Digital Transformation & Cyber Risk: What You Need to Know to Stay Safe

Sponsored by CyberGRX

Independently conducted by Ponemon Institute LLC

PUBLICATION DATE - JUNE 2020

Table of Contents

Part 1

Executive Summary

Digital transformation is the use of technologies to improve operations and customer relationships. CyberGRX and Ponemon Institute surveyed 581 IT security and 302 C-suite executives to determine what impact digital transformation is having on cybersecurity and how prepared organizations are to deal with that impact. In some instances, we highlight the differences between IT Security and C-level respondents. Otherwise, we show the consolidated findings for the 883 respondents.

The results show that while digital transformation is widely accepted as critical, the rapid adoption of it is creating significant vulnerabilities for most organizations — and these are only exacerbated by misalignment between IT security professionals and the C-suite. All 883 respondents are involved in managing digital transformation and cybersecurity activities within their organizations.

Here are the key themes being reviewed in this report

Digital transformation is increasing cyber risk.

IT security has very little involvement in directing efforts to ensure a secure digital transformation process.

ONLY **37%** of respondents say the CIO is most involved.

ONLY **24%** of respondents say the CISO is most involved.

82% of respondents believe their organizations experienced at least one data breach as a result of digital transformation.

55% of respondents say with certainty that at least one of these breaches was caused by a third party.

Digital transformation has significantly increased reliance on third parties.

58% of respondents say the primary change to their organizations is increased migration to the cloud.

58% of respondents say that despite the increased risk, their organizations do not have a third-party cyber risk management program.

63% of respondents say their organizations have difficulty ensuring there is a secure cloud environment.

56% of C-level executives say their organizations find it challenging to ensure third parties have policies and practices that guarantee the security of their information.

Conflicting priorities between IT security teams and the C-suite create vulnerabilities.

C-level and IT security respondents disagree on the importance of safeguarding high value assets and other areas of risk. **Only 16** percent of respondents say IT security and lines of business are fully aligned with respect to achieving a secure digital transformation process.

	C-SUITE	IT DEPT
Rushing to achieve digital transformation increases risk of a data breach	53%	71%
Do not want security measures to prevent the free flow of information in an open-business model	63%	45%

Budgets are and will continue to be inadequate to secure the digital transformation process.

ONLY **35%** say their organizations have budget for protecting data in the digital transformation process.

ALMOST **2x** the amount the average digital transformation budget should be increased to be more effective.

In two years, respondents believe the average IT security budget percentage will increase to **37** percent, although that will still be inadequate.

Unless things change, the future doesn't look any more secure.

ONLY **29%** of respondents say their organizations are very prepared to address top threats related to digital transformation.

ONLY **43%** of respondents are very optimistic their organizations will be prepared to reduce the risk of these threats within two years.

66% believe cyber security attacks, third party breaches, and system downtime will be their biggest threats in the next two years.

A few recommendations for a secure digital transformation

Collaboration between C-level and IT Security teams is essential to the success of your organization's digital transformation process.
Read more on pg. 34

Prioritize to ensure your most sensitive data is protected first.
Read more on pg. 36

Make sure your digital transformation strategy involves the assessment of third-party relationships in addition to the protection of data and assets.
Read more on pg. 37

Educate your organization – including C-level – about the cyber risk that comes with digital transformation.
Read more on pg. 38

Ensure your company's Digital Transformation budget reflects the industry's best practices.
Read more on pg. 40

Continuously invest in technologies that secure and protect your data and assets.
Read more on pg. 42

Part 2

Key Findings

The movement towards digital transformation has increased cyber risks

All respondents agree digital transformation has increased their vulnerability to a data breach, however IT security respondents and C-level respondents are not fully aligned on what is driving the vulnerabilities, and IT respondents are more cognizant of the risk if not enough time and resources are allocated to the digital transformation process.

- Both ITS (67%) and C-Level (71%) respondents agree they are more vulnerable to a data breach as a result of digital transformation.
- IT security respondents believe the rush to produce apps (50%) and increased use of Shadow IT (48%) are driving the vulnerabilities, whereas C-Level (56%) believes they are driven primarily by increased migration to the cloud.
- Less than half of C-level respondents (49 percent) say senior management recognizes the potential harm to their brand and reputation.

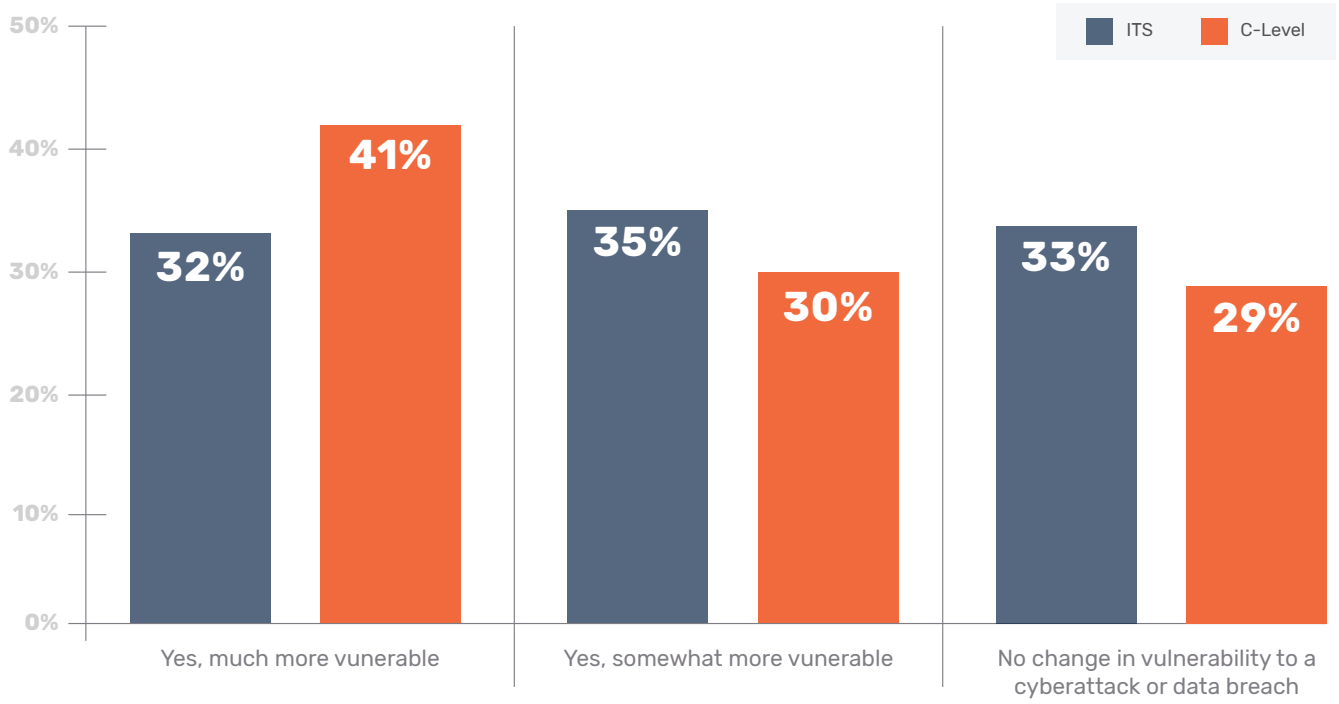


Figure 1
Is your organization more vulnerable to a cyberattack or data breach following digital transformation?

Most organizations do not believe they have a mature digital transformation process in place to manage the changes.

When it comes to maturity stage of the digital transformation process, Figure 2 shows that only 23 percent of respondents say they have achieved the mature stage while 57 percent have achieved early to the middle stage.

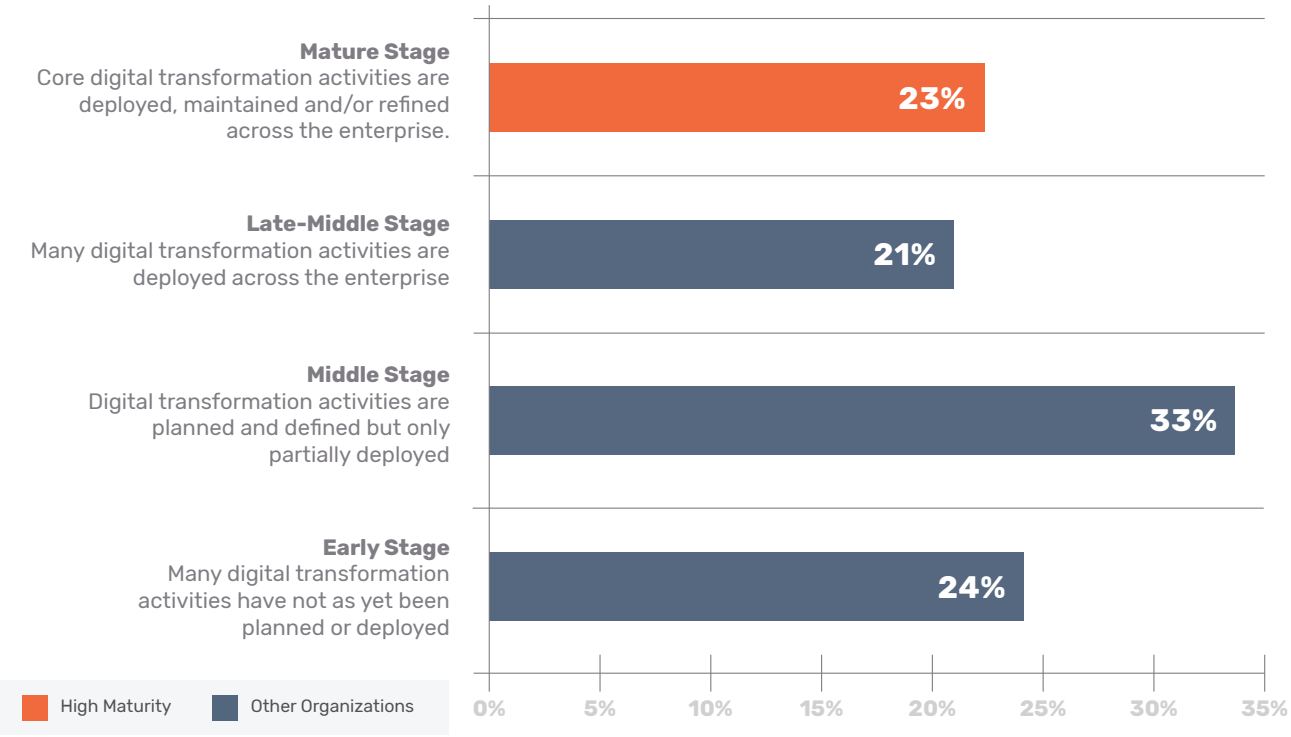


Figure 2
What best describes the maturity level of your organization's digital transformation process?

Organizations have experienced multiple data breaches as a result of digital transformation.

- According to respondents, the biggest causes of vulnerabilities today are the increased speed involved with digital transformation (48 percent), increased migration to the cloud (46 percent), and the use of shadow IT (46 percent).
- Eighty-two percent of respondents believe their organizations experienced at least one data breach during the digital transformation process.
- Forty-two percent of respondents say their organizations could have experienced between two and five data breaches and 22 percent say their organizations could have experienced between six and ten data breaches.
- Fifty-five percent of respondents say with certainty that at least one of these breaches was caused by a third party.

Organizations are not protecting what matters most.

- Analytics and private communications are the most difficult assets to secure according to 51 percent of IT respondents while 44 percent of C-suite respondents felt the same way.
- Only 35 percent of respondents say analytics is appropriately secured and only 38 percent of respondents say private communications are secured.
- Surprisingly, only 25 percent of respondents say consumer data, which is considered highly sensitive and confidential, is appropriately secured even though they feel the difficultly level of doing so is low.
- System downtime, cyber security attacks, and third-party breaches are the biggest threats respondents are worried about in the next two years.

Misalignment between the C-suite and IT security creates opportunities for risk.

- Only 16 percent of respondents say IT security and lines of business are fully aligned with respect to preserving cybersecurity during the digital transformation process.
- Sixty-four percent of IT security respondents and 41 percent of C-level respondents say that the digital economy significantly increases risk to high value assets such as intellectual property and trade secrets.
- Sixty-three percent of C-level respondents do not want the security measures used by IT to prevent the free flow of information and an open business model, while only 41 percent of IT security respondents feel the same way.

A secure digital transformation process is affected by a lack of expertise and visibility.

Fifty-three percent of respondents say a lack of expertise is the most significant barrier to achieving a secure digital transformation process followed by insufficient visibility into people and business processes (51 percent).

Digital transformation has significantly increased reliance on third parties, specifically cloud providers, IoT, and shadow IT

We believe organizations will become even more reliant on third parties as increased migration to the cloud, increased use of IoT, and shadow IT emerge.

- As Figure 3 shows, 58 percent of respondents say the primary change to their organizations is increased migration to the cloud. This is followed by the increased usage of IoT at 49 percent, and shadow IT at 39 percent.

- Since beginning the digital transformation process, organizations have seen an average 15 percent increase in the number of third parties they utilize. However, when you factor in cloud, IoT, and Shadow IT providers, we expect this number to increase significantly.

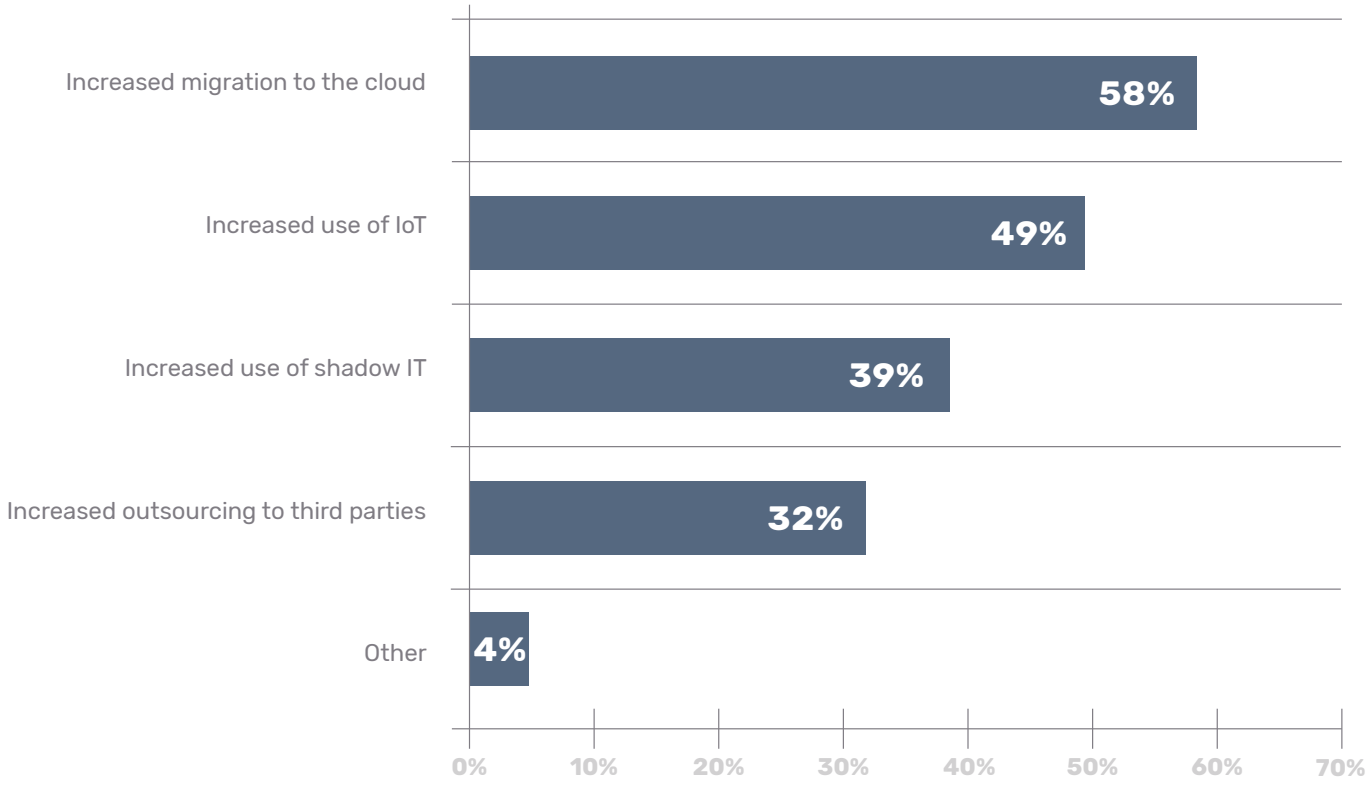


Figure 3
How has digital transformation changed your organization?

More than one response permitted

Current tools or solutions to manage third-party risk are still not considered effective.

- Slightly more than half (51 percent) of organizations represented have a strategy for achieving digital transformation and of these, 73 percent say their strategy involves assessing third-party relationships and vulnerabilities.
- Forty-two percent of respondents say their organizations have a third-party risk management program and more than half (52 percent) of those respondents say that assessments are the most used solution, as seen in Figure 4.
- Fifty-three percent say the tools and solutions used are only somewhat effective (28 percent) or not effective (25 percent).

*Since beginning the digital transformation process, organizations have seen an average **15 percent** increase in the number of third parties they utilize.*

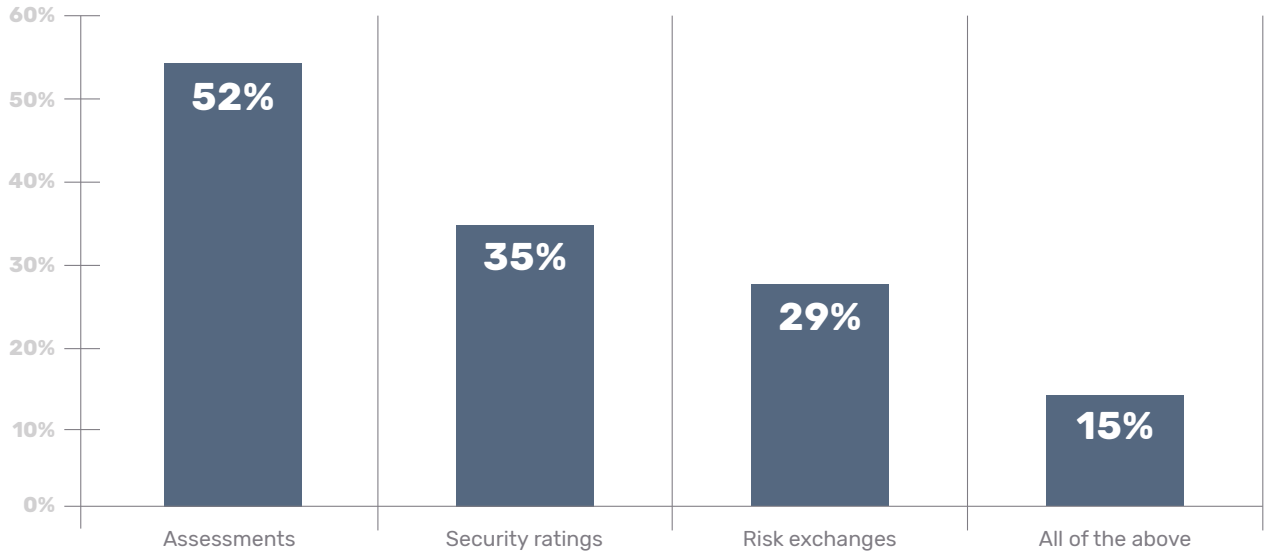


Figure 4
What tools or solutions does your organization use to manage third-party risk?
More than one response permitted

A secure cloud environment is a significant challenge to achieving a successful digital transformation process.

- Sixty-three percent of respondents say their organizations have difficulty ensuring there is a secure cloud environment and 54 percent of IT security say the ability to avoid security exploits is a challenge.
- Fifty-six percent of C-level executives say their organizations find it challenging to ensure third parties have policies and practices that guarantee the security of their information.

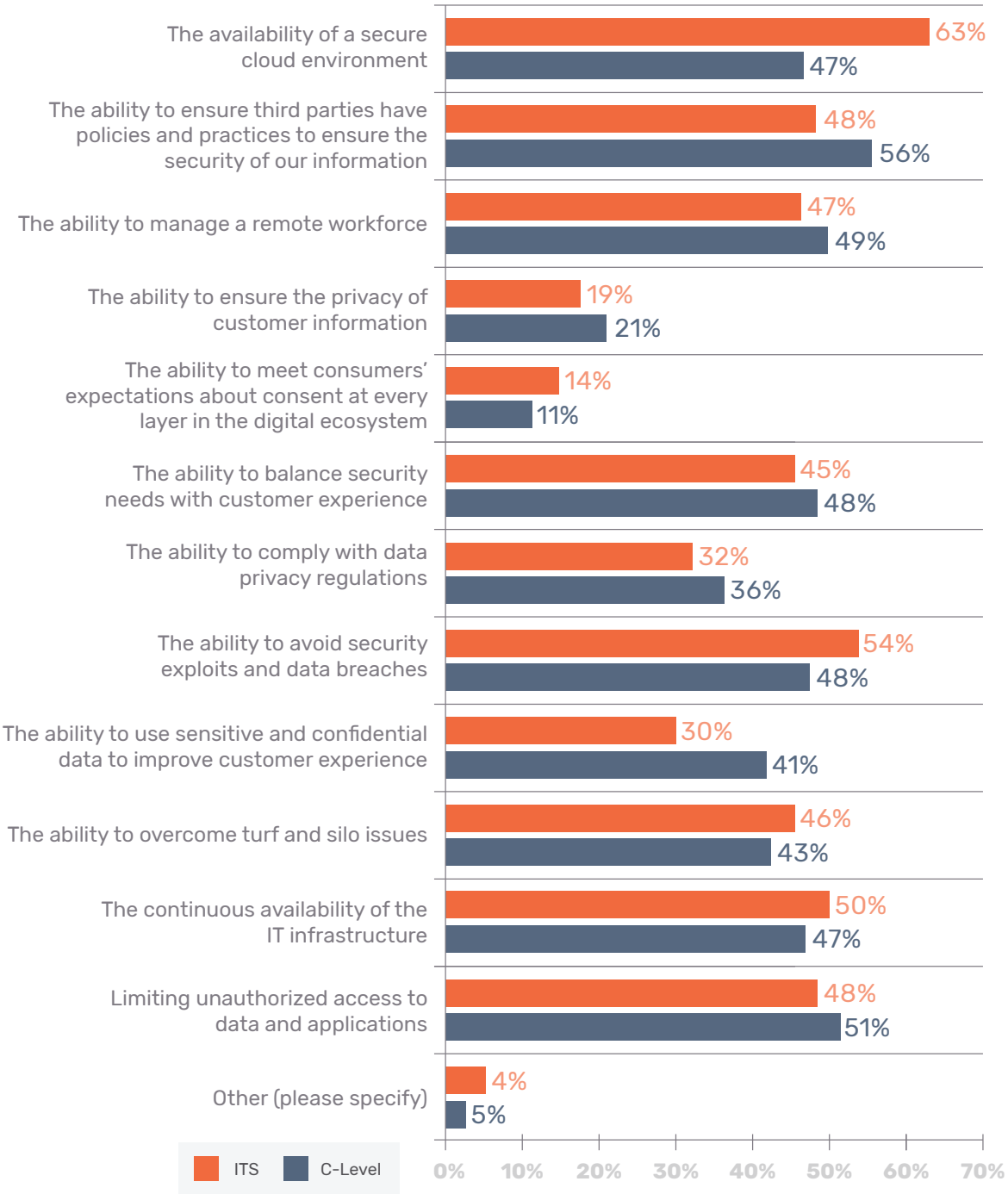


Figure 5
What do you see as the most significant challenges to achieving a secure digital transformation process in your organization today?

Please choose only your top five choices.

Organizations with mature digital transformation programs have more structure and processes in place, as well as higher IT security budgets.

In this study, we analyzed the responses from those organizations that self-reported they have a mature digital transformation process. Twenty-three percent (131) of IT security respondents self-reported that their organizations' core digital transformation activities are deployed, maintained, and refined across the enterprise. We compare the findings from this first group to the 77 percent (450) of the other IT security respondents who reported their organizations did not have a DTP.

Mature organizations are more likely to have strategies to protect data assets and assess third-party relationships.

- Fifty-six percent of the most mature organizations have a strategy for achieving digital transformation.
- In contrast, 47 percent of the other respondents say they have such a strategy.
- Those in mature organizations say their strategies are more likely to protect data assets and assess third-party relationships and vulnerabilities, including supply chain partners.

Mature organizations are more likely to understand and anticipate the risks associated with digital transformation.

- Respondents in mature organizations are far more likely than the other organizations (78 percent vs. 51 percent) to make reducing third-party risk a priority.
- Mature organizations are more likely to recognize the digital economy increases the risk to high value assets such as intellectual property and trade secrets (78 percent vs. 60 percent). Mature organizations are also more likely to believe in the importance of balancing the security of high value assets while enabling the free flow of information and an open business model.

Digital transformation is considered essential to the company's business.

More mature organizations are likely to believe in the importance of IT security to supporting innovation with minimal impact on the goals of digital transformation (90 percent vs. 81 percent) and that digital transformation is essential to the company's business (84 percent vs. 79 percent).

Regardless of size or industry, all organizations struggle with having an adequate budget for protecting data assets during the digital transformation process.

Forty-three percent of respondents in mature organizations vs. 34 percent of other organizations say their budgets are adequate for protecting data assets during the digital transformation process.

Digital transformation impacts industries differently

Across industries digital transformation has significantly increased reliance on third parties, specifically cloud providers, IoT, and shadow IT.

Respondents in healthcare, industrial, and retail say the most significant change caused by digital transformation is the increased migration to the cloud.

The public sector and healthcare industries are less likely to say the increased use of IoT has changed their organizations.

Retail and financial services respondents are most likely to say increased outsourcing to third parties because of digital transformation has had an impact.

Industrial manufacturing is most likely to have a strategy.

Industrial manufacturing has a plan for achieving digital transformation while healthcare is least likely to have a strategy. As part of their strategy, retailers are most likely to include assessing third-party relationships and vulnerabilities, including supply chain partners.

Perceptions of digital transformation risk vary among industries.

Leaders in services and financial services are most likely to recognize that digital transformation creates IT security risk, while leaders in the industrial manufacturing sector are least likely to recognize the risk according to respondents.

Retail, public sector, and services are most concerned about the rush to achieve digital transformation.

Sixty-eight percent of respondents in retail and 65 percent of respondents in both services and public sector say the rush to achieve digital transformation increases the risk of a data breach and/or a cybersecurity exploit.

A successful digital transformation process requires IT security to balance securing digital assets without stifling innovation.

Because digital transformation is considered essential, most industries say that IT security should support innovation with a minimal impact on the goals of digital transformation. Eighty-three percent of respondents in financial services say such a balance is essential.

Most industries do not have a security budget for protecting data assets during the digital transformation process.

Despite the need to have the necessary expertise and technologies to ensure a secure digital transformation process, industries are not allocating funds specifically to digital transformation. Healthcare organizations are most likely to have funds for protecting data assets during the digital transformation process.

Organizational size affects the digital transformation process

The following are the most salient differences according to organizational size. Our analysis looked at organizations with a headcount fewer than 5,000 and then greater than 10,000.

Larger organizations are seeing the greatest impact due to increased outsourcing to third parties.

The increased migration to the cloud and the use of IoT have the greatest impact on smaller organizations during the global transformation.

Larger organizations are far more likely to recognize the risk of digital transformation.

- Seventy-nine percent of respondents in larger organizations vs. 61 percent of respondents in smaller organizations believe the rush to achieve digital transformation increases the risk of a breach and/or cybersecurity exploit.
- Larger organizations are less likely to say that it is important to balance security with the need to enable the free flow of information.
- Seventy-two percent of respondents in larger organizations say digital transformation increases risk to high value assets such as intellectual property and trade secrets.

More larger organizations have a strategy for digital transformation.

- Larger organizations (54 percent of respondents) are more likely than smaller organizations (43 percent of respondents) to have a strategy for achieving digital transformation.
- As part of their strategy, 80 percent of respondents in larger organizations vs. 69 percent of respondents in smaller organizations are assessing third-party relationships and vulnerabilities, including supply chain partners, as part of their digital strategy.

Smaller organizations are more likely to be vulnerable to a cyberattack or data breach following digital transformation.

Seventy-one percent of respondents in smaller organizations and 64 percent of respondents in larger organizations believe the risk of digital transformation makes it more likely to have a data breach or cyberattack.

Larger organizations are more likely to say the rush to produce and release apps, the increased use of shadow IT, and increased migration to the cloud have made their organizations more vulnerable following digital transformation.

Challenges for securing the future of digital transformation

Budgets are and will continue to be inadequate to secure the digital transformation process.

Only 35 percent of respondents say they have such a budget. If they do, these budgets are and will continue to be inadequate to secure the digital transformation process.

Because of the risks created by digital transformation, respondents believe the percentage of IT security budget allocated to digital transformation today should almost be doubled from an average of 21 percent up to 37 percent.

In two years, the average percentage will be only 37 percent and respondents say ideally it should be 45 percent.

Only 29%
of respondents say they are very prepared to address these threats

More progress needs to be made in the ability to mitigate cyber threats.

- The top three threats respondents are most concerned about are system downtime, cybersecurity attacks, and data breaches caused by third parties.
- Currently, only 29 percent say they are very prepared to address these threats.
- In two years, only 43 percent are very optimistic their organizations will be very prepared to reduce the risk of these threats.

A secure digital transformation process is dependent upon the expertise of the IT security team and they are not very influential.

- Today, only 35 percent of respondents say IT security is very influential.
- In the next two years, their influence increases only slightly and 43 percent of respondents predict IT security will be very influential.

Part 3

Detailed Findings

In this section, we present a detailed analysis of the key findings. In some instances, we highlight the differences between IT Security and C-level respondents. Otherwise, we show the consolidated findings for the 883 respondents. The complete audited findings are presented in the Appendix of this report.

The report is organized according to the following themes:

- The impact of the digital transformation revolution on organizations
- Third-party risk in the digital transformation process
- Risks to the digital transformation process
- Industry differences in the digital transformation process
- Organizational size differences in the digital transformation process
- Conclusion: Recommendations on how to secure the digital transformation process

The impact of the digital transformation revolution on organizations.

Digital transformation has significantly increased reliance on third parties, specifically cloud providers, IoT, and shadow IT. It is important to focus on the security risks created by changes to the organization. Specifically, as shown in Figure 6, 58 percent of respondents say the primary change to their organizations is increased migration to the cloud. This is followed by the increased use of IoT and increased use of shadow IT.

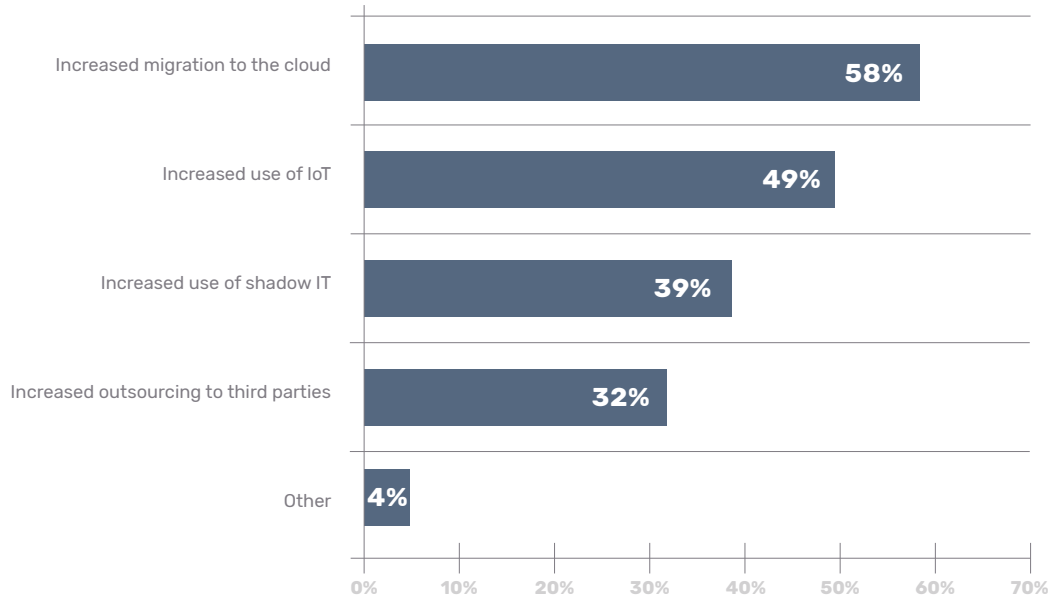


Figure 6
How has digital transformation changed your organization?

More than one response permitted

A successful digital transformation process requires IT security to balance the securing of digital assets without stifling innovation. By necessity, digital transformation requires innovation and new approaches to transform the organization for a digital world. As shown in Figure 7, 80 percent of respondents say it is essential that IT security supports innovation with minimal impact on the goals of digital transformation. Another 80 percent of respondents say digital transformation is essential to their businesses.

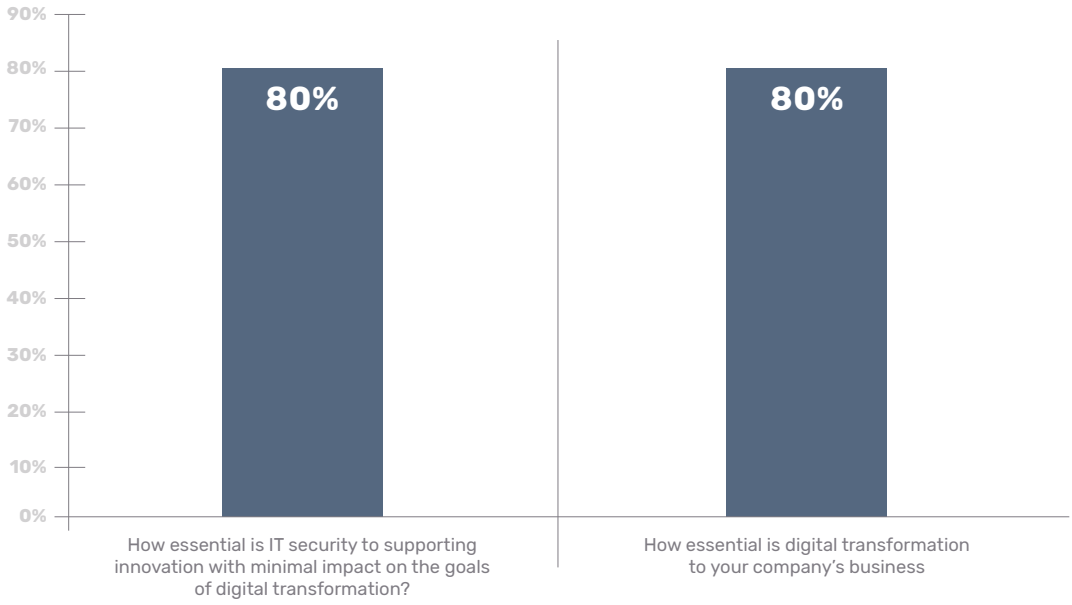


Figure 7
The importance of digital transformation and the role of IT security

Essential and Very important responses combined

More C-level respondents than IT security respondents say their organizations have a strategy for digital transformation. Forty-nine percent of IT security respondents and 56 percent of C-level respondents say their organizations have a strategy for achieving digital transformation. As shown in Figure 8, the top two issues covered in the strategies relate to the security of third-party relationships and the protection of data assets.

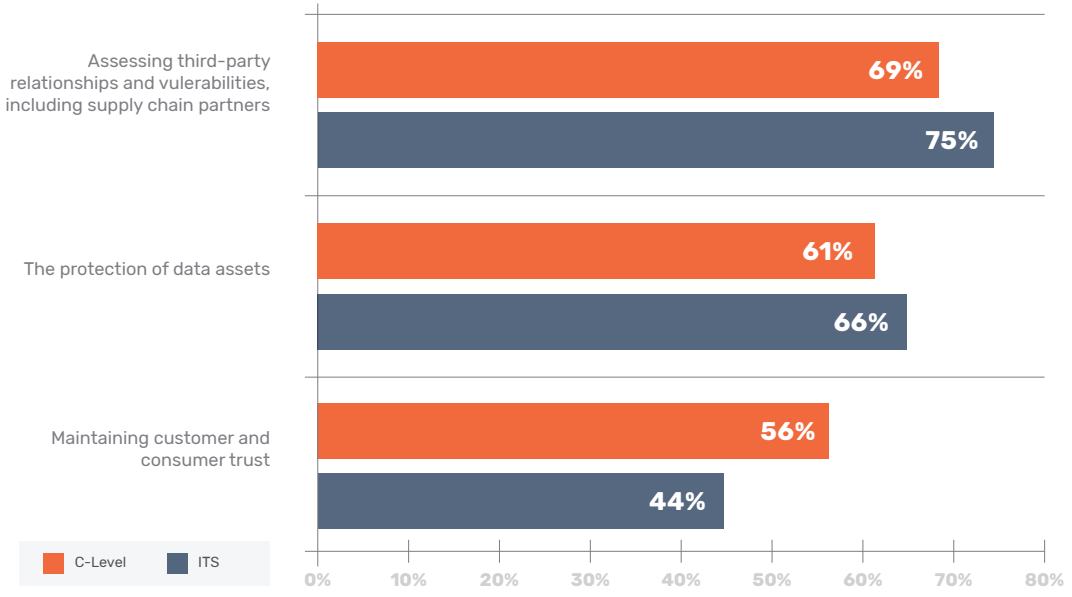


Figure 8
What does your organization's digital transformation strategy cover?

Yes responses presented

Organizations are mostly using a combination of in-house and outsourced service providers to manage the security of the digital transformation process. According to Figure 9, 39 percent of respondents say their organizations have a hybrid approach to securing the digital transformation process. Only 25 percent of respondents say security is totally outsourced.

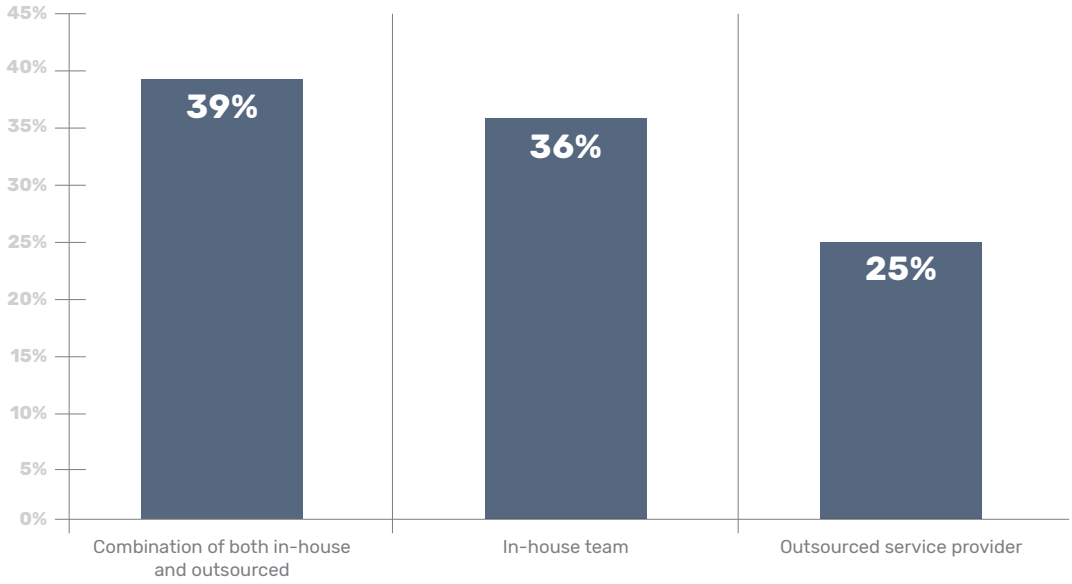


Figure 9
How does your organization manage the security of the digital transformation process?

The functions most responsible for the digital transformation process are sales and marketing. One of the most important goals of digital transformation is improved customer relations, which may explain why sales and marketing are most often the functions responsible for digital transformation. As shown in Figure 10, only 17 percent of respondents say IT security is mostly responsible for the process.

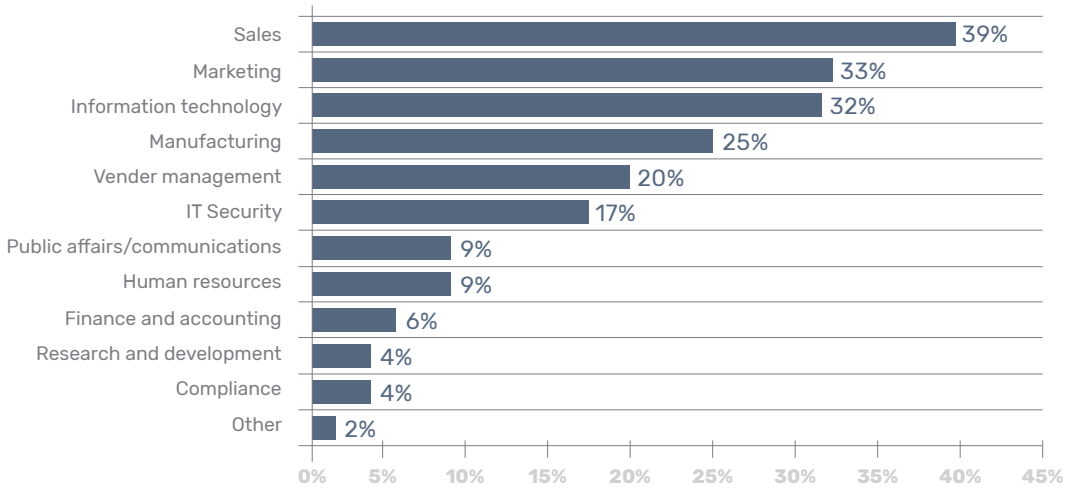


Figure 10
Which departments are assuming the most responsibility for the organization's digital transformation process?

Two responses permitted

IT security has very little involvement in directing efforts to ensure a secure digital transformation process. According to Figure 11, lines of business and the leader of data sciences are most responsible for ensuring the security of the digital transformation process. Thirty-seven percent of respondents say the CIO is most involved. Only 24 percent of respondents say it is the CISO.

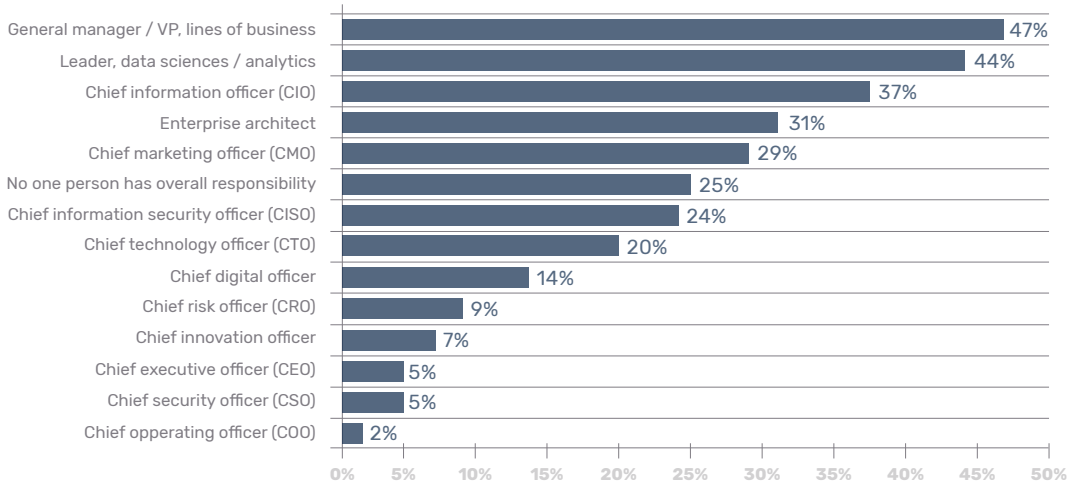


Figure 11
Who are most involved in directing efforts to ensure a secure digital transformation process?

Three responses permitted

While IT security is not often directing the digital transformation process, they are expected to increase their influence over the next two years, as shown in Figure 12.

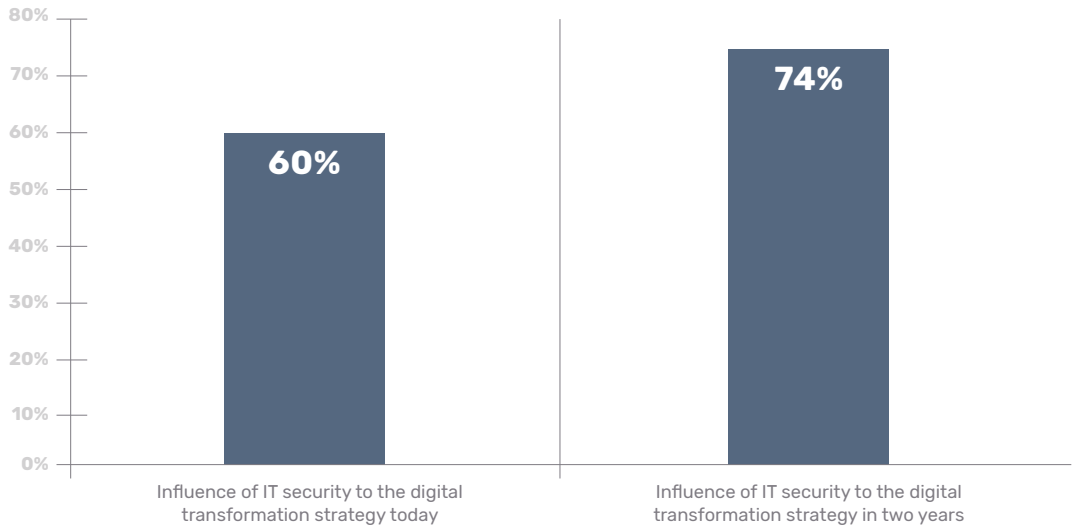


Figure 12
How influential is IT security to the digital transformation process today and in two years?

Very influential and influential responses combined

Third-party risks in the digital transformation process.

Digital transformation increases the number of organizations' third parties. According to Figure 13, on average, organizations have 5,884 third parties and this is expected to increase to 6,774 in the next 12 months.

Since beginning the digital transformation process, organizations have seen, on average, a 15 percent increase in the number of third parties used. However, we believe organizations will become even more reliant on third parties with the trends of increased migration to the cloud and increased use of shadow IT.

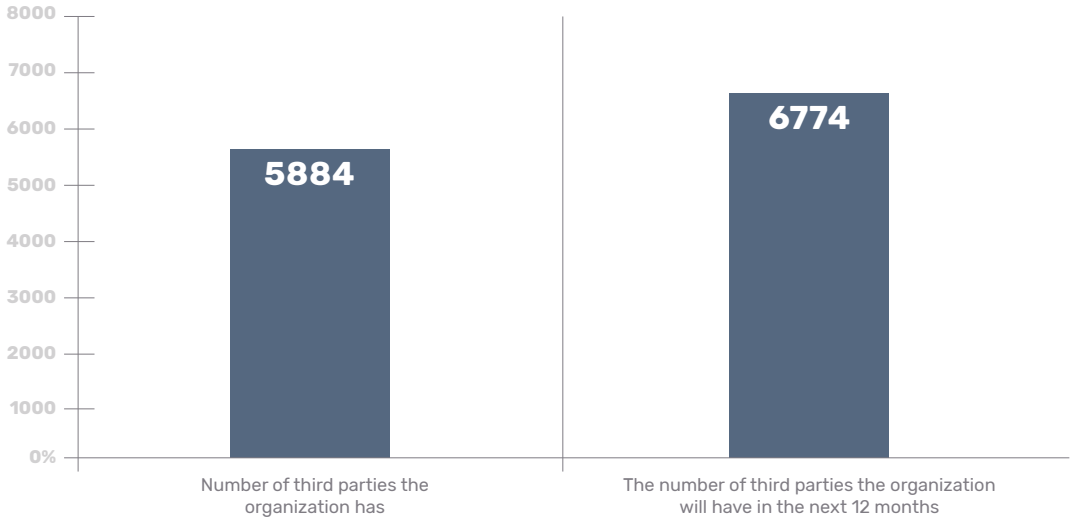


Figure 13
How many third parties does your organization have today vs. in the next 12 months?

Extrapolated values presented

IT security is more likely to believe their organization is managing third-party risk through due diligence but most C-level respondents do not believe their organization is making third-party risk management a priority. Only 42 percent of respondents say their organizations have a third-party cyber risk management program to ensure that their third parties have the appropriate data security practices in place.

As shown in Figure 14, more IT security respondents (62 percent) than C-level respondents (56 percent) believe their organization feel it's important to conduct due diligence before engaging third parties. And less than half (48 percent) of C-level respondents agree that their organization makes it a priority to determine if third parties have the people, processes, and technologies in place to ensure the data stored or shared with them is safeguarded.

By not making it a priority, organizations risk having a data breach. As discussed previously, 82 percent of respondents believe they had a data breach because of digital transformation and 55 percent of respondents say that at least one was caused by a third party.

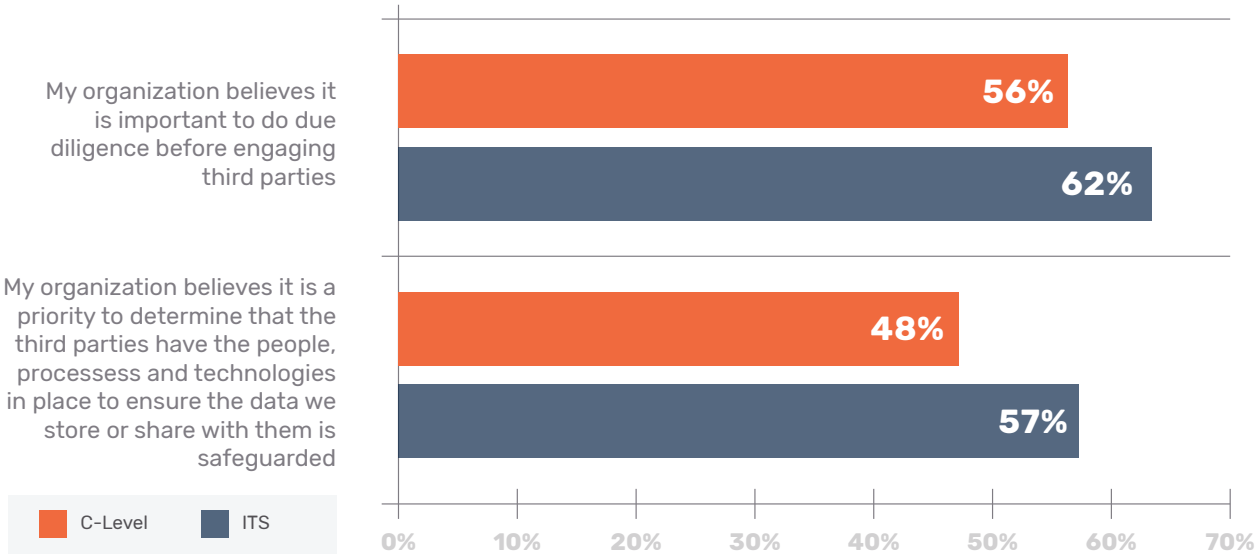


Figure 14
Perceptions about third-party risk

Strongly agree and Agree responses presented

Current tools or solutions to manage third-party risk are not effective. Slightly more than half (51 percent) of organizations represented in this research have a strategy for achieving digital transformation and of these, 73 percent say their strategy involves assessing third-party relationships and vulnerabilities.

As previously discussed, 42 percent of respondents have a third-party cyber risk management program. Figure 15 presents the tools or solutions their organizations use in their third-party risk management programs. The most commonly used are assessments (52 percent of respondents). Only 15 percent of respondents say they use all these solutions.

When asked if they are effective, 53 percent say the tools and solutions are only somewhat effective (28 percent) or not effective (25 percent). IT security respondents (61 percent) are more likely to say their organizations' leaders recognize the need to invest in emerging security technologies than C-level respondents (43 percent).

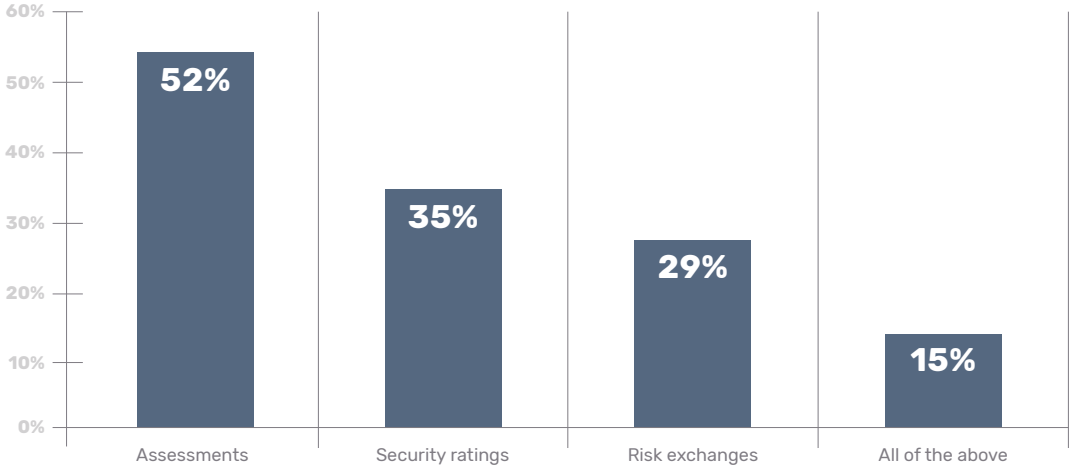


Figure 15
What tools or solutions does your organization use to manage third-party risk?

More than one response permitted

Security risks caused by digital transformation process

Conflicting priorities between IT security teams and the C-suite create vulnerabilities and risk. Only 16 percent of respondents say IT security and lines of business are fully aligned with respect to achieving a secure digital transformation process. As shown in Figure 16, there are significant gaps in perceptions about risks created by the digital transformation process.

Specifically, far more IT security respondents (64 percent) than C-level respondents (41 percent) say that the digital economy significantly increases risk to high value assets such as IP and trade secrets. Sixty-three percent of C-level respondents do not want the security measures used by IT security of these assets to prevent the free flow of information and an open business model vs. 41 percent of IT security respondents. IT security respondents also believe in having strict security safeguards to protect the sharing and using of data that is critical to operations (65 percent of IT security respondents vs. 53 percent of C-level respondents)

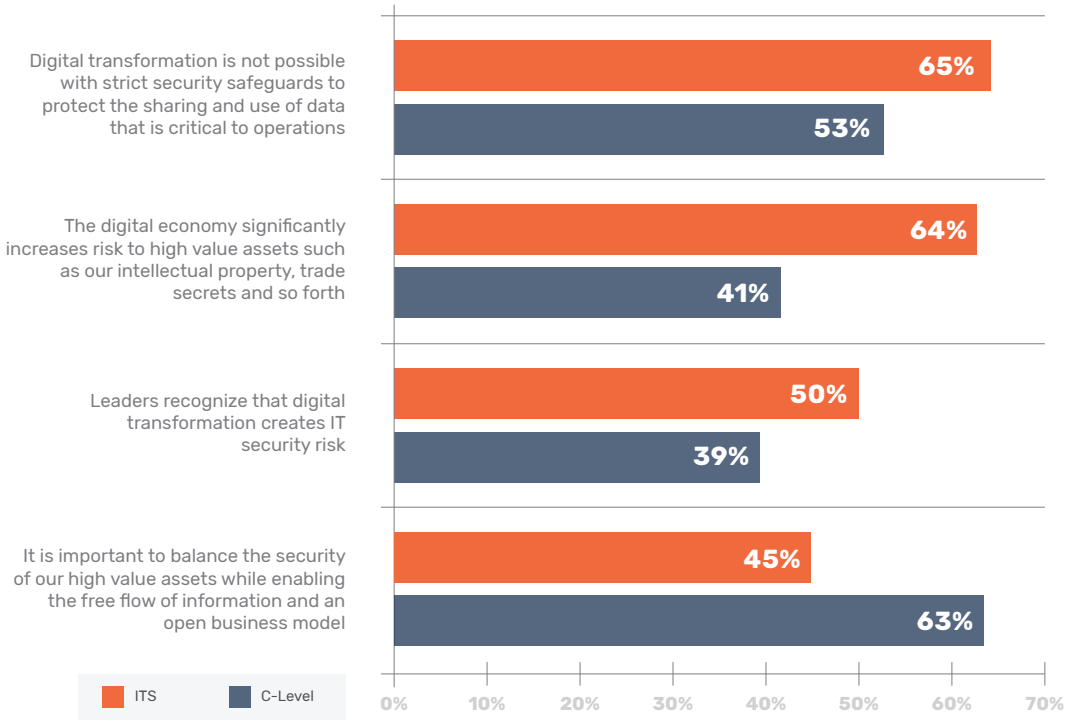


Figure 16
Perceptions about security risks caused by digital transformation process

Strongly agree and Agree responses presented

Digital transformation increases the likelihood of a data breach or cyberattack. Seventy-one percent of C-level respondents and 67 percent of IT security respondents say their organizations are much more vulnerable or somewhat vulnerable to a security incident following digital transformation, as shown in Figure 17.

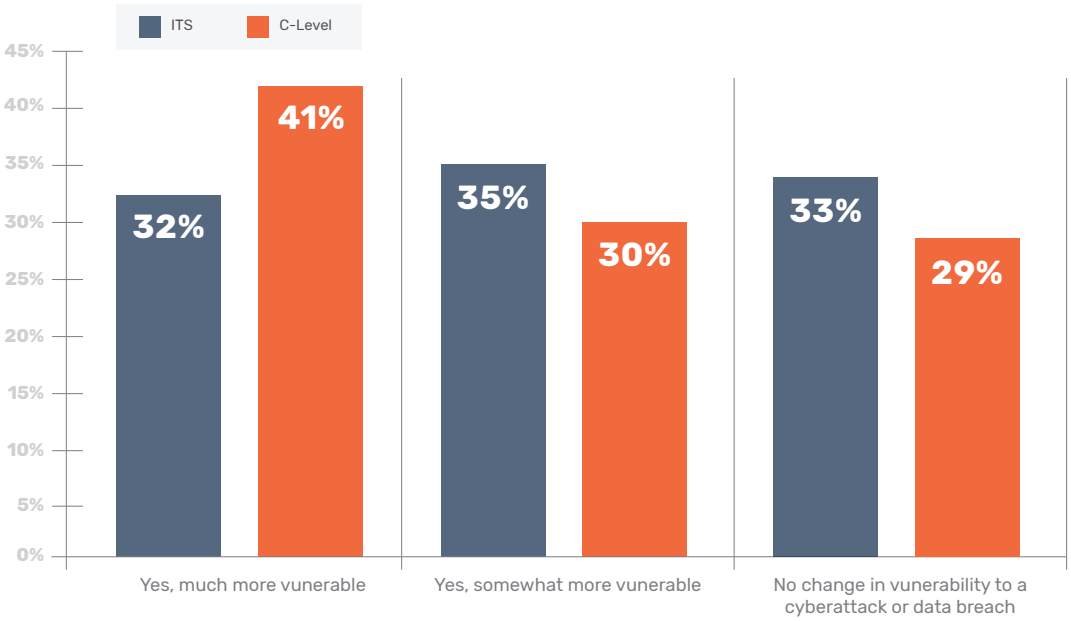


Figure 17
How vulnerable is your organization to a data breach or cyberattack following digital transformation?

IT security respondents are more likely to say the rush to produce and release apps and the increased usage of shadow IT are the primary reasons their organizations are more vulnerable following digital transformation, as shown in Figure 18. In contrast, C-level respondents say increased migration to the cloud and increased outsourcing to third parties makes a security incident more likely.

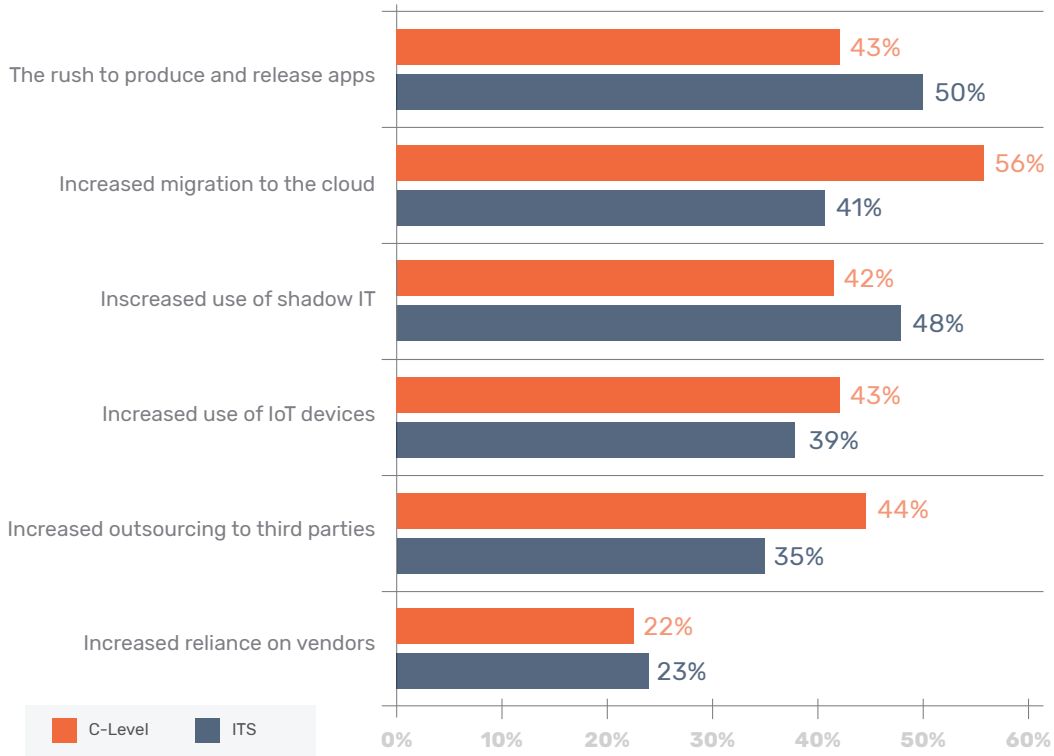


Figure 18
If yes, what caused the increase in vulnerability to a cyberattack or data breach?

More than one response permitted

Most respondents say with certainty or that it is likely their organization experienced at least one data breach or cyber exploit. As shown in Figure 19, 22 percent of respondents say with certainty their organizations had an average of four data breaches in the last 12 months during the digital transformation process. Fifty-five percent of respondents say that at least one of these breaches was caused by a third party. Twenty-two percent of respondents say with certainty their organizations had an average of 18 cyber exploits that infiltrated their networks or enterprise systems.

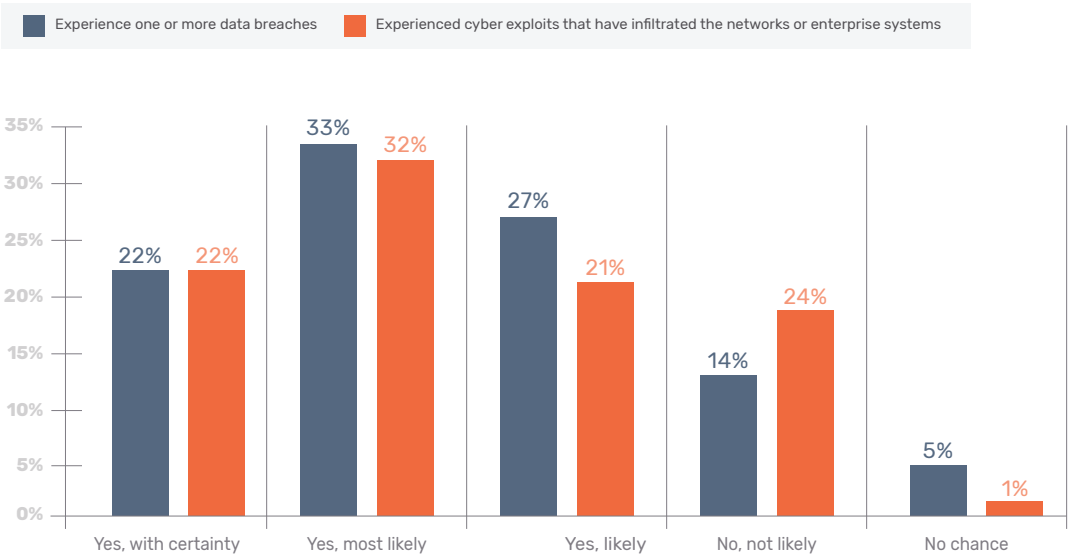


Figure 19
Has insecure digital transformation caused one or more data breaches or cyber exploits that infiltrated your networks or enterprise systems in the last 12 months?

As shown in Figure 20, the consequences of these data breaches or cyber exploits were disruptions or damages to critical infrastructure and lost intellectual property.

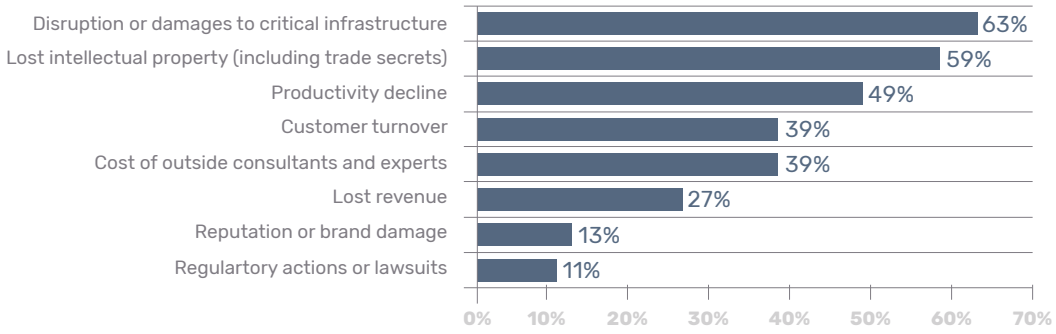


Figure 20
Which negative consequences could your organization have experienced because of these data breaches or cyber exploits?

Three responses permitted

Figure 21 shows that in the next two years the top three threats organizations will be most concerned about because of digital transformation are system downtime, cybersecurity attacks, and data breaches caused by third parties.

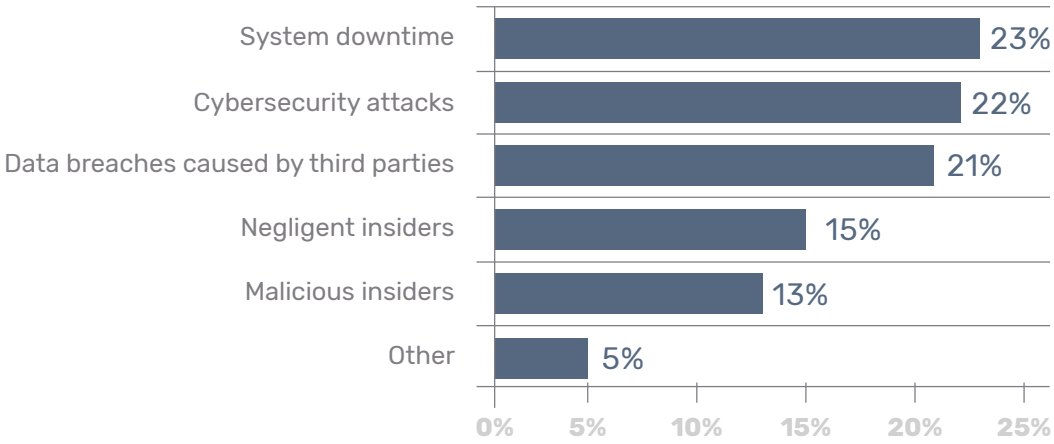


Figure 21
In two years, what threats will your organization be most concerned about because of digital transformation?

Please select only one choice

Furthermore, organizations are not confident that they will be prepared to reduce the risk of these threats. Respondents rated their preparedness to mitigate the threats listed above on a scale of 1= not prepared to 10= very prepared. Figure 22 presents the very prepared responses (9+).

As shown, C-level respondents and IT security respondents are not very confident in their preparedness to mitigate the risk of these threats. In two years, only 45 percent of IT security respondents say their organizations will be very prepared to reduce these threats and only 40 percent of C-level respondents rate their preparedness as very high.

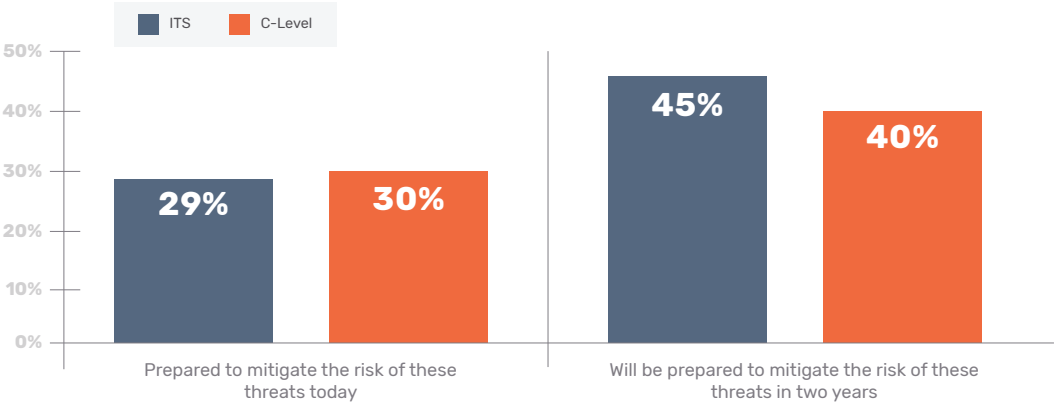


Figure 22
How prepared is your organization today and in two years to mitigate the risk of these threats?

On a scale from 1 = not prepared to 10 = very prepared, 9+ responses presented

Industry differences in digital transformation.

In this section, we provide the most salient differences among the industries represented in this research. Industries included are financial services (FS), healthcare (HC), services (SV), industrial (IM), retail (RT), and public sector (PS).

Across industries, digital transformation has significantly increased reliance on third parties, specifically cloud providers, IoT, and shadow IT. According to Figure 23, respondents in healthcare, industrial, and retail say the most significant change caused by digital transformation is the increased migration to the cloud. The public sector and healthcare industries are less likely to say the increased use of IoT has changed their organizations. Retail and financial services respondents are most likely to say increased outsourcing to third parties is the most significant change caused by digital transformation.

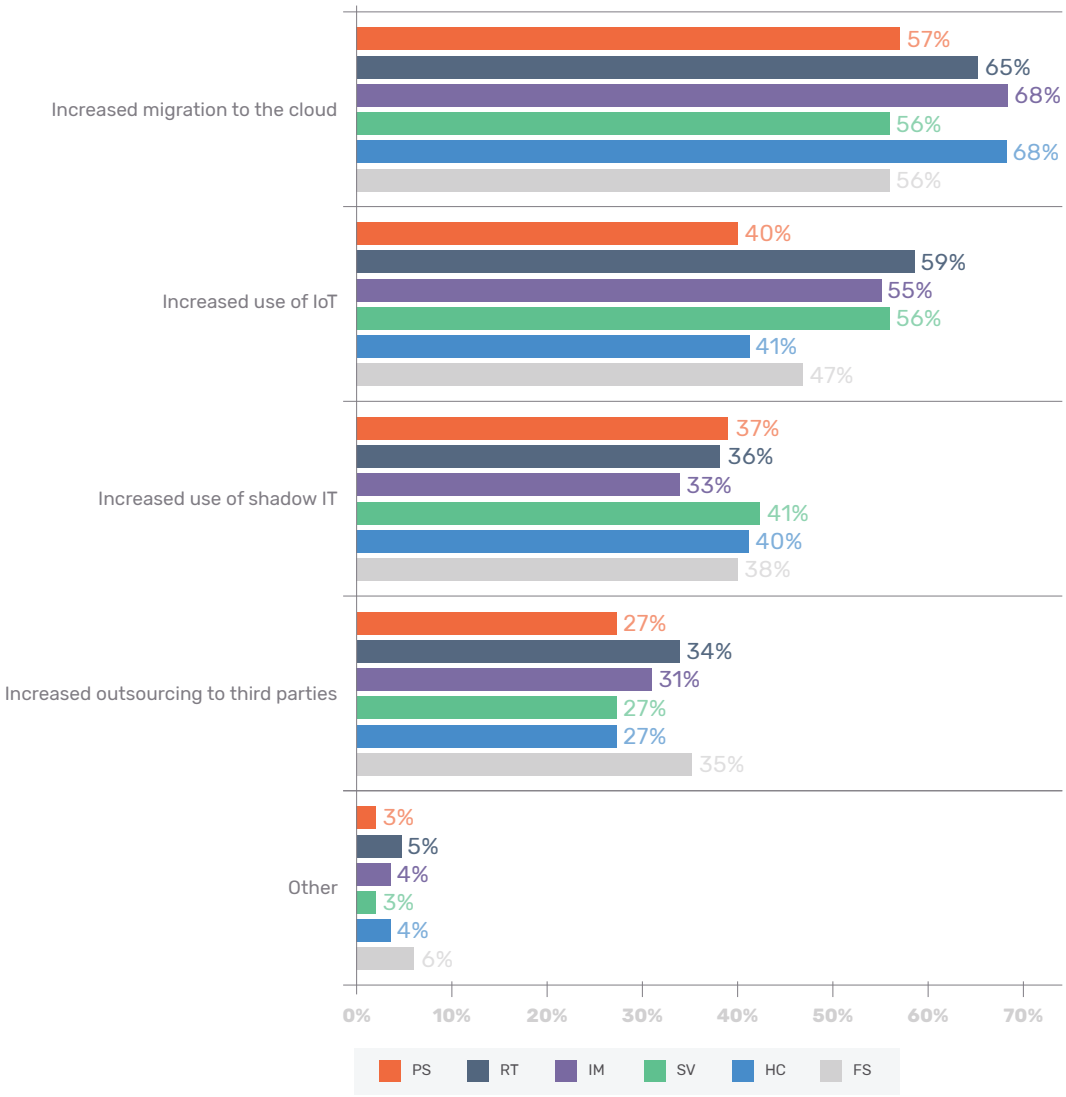


Figure 23
How has digital transformation changed your organization?

Perceptions about digital transformation varies among industries. Leaders in services and financial services are most likely to recognize that digital transformation creates IT security risk, as shown in Figure 24 while respondents in the industrial manufacturing sector are least likely to say their leaders recognize the risk.

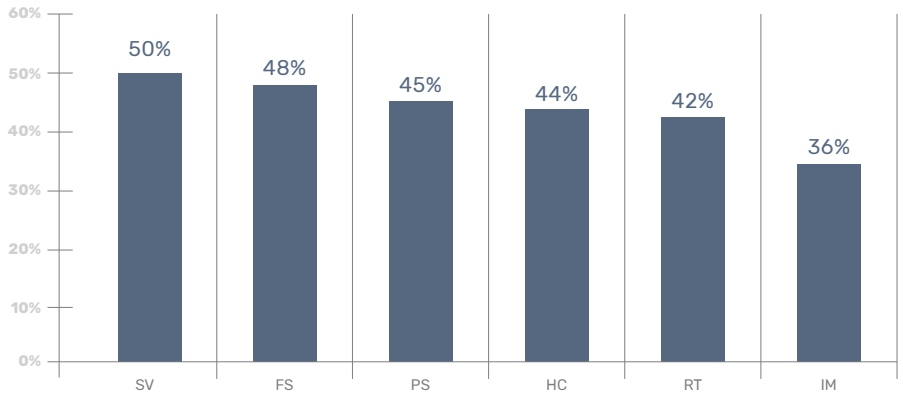


Figure 24
My organization's leaders recognize that digital transformation creates IT security risk

Strongly agree and Agree responses presented

Industrial manufacturing is most likely to have a strategy for achieving digital transformation while healthcare is least likely to have a strategy, as shown in Figure 25.

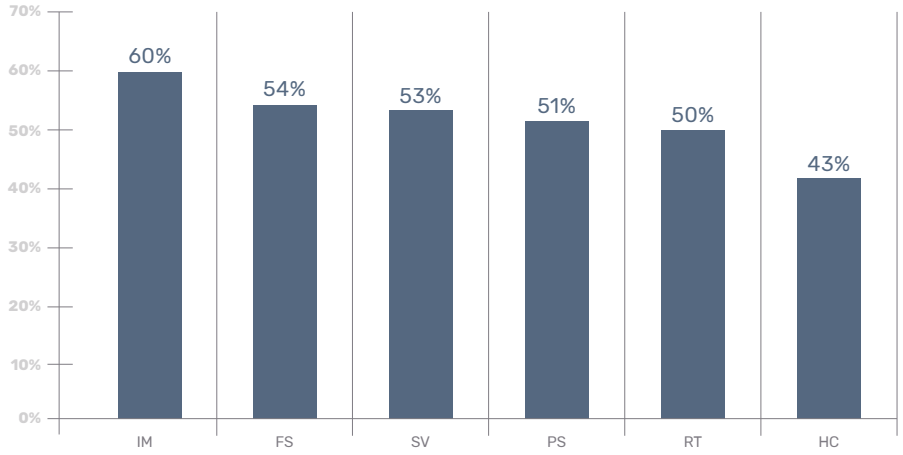


Figure 25
Figure 22. Does your organization have a strategy for achieving digital transformation?

Yes responses presented

According to Figure 26, as part of their strategy, retailers are most likely to include assessing third-party relationships and vulnerabilities, including supply chain partners.

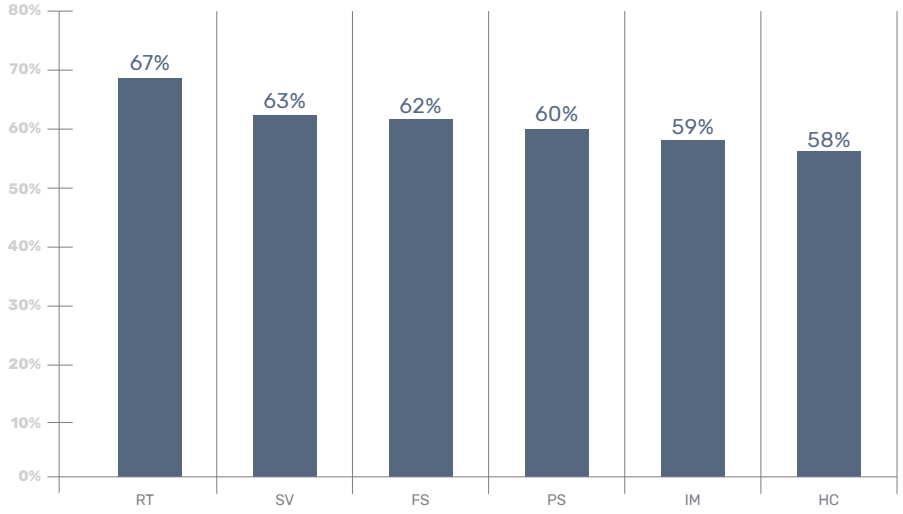


Figure 26
Does the strategy involve assessing third-party relationships and vulnerabilities, including supply chain partners?

Yes responses presented

Retail, public sector, and services are most concerned about the rush to achieve digital transformation. According to Figure 27, 68 percent of respondents in retail, 65 percent of respondents in services and public sector say the rush to achieve digital transformation increases the risk of a data breach and/or a cybersecurity exploit.

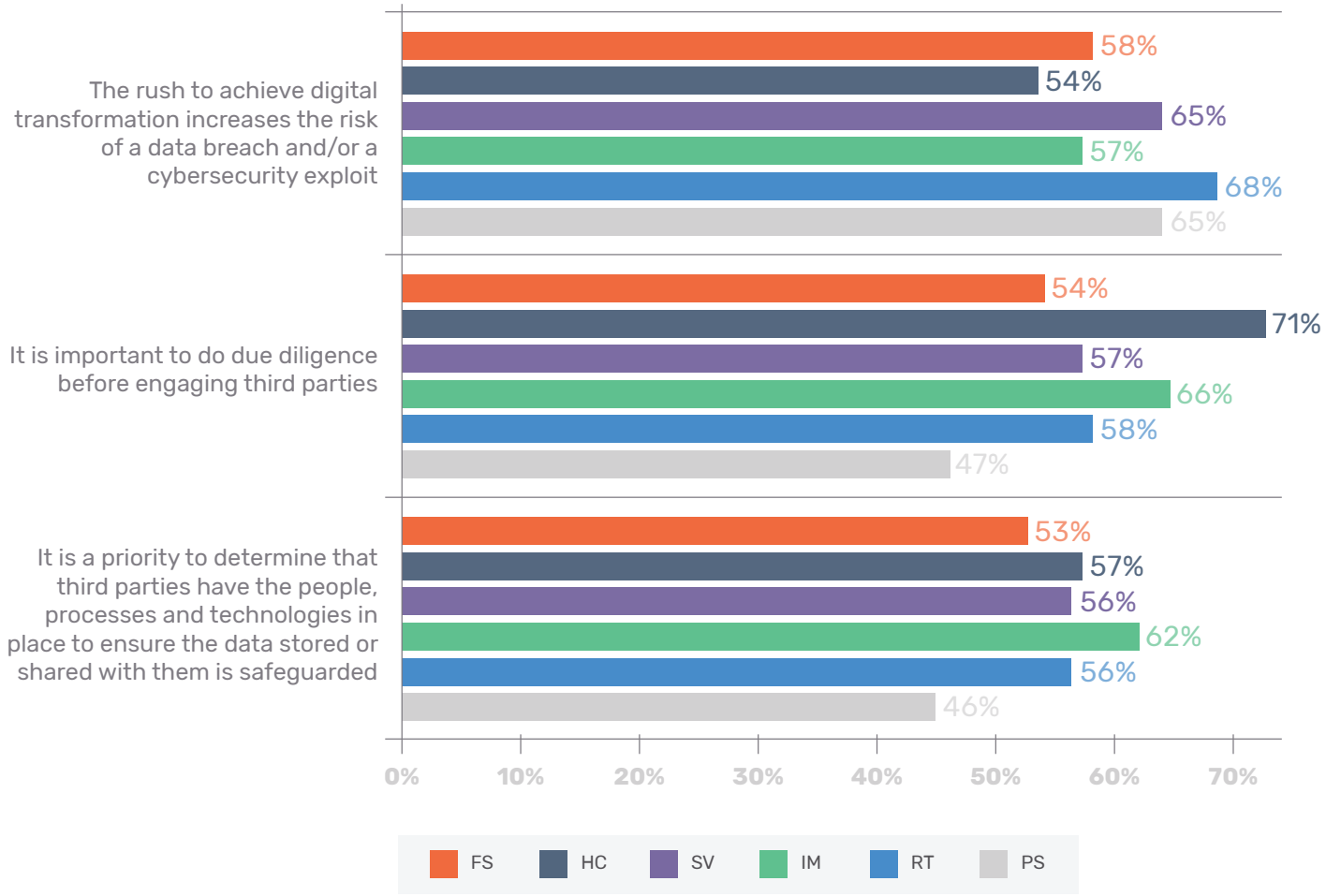


Figure 27
Perceptions about managing third-party risk

Strongly agree and Agree responses presented

A successful digital transformation process requires IT security to balance the securing of digital assets without stifling innovation. Because digital transformation is considered essential, most industries say that IT security should support innovation with a minimal impact on the goals of digital transformation. As shown in Figure 27, 83 percent of respondents in financial services say such a balance is essential.

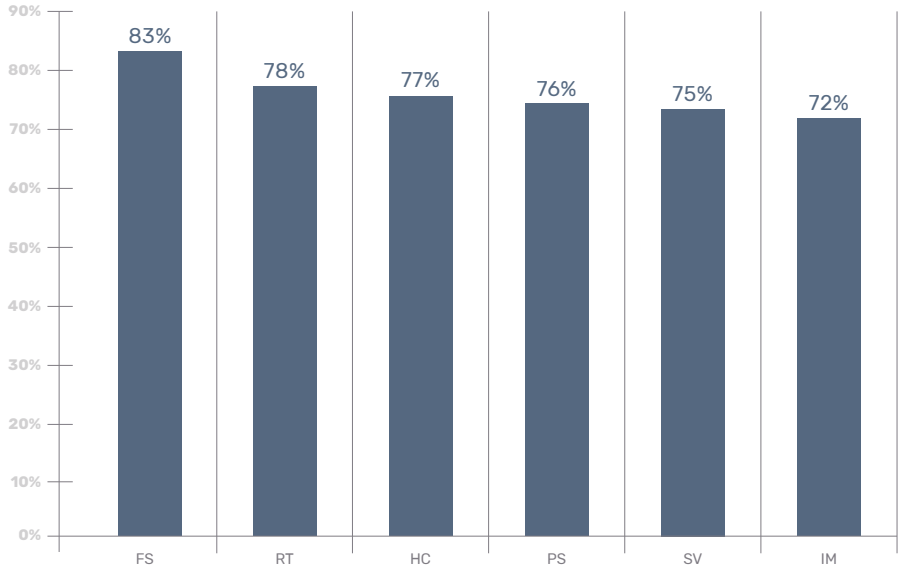


Figure 27
How essential is IT security to supporting innovation with minimal impact on the goals of digital transformation?

Essential and important responses presented

Most industries do not have a security budget for protecting data assets during the digital transformation process. Despite the need to have the necessary expertise and technologies to ensure a secure digital transformation process, industries are not allocating funds specifically to digital transformation. Healthcare organizations are most likely to have funds for protecting data assets during the digital transformation process, as shown in Figure 28.

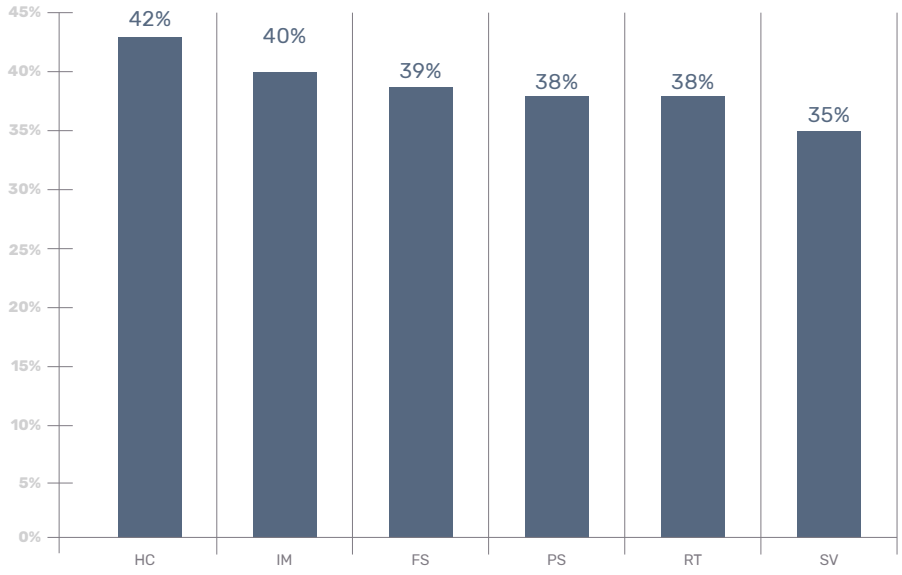


Figure 28
Does your organization have a security budget for protecting data assets during the digital transformation process?

Yes responses presented

Organizational size differences in digital transformation.

The following are the most salient differences according to organizational size. Our analysis looked at organizations with a headcount fewer than 5,000 and then greater than 10,000.

The increased migration to the cloud and the use of IoT are having the greatest impact during the global transformation on smaller organizations. Larger organizations are seeing the greatest impact due to increased outsourcing to third parties, as shown in Figure 29.

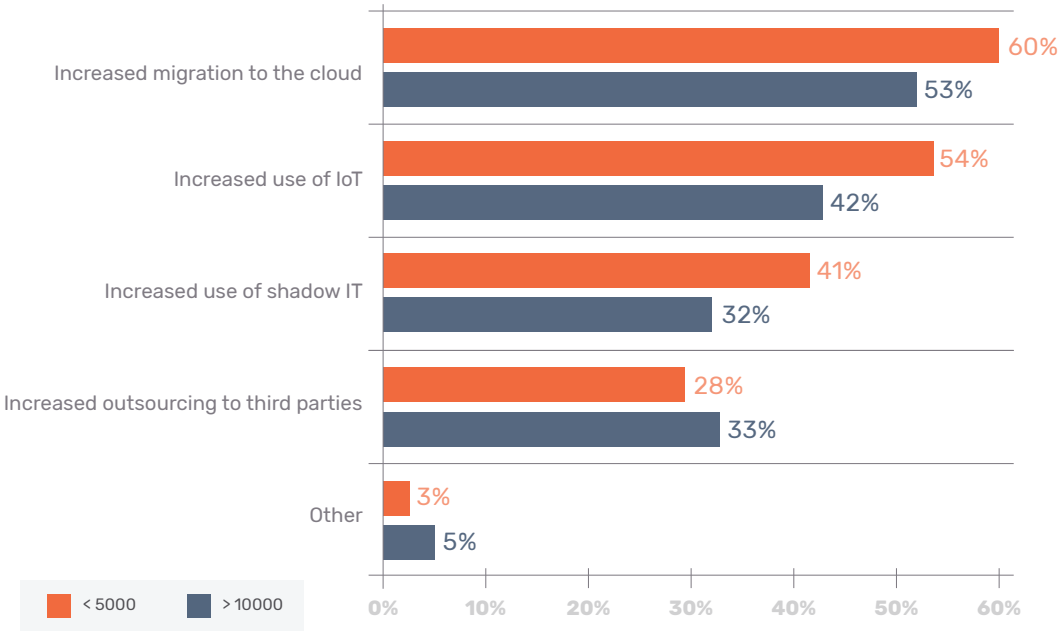


Figure 29
How has digital transformation changed your organization?

More than one response permitted

More larger organizations have a strategy for digital transformation. According to Figure 30, larger organizations (54 percent of respondents) are more likely than smaller organizations (43 percent of respondents) to have a strategy for achieving digital transformation.

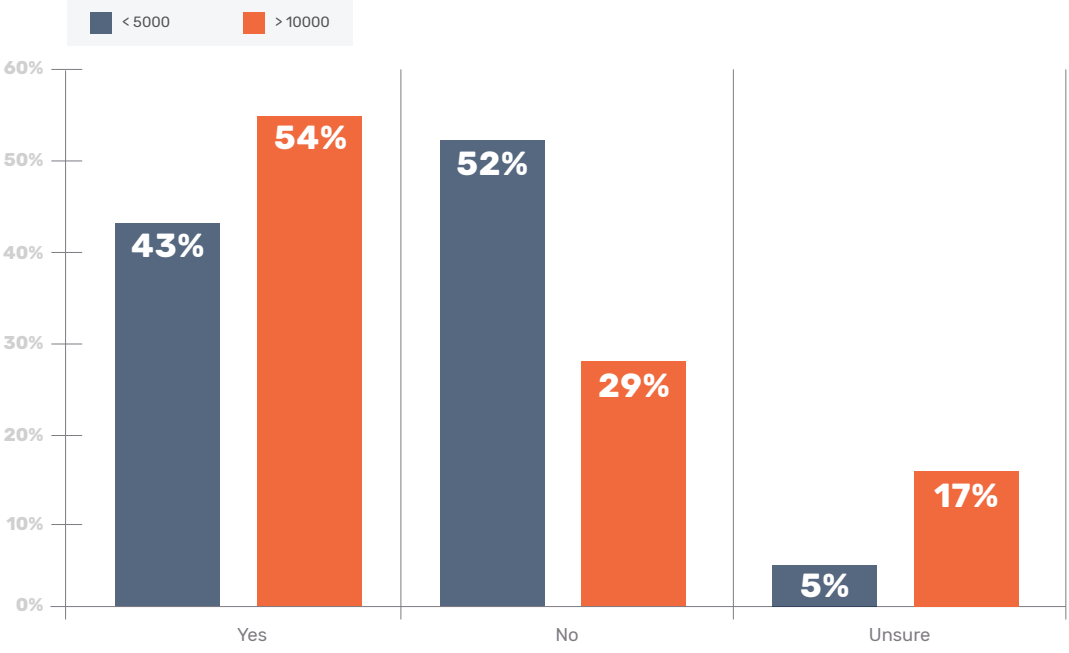


Figure 30
Does your organization have strategy for achieving digital transformation?

More larger organizations are assessing third-party relationships and vulnerabilities, including supply chain partners, as part of their digital transformational strategy, as shown in Figure 31.

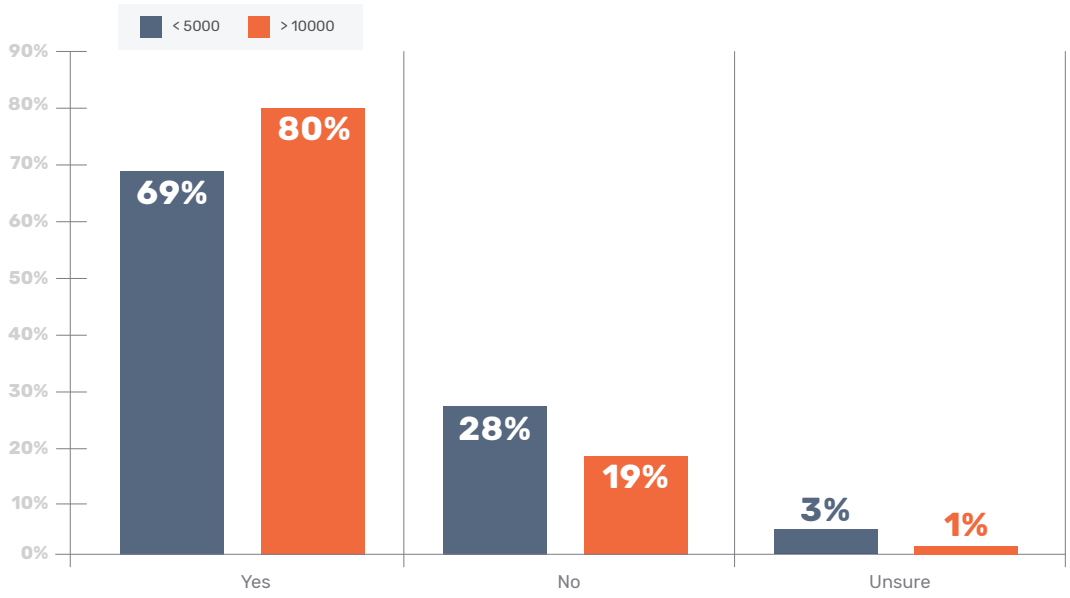


Figure 31
Does the strategy involve assessing third-party relationships and vulnerabilities, including supply chain partners?

Larger organizations are far more likely to recognize the risk of digital transformation. As shown in Figure 32, 79 percent of respondents in larger organizations vs. 61 percent of respondents in smaller organizations believe the rush to achieve digital transformation increases the risk of a breach and/or cybersecurity exploit. Larger organizations are less likely to say that it is important to balance security with the need to enable the free flow of information. Seventy-two percent of respondents in larger organizations say digital transformation increases risk to high value assets such as intellectual property and trade secrets.

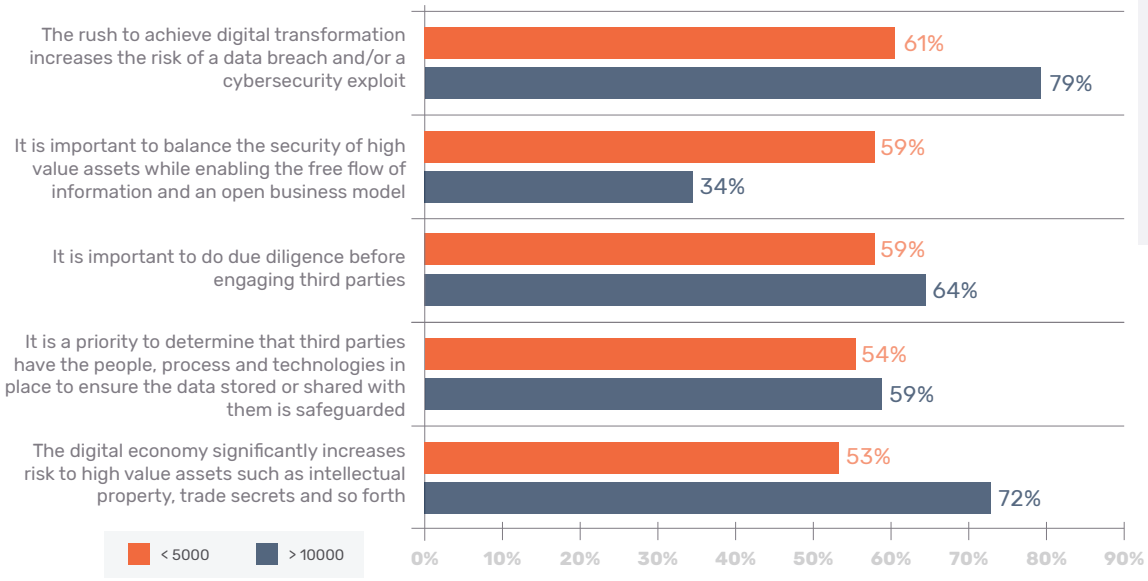


Figure 32
Perceptions about digital transformation

Strongly agree and Agree responses presented

Smaller organizations are more likely to be vulnerable to a cyberattack or data breach following digital transformation. Seventy-one percent of respondents in smaller organizations and 64 percent of respondents in larger organizations believe the risk of digital transformation makes it more likely to have a data breach or cyberattack.

According to Figure 33, larger organizations are more likely to say the rush to produce and release apps, the increased use of shadow IT, and increased migration to the cloud have made their organizations more vulnerable following digital transformation.

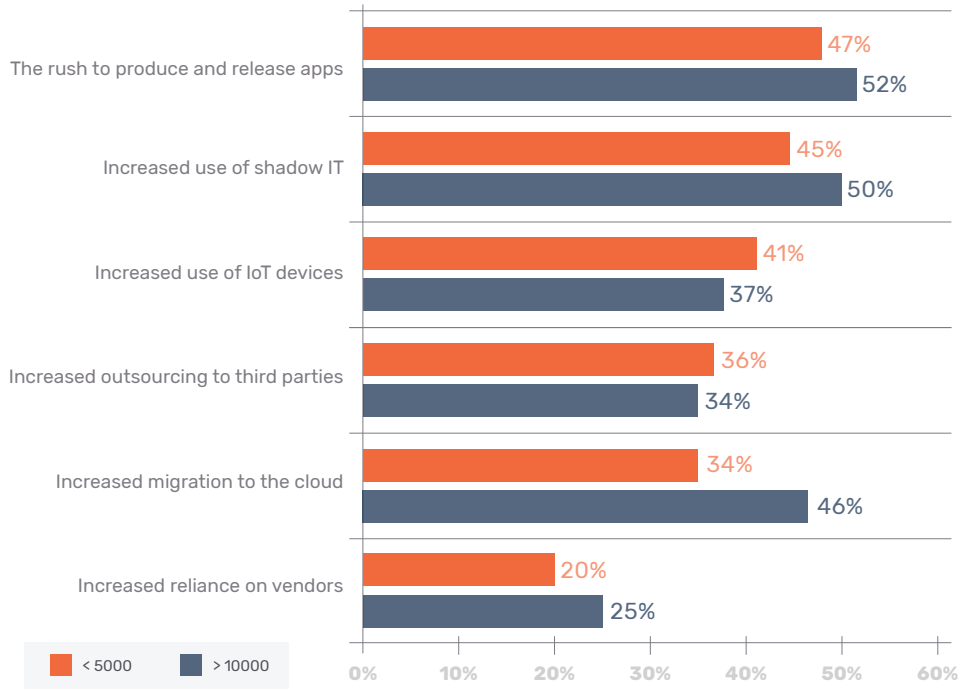


Figure 33
Is your organization more vulnerable to a cyberattack or data breach because of digital transformation?

Part 4

10 Recommendations on how to secure the digital transformation process

The recommendations in this section are based on the challenges and opportunities identified in the survey responses as well as best practices identified by the organizations that reported they have a mature digital transformation process in place.

1

Copy the best practices and security procedures that work best for your organization, organizations with mature digital transformation processes in place, and your peers.

Figure 34 presents the steps organizations are taking to secure confidential information during the digital transformation process. Encryption for data in transit and data at rest and extended manual procedures are the top three steps taken.

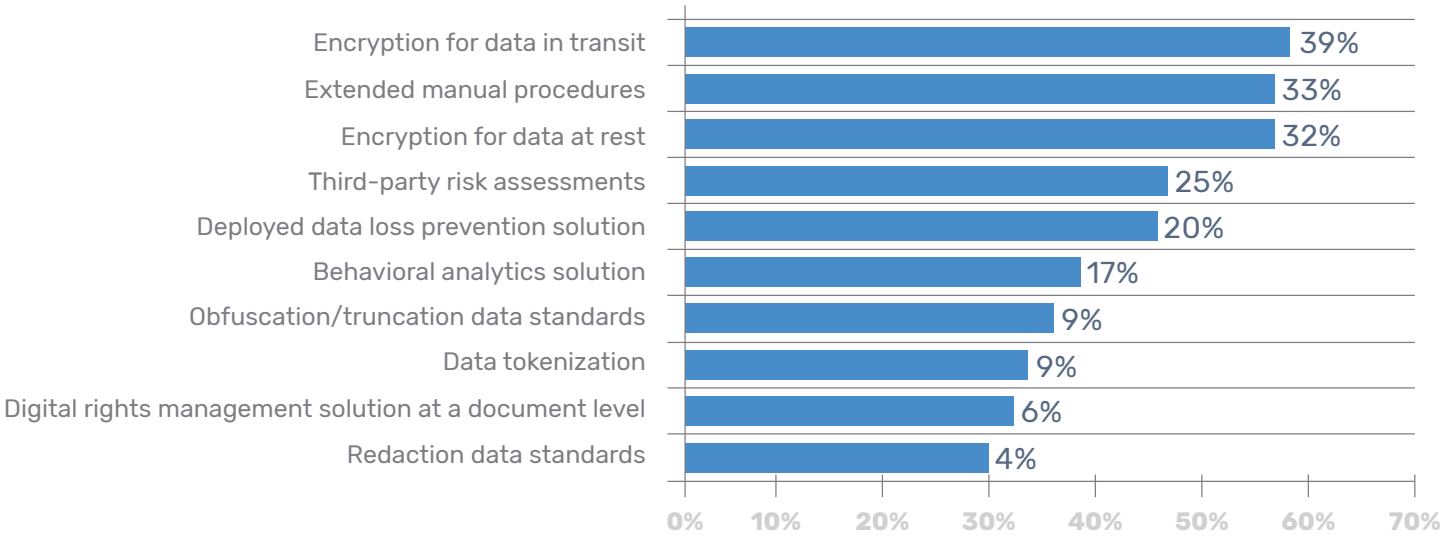


Figure 34
What steps does your organization take to protect sensitive and confidential information?

More than one response permitted

2

Involve your organization's IT security team in the digital transformation process.

As shown in Figure 35, more mature organizations are likely to believe in the importance of IT security to supporting innovation with minimal impact on the goals of digital transformation (90 percent vs. 81 percent) and that digital transformation is essential to the company's business (84 percent vs. 79 percent).

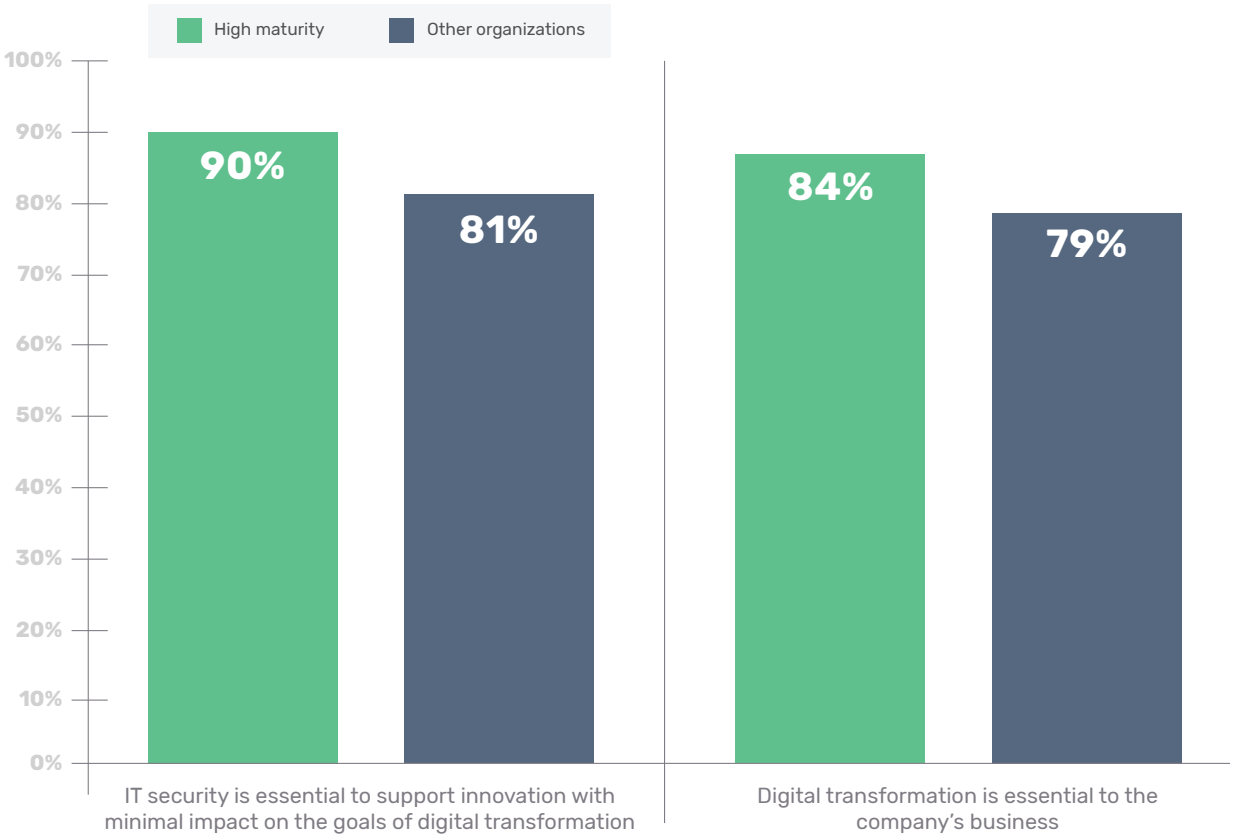


Figure 35
Essential components for a successful digital transformation process

Essential and Very important responses combined

3

Recognize and educate your colleagues on the risks associated with digital transformation.

Don't forget to educate your organization and C-Level. When asked about the top steps taken to provide a secure digital transformation process, educating the C-suite and board of directors was at the bottom of the list. As shown in figure 36, only 26 percent reported taking that step. This could explain the misalignment that currently exists between IT security and C-level respondents.

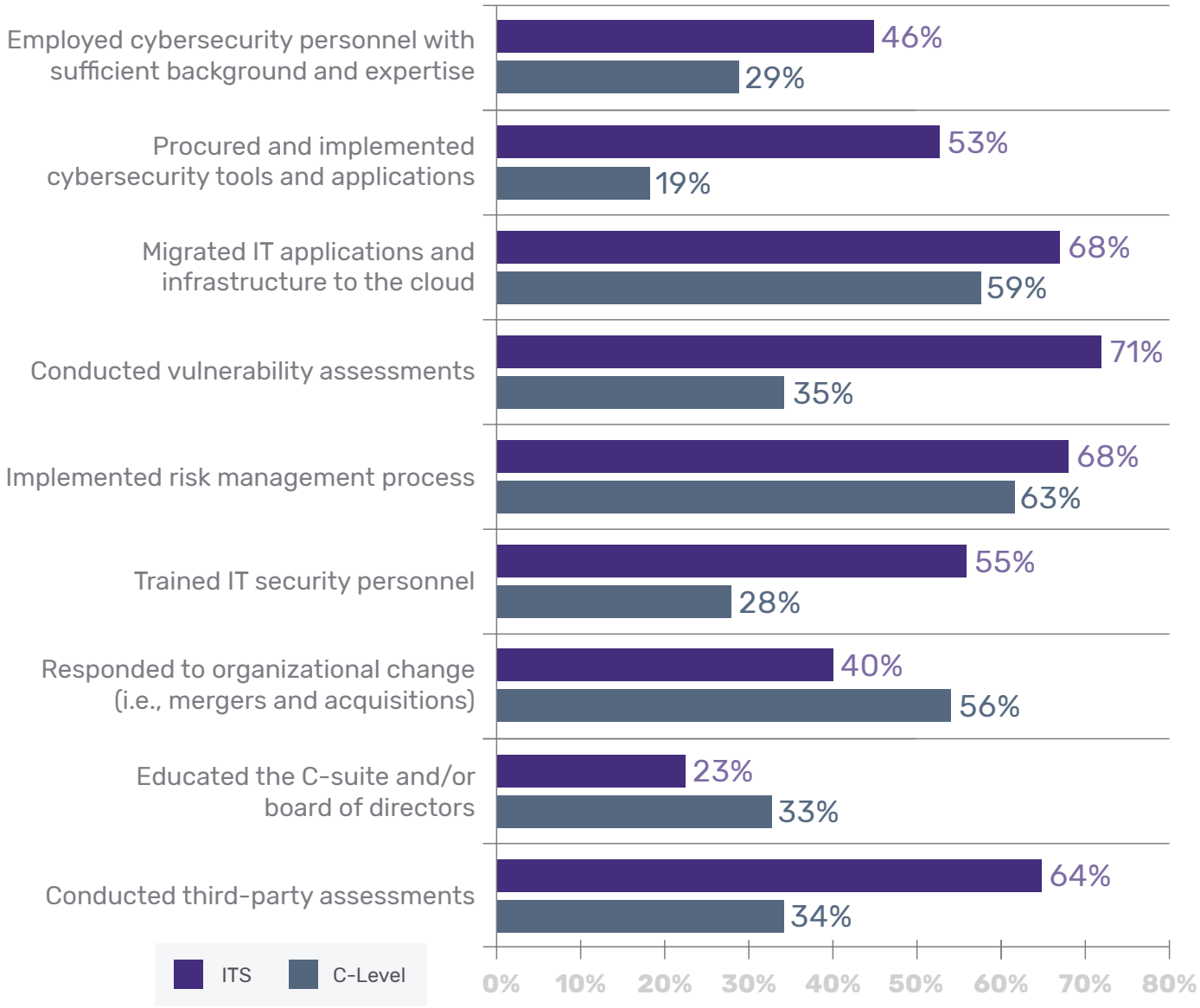


Figure 36
What are the top things you did to provide a secure digital transformation process within your organization?

Please select all that apply.

Mature organization understand and anticipate the risks associated with digital transformation. In Figure 37, respondents in mature organizations are far more likely to make reducing the third-party risk a priority than the other organizations (78 percent vs. 51 percent). Mature organizations are also more likely to recognize the digital economy increases the risk to high value assets such as intellectual property and trade secrets (78 percent vs. 60 percent). Mature organizations are also more likely to believe in the importance of balancing the security of our high value assets while enabling the free flow of information and an open business model (62 percent vs. 40 percent).

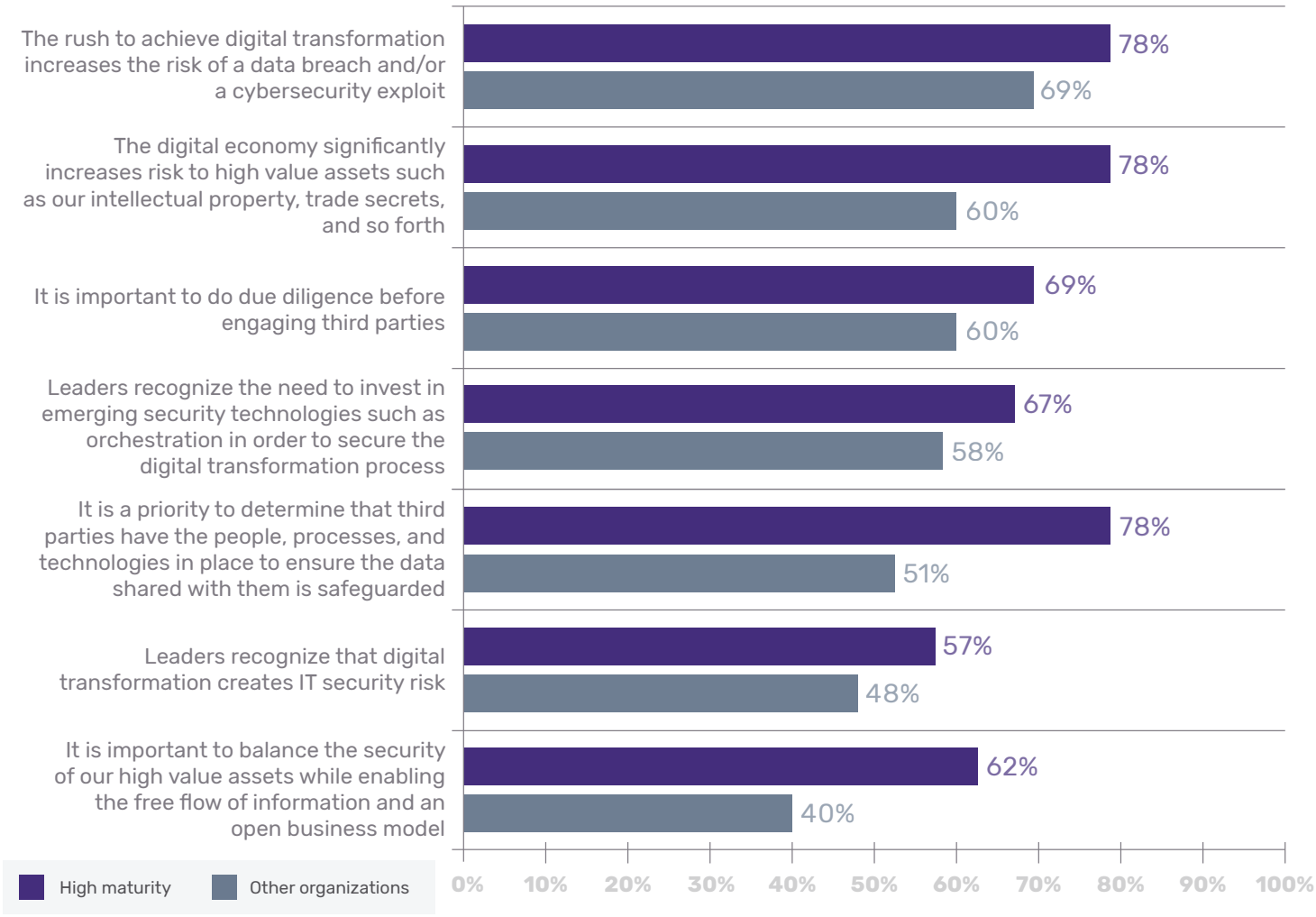


Figure 37
Perceptions about digital transformation

Strongly agree and Agree responses combined

4

Create a strategy to protect what matters most.

Currently, organizations are not protecting their most critical assets. Analytics (data models) are the most vulnerable during the digital transformation process. Figure 38 presents the digital assets that are the most difficult to secure and those that are appropriately secured. Fifty-one percent of respondents say analytics are the most difficult secure and only 35 percent of respondents say they are appropriately secured. This is followed by 44 percent of respondents who say private communications are the most difficult to secure and only 38 percent of respondents say they are appropriately secured.

In contrast, respondents are most confident that trade secrets and financial information are appropriately secured, however only 25 percent and 20 percent respectively say these assets are the most difficult to secure. It is also noteworthy that only 25 percent of respondents are confident that consumer data, which is considered sensitive and confidential, is secure, even though 90 percent do not believe it is difficult to secure that data.

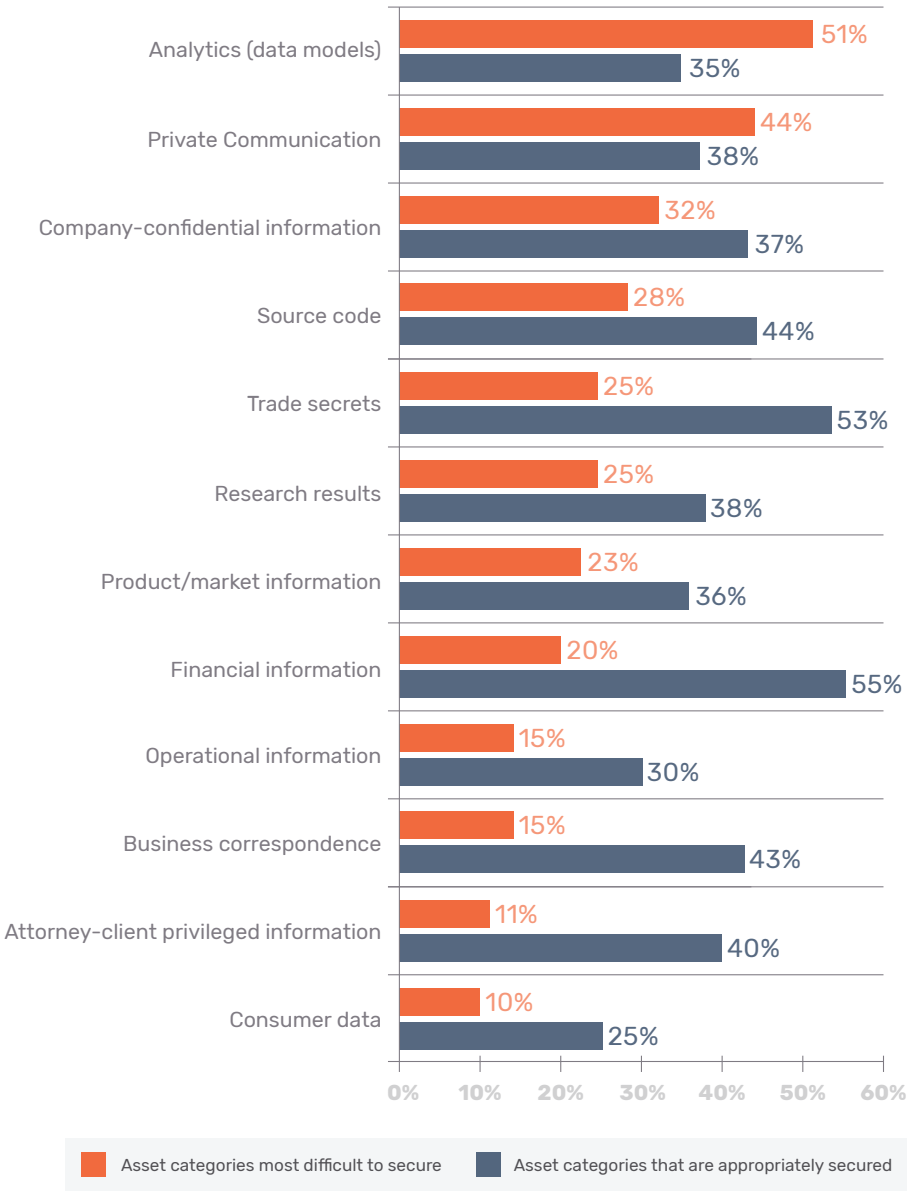


Figure 38
Which digital assets are most difficult to secure and are appropriately secured?

More than one response permitted

High Confidence and Some Confidence responses combined

5

Ensure your strategy involves the protection of data assets and assessment of third-party relationships.

Fifty-six percent of the most mature organizations have a strategy for achieving digital transformation. In contrast, 47 percent of the other respondents say they have such a strategy. As shown in Figure 39, those in mature organizations say their strategies are more likely to protect data assets and assess third-party relationships and vulnerabilities, including supply chain partners.

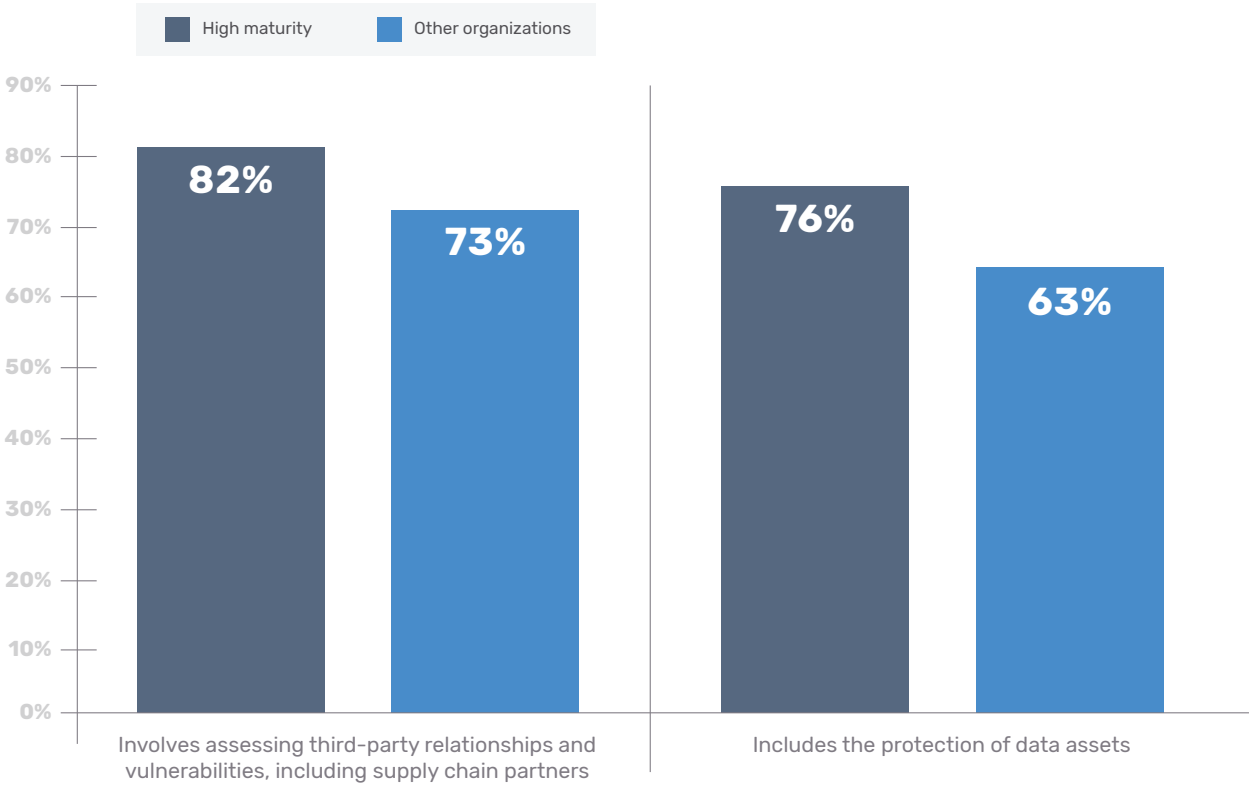


Figure 39
The differences between the strategies of mature and other organizations

Yes responses presented

6

Leverage the growing awareness among senior management to bring in innovative and emerging technologies to reduce risk.

As discussed, digital transformation means increased cyber risk due to the outsourcing to third parties. The good news is most of senior management recognize the need to use emerging technologies to have a secure digital management process.

According to Figure 40, 55 percent of respondents say their organizations' leaders recognize the need to invest in emerging security technologies such as modern third-party cyber risk management solutions to secure the digital transformation process. Fifty-nine percent of respondents say their senior management recognizes the need to invest in emerging technologies such as orchestration in order mitigate any risks.

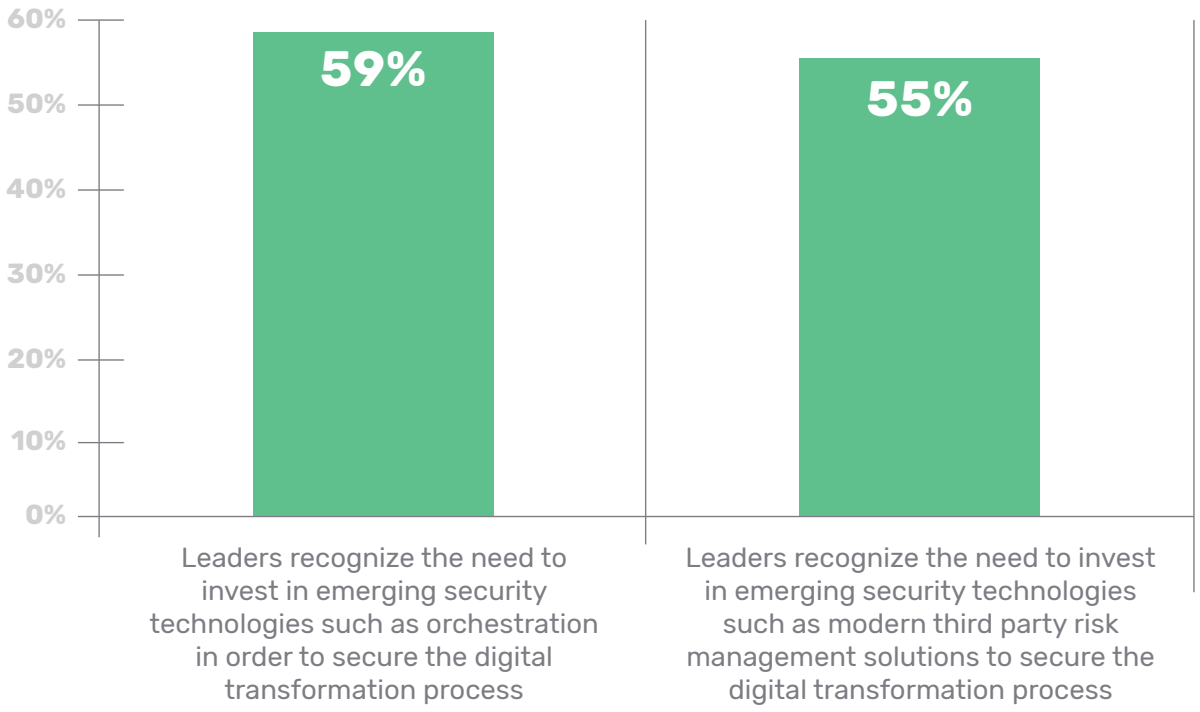


Figure 40
Perceptions about the need to invest in emerging security technologies

Strongly agree and Agree responses presented

7

Invest in skilled personnel and increase organizational visibility.

According to Figure 41, more than half of respondents say the lack of expertise and visibility into what employees are doing and business processes are the most significant barriers to achieving a secure digital transformation process.

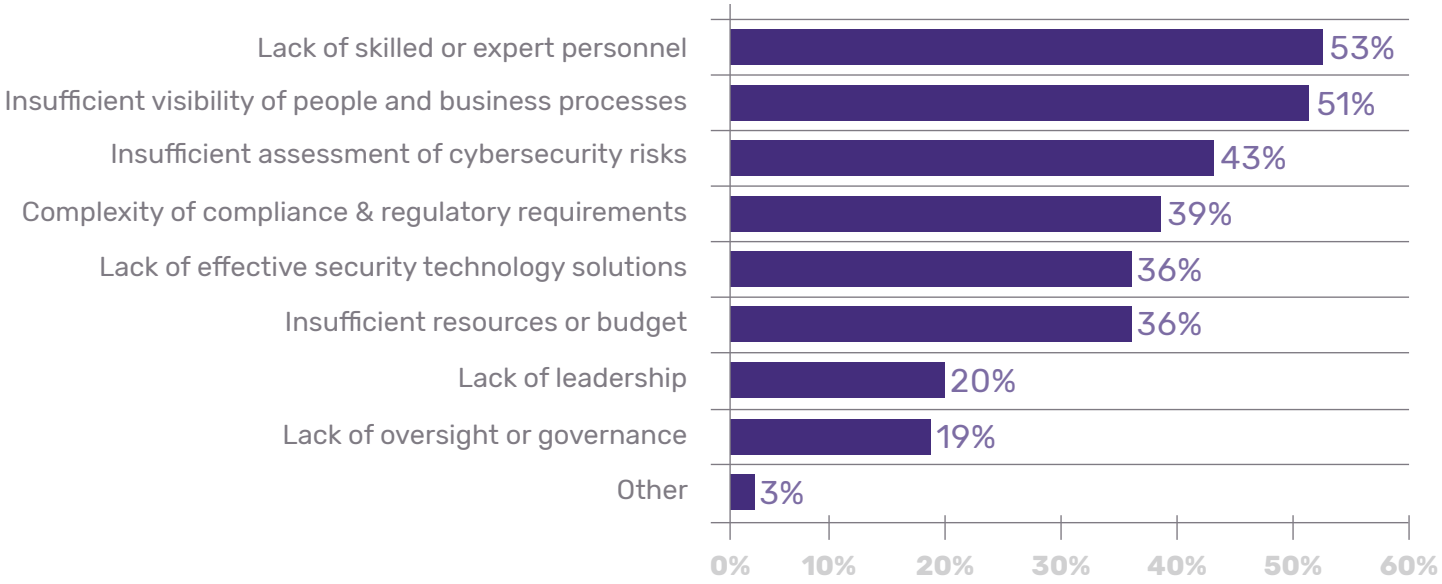


Figure 41
What are the most significant barriers to achieving a secure digital transformation process?

Three responses permitted

8

Continue to make the case for a digital transformation budget.

All the investments made in digital transformation can be canceled out by a data breach. Today, only 36 percent of respondents say their organizations have a security budget for protecting data assets during the digital transformation process. As shown in Figure 42, because of the risks created by digital transformation, respondents believe the percentage of IT security budget allocated to digital transformation should be almost doubled from an average of 21 percent to 37 percent of the IT security budget.

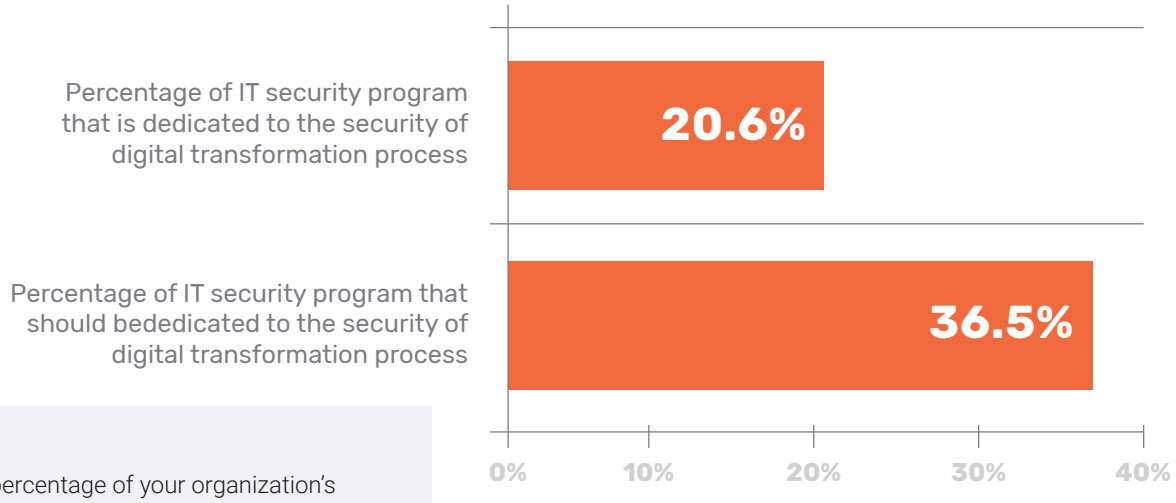


Figure 42
Today, what percentage of your organization's total IT security budget is dedicated to the security of the digital transformation process and what percentage should be dedicated to it?

Extrapolated values presented

As shown in Figure 43, in two years the ideal average percentage that should be allocated to digital transformation is 45 percent.

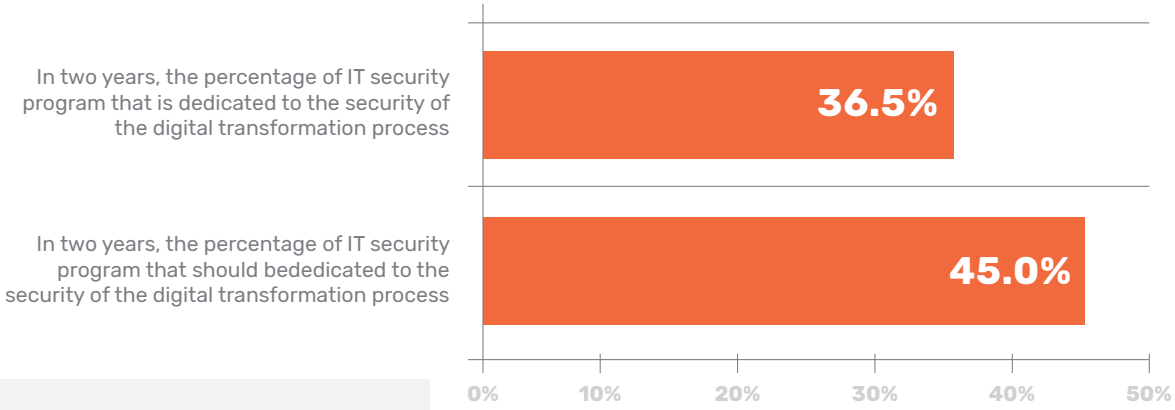


Figure 43
In two years, what percentage of your organization's total IT security budget will be dedicated to the security of the digital transformation process and what should it be?

Extrapolated values presented

More mature organizations than immature organizations report they have adequate budget, but it is still a struggle. The research reveals the struggle with having an adequate budget for protecting data assets during the digital transformation process. According to Figure 44, 43 percent of mature organizations vs. 34 percent of other organizations say their budgets are adequate for protecting data assets during the digital transformation process.

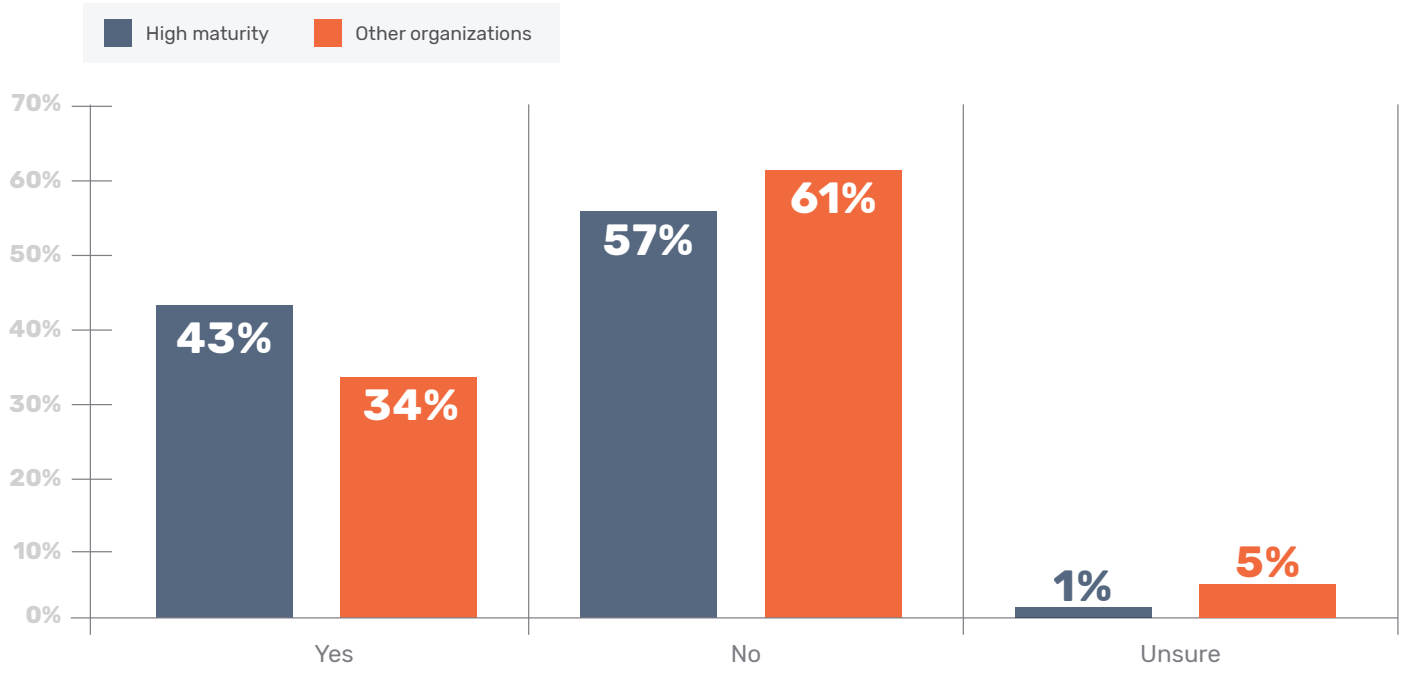


Figure 44
Does your organization have a security budget for protecting data assets during the digital transformation process?

9

Continue to invest in technologies that secure and protect your data and assets.

Figure 45 lists technologies that secure the digital transformation process as well as the confidence respondents have in their effectiveness to reduce the risk. As shown, respondents have the most confidence in technologies that secure information assets, protect data, protect the IT infrastructure, pinpoint vulnerabilities, and implement security patches in real time and secure endpoints.

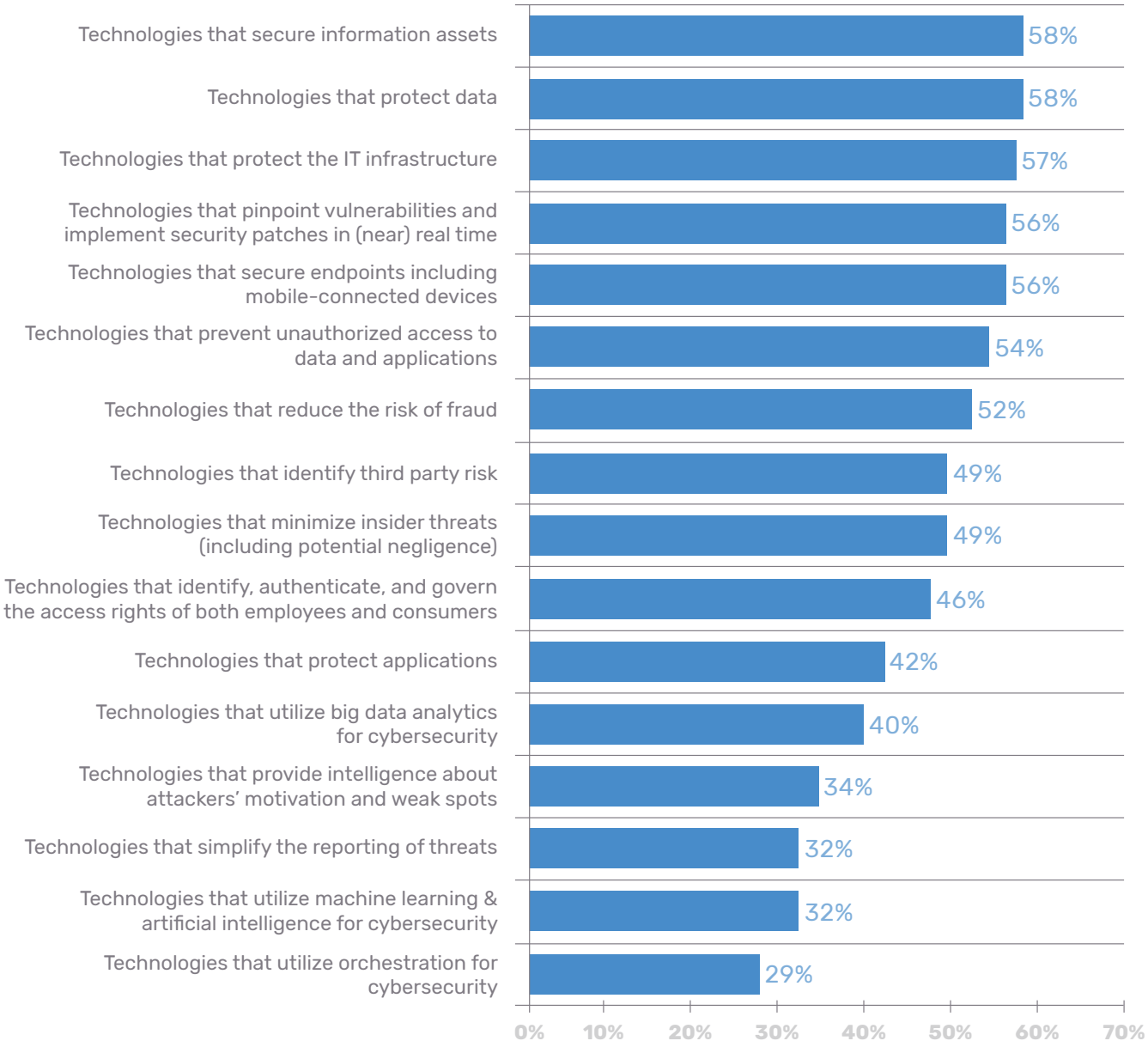


Figure 45
How confident are that the following technologies will secure the digital transformation of your organization?

Very Confident and Confident responses combined

10

Start Investing in technologies help you secure your cloud environment and reduce third party risk.

According to Figure 46, a secure cloud environment is the most significant challenge to achieving a secure digital transformation process for IT security respondents. Whereas, the C-level respondents consider the ability to ensure third parties have policies and practices to safeguard the security of their organization's information as a significant challenge.

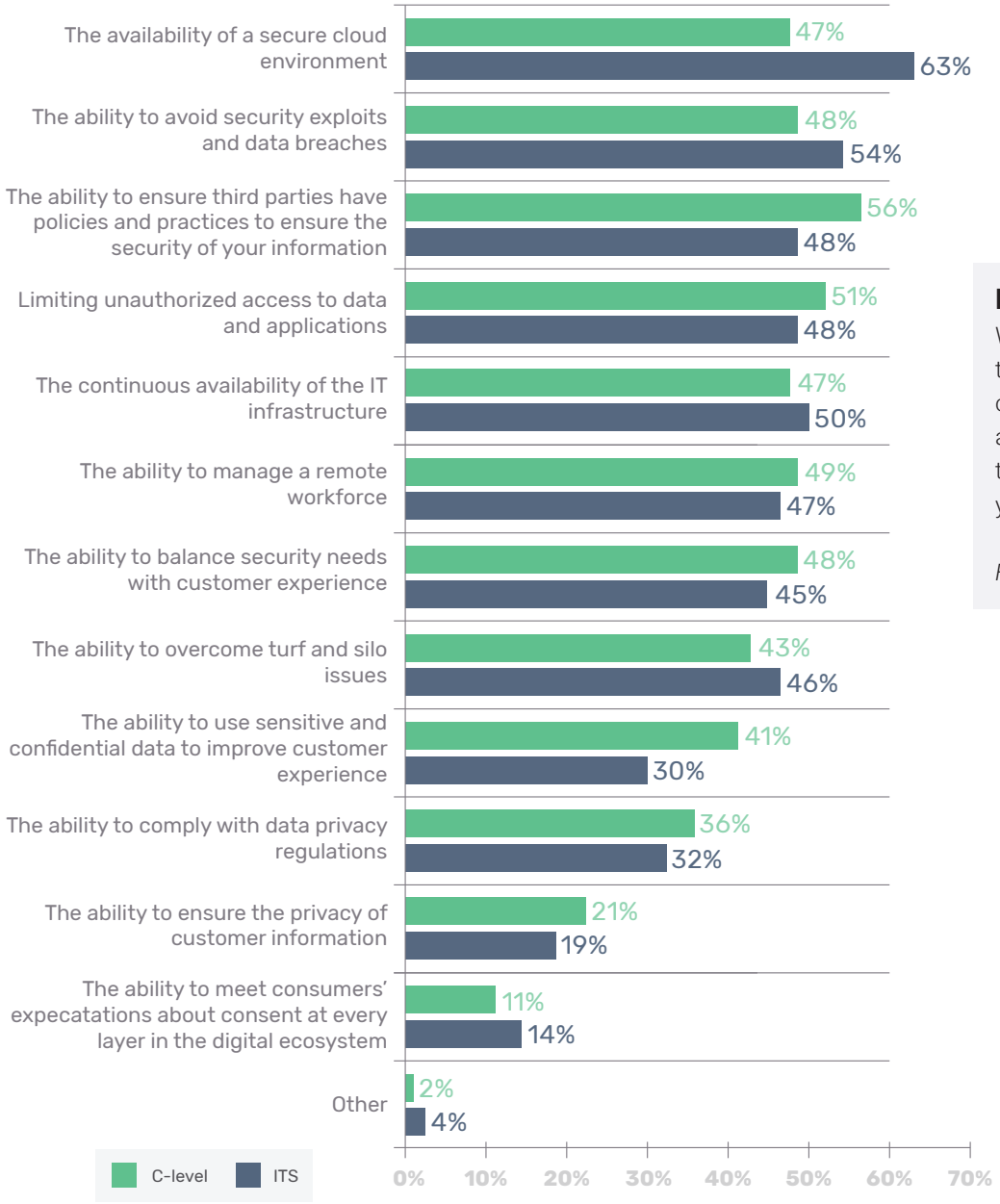


Figure 46
What do you see as the most significant challenges to achieving a secure digital transformation process in your organization today?

Five responses permitted

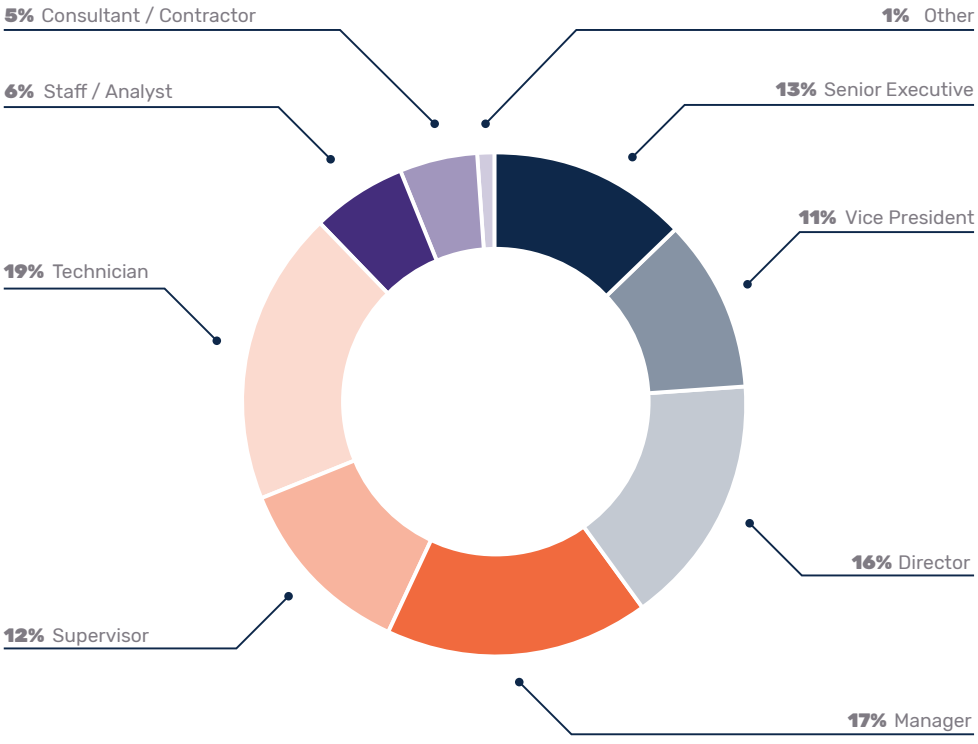
Part 5

Methods

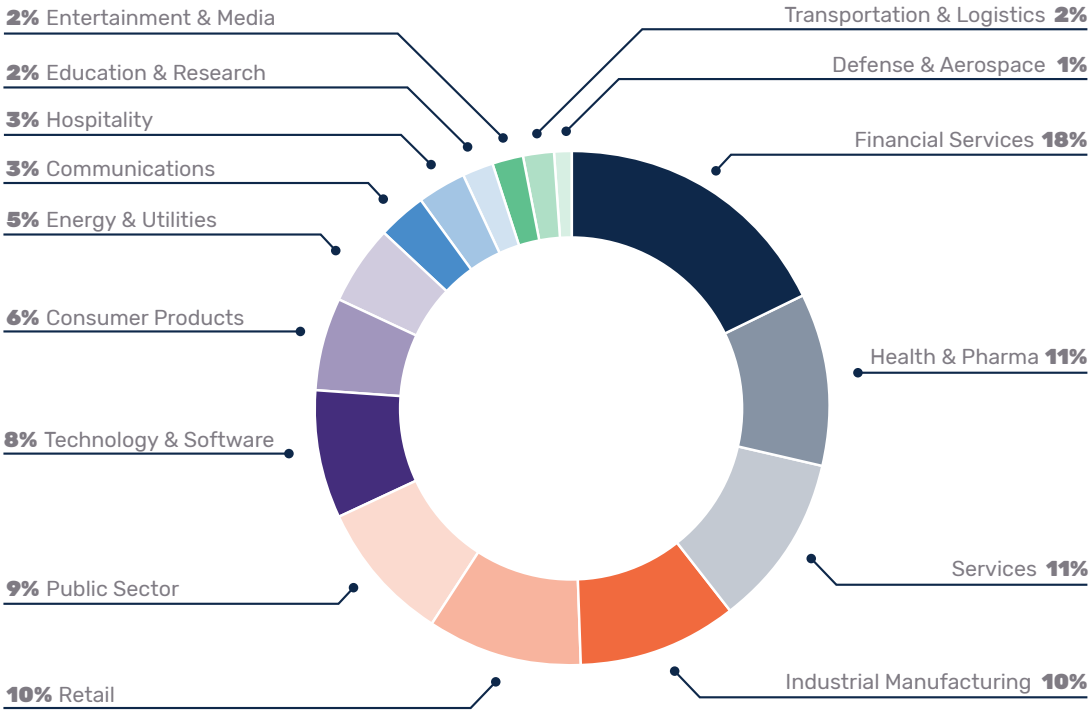
A sampling frame of 24,494 IT security and C-suite executives who are involved in managing digital transformation activities and cybersecurity activities within their organizations and are familiar with their organizations' third-party risk management were selected as participants in this survey. Table 1 shows 970 total returns. Screening and reliability checks required the removal of 87 surveys. Our final sample consisted of 883 surveys, or a 3.6 percent response rate.

Sample response	ITS	C-level	Total
Sampling frame	16,650	7,844	24,494
Total returns	633	337	970
Rejected or screened surveys	52	35	87
Final sample	581	302	883
Response rate	3.5%	3.9%	3.6%

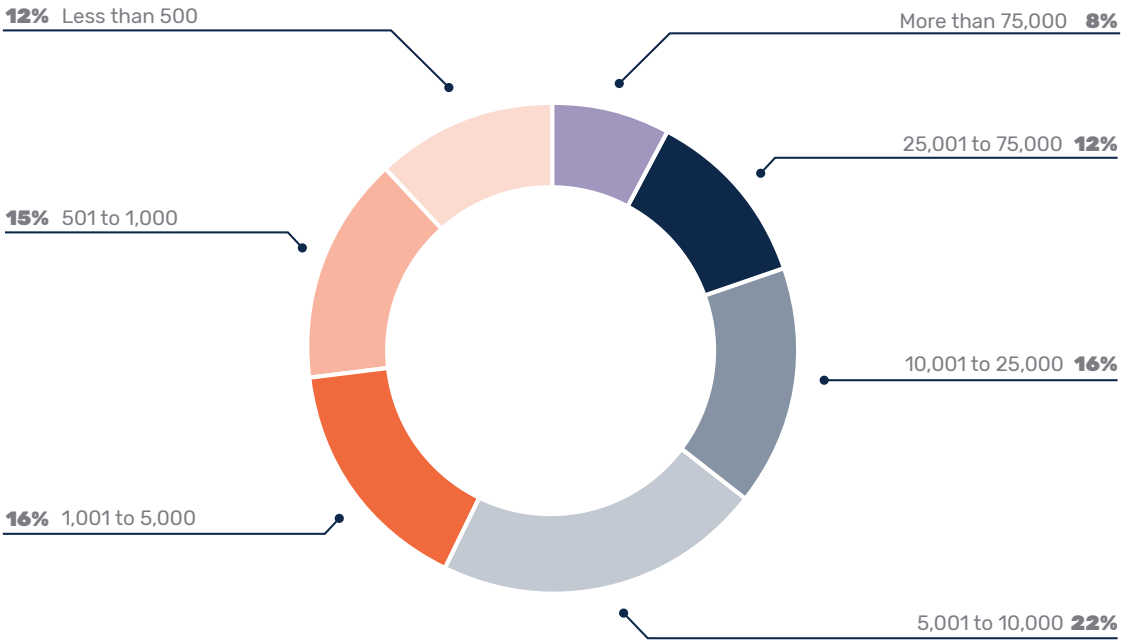
Pie Chart 1
reports the respondents' organizational levels within the participating organizations. By design, more than half of the respondents (69 percent) are at or above the supervisory levels and 19 percent of respondents described their position as technician.



Pie Chart 2
shows the percentage distribution of respondents' companies across 15 industries. Financial services represent the largest industry sector at 18 percent of respondents, which includes banking, insurance, brokerage, investment management, and payment processing. Other large verticals include health and pharmaceuticals and services, each at 11 percent of respondents.



Pie Chart 3
summarizes the total worldwide headcount of respondents' companies. In the context of this study, headcount serves as an indicator of size. At 22 percent, the largest segment contains larger-sized organizations with 5,001 to 10,000 full-time equivalent employees. The smallest segment (8 percent) includes larger-sized organizations with 75,000 or more employees. More than half (58 percent) of respondents are from organizations with a global headcount greater than 5,001 employees.



Part 6

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 many 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 IT or 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, the possibility remains that a subject did not provide accurate responses.

APP

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in March 2020.

Survey response	ITS	C-level	Total
Sampling frame	16,650	7,844	24,494
Total returns	633	337	970
Rejected surveys	52	35	87
Final sample	581	302	883
Response rate	3.5%	3.9%	3.6%

Part 1: Screening Questions

S1. How familiar are you with digital transformation as defined above?	ITS	C-level	Total
Very familiar	35%	31%	34%
Familiar	36%	35%	36%
Somewhat familiar	29%	34%	31%
No knowledge (Stop)	0%	0%	0%
Total	100%	100%	100%

S2. Do you have any involvement in managing digital transformation activities within your organization?	ITS	C-level	Total
Yes, fully involved	32%	30%	31%
Yes, partially involved	50%	45%	48%
Yes, minimally involved	18%	25%	20%
No involvement (Stop)	0%	0%	0%
Total	100%	100%	100%

S3. What best describes the maturity level of your organization's digital transformation today?	ITS	C-level	Total
Has not been launched (Stop)	0%	0%	0%
Early stage – many digital transformation activities have not as yet been planned or deployed	23%	25%	24%
Middle stage – digital transformation activities are planned and defined but only partially deployed	35%	29%	33%
Late-middle stage – many digital transformation activities are deployed across the enterprise	18%	26%	21%
Mature stage – Core digital transformation activities are deployed, maintained and/or refined across the enterprise	24%	20%	23%
Total	100%	100%	100%

S4. Do you have any involvement in managing cybersecurity activities within your organization?	ITS	C-level	Total
Yes, fully involved	39%	6%	28%
Yes, partially involved	47%	15%	36%
Yes, minimally involved	14%	79%	36%
No involvement (Stop)	0%	0%	0%
Total	100%	100%	100%

S5. How familiar are you with your organization's third-party risk management program?	ITS	C-level	Total
Very familiar	36%	40%	37%
Familiar	37%	41%	38%
Somewhat familiar	27%	19%	24%
No knowledge (Stop)	0%	0%	0%
Total	100%	100%	100%

S6. What are the top things you did to provide a secure digital transformation process within your organization? Please select all that apply.	ITS	C-level	Total
Employed cybersecurity personnel with sufficient background and expertise	46%	29%	40%
Procured and implemented cybersecurity tools and applications	53%	19%	41%
Migrated IT applications and infrastructure to the cloud	68%	59%	65%
Conducted vulnerability assessments	71%	35%	59%
Implemented risk management process	68%	63%	66%
Trained IT security personnel	55%	28%	46%
Responded to organizational change (i.e., mergers and acquisitions)	40%	56%	45%
Educated the C-suite and/or board of directors	23%	33%	26%
Conducted third-party assessments	64%	34%	54%
None of the above (stop)	0%	0%	0%

Part 2: Background on digital transformation

Q1. Approximately, how many third parties does your organization have?	ITS	C-level	Total
Less than 100	4%	5%	4%
100 to 500	9%	7%	8%
501 to 1,000	10%	11%	10%
1,001 to 2,500	13%	18%	15%
2,500 to 5,000	30%	29%	30%
5,001 to 10,000	14%	12%	13%
10,001 to 20,000	13%	10%	12%
More than 20,000	7%	8%	7%
Total	100%	100%	100%
Extrapolated value	5,997	5,669	5,884

Q2. In the next 12 months, how many third parties will your organization have?	ITS	C-level	Total
Less than 100	3%	5%	4%
100 to 500	6%	5%	6%
501 to 1,000	8%	9%	8%
1,001 to 2,500	17%	19%	18%
2,500 to 5,000	24%	21%	23%
5,001 to 10,000	19%	20%	19%
10,001 to 20,000	13%	10%	12%
More than 20,000	10%	11%	10%
Total	100%	100%	100%
Extrapolated value	6,852	6,625	6,774

Q3. By what percentage has the number of your organization's third parties increased as a result of digital transformation?	ITS	C-level	Total
Less than 5 percent	21%	25%	22%
6 percent to 10 percent	42%	23%	36%
11 percent to 25 percent	23%	28%	25%
26 percent to 50 percent	12%	21%	15%
51 percent to 75 percent	2%	3%	2%
76 percent to 100 percent	0%	0%	0%
Total	100%	100%	100%
Extrapolated value	14%	17%	15%

Q4. Which departments are assuming the most responsibility for the organization's digital transformation process? Please select the top two choices only.	ITS	C-level	Total
Compliance	3%	5%	4%
Finance and accounting	6%	5%	6%
Human resources	8%	11%	9%
Information technology	36%	25%	32%
IT security	18%	14%	17%
Manufacturing	23%	30%	25%
Marketing	31%	38%	33%
Public affairs/communications	8%	11%	9%
Research & development	5%	3%	4%
Sales	40%	36%	39%
Vendor management	20%	19%	20%
Other (please specify)	2%	3%	2%
Total	200%	200%	200%

Q5. How has digital transformation changed your organization? Please select all that apply.	ITS	C-level	Total
Increased outsourcing to third parties	31%	34%	32%
Increased use of shadow IT	36%	45%	39%
Increased migration to the cloud	56%	63%	58%
Increased use of IoT	47%	54%	49%
Other (please specify)	4%	3%	4%
Total	174%	199%	183%

Q6a. Does your organization have a strategy for achieving digital transformation?	ITS	C-level	Total
Yes	49%	56%	51%
No	39%	40%	39%
Unsure	12%	4%	9%
Total	100%	100%	100%

Q6b. If yes, does the strategy include the protection of data assets?	ITS	C-level	Total
Yes	66%	61%	64%
No	28%	36%	31%
Unsure	6%	3%	5%
Total	100%	100%	100%

Q6c. If yes, does the strategy involve assessing third-party relationships and vulnerabilities, including supply chain partners?	ITS	C-level	Total
Yes	75%	69%	73%
No	23%	28%	25%
Unsure	2%	3%	2%
Total	100%	100%	100%

Q6d. If yes, does the strategy involve maintaining customer and consumer trust?	ITS	C-level	Total
Yes	44%	56%	48%
No	47%	36%	43%
Unsure	9%	8%	9%
Total	100%	100%	100%

Part 3: Perceptions about digital transformation

Please express your opinion about each one of the following statements using the agreement scale. Strongly Agree and Agree response combined.	ITS	C-level	Total
Q7a. Digital transformation is not possible without strict security safeguards to protect the sharing and use of data that is critical to operations.	65%	53%	61%
Q7b. My organization makes it a priority to determine that our third parties have the people, processes, and technologies in place to ensure the data we store or share with them is safeguarded.	57%	48%	54%
Q7c. My organization believes it is important to do due diligence before engaging third parties.	62%	56%	60%
Q7d. The rush to achieve digital transformation increases the risk of a data breach and/or a cybersecurity exploit.	71%	53%	65%
Q7e. In my organization, it is important to balance the security of our high value assets while enabling the free flow of information and an open business model.	45%	63%	51%
Q7f. In my organization, the digital economy significantly increases risk to high value assets such as our intellectual property, trade secrets and so forth.	64%	41%	56%
Q7g. My organization's leaders recognize that digital transformation creates IT security risk.	50%	39%	46%
Q7h. My organization's leaders recognize that the inability to secure digital assets can significantly hurt its brand and reputation.	43%	49%	45%
Q7i. My organization's leaders recognize the need to invest in emerging security technologies such as modern third-party cyber risk management solutions to secure the digital transformation process.	61%	43%	55%
Q7j. My organization's leaders recognize the need to invest in emerging security technologies such as orchestration in order to secure the digital transformation process.	60%	56%	59%

Q8a. How essential is digital transformation to your company's business?	ITS	C-level	Total
Essential	60%	56%	59%
Very important	20%	23%	21%
Important	12%	13%	12%
Not important	5%	8%	6%
Irrelevant	3%	0%	2%
Total	100%	100%	100%

Q8b. How essential is IT security to supporting innovation with minimal impact on the goals of digital transformation?	ITS	C-level	Total
Essential	58%	51%	56%
Very important	25%	23%	24%
Important	9%	19%	12%
Not important	6%	5%	6%
Irrelevant	2%	2%	2%
Total	100%	100%	100%

Part 4: Security in the digital ecosystem

Q9. Of the following, who are most involved in directing your organization's efforts to ensure a secure digital transformation process? Please choose only your top three choices.	ITS	C-level	Total
Chief executive officer (CEO)	4%	8%	5%
Chief operating officer (COO)	2%	3%	2%
Chief marketing officer (CMO)	27%	34%	29%
Chief information officer (CIO)	38%	34%	37%
Chief technology officer (CTO)	19%	23%	20%
Chief risk officer (CRO)	9%	8%	9%
Chief security officer (CSO)	6%	3%	5%
Chief information security officer (CISO)	25%	21%	24%
Chief innovation officer	6%	10%	7%
Chief digital officer	12%	19%	14%
Enterprise architect	34%	25%	31%
General manager / VP, lines of business	50%	40%	47%
Leader, data sciences / analytics	43%	46%	44%
No one person has overall responsibility	25%	26%	25%
Total	300%	300%	300%

Q10. How does your organization manage the security of the digital transformation process?	ITS	C-level	Total
In-house team	39%	30%	36%
Outsourced service provider	21%	32%	25%
Combination of both in-house and outsourced	40%	38%	39%
Total	100%	100%	100%

Q11a. Is your organization more vulnerable to a cyberattack or data breach following digital transformation?	ITS	C-level	Total
Yes, much more vulnerable	32%	41%	35%
Yes, somewhat more vulnerable	35%	30%	33%
No change in vulnerability to a cyberattack or data breach	33%	29%	32%
Total	100%	100%	100%

Q11b. If yes, what caused the increase in vulnerability to a cyberattack or data breach? Please select all that apply.	ITS	C-level	Total
Increased use of shadow IT	48%	42%	46%
Increased use of IoT devices	39%	43%	40%
Increased outsourcing to third parties	35%	44%	38%
Increased reliance on vendors	23%	22%	23%
The rush to produce and release apps	50%	43%	48%
Increased migration to the cloud	41%	56%	46%
Other (please specify)	236%	250%	241%

Q12. In two years, what threats will your organization be most concerned about because of digital transformation? Please select one top choice.	ITS	C-level	Total
Data breaches caused by third parties	20%	24%	21%
Cybersecurity attacks	21%	25%	22%
System downtime	23%	23%	23%
Malicious insiders	14%	10%	13%
Negligent insiders	17%	12%	15%
Other (please specify)	5%	6%	5%

Q13a. Using the following 10-point scale, please rate how prepared your organization is to mitigate the risk of these threats today from 1 = not prepared to 10 = very prepared.	ITS	C-level	Total
1 or 2	7%	5%	6%
3 or 4	11%	6%	9%
5 or 6	23%	19%	22%
7 or 8	30%	40%	33%
9 or 10	29%	30%	29%
Total	100%	100%	100%
Extrapolated value	6.76	7.18	6.90

Q13b. Using the following 10-point scale, please rate how prepared your organization will be to mitigate the risk of these threats in two years from 1 = not prepared to 10 = very prepared.	ITS	C-level	Total
1 o2 2	3%	2%	3%
3 or 4	5%	1%	4%
5 or 6	13%	15%	14%
7 or 8	34%	42%	37%
9 or 10	45%	40%	43%
Total	100%	100%	100%
Extrapolated value	7.76	7.84	7.79

Q14. What information is your organization most concerned about protecting in the digital transformation process? Please select your top four choices.	ITS	C-level	Total
Company e-mail	35%	33%	34%
Confidential financial	32%	40%	35%
Corporate communications	37%	44%	39%
Current customers	50%	60%	53%
Employee/human resources	47%	51%	48%
Internet/social media	29%	29%	29%
Legal and compliance	14%	11%	13%
Marketing and sales	52%	50%	51%
Non-confidential financial	11%	8%	10%
Prospective customers	43%	35%	40%
Research and development	47%	35%	43%
Other (please specify)	3%	4%	3%
Total	400%	400%	400%

Q15. Please check all steps taken to protect your organization's sensitive and confidential information.	ITS	C-level	Total
Encryption for data at rest	62%	43%	56%
Encryption for data in transit	59%	55%	58%
Redaction data standards	31%	27%	30%
Obfuscation/truncation data standards	36%	29%	34%
Deployed data loss prevention solution	47%	43%	46%
Data tokenization	36%	26%	33%
Extended manual procedures	54%	60%	56%
Digital rights management solution at document level	29%	37%	32%
Third-party risk assessments	45%	50%	47%
Behavioral analytics solution	39%	35%	38%
Total	438%	405%	427%

Q16a. Today, how influential is IT security to your organization's digital transformation strategy?	ITS	C-level	Total
Very influential	38%	30%	35%
Influential	25%	25%	25%
Somewhat influential	21%	19%	20%
Not influential	11%	17%	13%
No influence at all	5%	9%	6%
Total	100%	100%	100%

Q16b. In two years, how influential will IT security be to your organization's digital transformation strategy?	ITS	C-level	Total
Very influential	42%	40%	41%
Influential	32%	34%	33%
Somewhat influential	15%	17%	16%
Not influential	8%	7%	8%
No influence at all	3%	2%	3%
Total	100%	100%	100%

Q17. What best describes the level of alignment between IT security and lines of business with respect to achieving security during the digital transformation process?	ITS	C-level	Total
Fully aligned	13%	21%	16%
Partially aligned	33%	40%	35%
Not aligned	54%	39%	49%
Total	100%	100%	100%

Q18. How important are the following organizational characteristics in securing digital transformation? Please rank order each factor from 1 = most important to 7 = least important.	ITS	C-level	Total
Agility	1.51	1.76	1.98
Ample budget	5.40	4.57	4.17
Knowledgeable or expert staff	2.62	3.04	2.83
Leadership	3.75	3.63	3.41
Preparedness	6.65	6.34	4.56
Resilience	2.31	1.53	1.64
Strong security posture	3.46	3.53	2.90

Q19. What do you see as the most significant barriers to achieving a secure digital transformation process in your organization today? Please choose only your top three choices.	ITS	C-level	Total
Insufficient resources or budget	34%	40%	36%
Insufficient visibility of people and business processes	52%	49%	51%
Insufficient assessment of cybersecurity risks	43%	44%	43%
Lack of effective security technology solutions	37%	35%	36%
Lack of skilled or expert personnel	51%	56%	53%
Lack of leadership	18%	23%	20%
Lack of oversight or governance	20%	17%	19%
Complexity of compliance and regulatory requirements	42%	34%	39%
Other (please specify.	3%	2%	3%
Total	300%	300%	300%

Q20. What do you see as the most significant challenges to achieving a secure digital transformation process in your organization today? Please choose only your top five choices.	ITS	C-level	Total
The availability of a secure cloud environment	63%	47%	58%
The ability to ensure third parties have policies and practices to ensure the security of our information	48%	56%	51%
The ability to manage a remote workforce	47%	49%	48%
The ability to ensure the privacy of customer information	19%	21%	20%
The ability to meet consumers' expectations about consent at every layer in the digital ecosystem	14%	11%	13%
The ability to balance security needs with customer experience	45%	48%	46%
The ability to comply with data privacy regulations	32%	36%	33%
The ability to avoid security exploits and data breaches	54%	48%	52%
The ability to use sensitive and confidential data to improve customer experience	30%	41%	34%
The ability to overcome turf and silo issues	46%	43%	45%
The continuous availability of the IT infrastructure	50%	47%	49%
Limiting unauthorized access to data and applications	48%	51%	49%
Other (please specify)	4%	2%	3%
Total	500%	500%	500%

Q21. Does your organization have a security budget for protecting data assets during the digital transformation process?	ITS	C-level	Total
Yes	36%	34%	35%
No	60%	57%	59%
Unsure	4%	9%	6%
Total	100%	100%	100%

Q22a. Today, what percentage of your company's total IT security program is dedicated to the security of the digital transformation process?	ITS	C-level	Total
None	14%	15%	14%
Less than 10%	21%	21%	21%
10% to 25%	39%	36%	38%
26% to 50%	18%	19%	18%
51% to 75%	6%	5%	6%
76% to 100%	2%	4%	3%
Total	100%	100%	100%
Extrapolated value	20.2%	21.2%	20.6%

Q22b. Today, what percentage of your company's total IT security budget should be dedicated to the security of the digital transformation process?	ITS	C-level	Total
None	5%	6%	5%
Less than 10%	7%	5%	6%
10% to 25%	33%	28%	31%
26% to 50%	27%	29%	28%
51% to 75%	21%	24%	22%
76% to 100%	7%	8%	7%
Total	100%	100%	100%
Extrapolated value	35.6%	38.2%	36.5%

Q23a. In two years, what percentage of your company's total IT security budget will be dedicated to the security of the digital transformation process? Your best guess is welcome.	ITS	C-level	Total
None	0%	3%	1%
Less than 10%	8%	7%	8%
10% to 25%	32%	31%	32%
26% to 50%	35%	34%	35%
51% to 75%	17%	19%	18%
76% to 100%	8%	6%	7%
Total	100%	100%	100%
Extrapolated value	36.9%	35.8%	36.5%

Q23b. In two years, what percentage of your company's total IT security program should be dedicated to the security of the digital transformation process?	ITS	C-level	Total
None	0%	2%	1%
Less than 10%	0%	3%	1%
10% to 25%	25%	20%	23%
26% to 50%	39%	39%	39%
51% to 75%	21%	23%	22%
76% to 100%	15%	13%	14%
Total	100%	100%	100%
Extrapolated value	45.4%	44.2%	45.0%

Q24a. Has insecure digital transformation caused your organization to experience one or more data breaches in the last 12 months?	ITS	C-level	Total
Yes, with certainty	23%	19%	22%
Yes, most likely	35%	28%	33%
Yes, likely	25%	30%	27%
No, not likely	14%	15%	14%
No chance	3%	8%	5%
Total	100%	100%	100%

Q24b. If yes, how many data breaches did your organization experience in the last 12 months?	ITS	C-level	Total
One	25%	42%	31%
2 to 5	42%	43%	42%
6 to 10	27%	12%	22%
More than 10	6%	3%	5%
Total	100%	100%	100%
Extrapolated value	4.60	3.25	4.14

Q24c. If yes, were any of these data breaches caused by a third party?	ITS	C-level	Total
Yes	59%	46%	55%
No	41%	54%	45%
Total	100%	100%	100%

Q25a. Does your organization have a third-party cyber risk management program?	ITS	C-level	Total
Yes	43%	40%	42%
No	57%	60%	58%
Total	100%	100%	100%

Q25b. If yes, what tools or solutions does your organization use to manage risk? Please select all that apply.	ITS	C-level	Total
Security ratings	36%	32%	35%
Assessments	56%	45%	52%
Risk exchanges	28%	32%	29%
All of the above	16%	14%	15%
Total	136%	123%	132%

Q25c. If yes, how effective are these tools?	ITS	C-level	Total
Very effective	23%	21%	22%
Effective	25%	24%	25%
Somewhat effective	27%	29%	28%
Not effective	25%	26%	25%
Total	100%	100%	100%

Q26a. Has insecure digital transformation caused your organization to experience cyber exploits that have infiltrated your organization's networks or enterprise systems in the last 12 months?	ITS	C-level	Total
Yes, with certainty	23%	20%	22%
Yes, most likely	33%	29%	32%
Yes, likely	19%	26%	21%
No, not likely	25%	21%	24%
No chance	0%	4%	1%
Total	100%	100%	100%

Q26b. If yes, how many cyber exploits did your organization experience?	ITS	C-level	Total
1 to 10	23%	39%	28%
11 to 15	26%	24%	25%
16 to 25	28%	24%	27%
26 to 50	17%	13%	16%
More than 50	6%	0%	4%
Total	100%	100%	100%
Extrapolated value	20.15	15.13	18.43

Q27. Which are the most negative consequences that your organization might have experienced as a result of a data breach or cyber exploit due to insecure digital transformation? Please select the top three most negative consequences.	ITS	C-level	Total
Cost of outside consultants and experts	43%	30%	39%
Customer turnover	36%	45%	39%
Disruption or damages to critical infrastructure	64%	62%	63%
Lost intellectual property (including trade secrets)	61%	55%	59%
Lost revenue	27%	26%	27%
Productivity decline	51%	46%	49%
Regulatory actions or lawsuits	12%	10%	11%
Reputation or brand damage	6%	26%	13%
Total	300%	300%	300%

Q28. From the list below, please select the three digital asset categories that in your experience are most difficult to secure.	ITS	C-level	Total
Analytics (data models)	50%	54%	51%
Attorney-client privileged information	12%	9%	11%
Business correspondence	15%	14%	15%
Company-confidential information	33%	29%	32%
Consumer data	9%	12%	10%
Financial information	17%	26%	20%
Operational information	15%	14%	15%
Private communications (i.e., emails, text messages, social media)	46%	40%	44%
Product/market information	20%	30%	23%
Research results	29%	17%	25%
Source code	28%	31%	29%
Trade secrets	26%	24%	25%
Total	300%	300%	300%

Q29. How confident are you that the above 12 digital asset categories are appropriately secured within your company? Please rate each information asset category using the confidence scale. High Confidence and Some Confidence responses combined.	ITS	C-level	Total
Analytics	36%	34%	35%
Attorney-client privileged information	41%	39%	40%
Business correspondence	42%	45%	43%
Company-confidential information	38%	35%	37%
Consumer data	24%	27%	25%
Financial information	56%	54%	55%
Operational information	29%	31%	30%
Private communications (i.e., emails, text messages, social media)	40%	35%	38%
Product/market information	30%	48%	36%
Research results	37%	40%	38%
Source code	43%	46%	44%
Trade secrets	55%	49%	53%
Total	471%	483%	475%

Part 6: Technologies in the digital ecosystem

Q30. How confident are you that the following technologies will secure the digital transformation of your organization? Very Confident and Confident responses combined.	ITS	C-level	Total
Q30a. Technologies that identify, authenticate, and govern the access rights of both employees and consumers	43%	51%	46%
Q30b. Technologies that identify third-party risk	51%	45%	49%
Q30c. Technologies that simplify the reporting of threats	37%	23%	32%
Q30d.Technologies that secure endpoints including mobile-connected devices	56%	55%	56%
Q30e. Technologies that minimize insider threats (including potential negligence)	47%	52%	49%
Q30f. Technologies that secure information assets	60%	54%	58%
Q30g. Technologies that protect the IT infrastructure	58%	54%	57%
Q30h. Technologies that pinpoint vulnerabilities and implement security patches in (near) real time	60%	49%	56%
Q30i. Technologies that utilize big data analytics for cybersecurity	38%	43%	40%
Q30j Technologies that utilize machine learning, artificial intelligence for cybersecurity	28%	39%	32%
Q30k. Technologies that utilize orchestration for cybersecurity	27%	32%	29%
Q30l.Technologies that provide intelligence about attackers' motivation and weak spots	33%	35%	34%
Q30m.Technologies that protect applications	41%	45%	42%
Q30n.Technologies that protect data	60%	53%	58%
Q30o.Technologies that prevent unauthorized access to data and applications	57%	48%	54%
Q30p.Technologies that reduce the risk of fraud	53%	49%	52%

Part 7: Your role and organization

D1. What organizational level best describes your current position?	ITS	C-level	Total
Senior Executive	4%	31%	13%
Vice President	5%	24%	11%
Director	15%	19%	16%
Manager	21%	8%	17%
Supervisor	15%	6%	12%
Technician	27%	3%	19%
Staff / Analyst	6%	5%	6%
Consultant / Contractor	5%	4%	5%
Other	2%	0%	1%
Total	100%	100%	100%

D2. Check the Primary Person you or your IT security leader reports to within the organization.	ITS	C-level	Total
C-level executives	0%	100%	100%
IT security leadership	100%	0%	100%

D3. What industry best describes your organization's industry focus?	ITS	C-level	Total
Agriculture & food services	0%	0%	0%
Communications	3%	2%	3%
Consumer products	6%	6%	6%
Defense & aerospace	1%	0%	1%
Education & research	2%	2%	2%
Energy & utilities	5%	6%	5%
Entertainment & media	2%	2%	2%
Financial services	18%	17%	18%
Health & pharmaceutical	11%	10%	11%
Hospitality	3%	2%	3%
Industrial & manufacturing	9%	12%	10%
Public sector	9%	10%	9%
Retail	10%	9%	10%
Services	11%	10%	11%
Technology & software	8%	9%	8%
Transportation & logistics	2%	2%	2%
Other	0%	1%	0%
Total	100%	100%	100%

D5. What is the worldwide headcount of your organization?	ITS	C-level	Total
Less than 500	12%	11%	12%
501 to 1,000	14%	16%	15%
1,001 to 5,000	17%	15%	16%
5,001 to 10,000	21%	24%	22%
10,001 to 25,000	16%	16%	16%
25,001 to 75,000	12%	11%	12%
More than 75,000	8%	7%	8%
Total	100%	100%	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

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.