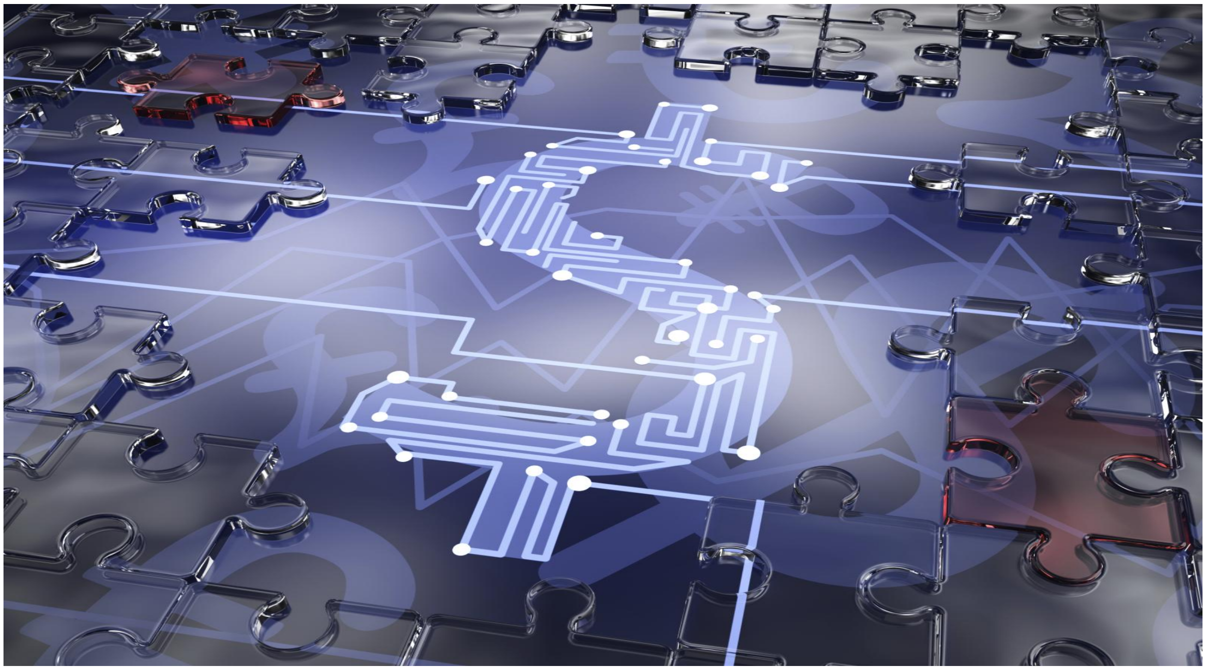


The Costs of Authentication Failure and Negligence

Sponsored by Nok Nok Labs
Independently conducted by Ponemon Institute LLC
Publication Date: March 2022

The Costs of Authentication Failure and Negligence

Ponemon Institute, March 2022

Part 1. Introduction

Authentication failures--defined as a weakness in an organization's authentication processes resulting in an inability to verify user identity not only pose great risk resulting in the theft of credentials but are costly. According to the research, organizations are spending an average of approximately $3 million on activities relating to authentication failures annually.

Participants in this research also estimate that the maximum loss as a result of one authentication failure can range from $39 million to $42 million and the average maximum loss as a result of a material business disruption caused by an authentication failure can range from an average of $34 million to $40 million. Reasons that authentication failures can be costly, as confirmed in this research, is the downtime to resolve authentication failure, disruption of business processes, loss of customers and the negative impact on third party and business relationships.

Sponsored by Nok Nok, Ponemon Institute surveyed 1,007 IT staff (360), IT security leaders (339) and non-IT security leader or lines of business leaders (LoBs) (308). All respondents are familiar with authentication processes in their organizations and have some level of responsibility for the security of their organization's authentication processes.

A key takeaway from this research is the gap between IT security and LoBs in the seriousness of authentication risks facing their organizations. In this report, we present these differences and discuss how they may be affecting the security posture of organizations represented in this research.

In the context of this research, credential theft involves stealing the user's exact password rather than randomly guessing it. The focus of this crime can be to make fraudulent purchases, make fraudulent financial transactions and steal confidential information.

The authentication failures perception gap in organizations

Based on the findings, the following are the most significant gaps in understanding the state of authentication processes in organizations among the IT security staff, IT security leaders and lines of business leaders. These differences can be a barrier to achieving a secure and holistic response and strategy to addressing the risks and cost of authentication failures. According to the research, most organizations do not have an enterprise-wide strategy for reducing the risk of authentication failures.

- Lines of business leaders are not likely to recognize the difficulty in knowing the "real" employees, customers and/or users from criminal imposters who are using stolen credentials. Sixty-six percent of IT security staff respondents say it is very difficult or difficult. Less than half (48 percent) of lines of business respondents say it is very difficult or difficult.

- Authentication processes are out of control, according to IT security respondents. Only 32 percent of IT security respondents and 44 percent of IT security leaders say their organizations have a high level of control over their authentication processes. However, 67 percent of lines of business respondents are confident in their organizations' controls.

- IT security staff respondents detect more authentication failures. IT security staff estimates a per-user average of 28 authentication failures occur in a month vs. lines of business leaders who estimate an average of 19 authentication failures occur per user monthly.

- IT security staff says on average there are significantly more undetected authentication failures than the IT security and lines of business say there are. IT security staff respondents say on average 45 percent of authentication failures go undetected—almost twice as much as reported by lines of business leaders.

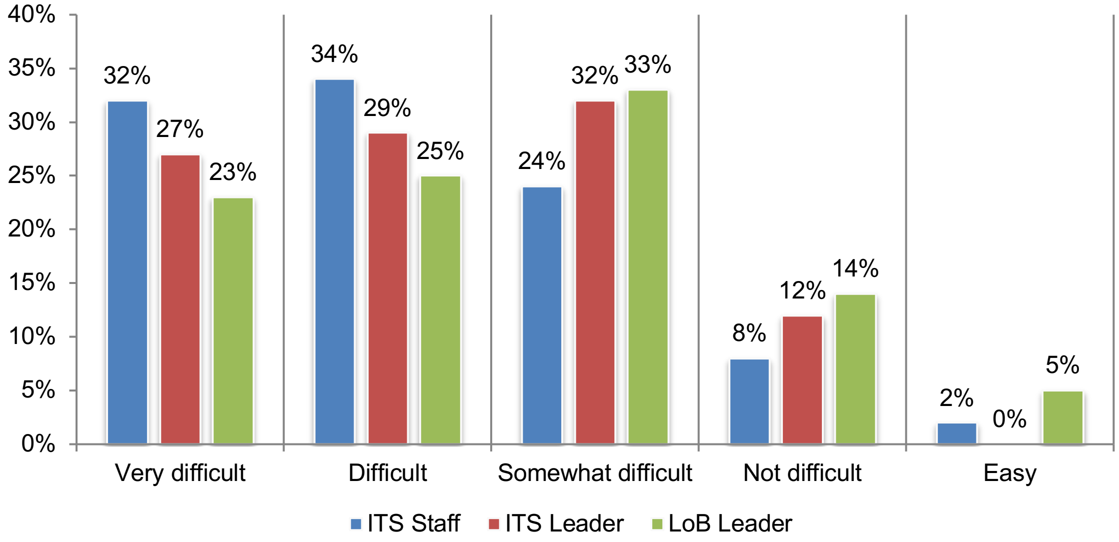
- IT security staff report a higher percentage of the volume and frequency of authentication failures. Seventy-one percent of IT security respondents vs. 55 percent of lines of business leader respondents say authentication failures have significantly increased or increased. Fifty-nine percent of respondents say the severity of failures have increased vs. 51 percent of business leader respondents.

- IT security staff respondents are not as confident that the risk of authentication failures can be reduced. Today, 66 percent of lines of business respondents say their organizations are very prepared or highly prepared to reduce the risk of authentication failures and this will increase to 82 percent of these respondents who are very prepared or highly prepared. Only 40 percent of IT security staff respondents say their organizations are very prepared or highly prepared and in two years 53 percent say their organization will be very or highly prepared.

- Only 28 percent of IT security staff respondents believe an annual budget of $2.5 million allocated to staff and technologies to prevent detect, contain and resolve authentication failures is sufficient. Whereas, 45 percent of lines of business leaders say the budget is sufficient. Only 45 percent of IT security staff say their organizations' leaders recognize the need to invest in automation, AI and orchestration as part of its efforts to prevent authentication failures.

The risk of credential theft is high and only 30 percent of respondents say their companies have good visibility into credential theft attacks. Figure 1 presents respondents' opinions about the difficulty in knowing the "real" employees, customers and/or users from criminal imposters who are using stolen credentials. As shown, 66 percent of IT security staff respondents say it is very difficult (32 percent) or difficult (34 percent). In contrast, less than half (48 percent) of LoB respondents say it is very difficult or difficult.

Figure 1. How difficult is to know the "real" employees, customers and/or users from criminal imposters who are using stolen credentials?



Part 2. Key findings

In this section, we provide an analysis of the research. The complete findings are presented in the Appendix of this report. We have organized the report according to the following topics.

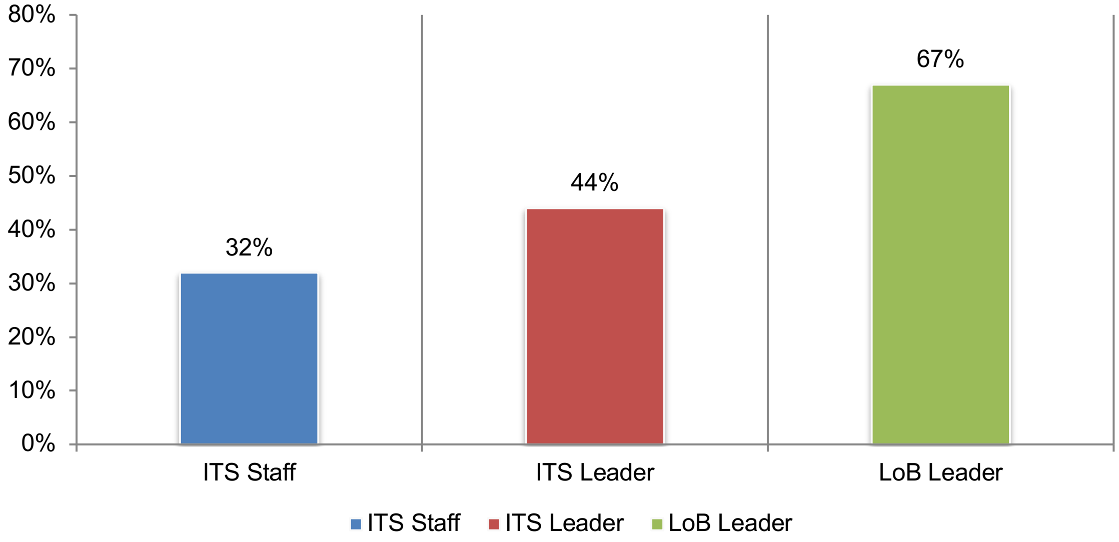
- The risk of authentication failures
- The struggle to prevent authentication failures
- Digital transformation and authentication failures
- The cost of authentication failure

The risk of authentication failures

Authentication processes are out of control, according to IT security respondents. There is a significant gap between respondents in security and the lines of business in understanding the amount of control organizations have over their authentication processes. Respondents were asked to rate how much control companies have over their authentication processes on a scale from 1 = no control to 10 = high level of control.

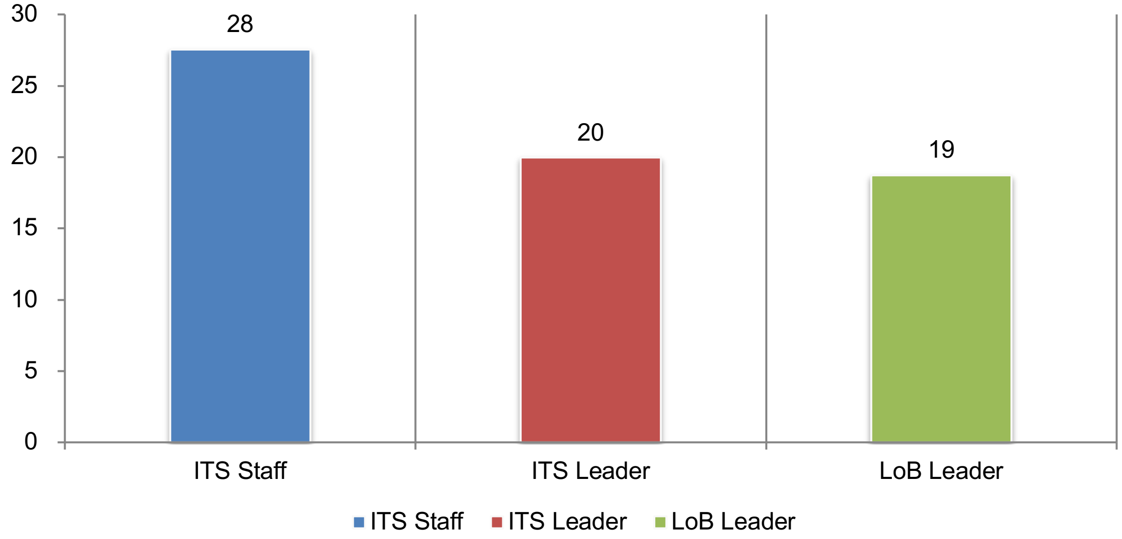
As shown in Figure 2, only 32 percent of IT security respondents and 44 percent of IT security leaders say their organizations have a high level of control over their authentication processes (7+ on the 10-point scale). However, 67 percent of lines of business leaders are confident in their organizations' controls.

Figure 2. How much control does your company have over its authentication processes?
On a scale from 1 = no control to 10= a high level of control, 7+ responses combined



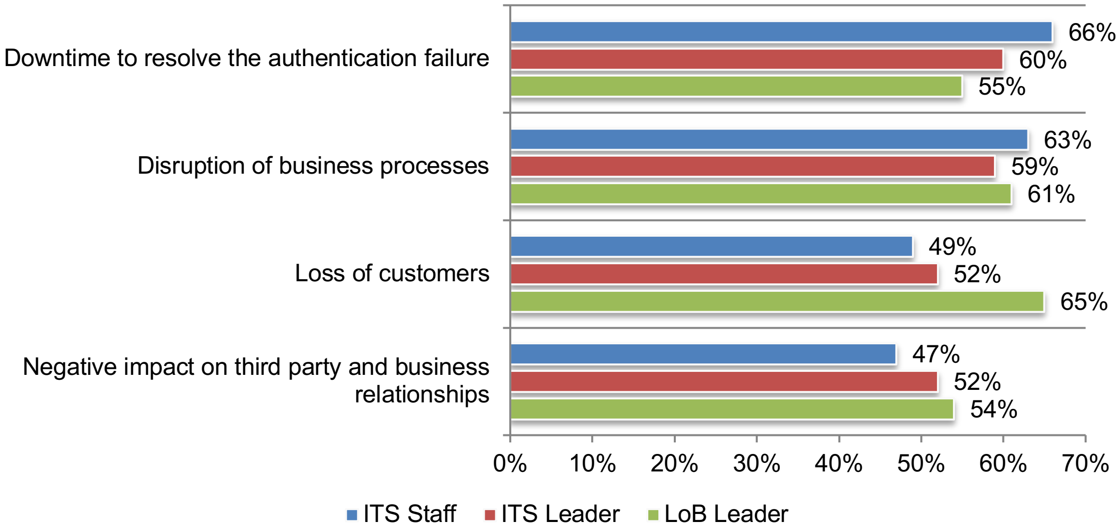
Knowledge about the detection of authentication failures varies among functions. IT security staff respondents say their companies are able to detect an average of 28 authentication failures in a month, as shown in Figure 3. The IT security and lines of business leaders say their companies detect an average of 20 and 19 authentication failures per user monthly, respectively. An average of 12 percent of these authentication failures result in the attacker being able to obtain the credentials of bona fide users.

Figure 3. In an average month, how many authentication failures per user does your company detect?
Extrapolated values presented



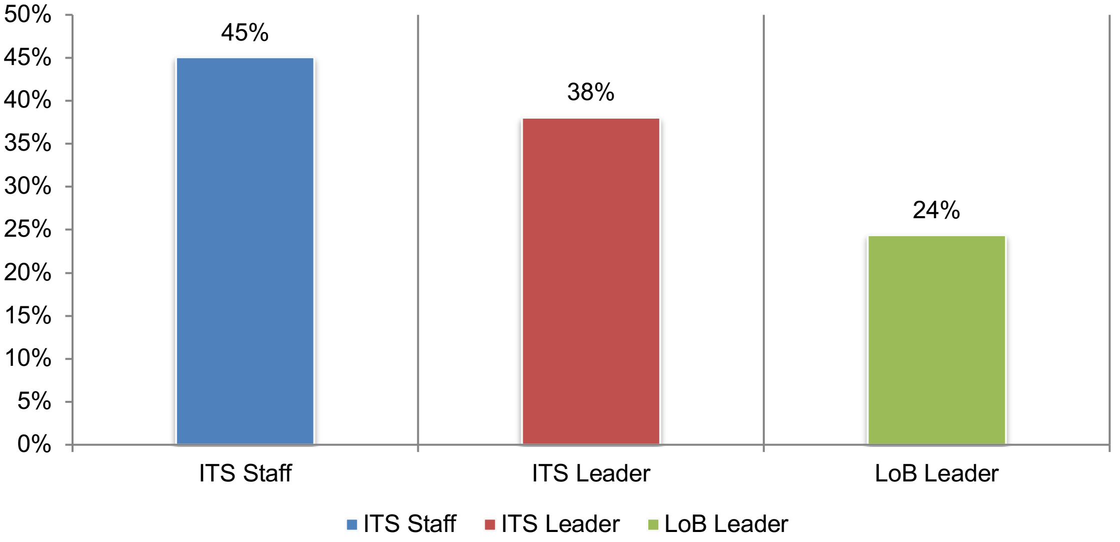
The consequences of authentication failures can be costly. Figure 4 shows the top four results from authentication failures that can affect an organization's finances. The most frequent consequences, according to IT security staff, is the downtime to resolve the authentication failure and disruption of business processes (66 percent and 63 percent of respondents, respectively). According to 65 percent of lines of business leaders, the loss of customers most frequently occurs.

Figure 4. What were the consequences of these authentication failures?
More than one response permitted



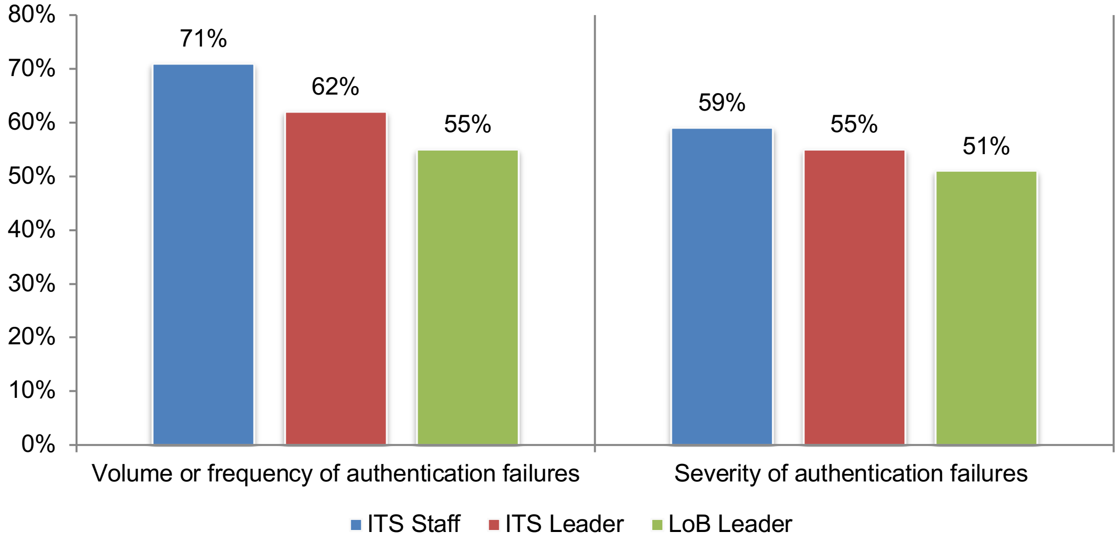
The IT security staff says on average there are significantly more undetected authentication failures than the IT security and lines of business say there are. As shown in Figure 5, IT security staff respondents say on average 45 percent of authentication failures go undetected—almost twice as much as reported by lines of business leaders.

Figure 5. Percentage of undetected authentication failures
Extrapolated values presented



More authentication failures are occurring. According to Figure 6, there is a gap between the understanding of IT security staff respondents and the lines of business leader respondents about the increase in the volume and severity of authentication failures over the past 12 months. Seventy-one percent of IT security staff respondents vs. 55 percent of lines of business leader respondents say authentication failures have significantly increased or increased. Fifty-nine percent of IT security staff respondents say severity has increased vs. 51 percent of lines of business leader respondents.

Figure 6. How has the volume or frequency of authentication failures changed over the past 12 months?
Significantly increased and Increased responses combined

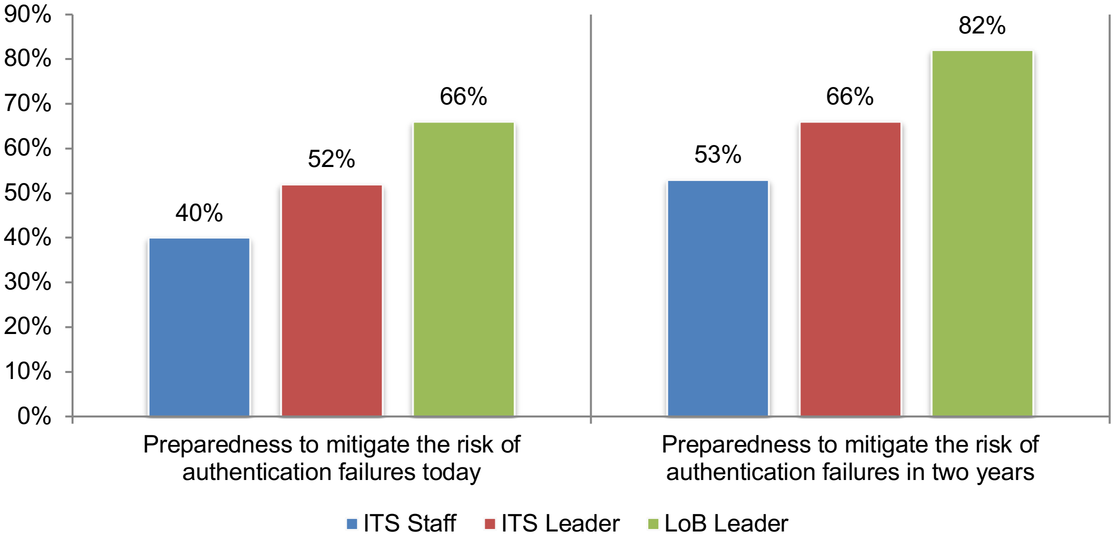


The struggle to prevent authentication failures

Lines of business leaders are more optimistic about the ability to reduce the risk of authentication failures in two years than the IT security staff. Respondents were asked to rate their organizations' preparedness to mitigate the risk of authentication failures today and in two years on a scale from 1 = not prepared to 10 = very prepared.

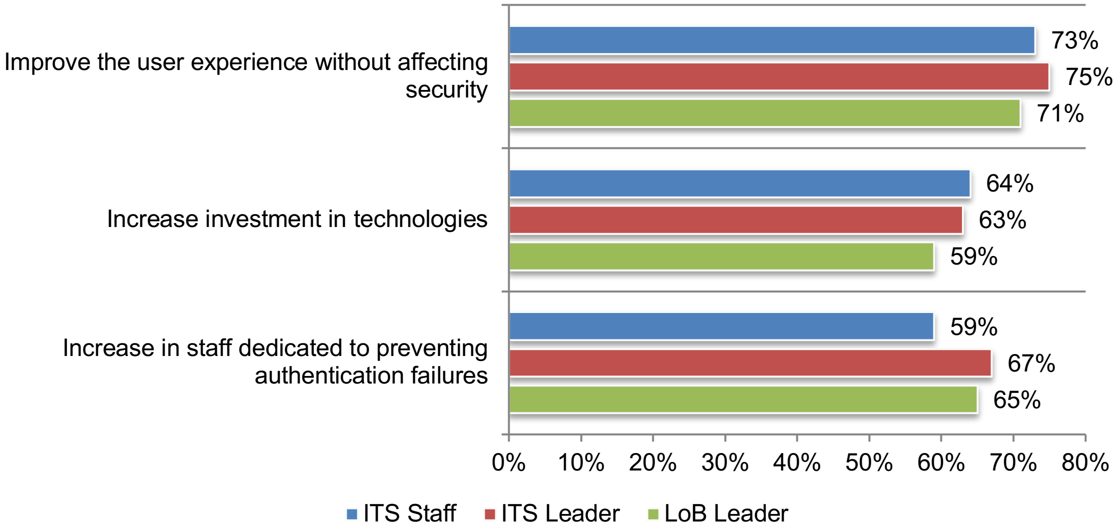
Figure 7 shows the high and very prepared responses (7+ on the 10-point scale). Today, 66 percent of the lines of business leaders rate their preparedness as high or very prepared and in two years 82 percent of these respondents say their organizations will be more prepared. In contrast, 40 percent of IT security staff respondents say preparedness to reduce the risk of authentication failures today as high or very prepared and this increases to 53 percent of IT security staff respondents in two years.

Figure 7. How prepared is your organization to reduce the risk of authentication failures today and in two years?
On a scale from 1 = not prepared to 10 = very prepared, 7+ responses combined



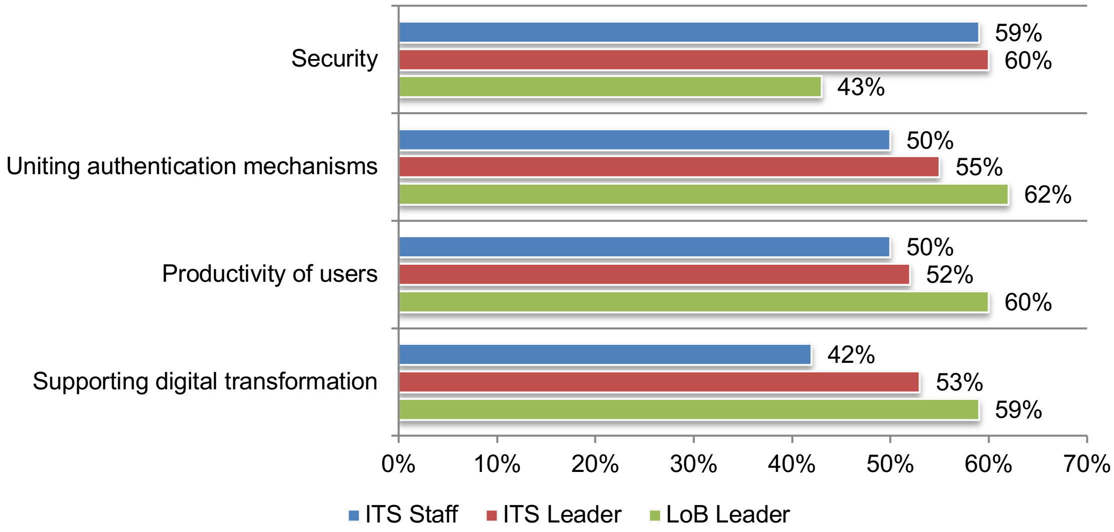
Few organizations have a strategy for reducing authentication failures. Only 33 percent of the IT security staff say their organizations have a strategy in place to reduce authentication failures. Forty-one percent of IT security leaders and 49 percent of LoB leaders say there is a strategy in place. If organizations do have a strategy, all respondents agree that the focus is on improving the user experience without affecting security, as shown in Figure 8. IT security leaders and lines of business leaders are more likely to say the strategy includes an increase in staff dedicated to preventing authentication failures.

Figure 8. If yes, does the strategy include any of the following actions?
More than one response permitted



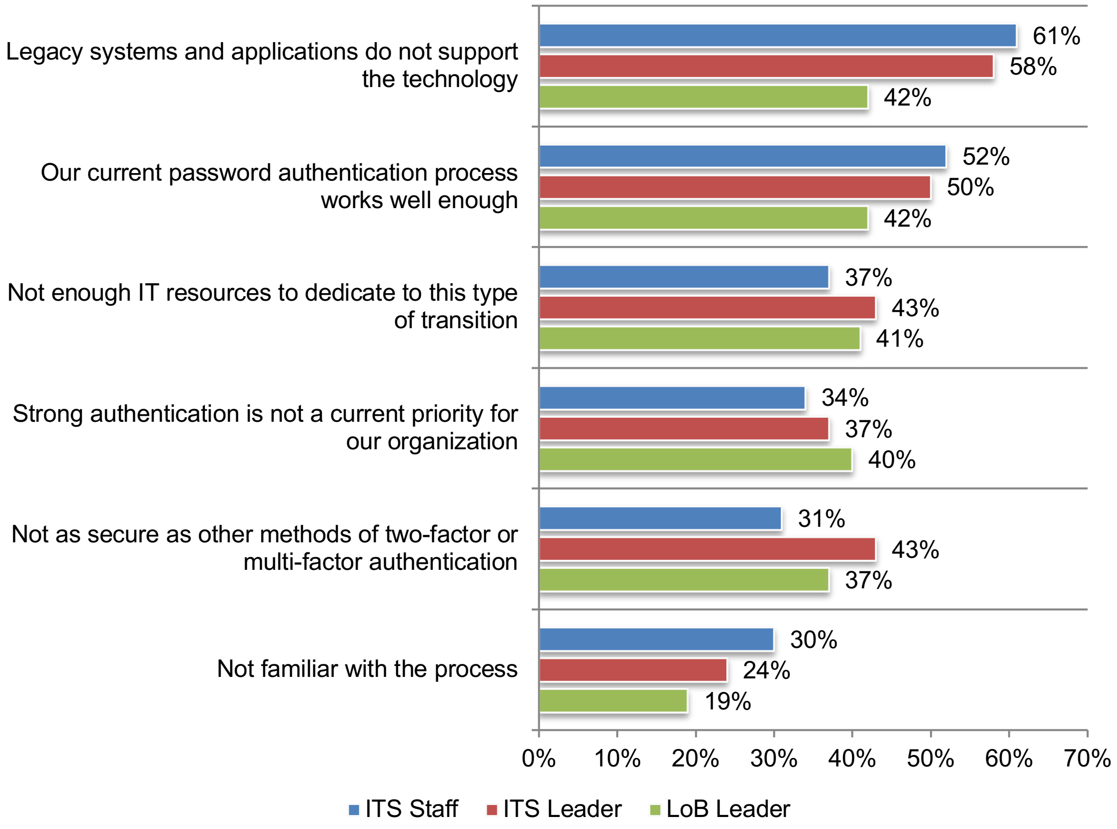
Security is the primary reason to adopt passwordless authentication. Twenty-two percent of respondents have adopted passwordless authentication. The IT security staff respondents and IT security leader respondents are more likely to say their organizations adopted passwordless authentication because of security (59 percent and 60 percent, respectively). Lines of business leaders support it because it unites authentication mechanisms and improves productivity (62 percent and 60 percent of respondents, respectively).

Figure 9. Why did your organization adopt passwordless authentication?
More than one response permitted



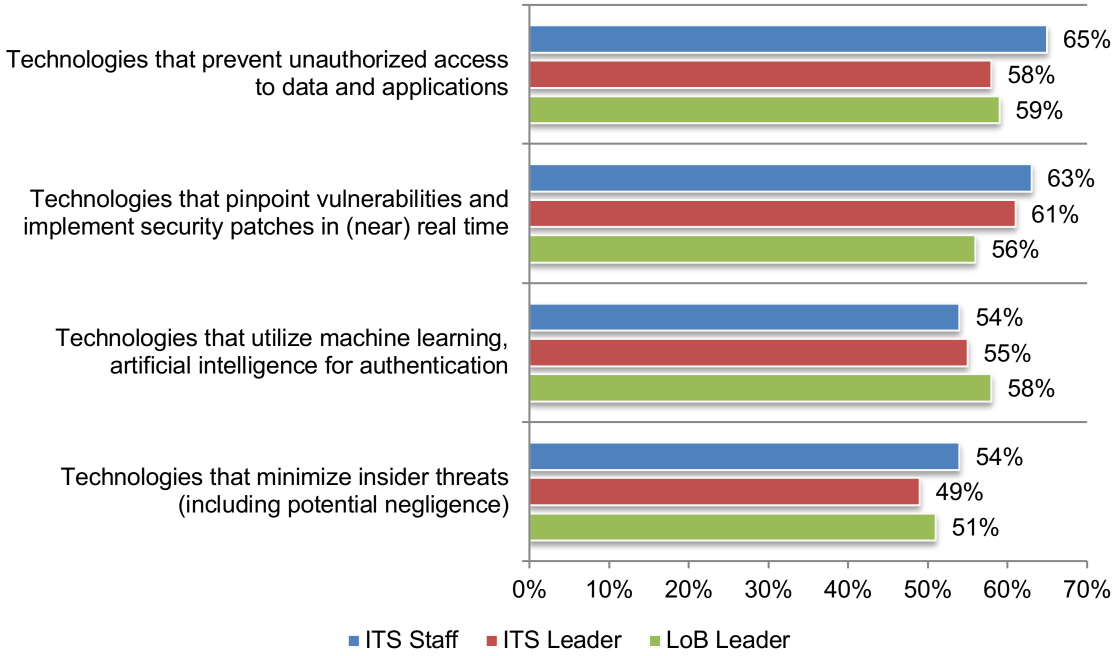
The primary barrier to adopting passwordless authentication is that legacy systems and applications do not support the technology. For those organizations that have not adopted passwordless authentication, IT security staff and IT security leaders agree that it is because legacy systems and applications do not support the technology (61 percent and 58 percent, respectively). They also agree that current password authentication process works well enough according to 52 percent and 50 percent, respectively.

Figure 10. What are barriers to adopting passwordless authentication?
More than one response permitted



Organizations have confidence in technologies that prevent unauthorized access to data and applications. Figure 11 lists technologies that are used to secure authentication processes. IT security staff and IT security leaders have the most confidence in technologies that prevent unauthorized access to data and applications (65 percent and 58 percent, respectively) and technologies that pinpoint vulnerabilities and implement security patches in (near) real time (63 percent and 61 percent, respectively). Lines of business leaders also have the most confidence in technologies that prevent unauthorized access to data and applications (59 percent).

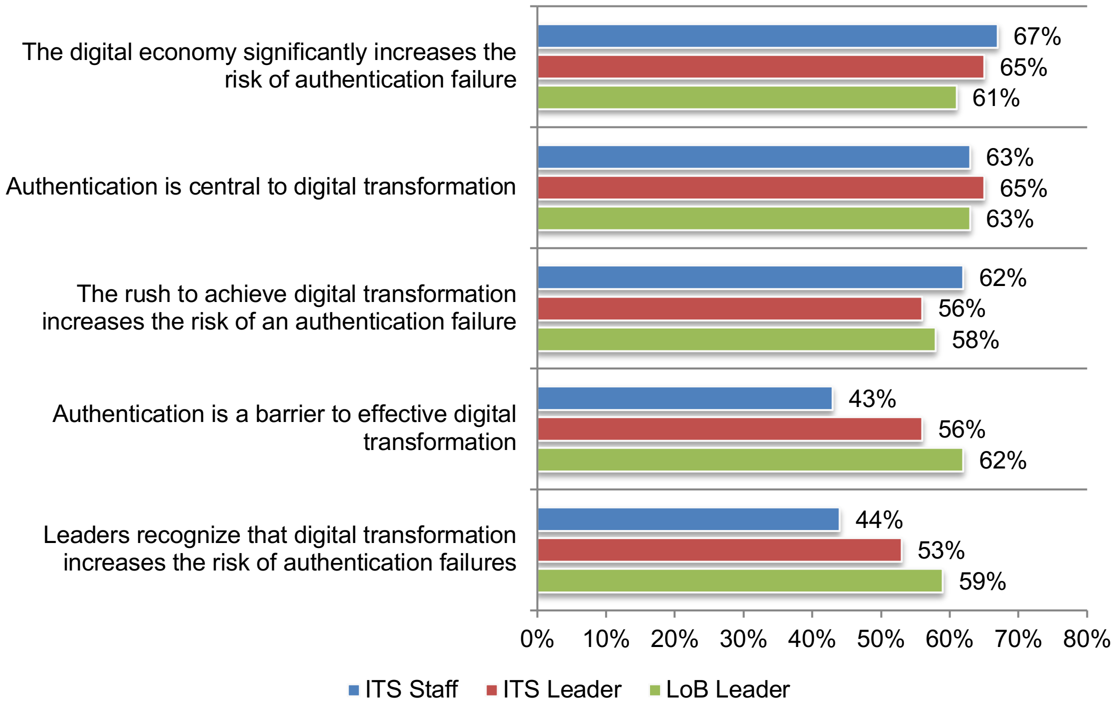
Figure 11. Confidence in technologies that will secure the authentication processes
Very Confident and Confident responses combined



Digital transformation & authentication failures

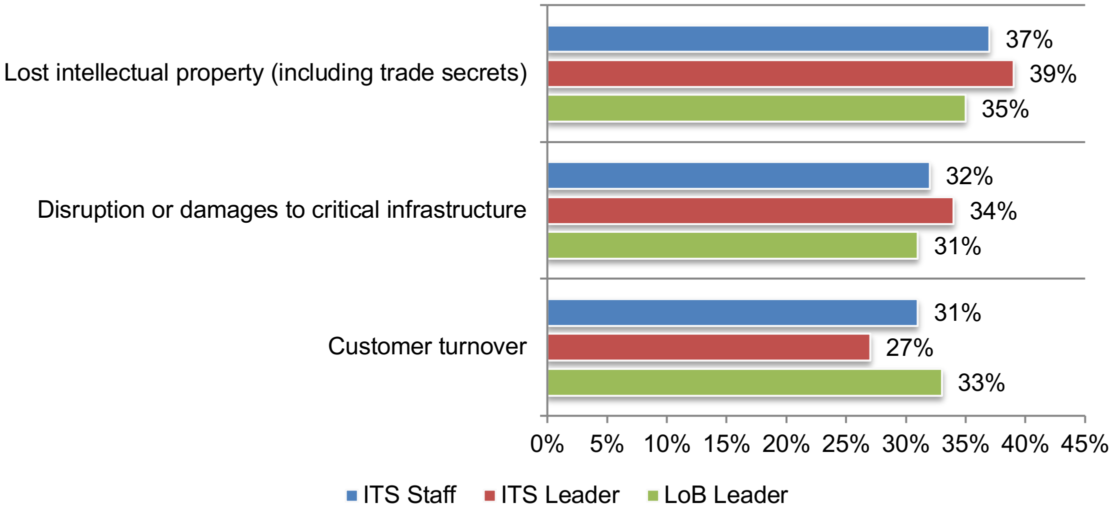
The digital economy increases the risk of authentication failure. As shown in Figure 12, while the digital economy increases the risk of authentication failures, authentication is central to digital transformation, according to IT security and lines of business leaders. Sixty-two percent of lines of business leaders say authentication is a barrier to effective digital transformation. Only 44 percent of IT security staff believes their organization recognizes that digital transformation increases the risk of authentication failures, but 59 percent of lines of business leaders say they do recognize the risk.

Figure 12. Perceptions about digital transformation and authentication failures
Strongly Agree and Agree responses combined



Organizations are more vulnerable to authentication failures caused by insecure digital transformation. Sixty-six percent of respondents say their organizations are much more vulnerable (45 percent) or somewhat more vulnerable (21 percent) to an authentication failure following digital transformation. As discussed previously, respondents recognize that digital transformation increases the risk of authentication failure. As shown in Figure 13, the top three negative consequences are loss of intellectual property, disruption or damages to critical infrastructure and customer turnover.

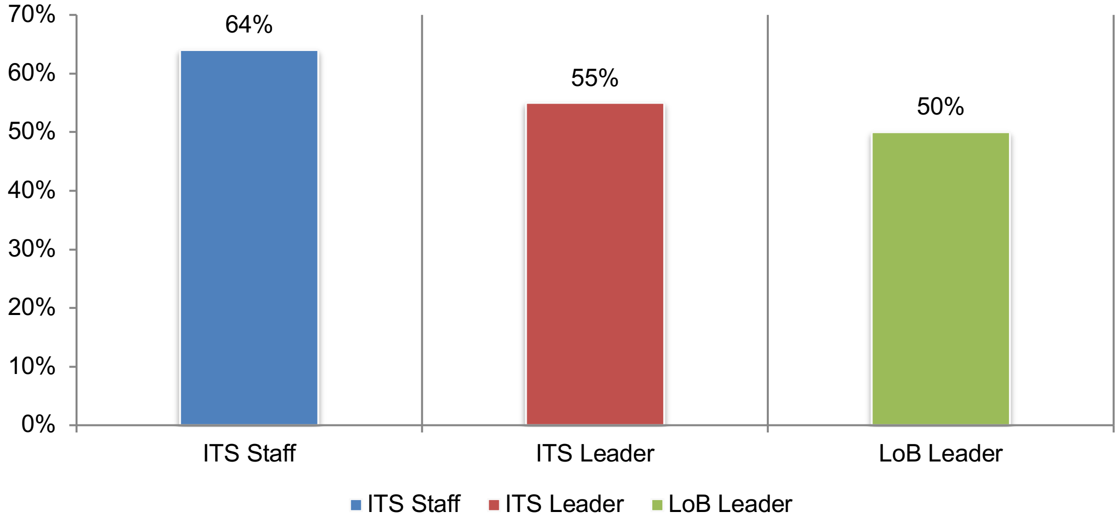
Figure 13. What are the most negative consequences from an authentication failure caused by insecure digital transformation?
Top two responses presented



The cost of authentication failures and what companies are spending to reduce the risk

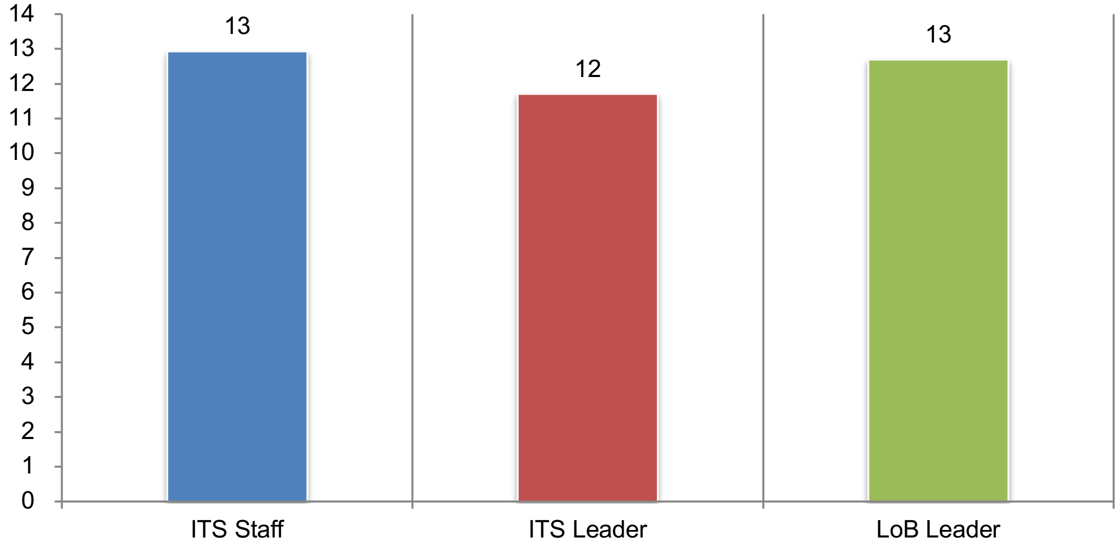
Resolving authentication failures is becoming more costly. According to Figure 14, 64 percent of IT security staff respondents report that the cost to detect, contain and resolve authentication failures has significantly increased or increased. In contrast, 50 percent of lines of business leaders say the cost has increased in the past 12 months.

Figure 14. How has the cost to detect, contain and resolve authentication failures changed over the past 12 months?
Significantly increased and Increased responses combined



On average between 12 and 13 IT security or anti-fraud personnel are involved in the resolution of authentication failure, as shown in Figure 15.

Figure 15. How many IT security or anti-fraud personnel are involved in the detection and containment of authentication failures?
Extrapolated values presented



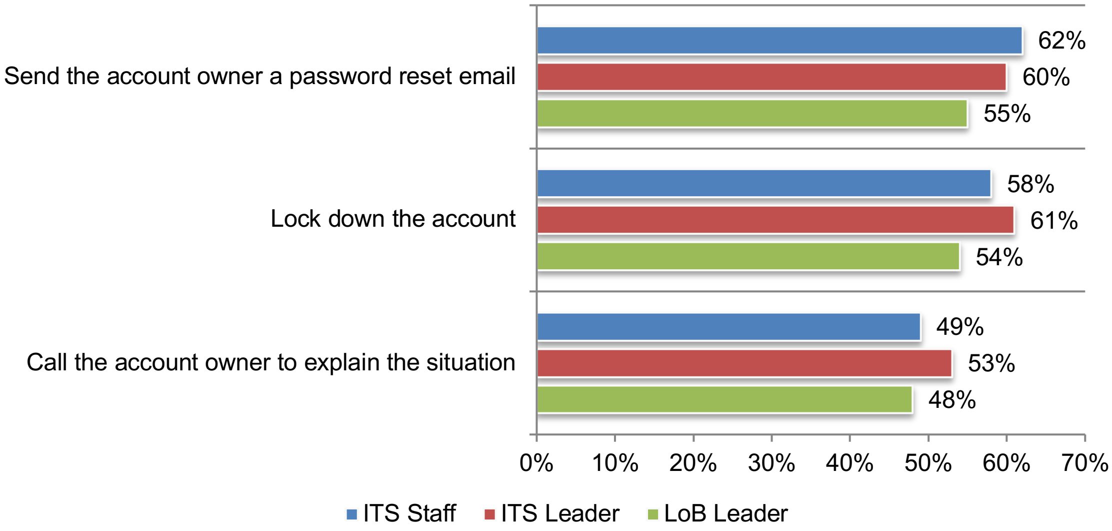
The annual cost of authentication failure activities can average $3 million. Table 1 presents the hours spent each week on authentication failures, according to IT staff, IT security leaders and lines of business leaders. As shown, all respondents have a similar understanding of the time spent on authentication failures.

The total cost is based on an average hourly rate for an IT security practitioner of $63.50. The average weekly cost ranges, as shown, ranges from $61,456 to $63,726. Annually that would be an average of more than $3 million.

Table 1. Hours spent each week on authentication failure activities	ITS Staff	ITS Leader	LoB Leader
Organizing and planning detection and containment of authentication failures	265	276	266
Analyzing and investigating authentication failures	329	332	314
Conducting forensic analysis	194	170	187
Documenting and/or reporting authentication failures	85	78	90
Containing and remediating authentication failures	131	137	112
Total hours	1,004	993	968
Total cost (based on hourly rate of $63.50)	$63,726	$63,061	$61,456

A password reset email is the primary remediation effort made when a compromised account is identified. As discussed above IT security staff respondents say they spend on average 131 hours each week remediating authentication failures. According to Figure 16, 62 percent of IT staff respondents say a password reset email is sent to the account owner. Both IT security staff respondents and IT security leaders say the account is locked down (58 percent and 61 percent, respectively).

Figure 16. What remediation efforts are made when a compromised account is identified?
More than one response permitted



In addition to the cost spent remediating activities each week, respondents on average predict the maximum loss of one authentication failure ranging from $39 million to $42 million. The average maximum loss as a result of a material distribution caused by an authentication failure can range from $34 million to $40 million.

Figure 17. The maximum loss as a result of one authentication failure and a material business disruption
Extrapolated values presented (US$ millions)

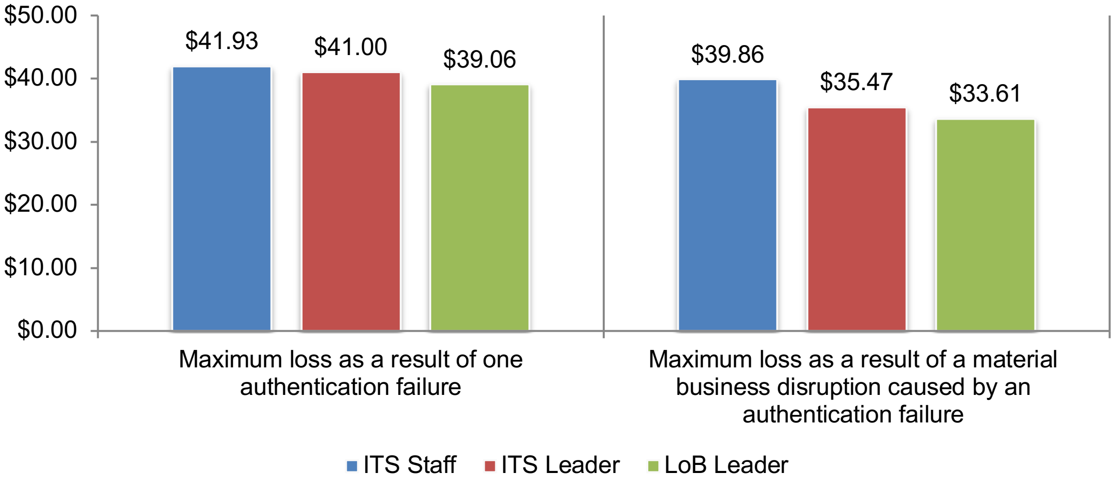
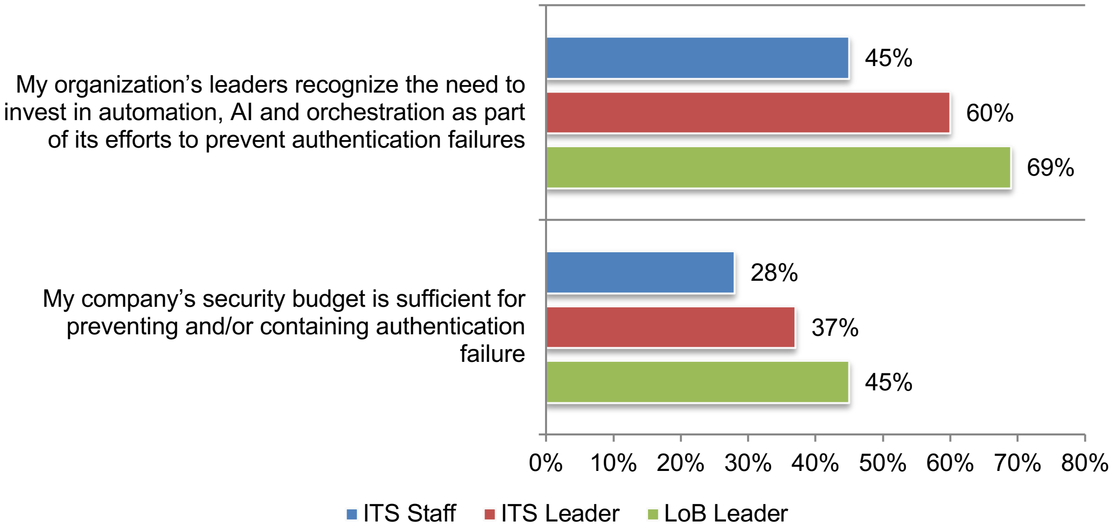


Table 2 presents the average budget for the 2021 IT, IT security and the prevention, detection, containment and resolution of authentication failures. As shown, the average budget for authentication failures ranges from $2.5 million to $3.2 million, which according to the research equals the cost of activities relating to authentication failures (Table 1).

Table 2. Budget Extrapolated values presented	ITS Staff	ITS Leader	LoB Leader
2021 IT budget (US$ millions)	$ 135.7	$ 143.6	$ 153.2
Percentage of the IT budget will be allocated to IT security	16.4%	16.3%	17.3%
IT Security budget (US$ millions)	$ 22.26	$ 23.35	$ 26.42
Percentage of IT security budget allocated to staff and technologies to prevent, detect, contain and resolve authentication failures	11.2%	12.3%	12.0%
Budget allocated to staff and technologies to prevent, detect, contain and resolve authentication failures (US$ millions)	$ 2.50	$ 2.86	$ 3.17

IT security staff do not believe the budget outlined above is sufficient to address the risks of authentication failures. As shown in Figure 18, only 28 percent of the IT security staff say the security budget is sufficient for preventing and/or containing authentication failure and less than half (45 percent) say their organizations' leaders recognize the need to invest in automation, AI and orchestration as part of its efforts to prevent authentication failures.

Figure 18. Perceptions about the budget for minimizing the risk of authentication failures
Strongly agree and Agree responses combined



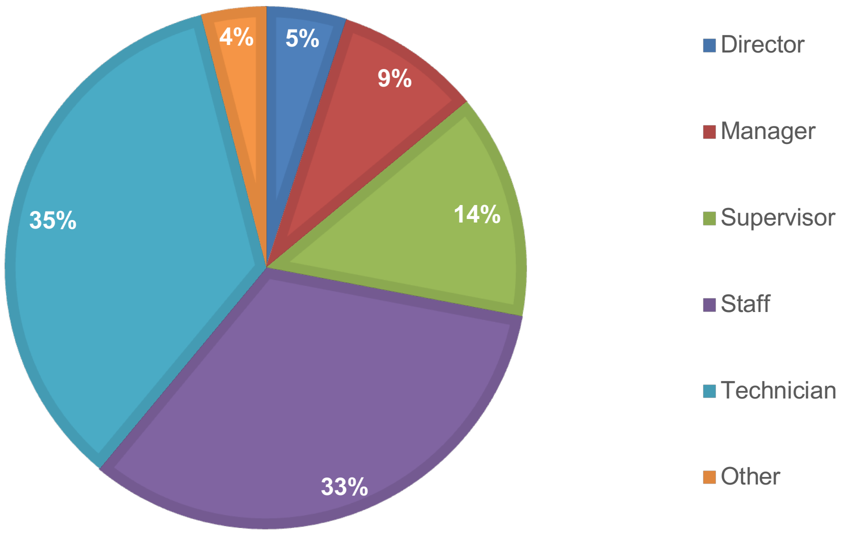
Part 3. Methodology

A sampling frame of 26,131 ITS staff, ITS leaders and line of business leaders were selected as participants to this survey. All respondents are familiar with authentication processes in their organizations and have some level from full, some and minimum responsibility for the security of their organization's authentication processes. Table 3 shows 1,152 total returns. Screening and reliability checks required the removal of 145 surveys. Our final sample consisted of 360 ITS staff surveys, 339 ITS leader surveys and 308 LoB leader surveys for a combined total of 1,007 surveys or a 3.9 percent response.

Table 3. Sample response	ITS Staff	ITS Leader	LoB Leader	Combined
Sampling frame	9,450	8,872	7,809	26,131
Total returns	405	388	359	1,152
Rejected or screened surveys	45	49	51	145
Final sample	360	339	308	1,007
Response rate	3.8%	3.8%	3.9%	3.9%

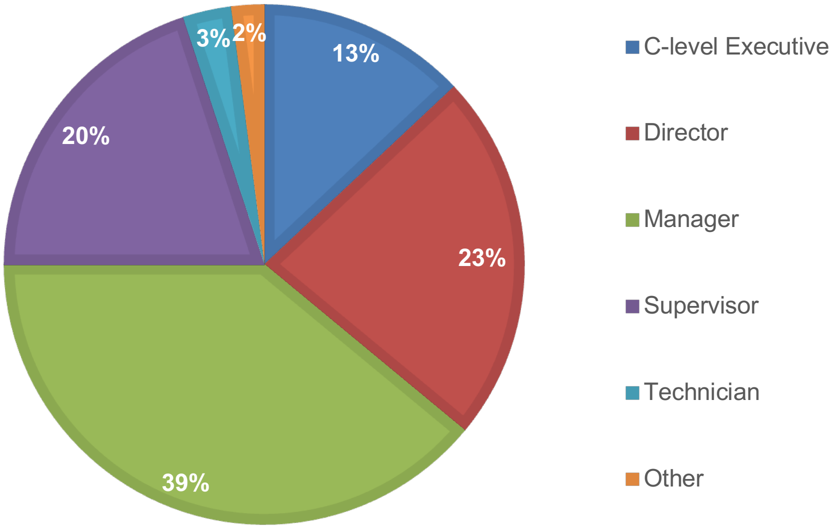
Pie Chart 1 reports the ITS staff respondent's position level within participating organizations. The largest category at 35 percent of respondents is technician. This is followed by staff (33 percent of respondents) and supervisor (14 percent of respondents).

Pie Chart 1. ITS staff position level within the organization



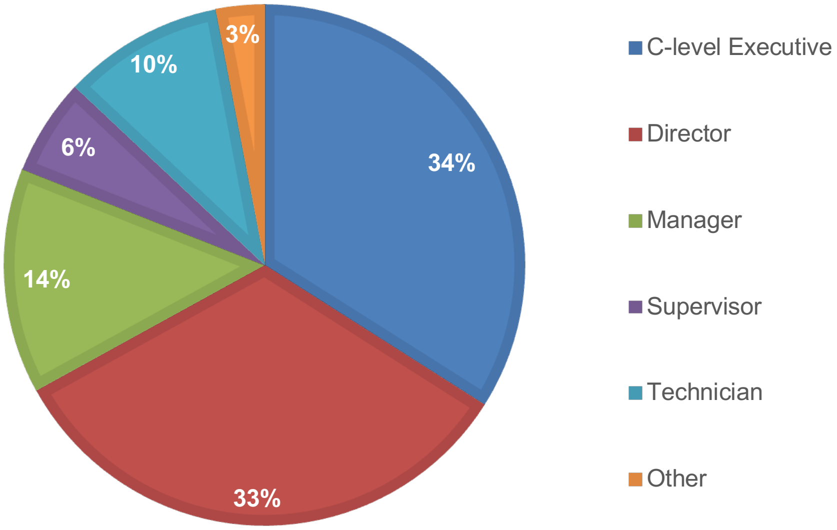
Pie Chart 2 reports the ITS leader respondent's position level within participating organizations. The largest category at 39 percent of respondents is manager. This is followed by director (23 percent of respondents) and supervisor (20 percent of respondents).

Pie Chart 2. ITS leader position level within the organization



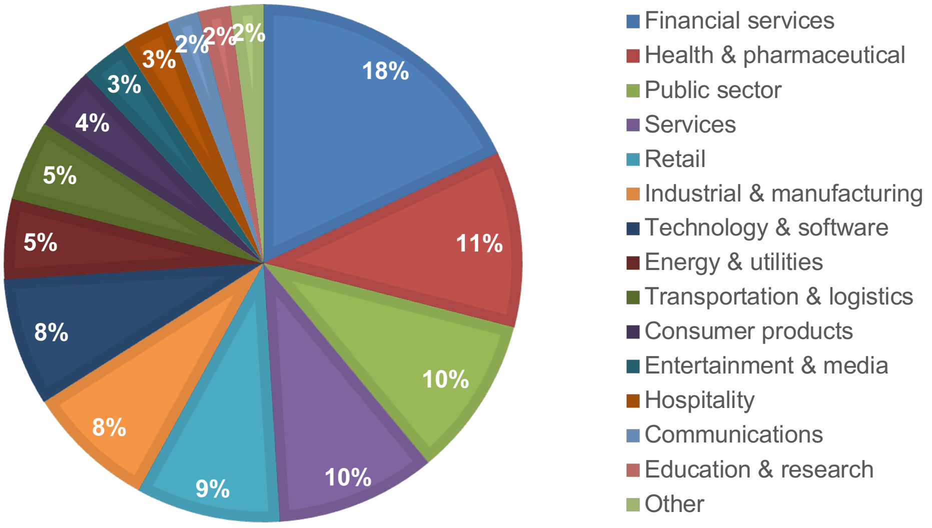
Pie Chart 3 reports the LoB leader respondent's position level within participating organizations. The largest category at 34 percent of respondents is C-level executive. This is followed by director (33 percent of respondents) and manager (14 percent of respondents).

Pie Chart 3. LoB leader position level within the organization



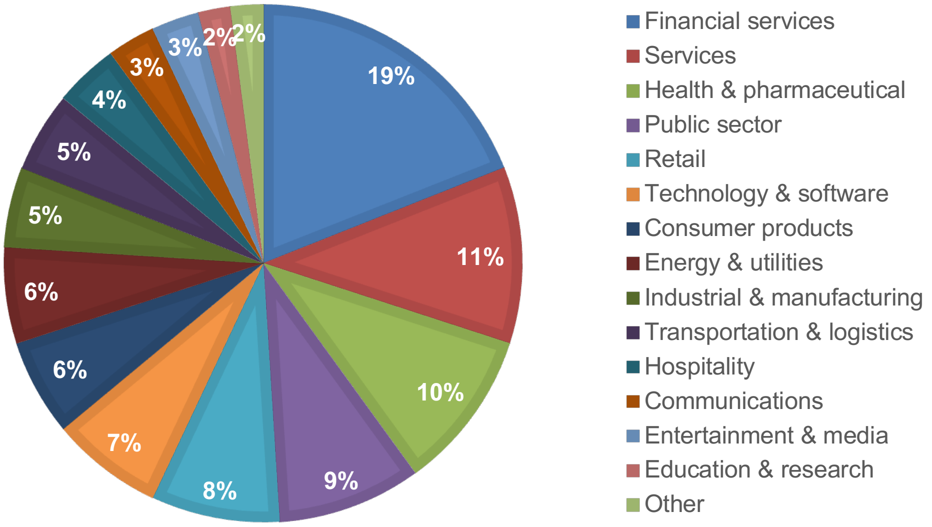
Pie Chart 4 reports the ITS staff respondent's industry classification. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (11 percent of respondents), public sector (10 percent of respondents), and retail (10 percent of respondents).

Pie Chart 4. ITS staff primary industry classification



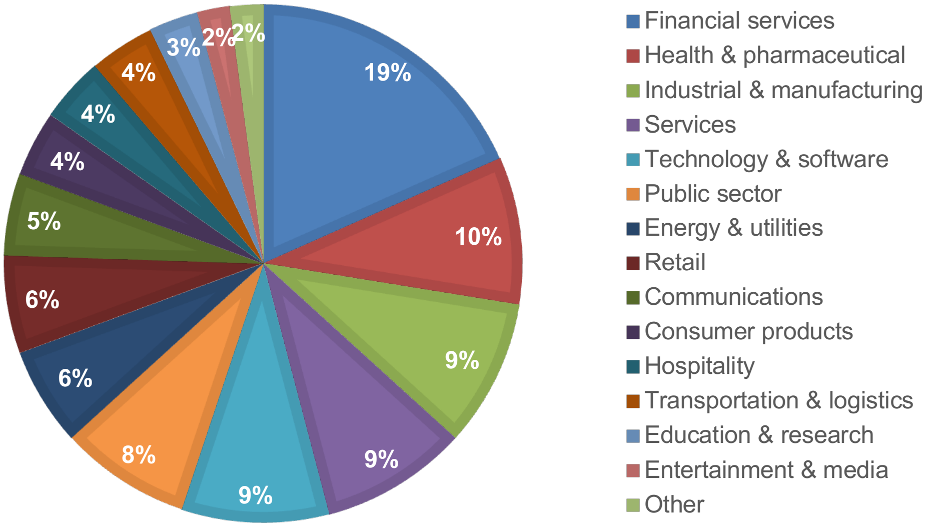
Pie Chart 5 reports the ITS leader respondent's industry classification. This chart identifies financial services (19 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by services (11 percent of respondents), health and pharmaceuticals (10 percent of respondents) and public sector (9 percent of respondents).

Pie Chart 5. ITS leader primary industry classification



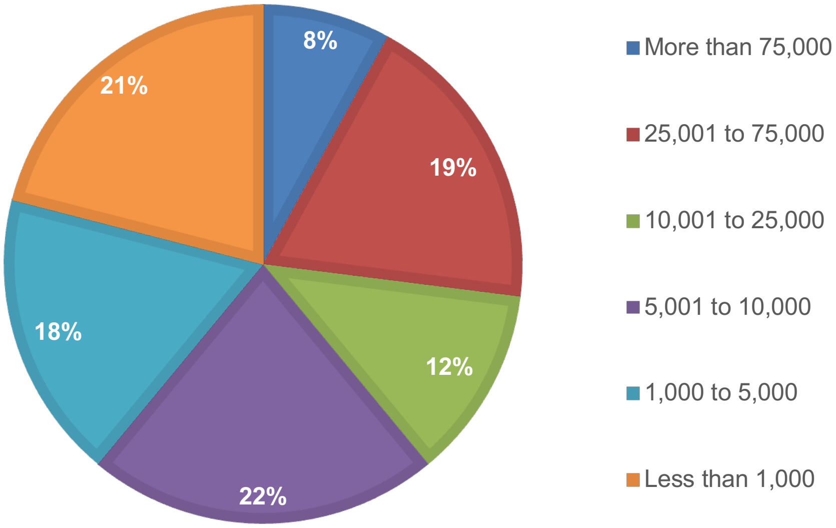
Pie Chart 6 reports the LoB leader 's industry classification. This chart identifies financial services (19 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by health and pharmaceuticals (10 percent of respondents), industrial and manufacturing (9 percent of respondents), and services (9 percent of respondents).

Pie Chart 6. LoB leader primary industry classification



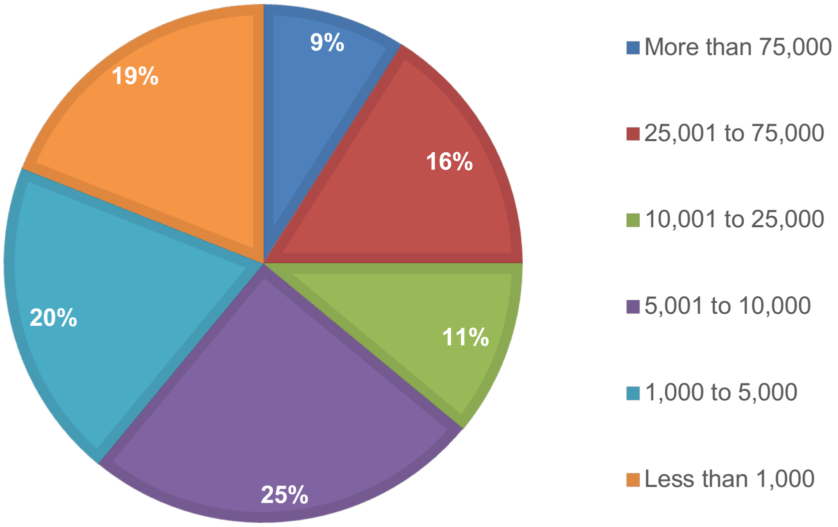
Sixty-one percent of ITS staff respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 7.

Pie Chart 7. Worldwide headcount of the ITS staff's organization



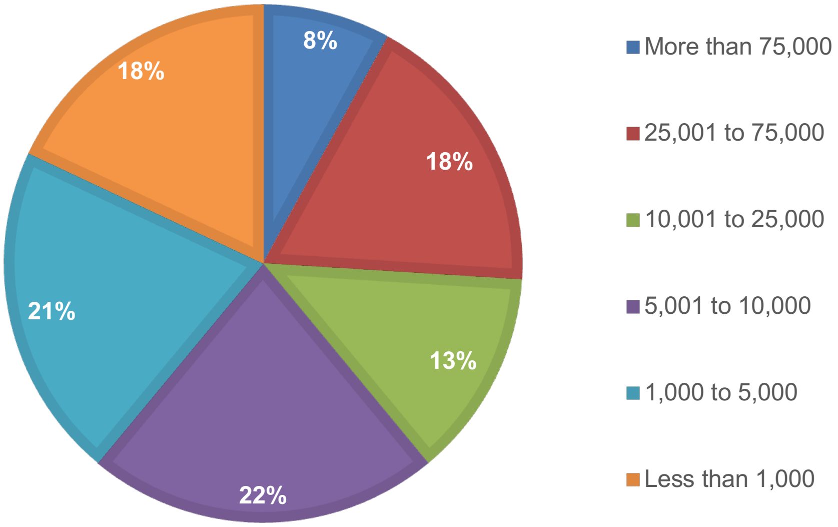
Sixty-one percent of ITS leader respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 8.

Pie Chart 8. Worldwide headcount of the ITS leader's organization



Sixty-one percent of LoB leader respondents are from organizations with a global headcount of more than 5,000 employees, as shown in Pie Chart 9.

Pie Chart 9. Worldwide headcount of the LoB leader's organization



Part 4. 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 instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are ITS staff, ITS leader or LoB leader. 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.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to al survey questions. All survey responses were captured in August 2021.

Survey response	ITS Staff	ITS Leader	LoB Leader	Combined
Total sampling frame	9,450	8,872	7,809	26,131
Total survey returns	405	388	359	1,152
Rejected surveys	45	49	51	145
Final sample	360	339	308	1,007
Response rate	3.8%	3.8%	3.9%	3.9%
Sampling weights	35.7%	33.7%	30.6%	100.0%

Part 1. Screening questions

S1. How familiar are you with authentication processes in your organization?	ITS Staff	ITS Leader	LoB Leader	Combined
Very familiar	39%	34%	31%	35%
Familiar	40%	36%	37%	38%
Somewhat familiar	21%	30%	32%	27%
No knowledge (Stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

S2. Do you have any responsibility for the security of your organization’s authentication processes in your organization?	ITS Staff	ITS Leader	LoB Leader	Combined
Yes, full responsibility	30%	41%	25%	32%
Yes, some responsibility	58%	48%	49%	52%
Yes, minimum responsibility	12%	11%	26%	16%
No responsibility (Stop)	0%	0%	0%	0%
Total	100%	100%	100%	100%

Part 2. Attributions

Q1. Please rate each one of the following statements using the agreement scale. **Strongly Agree and Agree response combined.**	ITS Staff	ITS Leader	LoB Leader	Combined
Q1a. Authentication failure represents a significant security challenge for my company.	60%	51%	44%	52%
Q1b. My company has good visibility into credential theft attacks.	35%	26%	30%	30%
Q1c. My company's security budget is sufficient for preventing and/or containing authentication failure.	28%	37%	45%	36%
Q1d. My company has sufficient solutions and technologies today for preventing and/or containing	31%	36%	50%	38%
Q1e. My company's migration to the cloud has increased the risk of authentication failure.	58%	49%	38%	49%
Q1f. Preventing authentication failure is difficult because fixes that curtail criminals may diminish the user's experience	54%	49%	43%	49%
Q1g. My organization's leaders recognize the need to invest in automation, AI and orchestration as part of its efforts to prevent authentication failures.	45%	60%	69%	57%

Part 3. Companies' experience with authentication failure

Q2. Using the following 10-point scale, please rate how much control your company has over its authentication processes from 1 = no control to 10= a high level of control.	ITS Staff	ITS Leader	LoB Leader	Combined
1 or 2	16%	12%	6%	12%
3 or 4	23%	18%	10%	17%
5 or 6	29%	26%	17%	24%
7 or 8	21%	29%	35%	28%
9 0r 10	11%	15%	32%	19%
Total	100%	100%	100%	100%
Extrapolated value	5.26	5.84	7.04	6.00

Q3a. Using the following 10-point scale, please rate how prepared your organization is to mitigate the risk of authentication failures from 1 = not prepared to 10 = very prepared.	ITS Staff	ITS Leader	LoB Leader	Combined
1 or 2	14%	10%	7%	11%
3 or 4	21%	16%	13%	17%
5 or 6	25%	22%	14%	21%
7 or 8	26%	32%	30%	29%
9 0r 10	14%	20%	36%	23%
Total	100%	100%	100%	100%
Extrapolated value	5.60	6.22	7.00	6.24

Q3b. Using the following 10-point scale, please rate how prepared your organization will be to mitigate the risk of authentication failures **in two years** from 1 = not prepared to 10 = very prepared.	ITS Staff	ITS Leader	LoB Leader	Combined
1 or 2	10%	8%	5%	8%
3 or 4	16%	9%	4%	10%
5 or 6	21%	17%	9%	16%
7 or 8	30%	26%	35%	30%
9 0r 10	23%	40%	47%	36%
Total	100%	100%	100%	100%
Extrapolated value	6.3	7.1	7.8	7.0

Q4. In an average **month**, how many authentication failures does your company detect? Your best guess is welcome.	ITS Staff	ITS Leader	LoB Leader	Combined
None	5%	0%	3%	3%
1 to 5	9%	11%	15%	12%
6 to 10	17%	28%	24%	23%
11 to 20	30%	34%	36%	33%
21 to 50	23%	21%	15%	20%
51 to 100	13%	5%	6%	8%
100+	3%	1%	1%	2%
Total	100%	100%	100%	100%
Extrapolated value	27.5	20.0	18.7	22.3

Q5. What were the consequences of these detected authentication failures? Please select all that apply.	ITS Staff	ITS Leader	LoB Leader	Combined
Ransomware	23%	19%	15%	19%
Downtime to resolve the authentication failure	66%	60%	55%	61%
Loss of customers	49%	52%	65%	55%
Substantial cost to rebuild the authentication processes	41%	43%	25%	37%
Disruption of business processes	63%	59%	61%	61%
Negative impact on third party and business relationships	47%	52%	54%	51%
Cost to remediate compromised accounts, including call center time or manual investigation/analysis by the security or fraud team	40%	37%	49%	42%
Reputation damage	31%	38%	44%	37%
Other (please specify)	2%	4%	1%	2%
Total	362%	364%	369%	365%

Q6. What percentage of authentication failures monthly do you think go undetected by your company? Your best guess is welcome.	ITS Staff	ITS Leader	LoB Leader	Combined
None	0%	3%	10%	4%
1 or 10%	15%	16%	26%	19%
11 or 25%	27%	31%	24%	27%
26 or 50%	13%	14%	25%	17%
51 or 75%	19%	20%	15%	18%
76 or 100%	26%	16%	0%	15%
Total	100%	100%	100%	100%
Extrapolated value	45%	38%	24%	36%

Q7. What percentage of authentication failures result in the attacker being able to obtain credentials of bona fide users? Your best guess is welcome.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 1%	0%	4%	0%	1%
1 to 2%	0%	8%	7%	5%
3 to 4%	2%	16%	9%	9%
5 to 6%	1%	12%	15%	9%
7 to 8%	10%	13%	14%	12%
9 to 10%	23%	9%	12%	15%
11 to 20%	31%	18%	19%	23%
More than 20%	33%	20%	24%	26%
Total	100%	100%	100%	100%
Extrapolated value	15%	10%	12%	12%

Q8. In your opinion, how difficult is it to know the “real” employees, customers and/or users from criminal imposters who are using stolen credentials?	ITS Staff	ITS Leader	LoB Leader	Combined
Very difficult	32%	27%	23%	28%
Difficult	34%	29%	25%	30%
Somewhat difficult	24%	32%	33%	29%
Not difficult	8%	12%	14%	11%
Easy	2%	0%	5%	2%
Total	100%	100%	100%	100%

Q9. In your opinion, how has the **volume or frequency** of authentication failures changed over the past 12 months?	ITS Staff	ITS Leader	LoB Leader	Combined
Significantly increased	30%	28%	24%	27%
Increased	41%	34%	31%	36%
Stayed the same	18%	27%	29%	24%
Decreased	9%	11%	13%	11%
Significantly decreased	2%	0%	3%	2%
Total	100%	100%	100%	100%

Q10. In your opinion how has **the severity of authentication failures** changed over the past 12 months?	ITS Staff	ITS Leader	LoB Leader	Combined
Significantly increased	25%	23%	22%	23%
Increased	34%	32%	29%	32%
Stayed the same	29%	31%	34%	31%
Decreased	9%	12%	12%	11%
Significantly decreased	3%	2%	3%	3%
Total	100%	100%	100%	100%

Q11. In your opinion, how has **cost to detect, contain and resolve authentication failures** changed over the past 12 months?	ITS Staff	ITS Leader	LoB Leader	Combined
Significantly increased	29%	23%	25%	26%
Increased	35%	32%	25%	31%
Stayed the same	25%	32%	33%	30%
Decreased	9%	13%	14%	12%
Significantly decreased	2%	0%	3%	2%
Total	100%	100%	100%	100%

Part 4. Approaches to minimize the risk of authentication failures

Q12. Who is **most responsible** for preventing, detecting, containing and resolving authentication failures? Please check only **one** response.	ITS Staff	ITS Leader	LoB Leader	Combined
Chief digital officer (CDO)	1%	0%	2%	1%
Chief financial officer and other senior finance or accounting personnel	2%	1%	2%	2%
Chief information officer (CIO)	21%	25%	24%	23%
Chief information security officer (CISO)	19%	21%	18%	19%
Chief risk officer (CRO)	3%	5%	6%	5%
Chief security architect	2%	2%	1%	2%
Chief security officer (CSO)	2%	0%	0%	1%
Chief technology officer (CTO)	6%	8%	5%	6%
Data center management	4%	3%	1%	3%
Head, IT operations	21%	20%	26%	22%
IT compliance leader	7%	5%	4%	5%
No one function has overall responsibility	11%	10%	11%	11%
Other (please specify)	1%	0%	0%	0%
Total	100%	100%	100%	100%

Q13. How important are the following organizational characteristics in preventing authentication failures? Please select the top two characteristics	ITS Staff	ITS Leader	LoB Leader	Combined
Agility	24%	33%	39%	32%
Ample budget	29%	25%	21%	25%
Knowledgeable or expert staff	41%	45%	39%	42%
Leadership	18%	23%	9%	17%
Preparedness	23%	15%	14%	18%
Resilience	35%	30%	43%	36%
Strong security posture	28%	28%	35%	30%
Other (please specify)	2%	1%	0%	1%
Total	200%	200%	200%	200%

Q14a. Does your company have a strategy to mitigate authentication failures?	ITS Staff	ITS Leader	LoB Leader	Combined
Yes	33%	41%	49%	41%
No	67%	59%	51%	59%
Total	100%	100%	100%	100%

Q14b. If yes, does the strategy include any of the following actions?	ITS Staff	ITS Leader	LoB Leader	Combined
Assessment of potential vulnerabilities in authentication processes	54%	48%	50%	51%
Increase investment in technologies	64%	63%	59%	62%
Increase in staff dedicated to preventing authentication failures	59%	67%	65%	64%
Improve the user experience without affecting security	73%	75%	71%	73%
Assessments of the effectiveness of current authentication methods in use	50%	47%	53%	50%
Other (please specify)	3%	4%	2%	3%
Total	303%	304%	300%	302%

Q15a. Does your organization use passwordless authentication where users don’t know or manage their account password?	ITS Staff	ITS Leader	LoB Leader	Combined
Yes,	19%	24%	23%	22%
No (please skip to Q16.)	81%	76%	77%	78%
Total	100%	100%	100%	100%

Q15b. If yes, why did your organization adopt passwordless authentication? Select all that apply.	ITS Staff	ITS Leader	LoB Leader	Combined
End-user experience	44%	40%	60%	48%
Security	59%	60%	43%	54%
Productivity of users	50%	52%	60%	54%
Cost effectiveness of authentication	46%	51%	57%	51%
Visibility over end-users' access to the organization's assets	47%	41%	38%	42%
Uniting authentication mechanisms	50%	55%	62%	55%
Reducing the complexity of IAM infrastructure	48%	38%	34%	40%
Reducing helpdesk calls	45%	46%	37%	43%
Supporting digital transformation	42%	53%	59%	51%
Other (please specify)	3%	2%	3%	3%
Total	434%	438%	453%	441%

Q16. What are barriers to adopting passwordless authentication, why? Please select all that apply.	ITS Staff	ITS Leader	LoB Leader	Combined
Legacy systems and applications do not support the technology	61%	58%	42%	54%
Not as secure as other methods of two-factor or multi-factor authentication	31%	43%	37%	37%
Not enough IT resources to dedicate to this type of transition	37%	43%	41%	40%
Not familiar with the process	30%	24%	19%	25%
Our current password authentication process works well enough	52%	50%	42%	48%
Strong authentication is not a current priority for our organization	34%	37%	40%	37%
Too expensive	12%	16%	15%	14%
Other (please specify)	5%	4%	4%	4%
Total	262%	275%	240%	260%

Q17. Within your organization, how many IT security or anti-fraud personnel are involved in the detection and containment authentication failures?	ITS Staff	ITS Leader	LoB Leader	Combined
None	0%	5%	2%	2%
Less than 5	18%	15%	17%	17%
5 to 10	26%	23%	20%	23%
11 to 15	21%	26%	23%	23%
16 to 20	16%	18%	22%	19%
21 to 25	11%	13%	14%	13%
More than 25	8%	0%	2%	3%
Total	100%	100%	100%	100%
Extrapolated value	12.9	11.7	12.7	12.5

Q18. Approximately, how many hours each week are spent **organizing and planning** the organization's approaches to the detection and containment of authentication failures? Please estimate the aggregate hours of the IT and IT security (SecOps) and fraud teams.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 5	0%	2%	0%	1%
5 to 10	4%	3%	4%	4%
11 to 25	7%	5%	8%	7%
26 to 50	11%	10%	10%	10%
51 to 100	13%	14%	12%	13%
101 to 250	18%	16%	20%	18%
251 to 500	23%	24%	21%	23%
More than 500	24%	26%	25%	25%
Total	100%	100%	100%	100%
Extrapolated value	265.2	276.5	265.8	269.2

Q19. Approximately, how many hours each week are spent **analyzing and investigating** authentication failures? Please estimate the aggregate hours of the IT security (SecOps) and fraud team.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 5	0%	0%	0%	0%
5 to 10	0%	1%	1%	1%
11 to 25	2%	4%	3%	3%
26 to 50	7%	6%	10%	11%
51 to 100	11%	10%	13%	11%
101 to 250	22%	19%	15%	19%
251 to 500	23%	24%	26%	24%
More than 500	35%	36%	32%	34%
Total	100%	100%	100%	100%
Extrapolated value	328.5	331.8	313.9	326.5

Q20. Approximately, how many hours each week are spent conducting **forensic analysis** for those accounts, believed to have been compromised due to authentication failure? Please estimate the aggregate hours of the IT security (SecOps) and fraud team.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 5	2%	3%	0%	2%
5 to 10	5%	8%	8%	7%
11 to 25	3%	6%	9%	6%
26 to 50	16%	18%	14%	11%
51 to 100	20%	22%	20%	21%
101 to 250	26%	18%	16%	20%
251 to 500	16%	14%	26%	18%
More than 500	12%	11%	7%	10%
Total	100%	100%	100%	100%
Extrapolated value	193.5	169.6	186.5	181.4

Q21. Approximately, how many hours each week are spent **documenting and/or reporting** upon authentication failure in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the IT, security (SecOps) and fraud team.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 5	9%	7%	8%	8%
5 to 10	15%	16%	17%	16%
11 to 25	12%	17%	18%	16%
26 to 50	31%	29%	25%	11%
51 to 100	13%	11%	11%	12%
101 to 250	11%	13%	10%	11%
251 to 500	5%	4%	6%	5%
More than 500	4%	3%	5%	4%
Total	100%	100%	100%	100%
Extrapolated value	85.0	78.0	90.0	77.5

Q22. How confident are you that the following technologies will secure the authentication processes of your organization? **Very Confident and Confident response combined.**	ITS Staff	ITS Leader	LoB Leader	Combined
Q22a. Technologies that identify, authenticate and govern the access rights of both employees and consumers	44%	39%	36%	40%
Q22b. Technologies that simplify the reporting of threats	41%	37%	33%	37%
Q22c.Technologies that secure endpoints including mobile-connected devices	46%	41%	32%	40%
Q22d. Technologies that minimize insider threats (including potential negligence)	54%	49%	51%	51%
Q22e. Technologies that pinpoint vulnerabilities and implement security patches in (near) real time	63%	61%	56%	60%
Q22f. Technologies that utilize machine learning, artificial intelligence for authentication	54%	55%	58%	56%
Q22g.Technologies that prevent unauthorized access to data and applications	65%	58%	59%	61%
Q22h.Technologies that reduce the risk of fraud	57%	51%	325%	137%

Part 4. Estimating the cost of authentication failures

Q23. What remediation efforts are made when a compromised account is identified? Please select all that apply	ITS Staff	ITS Leader	LoB Leader	Combined
Send the account owner a password reset email	62%	60%	55%	59%
Call the account owner to explain the situation	49%	53%	48%	50%
Lock down the account	58%	61%	54%	58%
Investigate the history of the account to identify previously undetected fraud	37%	34%	31%	34%
Other (please specify)	3%	4%	3%	3%
Total	209%	212%	191%	205%

Q24. Approximately, how many hours each week are spent **containing and remediating** authentication failures? Please estimate the aggregate hours of the IT and IT security (SecOps) team.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 5	7%	9%	8%	8%
5 to 10	12%	10%	13%	12%
11 to 25	15%	15%	20%	17%
26 to 50	13%	12%	16%	11%
51 to 100	15%	16%	15%	15%
101 to 250	20%	18%	13%	17%
251 to 500	13%	14%	9%	12%
More than 500	5%	6%	6%	6%
Total	100%	100%	100%	100%
Extrapolated value	131.2	137.2	111.6	126.3

Q25. In an average month, how much **downtime** results from authentication failures your organization experiences?	ITS Staff	ITS Leader	LoB Leader	Combined
None	0%	4%	5%	3%
Less than 1 hour	12%	23%	25%	20%
1 to 2 hours	21%	22%	24%	22%
3 to 5 hours	25%	21%	26%	24%
6 to 10	19%	17%	13%	16%
11 to 24 hours	11%	7%	4%	8%
24 hours+	12%	6%	3%	7%
Total	100%	100%	100%	100%
Extrapolated value	7.76	5.43	4.11	5.86

Q26. Annually, what is the percentage of customers that leave or switch to a competitor after an authentication failure?	ITS Staff	ITS Leader	LoB Leader	Combined
None	10%	8%	12%	10%
Less than 1%	18%	15%	10%	15%
1 to 10%	32%	33%	35%	33%
11 to 20%	24%	21%	20%	22%
21 to 50%	11%	17%	18%	15%
51 to 100%	5%	6%	5%	5%
Total	100%	100%	100%	100%
Extrapolated value	13%	15%	15%	14%

Q27. What best describes the maximum loss that could be realized by your organization as a result of **one** authentication failure in the next 12 months? (please include decrease in revenues and fines)	ITS Staff	ITS Leader	LoB Leader	Combined
Less than $100,000	3%	0%	1%	1%
$100,000 to $250,000	5%	6%	8%	6%
$250,001 to $500,000	9%	8%	12%	10%
$500,001 to $1,000,000	9%	18%	13%	13%
$1,000,001 to $5,000,000	44%	40%	42%	42%
More than $5,000,000	30%	28%	24%	27%
Total	100%	100%	100%	100%
Extrapolated value (US$ Millions)	$ 41.93	$ 41.00	$ 39.06	$ 40.74

Q28. What best describes the **likelihood** of a material authentication failure cause by an authentication failure within the next 12 months?	ITS Staff	ITS Leader	LoB Leader	Combined
0.01%	2%	3%	0%	2%
0.05%	4%	5%	4%	4%
0.10%	8%	10%	9%	9%
0.50%	11%	12%	13%	12%
1.00%	19%	23%	16%	19%
2.00%	26%	23%	25%	25%
2.50%	13%	12%	11%	12%
3.00%	4%	5%	10%	6%
4.00%	3%	2%	3%	3%
5.00%	5%	2%	5%	4%
5.50%	5%	3%	4%	4%
Total	100%	100%	100%	100%
Extrapolated value	1.87%	1.56%	1.90%	1.77%

Q29. What best describes the maximum loss that could be realized by your organization as a result of a material business disruption caused by an authentication failure in the next 12 months.	ITS Staff	ITS Leader	LoB Leader	Combined
Less than $100,000	6%	7%	6%	6%
$100,000 to $250,000	7%	9%	10%	9%
$250,001 to $500,000	8%	9%	11%	9%
$500,001 to $1,000,000	11%	19%	23%	17%
$1,000,001 to $5,000,000	30%	30%	26%	29%
More than $5,000,000	38%	26%	24%	30%
Total	100%	100%	100%	100%
Extrapolated value (US$ Millions)	$ 39.86	$ 35.47	$ 33.61	$ 36.47

Q30. What best describes the **likelihood** of a material business disruption caused by an authentication failure in the next 12 months.	ITS Staff	ITS Leader	LoB Leader	Combined
0.01%	0%	0%	0%	0%
0.05%	0%	1%	2%	1%
0.10%	5%	9%	3%	6%
0.50%	5%	11%	12%	9%
1.00%	21%	19%	18%	19%
2.00%	18%	19%	12%	17%
2.50%	11%	10%	11%	11%
3.00%	17%	13%	20%	17%
4.00%	13%	12%	14%	13%
5.00%	5%	3%	4%	4%
5.50%	*5%*	3%	4%	4%
Total	100%	100%	100%	100%
Extrapolated value	2.43%	2.07%	2.34%	2.28%

Part 5. Digital transformation and authentication failure				
Q31. Please rate each one of the following statements using the opinion scale from "strongly agree" to "strongly disagree" provided below each item. **Strongly Agree and Agree response**.	ITS Staff	ITS Leader	LoB Leader	Combined
Q31a. Digital transformation is not possible without strict security safeguards to protect the sharing and use	46%	43%	39%	43%
Q31b. The rush to achieve digital transformation increases the risk of an authentication failure.	62%	56%	58%	59%
Q31c. In my organization, the digital economy significantly increases the risk of authentication failure.	67%	65%	61%	64%
Q31d. My organization's leaders recognize that digital transformation increases the risk of authentication failures.	44%	53%	59%	52%
Q31e. Authentication is a barrier to effective digital transformation.	43%	56%	62%	53%
Q31f. Authentication is central to digital transformation.	63%	65%	63%	64%
Q31g. Authentication has a negative impact on the agility and security of software development efforts.	54%	49%	53%	52%

Q32. Of the following, who is most involved in directing your organization's efforts to ensure **a secure** digital transformation process? Please choose only your top one choice only.	ITS Staff	ITS Leader	LoB Leader	Combined
Chief digital officer	9%	8%	13%	10%
Chief financial officer (CFO) (and other senior finance or accounting personnel)	0%	2%	3%	2%
Chief information officer (CIO)	24%	29%	30%	28%
Chief information security officer (CISO)	18%	16%	13%	16%
Chief privacy officer (CPO)	0%	0%	1%	0%
Chief risk officer (CRO)	0%	1%	2%	1%
Chief security architect	4%	2%	1%	2%
Chief security officer (CSO)	0%	0%	1%	0%
Chief technology officer (CTO)	20%	15%	13%	16%
Data center management	2%	3%	2%	2%
General manager / VP, lines of business	11%	12%	10%	11%
IT compliance leader	2%	3%	2%	2%
No one person has overall responsibility	9%	9%	8%	9%
Other (please specify)	1%	0%	1%	1%
Total	100%	100%	100%	100%

Q33. Is your organization more vulnerable to authentication failure following digital transformation?	ITS Staff	ITS Leader	LoB Leader	Combined
Yes, much more vulnerable	44%	49%	43%	45%
Yes, somewhat more vulnerable	21%	19%	23%	21%
No change in vulnerability to a cyberattack or data breach	35%	32%	34%	34%
Total	100%	100%	100%	100%

Q34. What are the most negative consequences that your organization might have experienced as a result of authentication failure caused by insecure digital transformation? Please select the top **two** most negative consequences.	ITS Staff	ITS Leader	LoB Leader	Combined
Cost of outside consultants and experts	16%	21%	23%	20%
Customer turnover	31%	27%	33%	30%
Disruption or damages to critical infrastructure	32%	34%	31%	32%
Lost intellectual property (including trade secrets)	37%	39%	35%	37%
Lost revenue	23%	25%	23%	24%
Productivity decline	28%	23%	25%	25%
Regulatory actions or lawsuits	12%	11%	15%	13%
Reputation or brand damage	19%	16%	13%	16%
Other (please specify)	2%	4%	2%	3%
Total	200%	200%	200%	200%

Part 6. Budget

Q35. Approximately, what range best defines your organization’s 2021 IT budget?	ITS Staff	ITS Leader	LoB Leader	Combined
< $1 million	2%	0%	0%	1%
$1 to 5 million	5%	4%	3%	4%
$6 to $10 million	16%	15%	17%	16%
$11 to $50 million	19%	20%	14%	18%
$51 to $100 million	21%	20%	19%	20%
$101 to $250 million	18%	25%	29%	24%
$251 to $500 million	15%	10%	13%	13%
$501 to $750 million	4%	5%	4%	4%
$751 million to $1 billion	0%	1%	1%	1%
More than $1 billion	0%	0%	0%	0%
Total	100%	100%	100%	100%
Extrapolated value (US$ millions)	$ 135.7	$ 143.6	$ 153.2	$ 143.7

Q36. Approximately, what percentage of the IT budget will be allocated to IT security?	ITS Staff	ITS Leader	LoB Leader	Combined
< 1%	5%	3%	4%	4%
1% to 2%	6%	5%	6%	6%
3% to 5%	9%	10%	8%	9%
6% to 10%	12%	14%	15%	14%
11% to 15%	23%	25%	20%	23%
16% to 20%	17%	18%	15%	17%
21% to 30%	12%	11%	17%	13%
31% to 40%	13%	9%	8%	10%
41% to 50%	3%	5%	6%	5%
More than 50%	0%	0%	1%	0%
Total	100%	100%	100%	100%
Extrapolated value	16.4%	16.3%	17.3%	16.6%

Q37. Approximately, what percentage of the IT security budget will be allocated to staff and technologies to prevent, detect, contain and resolve authentication failures?	ITS Staff	ITS Leader	LoB Leader	Combined
< 1%	6%	6%	5%	6%
1% to 2%	11%	12%	9%	11%
3% to 5%	17%	16%	15%	16%
6% to 10%	21%	15%	25%	20%
11% to 15%	16%	17%	17%	17%
16% to 20%	17%	19%	15%	17%
21% to 30%	8%	9%	9%	9%
31% to 40%	3%	4%	3%	3%
41% to 50%	1%	2%	1%	1%
More than 50%	0%	0%	1%	0%
Total	100%	100%	100%	100%
Extrapolated value	11.2%	12.3%	12.0%	11.8%

Part 7. Your role and organization

What best defines your position level within your organization?	ITS Staff	ITS Leader	LoB Leader	Combined
C-level Executive	0%	13%	34%	15%
Director	5%	23%	33%	20%
Manager	9%	39%	14%	21%
Supervisor	14%	20%	6%	14%
Staff	33%	0%	0%	12%
Technician	35%	3%	10%	17%
Other	4%	2%	3%	3%
Total	100%	100%	100%	100%

D2. What industry best describes your organization's industry focus?	ITS Staff	ITS Leader	LoB Leader	Combined
Agriculture & food services	1%	0%	1%	1%
Communications	2%	3%	5%	3%
Consumer products	4%	6%	4%	5%
Defense & aerospace	1%	0%	1%	1%
Education & research	2%	2%	3%	2%
Energy & utilities	5%	6%	6%	6%
Entertainment & media	3%	3%	2%	3%
Financial services	18%	19%	18%	18%
Health & pharmaceutical	11%	10%	9%	10%
Hospitality	3%	4%	4%	4%
Industrial & manufacturing	8%	5%	9%	7%
Public sector	10%	9%	8%	9%
Retail	9%	8%	6%	8%
Services	10%	11%	9%	10%
Technology & software	8%	7%	9%	8%
Transportation & logistics	5%	5%	4%	5%
Other (please specify)	0%	2%	2%	1%
Total	100%	100%	100%	100%

D4. What is the worldwide headcount of your organization?	ITS Staff	ITS Leader	LoB Leader	Combined
Less than 1,000	21%	19%	18%	19%
1,000 to 5,000	18%	20%	21%	20%
5,001 to 10,000	22%	25%	22%	23%
10,001 to 25,000	12%	11%	13%	12%
25,001 to 75,000	19%	16%	18%	18%
More than 75,000	8%	9%	8%	8%
Total	100%	100%	100%	100%

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

Ponemon Institute
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.