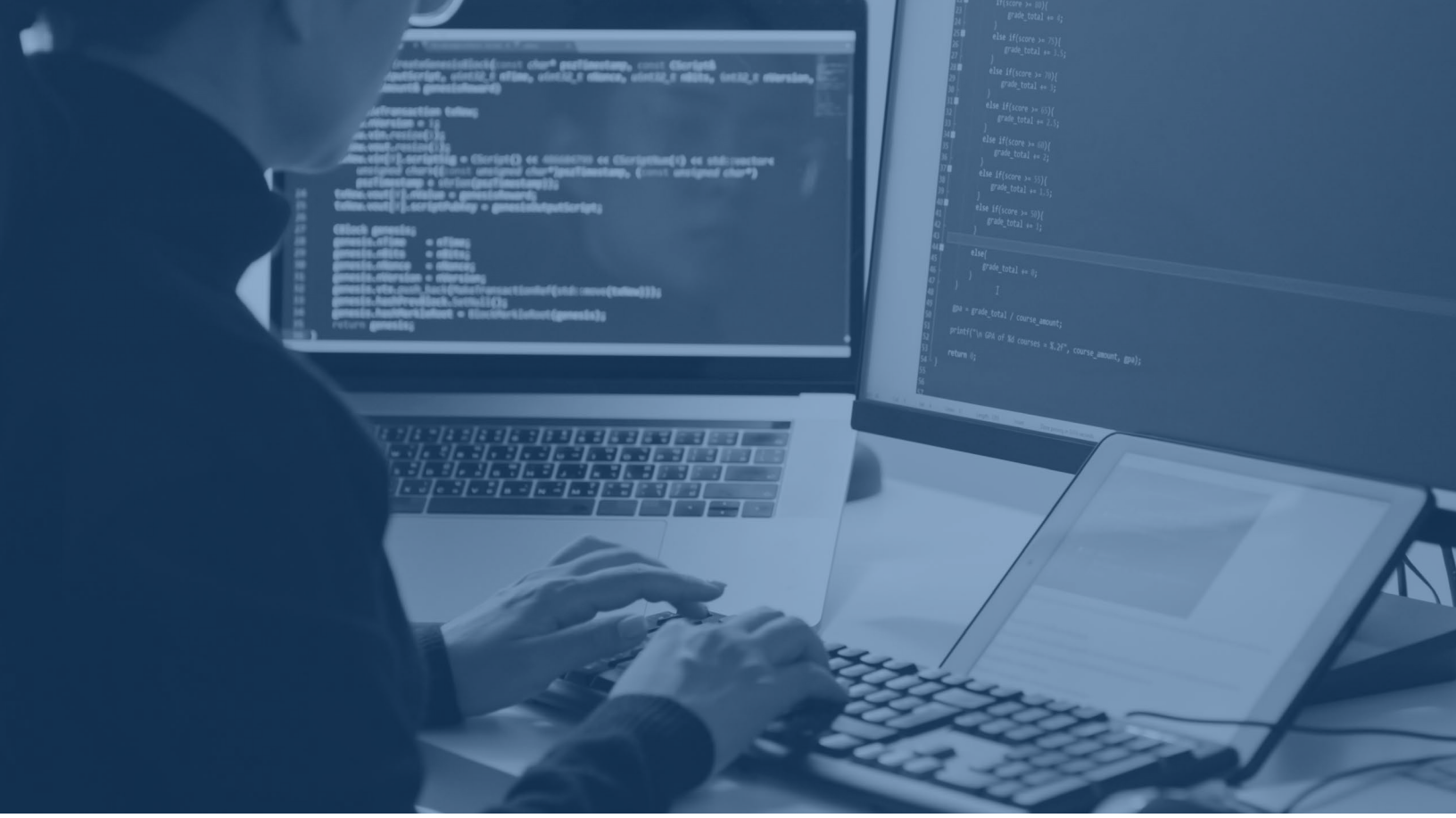
45%

Not one industry stands out as being very effective in protecting sensitive data on lost devices. Only 45% of respondents in all industries say their organizations are highly effective in protecting sensitive data on lost devices.

Figure 22. Percentage of organizations that are highly effective at protecting sensitive data on lost devices

Data represents percentage of respondents who ranked their effectiveness as a 7+ on a scale of 1 = not effective to 10 = highly effective

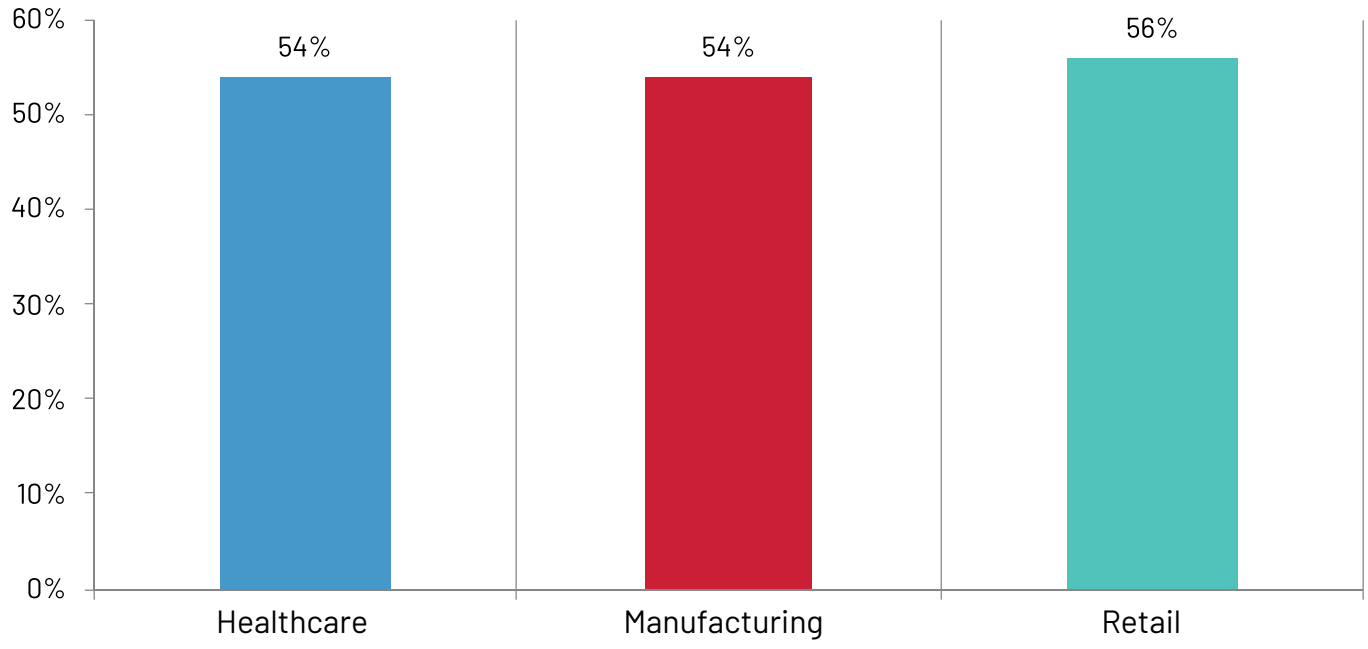




Most respondents in all industries say maintaining access controls on shared devices is very difficult, as shown in Figure 23.

Figure 23. Percentage of organizations that find it very difficult to maintain access controls on shared devices

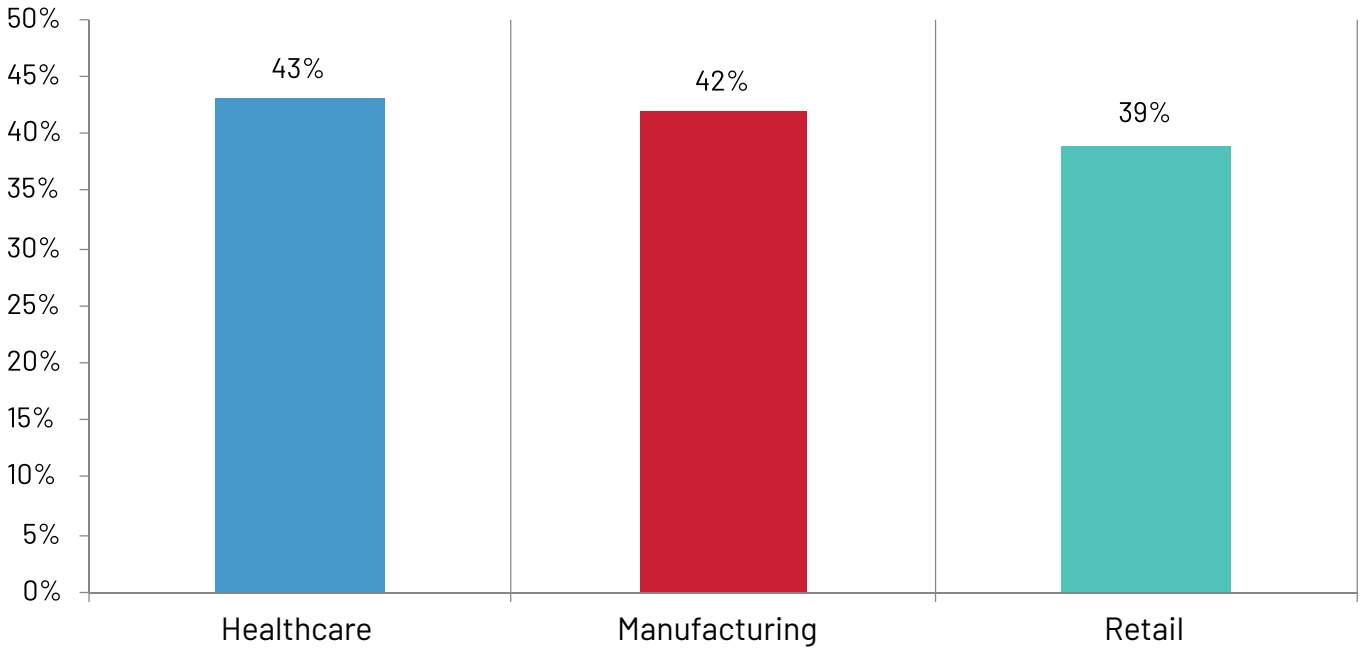
Data represents percentage of respondents who ranked their difficulty as a 7+ on a scale of 1 = not difficult to 10 = very difficult



Healthcare and manufacturing are slightly more effective than retail in controlling access to applications and data on shared mobile devices. As shown in Figure 24, only 39% of respondents in retail say their organizations are very effective in controlling access to shared devices.

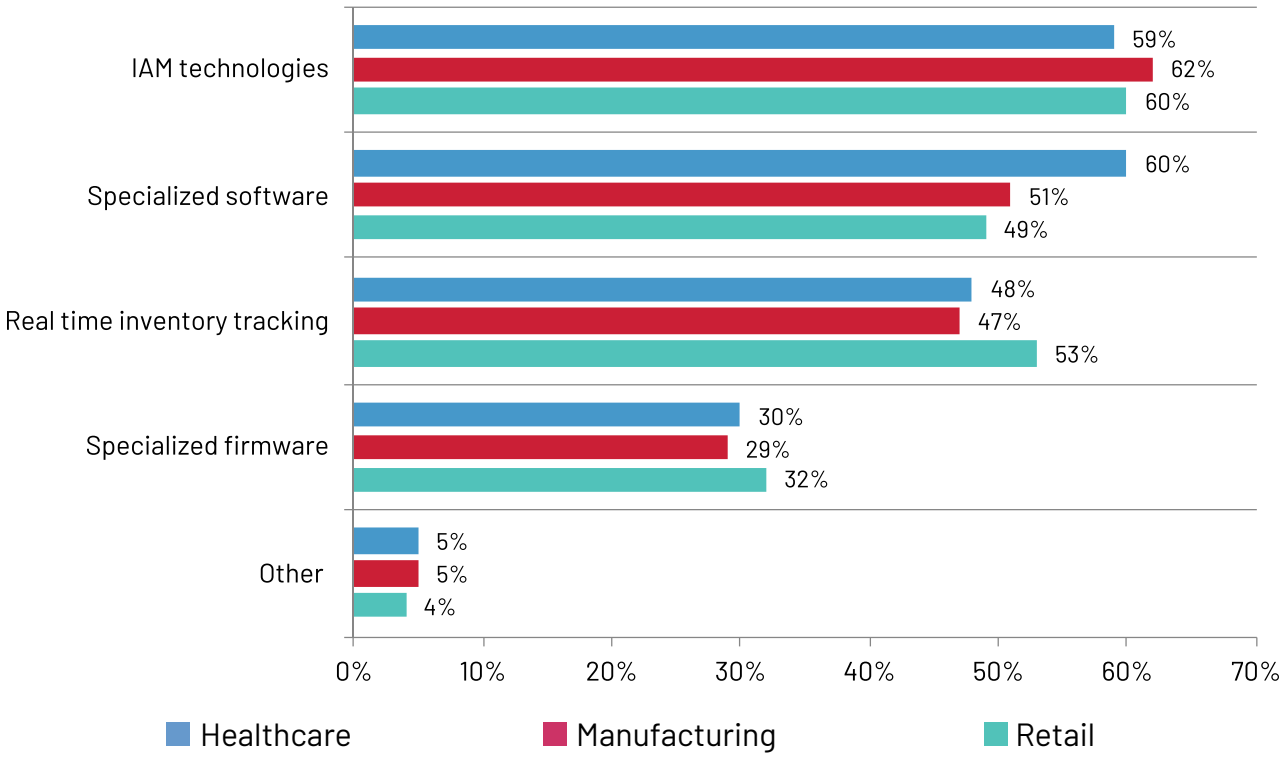
Figure 24. Percentage of organizations that are highly effective at controlling access to applications and data on shared mobile devices

Data represents percentage of respondents who ranked their effectiveness as a 7+ on a scale of 1 = not effective to 10 = highly effective



Most industries are using IAM technologies when tracking devices. As shown in Figure 25, 62% of respondents in manufacturing say their organizations use IAM. Retail is more likely to use real time inventory tracking.

Figure 25. Methods used to support asset tracking as devices move throughout facilities
More than one response permitted



05

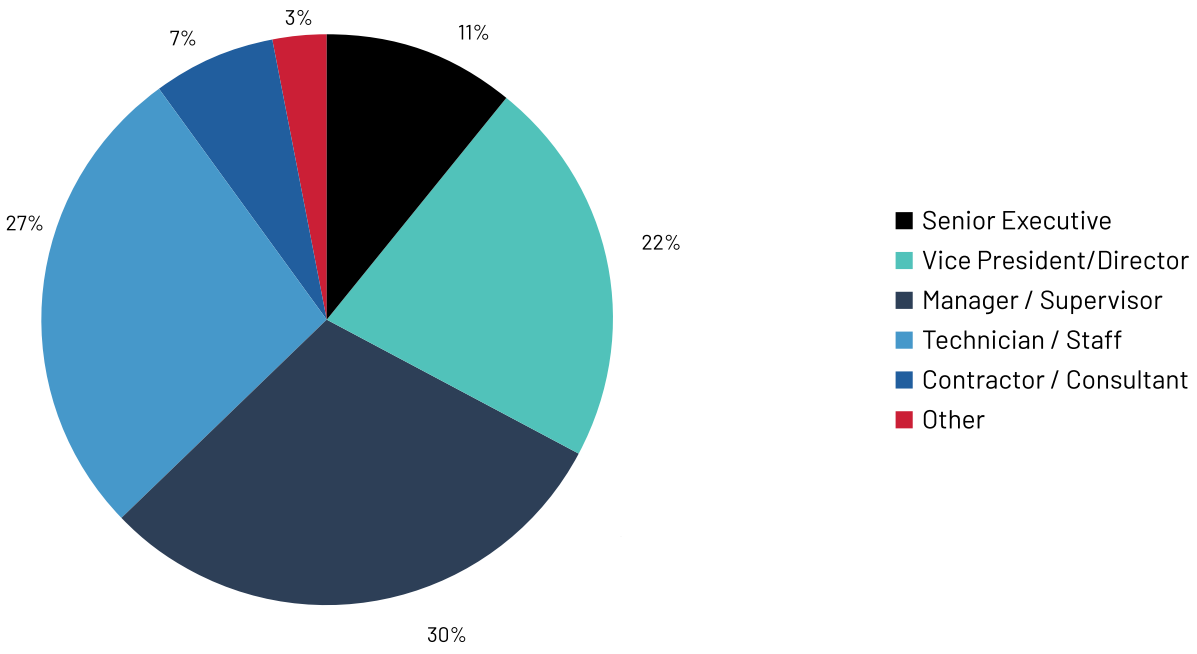
METHODOLOGY

A sampling frame of 45,710 IT and IT security practitioners who are familiar with their organizations' strategy for mobile workflow requirements and security practices were selected as participants to this survey. Table 4 shows 2,001 total returns. Screening and reliability checks required the removal of 206 surveys. Our final sample consisted of 1,795 surveys or a 3.9% response rate.

Table 4. Sample response	Freq	Pct%
Sampling frame	45,710	100.00%
Total returns	2,001	4.40%
Rejected or screened surveys	206	0.50%
Final sample	1,795	3.90%

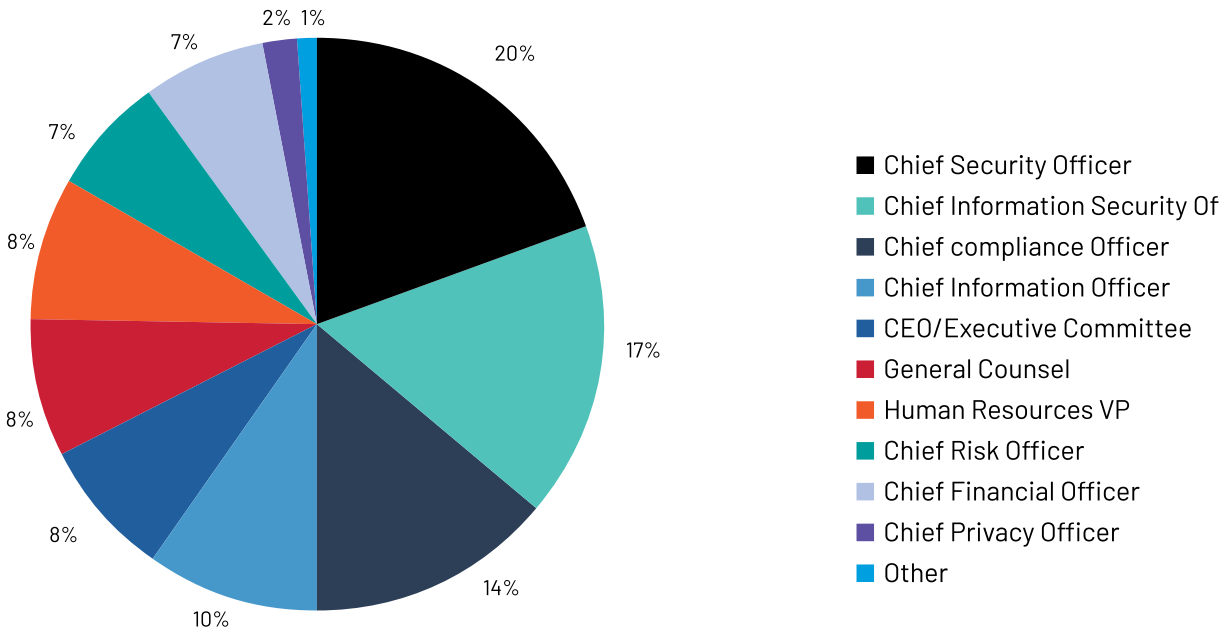
Pie chart 1 reports the respondents' organizational level within participating organizations. By design, more than half (63%) of respondents are at or above the supervisory levels. The largest category at 30% of respondents is manager/supervisor.

Pie chart 1. Current position within the organization



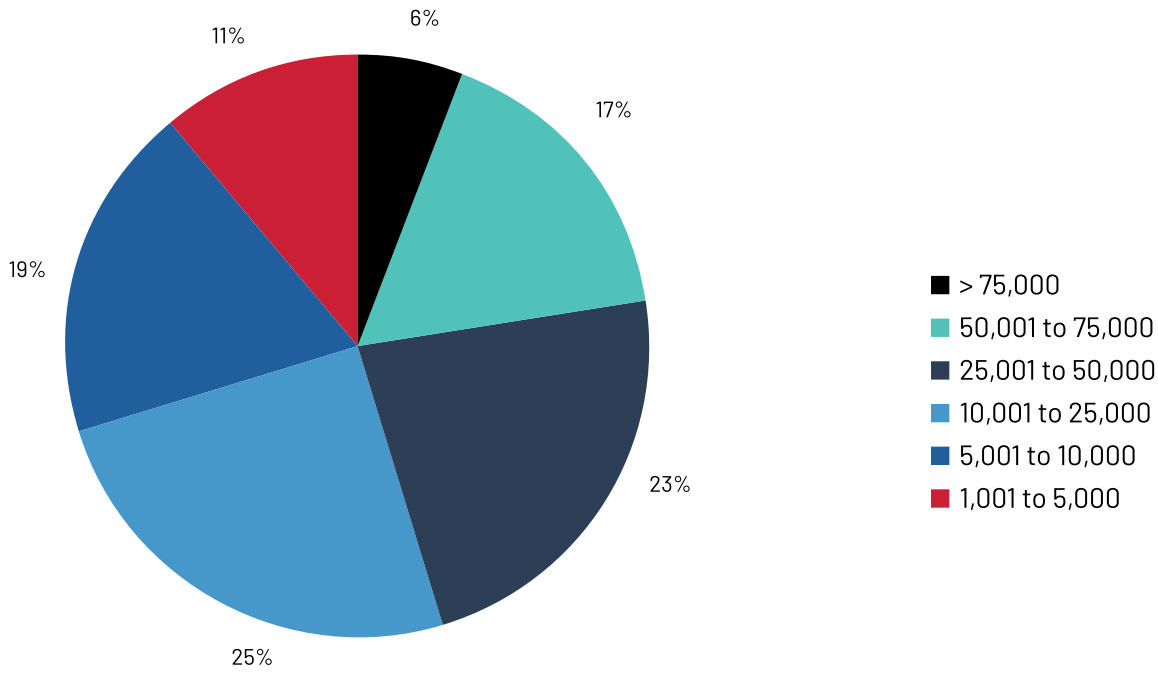
As shown in Pie chart 2, 19% of respondents report to the chief security officer, 17% of respondents report to the chief information security officer, 14% of respondents report to the chief compliance officer, and 10% of respondents report to the chief information officer.

Pie chart 2. Direct reporting channel



As shown in Pie chart 3, 60% of respondents are from organizations with a headcount of more than 10,000 employees.

Pie chart 3. Organizational headcount



06

CAVEATS TO THIS STUDY

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT and IT Security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

07

APPENDIX

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in December 2023.

Survey response	Total
Total sampling frame	45,710
Total survey returns	2,001
Rejected surveys	206
Final sample	1,795
Response rate	3.90%

Part 1. Screening questions

S1. Which types of mobile devices are provided to users? Please select one choice only.	Consolidated
Enterprise-owned 1:1	38%
Enterprise-owned shared	33%
Both enterprise-owned 1:1 and enterprise-owned shared	29%
BYOD (Stop)	0%
Total	100%

S2. How familiar are you with your organization's strategy for mobile workflow requirements and security practices?	Consolidated
Very familiar	34%
Familiar	37%
Somewhat familiar	29%
We don't have a mobile management strategy (stop)	0%
Total	100%

S3. What best describes your position in the organization?	Consolidated
Chief Information Officer (CIO)	9%
Chief Information Security Officer (CISO)	10%
Chief Nurse Informatics Officer/Chief Medical Information Officer (CNIO/CMIO)	8%
Director/VP IT	11%
Director /VP IT security	9%
Manager IT	11%
Manager IT security	11%
Mobile device administrator	10%
Network administrator (wireless and wired)	9%
System administrator	8%
Application analyst	6%
None of the above (Stop)	0%
Total	100%

S4. What is your industry sector?	Consolidated
Healthcare	20%
Manufacturing	24%
Retail	22%
Gaming (on-line and casino)	14%
Transportation & logistics	21%
None of the above (Stop)	0%
Total	100%

Part 2. State of mobile device management

Q1. Who is most responsible for your organization's mobile device management strategy? Please select one choice only.	Consolidated
Chief information officer (CIO)	22%
Chief technology officer (CTO)	22%
Chief operating officer (COO)	9%
Chief financial officer (CFO)	1%
Chief executive officer (CEO)	3%
Chief information security officer (CISO)	10%
LOB senior management	14%
Not one owner/shared responsibility	19%
Other (please specify)	0%
Total	100%

Q2. Approximately, how many mobile devices are in use by employees within your organization today?	Consolidated
Less than 500	6%
501 to 1,000	9%
1,001 to 5,000	12%
5,001 to 10,000	18%
10,001 to 50,000	21%
50,001 to 100,000	20%
More than 100,000	15%
Total	100%
Extrapolated value	39,439

Q3. What percentage of these mobile devices are typically lost annually?	Consolidated
Less than 5%	10%
5%to 10%	24%
11%to 20%	27%
21%to 30%	25%
31%to 40%	11%
Cannot determine	5%
Total	100%
Extrapolated value	16%

Q4. What is the average replacement cost of one mobile device?	Consolidated
$100 to $500	18%
$501 to $750	29%
$751 to $1,250	34%
More than $1,250	19%
Total	100%
Extrapolated value	$864

Q5. Which sensitive and confidential data are accessed by employees' mobile devices? Please select all that apply.	Consolidated
Proprietary company data involving its strategy and goals	51%
Intellectual property such as designs and patents	34%
Confidential financial data	40%
Non-confidential financial data	40%
Customers' personally identifiable data	55%
If applicable, patients' personally identifiable data	34%
Third-party or business partners' personally identifiable data	42%
Employees' personally identifiable data	37%
Credit card or payment information	42%
Access credentials such as user names, encryption keys and pins	44%
Other (please specify)	5%

Q6. On a scale of 1 = not effective to 10 = very effective, how effective is your organization in protecting sensitive or confidential data on lost devices?	Consolidated
1 or 2	7%
3 or 4	20%
5 or 6	28%
7 or 8	24%
9 or 10	22%
Total	100%

Q7. How many frontline workers are in your organization?	Consolidated
Less than 100	9%
100 to 250	14%
251 to 500	14%
501 to 1,000	13%
1,001 to 2,500	28%
2,501 to 5,000	13%
5,001 to 10,000	6%
More than 10,000	3%
Total	100%
Extrapolated value	1,991

Q8. Are enterprise-owned devices shared in your organization?	Consolidated
Yes	62%
No (please skip to Q14)	38%
Total	100%

Q9. On a scale from 1 = not difficult to 10 = very difficult, how difficult is it to maintain access controls on shared devices?	Consolidated
1 or 2	7%
3 or 4	9%
5 or 6	24%
7 or 8	32%
9 or 10	29%
Total	100%

Q10. On a scale from 1 = not difficult to 10 = very difficult, how difficult is it to audit usage information on shared devices?	Consolidated
1 or 2	9%
3 or 4	10%
5 or 6	21%
7 or 8	32%
9 or 10	28%
Total	100%

Q11. On a scale from 1 = not easy to 10 = very easy, how easy is it for your users to access applications and data on shared mobile devices?	Consolidated
1 or 2	14%
3 or 4	25%
5 or 6	31%
7 or 8	19%
9 or 10	12%
Total	100%

Q12. On a scale from 1 = not effective to 10 = highly effective, how effective is your organization in controlling access to applications and data on shared mobile devices?	Consolidated
1 or 2	9%
3 or 4	25%
5 or 6	25%
7 or 8	23%
9 or 10	19%
Total	100%

Q13. On a scale from 1 = not satisfied to 10 = very satisfied, how satisfied are your shared mobile device users with their experience accessing applications and data?	Consolidated
1 or 2	9%
3 or 4	17%
5 or 6	32%
7 or 8	22%
9 or 10	20%
Total	100%

Q14. Is your organization's mobile device program or strategy currently able to do any of the following? Please select all that apply.	Consolidated
Enable secure access to mobile devices without the use of shared pins	44%
Enable quick access to mobile applications without repetitive, manual authentication	40%
Protect data and privacy by locking down devices between each use	40%
Maintain control over who has access to what devices and when	51%
De-personalize mobile devices after use with minimal time and effort	32%
Secure devices and access to sensitive and confidential data	28%
Automate and trigger mobile device management (MDM) workflows on deployed devices via USB	28%
None of the above	27%

Q15. Does your organization's mobile device program or strategy include any of the following requirements? Please select all that apply.	Consolidated
Complete visibility into fleet status beyond what the MDM can deliver	44%
Automation to amplify what a few key IT staff can manage at scale	44%
Deliver a consistent end user experience across any device at any time	37%
Save time with automated authentication	30%
Increase security by replacing app-level pins and shared passcodes	46%
Create an auditable trail of user access as devices change hands	40%
None of the above	24%

Part 3. Mobile device security practices and financial consequences of a data breach

Q16. How many staff are dedicated to the security and management of mobile devices?	Consolidated
One	22%
2 to 3	28%
4 to 5	24%
6 to 10	17%
More than 10	9%
Total	100%
Extrapolated value	4

Q17. What measures does your organization take to manage data accessible on mobile devices? Please check all that apply.	Consolidated
Application wrapping	30%
Containerization	39%
Password enforcement	51%
Remote lock/wipe	45%
Mobile device management (MDM)	37%
Access controls (complex passwords, multifactor authentication, etc.)	52%
Application blacklist/whitelist	47%
Manual policies, audits and SOPs	65%

Q18. What measures does your organization take to secure data accessible on enterprise-owned mobile devices? Please check all that apply.	Consolidated
Anti-malware	51%
Jailbreak/root detection	45%
Device encryption	51%
Securing data in transit	44%
Securing vulnerable apps	47%
Risky app protection	37%
Sideloaded app detection	31%

Q19. In the past year, do you believe your organization has had a data breach due to inappropriate access of an employees' mobile device and its sensitive and confidential information?	Consolidated
Yes	54%
No (please skip to Q21)	40%
Unsure (please skip to Q21)	6%
Total	100%

Q20a. If one or more, please estimate the cost to detect, contain and remediate the most expensive data breach caused by inappropriate access of an employees' mobile device and its sensitive and confidential information?	Consolidated
Zero	2%
Less than $10,000	5%
$10,001 to $100,000	13%
$100,001 to $250,000	15%
$250,001 to $500,000	22%
$500,001 to $1,000,000	20%
$1,000,001 to $5,000,000	12%
$5,000,001 to $10,000,000	8%
$10,000,001 to $25,000,000	3%
More than $25,000,000	2%
Total	100%
Extrapolated value	$2,188,350

Q20b. What percentage of the above estimated cost is based on the value of the data or device compromised?	Consolidated
None	2%
Less than 5%	7%
5%to 10%	23%
11%to 25%	33%
26%to 50%	20%
More than 50%	15%
Total	100%
Extrapolated value	23%

Q20c. What percentage of the above estimated cost of the data breach was due to non-compliance or regulatory violations?	Consolidated
None	2%
Less than 5%	8%
5%to 10%	20%
11%to 25%	27%
26%to 50%	30%
More than 50%	15%
Total	100%
Extrapolated value	25%

Q20d. What percentage of the above cost was due to loss of reputation and customer goodwill?	Consolidated
None	4%
Less than 5%	8%
5%to 10%	16%
11%to 25%	29%
26%to 50%	31%
More than 50%	13%
Total	100%
Extrapolated value	25%

Part 4. Quantifying the challenges associated with device loss

Q21. Which roles are financially responsible for replacing lost mobile devices? Please check all that apply.	Consolidated
Chief Information Officer (CIO)	9%
Chief Information Security Officer (CISO)	12%
Director/VP IT	14%
Director /VP IT security	12%
Manager IT	18%
Manager IT security	17%
Lines of business	9%
Shared responsibility	9%
Total	100%

Q22. What methods does your organization use to support asset tracking as devices move throughout the facilities?	Consolidated
Specialized software	56%
Specialized firmware	30%
Real time inventory tracking	52%
IAM technologies	61%
Other (please specify)	4%

Q23a. IT help desk support	Consolidated
Less than $1,000	7%
$1,000 to $5,000	12%
$5,001 to $10,000	14%
$10,001 to $50,000	23%
$50,001 to $100,000	21%
$100,001 to $500,000	15%
$500,001 to $1,000,000	8%
More than $1,000,000	2%
Total	100%
Extrapolated value	$140,000

Q23b. IT security support (including investigation and forensics)	Consolidated
Less than $1,000	1%
$1,000 to $5,000	2%
$5,001 to $10,000	2%
$10,001 to $50,000	2%
$50,001 to $100,000	5%
$100,001 to $500,000	11%
$500,001 to $1,000,000	36%
More than $1,000,000	41%
Total	100%
Extrapolated value	$716,411

Q23c. Diminished productivity or idle time	Consolidated
Less than $1,000	1%
$1,000 to $5,000	1%
$5,001 to $10,000	3%
$10,001 to $50,000	4%
$50,001 to $100,000	10%
$100,001 to $500,000	15%
$500,001 to $1,000,000	25%
More than $1,000,000	43%
Total	100%
Extrapolated value	$668,249

Q24. Approximately, how many hours each week is spent finding lost devices? Please estimate the aggregate hours of the IT team and frontline workers?	Consolidated
Less than 5	7%
5 to 10	12%
11 to 25	17%
26 to 50	21%
51 to 100	20%
101 to 250	15%
More than 250	9%
Total	100%
Extrapolated value	78

Q25. Approximately, how many hours annually is spent replacing lost devices? Please estimate the aggregate hours of the IT and mobile teams.	Consolidated
Less than 50	14%
50 to 100	22%
101 to 200	26%
201 to 400	22%
401 to 500	10%
More than 500	6%
Total	100%
Extrapolated value	203

Q26. Approximately, how many hours each week are spent managing, maintaining, tracking and monitoring mobile devices? Please estimate the aggregate hours of the IT and mobile teams.	Consolidated
Less than 5	2%
5 to 10	7%
11 to 25	14%
26 to 50	20%
51 to 100	19%
101 to 250	18%
More than 250	21%
Total	100%
Extrapolated value	112

Q27. What best describes the process for maintaining and managing mobile devices? Please select one choice only.	Consolidated
Fully manual	21%
Partially automated	34%
Fully automated	45%
Total	100%

Q28. Does the process have to take place on-site?	Consolidated
Yes, all the time	32%
Yes, part of the time	35%
Can be done remotely (please skip to Q30)	34%
Total	100%

Q29. On a scale of 1 = no impact to 10 = extreme impact, if the maintaining and managing of mobile devices cannot be done remotely, what is the impact on users' productivity?	Consolidated
1 or 2	12%
3 or 4	23%
5 or 6	13%
7 or 8	27%
9 or 10	25%
Total	100%

Q30. Approximately, how much unplanned downtime occurs each week due to un-useable mobile devices? Please estimate the aggregate hours of users.	Consolidated
Less than 50	7%
50 to 100	9%
101 to 250	14%
251 to 500	23%
501 to 1,000	25%
1.001 to 2,500	14%
2,501 to 5,000	6%
More than 5,000	2%
Total	100%
Extrapolated value	872

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	11%
Vice President/Director	22%
Manager/ Supervisor	30%
Technician/ Staff	27%
Contractor/ Consultant	7%
Other	3%
Total	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	Consolidated
CEO/Executive Committee	8%
Chief Financial Officer	7%
General Counsel	8%
Chief Information Officer	10%
Chief compliance Officer	14%
Human Resources VP	8%
Chief Security Officer	20%
Chief Information Security Officer	17%
Chief Privacy Officer	2%
Chief Risk Officer	7%
Other	1%
Total	100%

D3. What is the worldwide headcount of your organization?	Consolidated
1,001 to 5,000	11%
5,001 to 10,000	19%
10,001 to 25,000	25%
25,001 to 50,000	23%
50,001 to 75,000	17%
> 75,000	6%
Total	100%

Imprivata is the digital identity company for life- and mission-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enable organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

For more information, please contact us at +1 781 674 2700
or visit us online at **www.imprivata.com**