State of Automation in Incident Management

2020

(x) matters®

Table of Contents

3 Executive Summary

4 Key Findings

5 Pandemic Forces Digital Transformation

7 Removing Roadblocks to Innovation and Business Success

9 Incident Management Requires its Own Transformation

14 Trends: Collaboration, Constant Learning and Automation

18 A New Era for Incident Management

19 Survey Respondent Demographics

Executive Summary

Companies are investing heavily in digital transformation to build a better experience for customers and drive business growth in new and existing markets. Digital transformation spend continues to rise at more than three times the rate of IT spending overall, according to the May 2020 Deloitte Insights Digital Transformation Survey.

The COVID-19 pandemic has amplified a conundrum that exists for many organizations. To meet rising consumer and business demands, digital transformation and the deployment of digital services has been accelerating. This increased tempo often results in digital service issues and interruptions that negatively impact the customer experience. Many teams now spend more time fixing digital services and less time on innovation. It's clear that just moving faster isn't enough. Teams also need to develop digital service resilience.

Digital service resilience is the ability to satisfy performance expectations and deliver superior experiences that attract and retain customers.

The *State of Automation in Incident Management* research was designed to understand how organizations approach digital service issues and interruptions. We evaluated where companies are currently positioned in the Incident Management Spectrum and in their journey to digital service resilience. The research revealed that **incident management is due for its own transformation**.

We compared these new findings to our previous studies over the past year which examined the growing challenges faced by those tasked with the delivery and maintenance of digital services: the November 2019 *Incident Management in the Age of Customer-Centricity* research and the April 2020 *Impact of COVID-19 on Digital Transformation* research.

In this *State of Automation in Incident Management* study we sought to determine which approach to incident management is the most effective for achieving digital service resilience and, ultimately, meeting today's business imperatives. We explored:

- What role incident management plays in the delivery of digital services
- The effect of customer-impacting issues on the ability to build new services and features
- The varying degrees of incident management readiness or preparedness within an organization

Key Findings

1. Even in a recession, enterprises have increased their budget for digital transformation since November 2019. **Twenty percent** of companies with 1,001-5,000 employees are budgeting more than $10 million on digital transformation initiatives, compared with **9.3%** in November 2019.

2. A majority (**84.3%**) of technology professionals say their ability to innovate is affected by customer-impacting issues—an increase of 10 percent compared to November 2019.

3. IT (**44.7%**), financial services (**23.7%**), and healthcare (**23%**) are the top industries where customer-reported outages or issues are the most common triggers for incidents.

4. Nearly three-quarters (**72.3%**) of technology professionals say at least half of their team's time is spent resolving incidents compared to innovating.

5. Upon evaluation of where companies are positioned in the Incident Management Spectrum, findings indicate that respondents employ either a traditional (**40.1%**) or modern **(58.6%**) approach to incident management. Only the most advanced organizations have isolated keys to success across business and incident management functions.

6. More than two-thirds of respondents (**69.2%**) report that leadership plays a role in their organization's incident response and management process.

7. Nearly half of technology professionals **(43.4%**) deploy less sophisticated processes such as email, conference bridges, or manual setup and outreach to engage team members, stakeholders, and customers during an incident.

8. Service desks (**44.5%**) are the most common incident management tool used by organizations in the traditional spectrum. Incident management tools (**42.2%**) are most commonly used for incident response and management by organizations in the modern spectrum.

9. While a majority of respondents (**73.9%**) report that operations and development teams collaborate to assess the cause of an incident, after an incident is identified, there is an opportunity to automate the postmortem process.

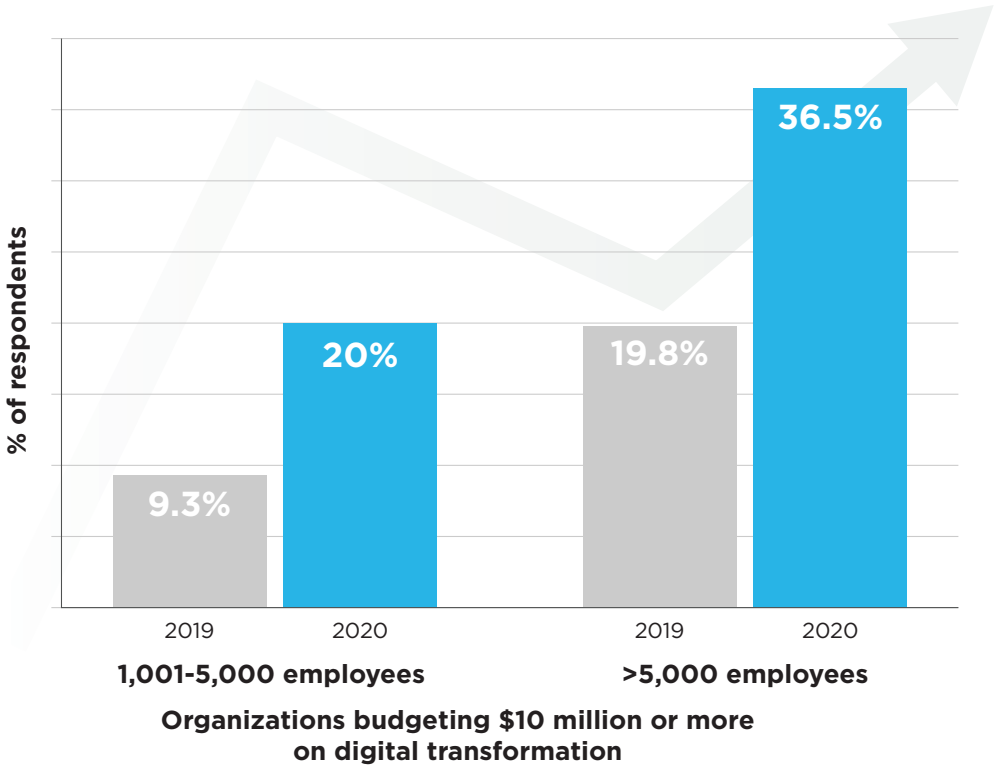
10. Automated post-incident reporting is essential for raising an organization's awareness about the things that can go wrong so corrective and preventative actions can be taken promptly. According to respondents, top benefits of using artificial intelligence or machine learning for incident management include informing post-incident reporting with data from previous, related incidents (**36%**) and aggregation of data to detect anomalies early (**28.9%**).

Pandemic Forces Digital Transformation

Spending on digital transformation will reach $2.3 trillion in 2023, accounting for the majority of IT spending (53%) for the first time[1]. With so many dollars on the line, digital services adopted as part of a company's digital transformation initiative need to run smoothly and efficiently.

Large enterprises, companies with more than 1,000 employees, have significantly increased their budgets to support and manage digital transformation initiatives, compared to findings from the November 2019 *Incident Management in the Age of Customer-Centricity* research.

More than double the amount of respondents from companies with 1,001-5,000 employees (20%) report that they are budgeting $10 million or more on digital transformation, compared to 9.3% of respondents in November 2019. Additionally, over a third of respondents from companies with more than 5,000 employees (36.5%) budget $10 million or more to support and manage digital transformation initiatives, an increase of 16.7% from November 2019.



1 IDC. (2020). Worldwide Semiannual Digital Transformation Spending Guide https://www.idc.com/getdoc.jsp?containerId=IDC_P32575

The COVID-19 pandemic quickly forced many companies to adapt and undergo digital transformation in order to deliver accessible digital experiences for customers and employees.

Findings from the April 2020 *Impact of COVID-19 on Digital Transformation* survey show despite technology professionals' confidence in their ability to support today's much greater dependence on digital services, more than half of consumers report a rise in application performance issues. Additionally, the report found that the sudden surge in reliance on digital services and rapid digital transformation is diverting attention from core functions to new unplanned operational challenges. These include more complex IT environments, capacity planning and an increase in data to manage.

Root causes for gap in IT readiness and consumer experience during COVID-19

50.2%
IT environments now more complex

49.8%
capacity planning is more difficult

47.5%
more data to manage

43.6%
need to learn new technologies in the realm of automation, orchestration & cloud computing

38%
increased number of tools makes jobs more difficult

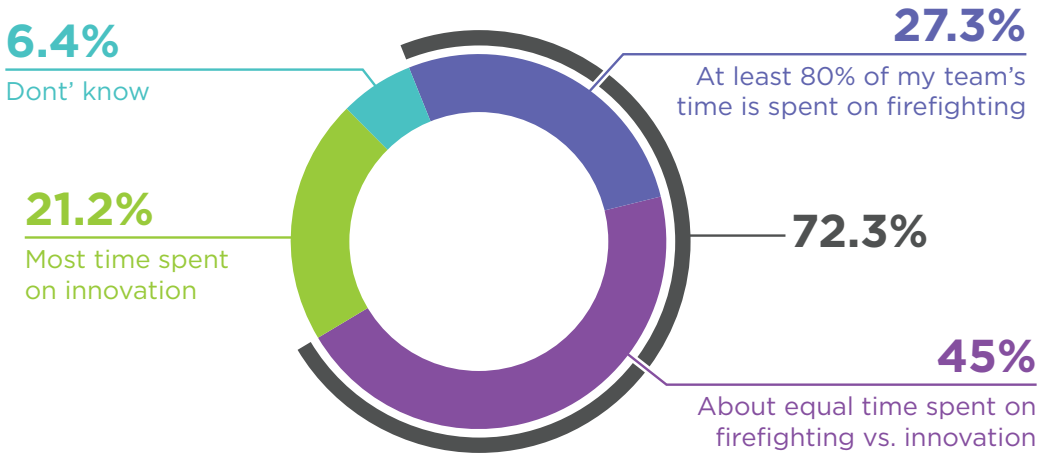
36%
need to understand incident management and issue resolution best practices

Removing Roadblocks to Innovation and Business Success

Customer-impacting issues are a roadblock to innovation. The proportion of technology professionals who report that their ability to build out services is affected by customer-impacting issues has increased by almost 10 percent to 84.3% today compared to November 2019. The increase may be the result of the pandemic-accelerated adoption of digital services by customers and employees.

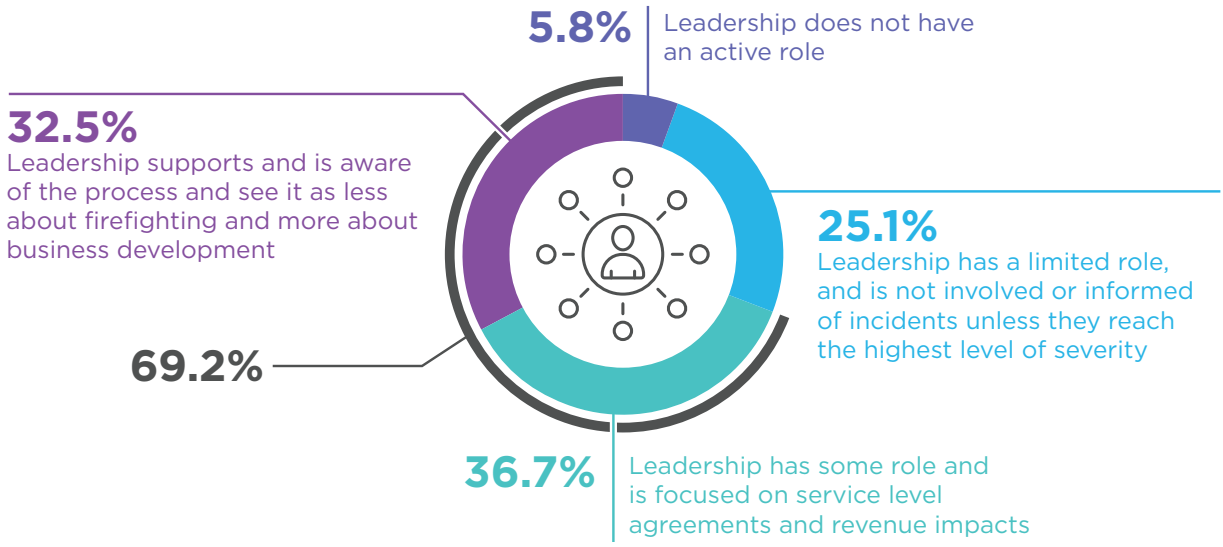
Responses when asked to complete the sentence: My (or my team's) ability to build out new services and features is _____ affected by customer-impacting issues.

A majority of respondents (72.3%) also reported that at least half of their team's time is spent resolving incidents compared to time spent on innovation. Of these respondents, over a quarter (27.3%) said at least 80% of their team's time is spent firefighting and working on incidents and issues.



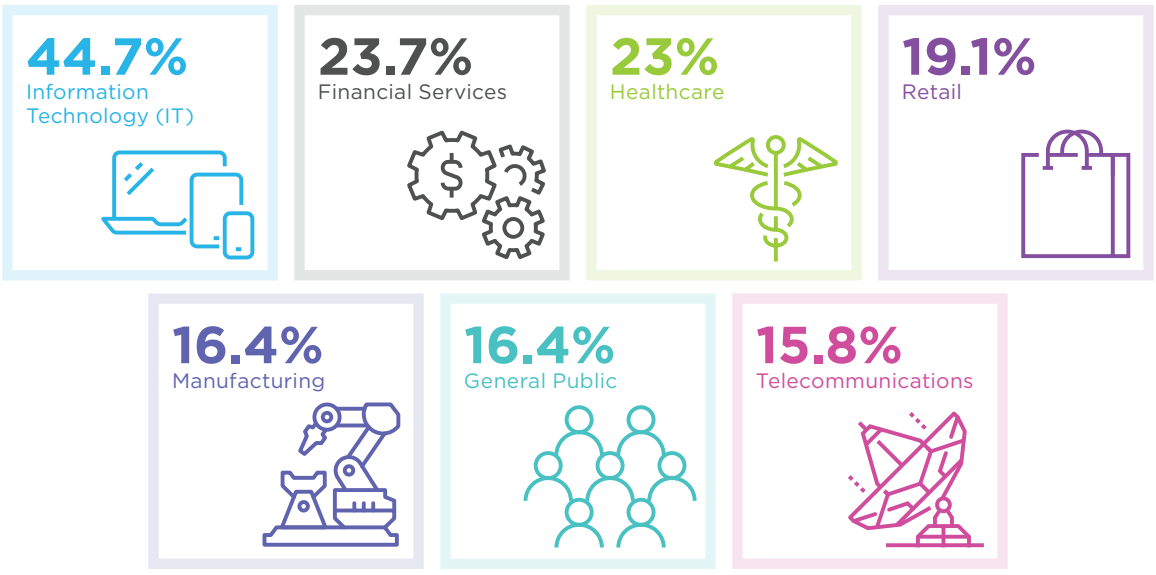
Incident management can play a critical role not only in ensuring digital transformation success, but also in delivering an overall positive customer experience and continued innovation, core components of a business's overall success—business and technical leaders agree.

More than two-thirds of respondents (69.2%) report that leadership plays a role in their organization's incident response and management process.



Overall, there is a marked need for improvement in customer experiences and an organizational commitment to innovation across industries.

The top three industries served by respondents who said customer-reported outages or issues most commonly trigger incidents in their organization are IT (44.7%), financial services (23.7%), and healthcare (23%).



Incident Management Requires its Own Transformation

For many teams, depending on their approach to incident management, time is lost because it is a manual, toil-filled process. To assess the efficacy of incident management in organizations, we evaluated components of a comprehensive incident management practice which consist of its foundation and how organizations detect, resolve, and learn about incidents:

Foundation – the basic building blocks of an enterprise's incident management structure (e.g., team types, processes and tools)

Detection – an organization's ability to identify primary incident triggers, see impacted systems, isolate issues, and retrieve informative context about the global situation

Resolution – an enterprise team's on-call sophistication, collaboration and stakeholder notification, as well as the approximate amount of time teams spend firefighting versus innovating

Learning – an organization's post-incident process and how learnings contribute to future incident avoidance and automation

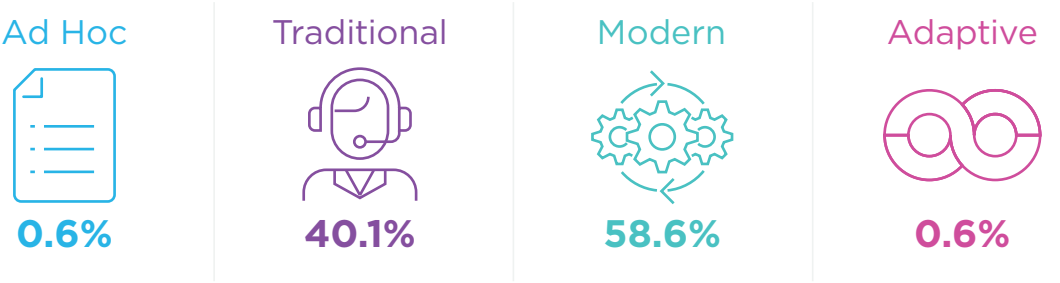
Based on the assessment of incident management processes, we then defined the Incident Management Spectrum. This Spectrum includes four categories: ad hoc, traditional, modern, and adaptive. Below are approximate descriptions of each, but note that some attributes may exist across multiple approaches.

Ad Hoc	Traditional	Modern	Adaptive
Smaller and newly-formed companies often lack a formal incident management process and rely on customer-reported outages to learn of incidents. Spreadsheets and email are used rather than incident management tools.	This approach combines human insight with strict processes to detect and resolve incidents. It is highly structured and service desks play a significant role.	This approach combines manual and automated processes to detect and resolve incidents. It employs issue tracking tools, monitoring platforms, and chat applications to respond to alerts and notifications.	Whether it's a small technical issue or an enterprise-wide outage, this approach delivers resilience by automating resolution, facilitating dynamic collaboration, and using data to inform and evolve processes.

These related but separate processes often exist within the same organization, which lead to challenges with achieving alignment for swift resolution and mutual understanding of events.

Market Presence Within the Incident Management Spectrum

We designed and conducted the *State of Automation in Incident Management* research to determine an organization's position in the Incident Management Spectrum. This research found that almost all respondents employ either a traditional (40.1%) or modern (58.6%) approach to incident management. Findings also showed that enterprise-scale incident management tools are critical across the spectrum.



Only the most advanced organizations have isolated keys to success across business and incident management functions, which are replicable across the industry with the appropriate investments and commitments. However, not all ITOps and DevOps/SRE teams apply a modern approach to incident management. More than a third of those who said ITOps teams utilize incident response and management processes and tools in their organization (36.1%), apply a traditional approach to incident management. Similarly, more than a third of those who said DevOps/SRE teams utilize incident response and management processes and tools in their organization (35.1%) apply a traditional approach. Organizations who employ ad hoc, traditional, and even modern methods need a new approach to incident management.

Differences in the Incident Management Spectrum

	Ad Hoc	Traditional	Modern	Adaptive
Incidents vs. Innovation	Don't measure	Majority of time spent firefighting	Equal time resolving incidents / building features	Majority of time spent on new features, incident prevention
Digital Transformation Budget	None	<$1M	>$1M	>$1M
Top Tools	None specified	Service desks	Incident management	AIOps
Incident Triggers	Customer-reported	System-reported	Automated indicators	Automated indicators
Leadership Alignment	No role	No role	Support and process-aware	Support and process-aware

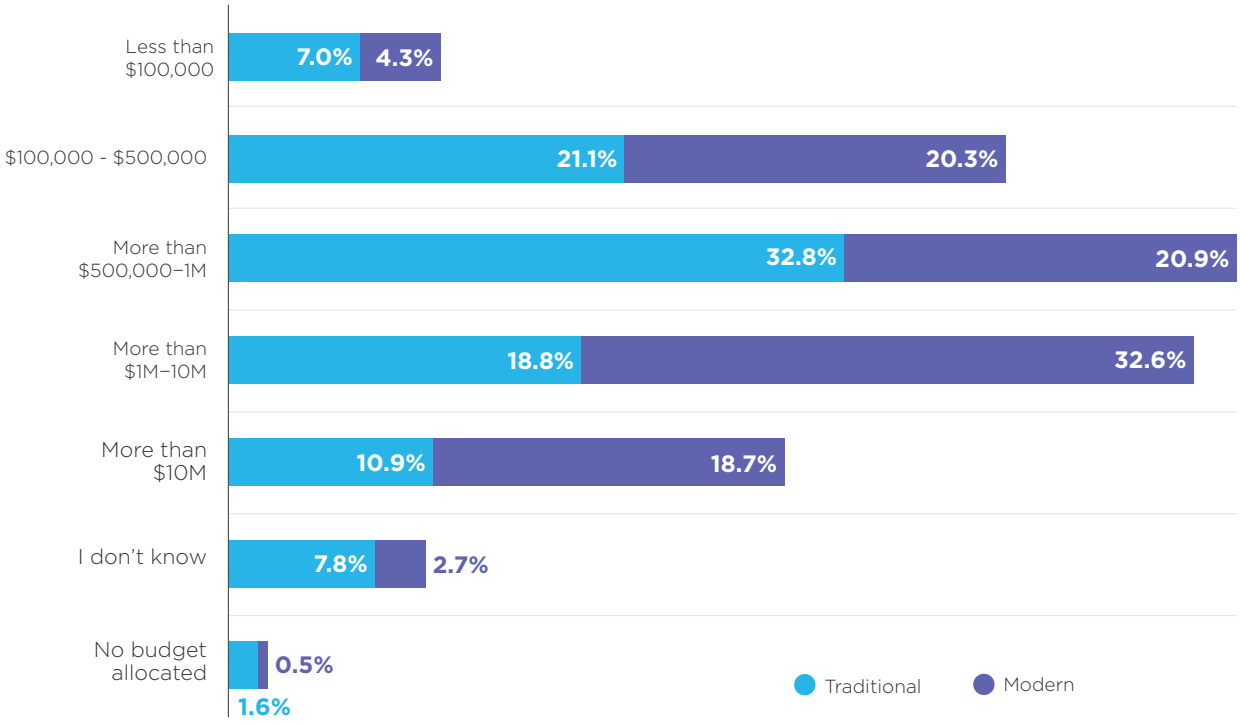
Spectrum: Traditional

Technology professionals who identified a traditional approach to incident management have smaller digital transformation budgets, a lack of executive leadership support, and focus more on firefighting compared to innovation. The most common situations that trigger incidents include system-reported issues. Service desks are also the most common incident management tool used by organizations in this category.

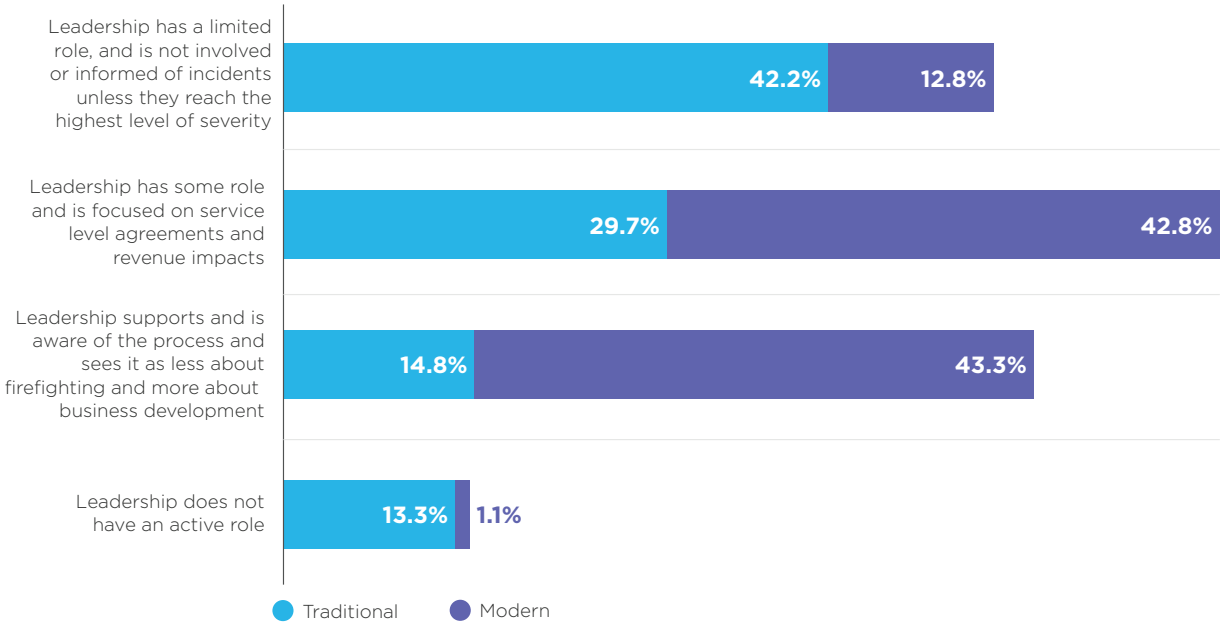
Spectrum: Modern

Technology professionals who identified a modern approach to incident management allocated more of their budget to digital transformation. Their organizations have executive leadership support and their teams spend equal to most of their time on new features, delivering digital services, and preventing recurring incidents. They also take a more advanced, automated approach compared to organizations who employ a traditional approach. Triggers include changes in system performance beyond pre-determined thresholds which cause automatic responses (67.4%) and proactive indicators of poor customer experience and engagement (69.5%). Incident management tools (e.g., PagerDuty, xMatters, OpsGenie, VictorOps) are most commonly used for incident response and management by organizations in this category.

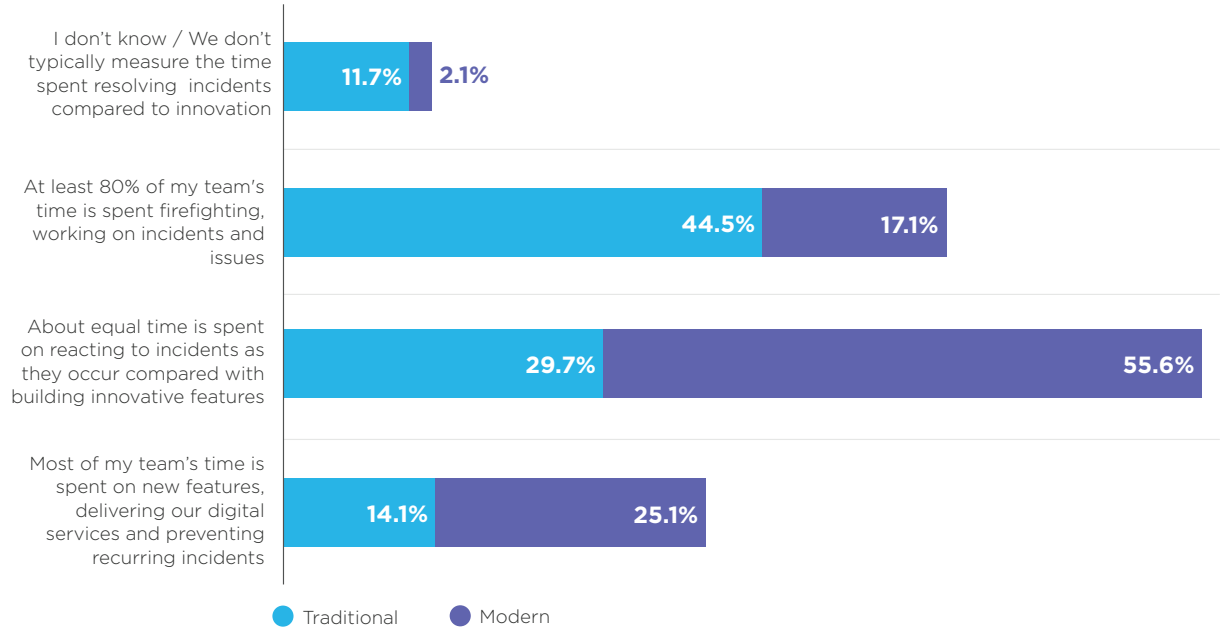
How much are you budgeting (personnel + discretionary) to support and manage digital transformation initiatives within your organization?



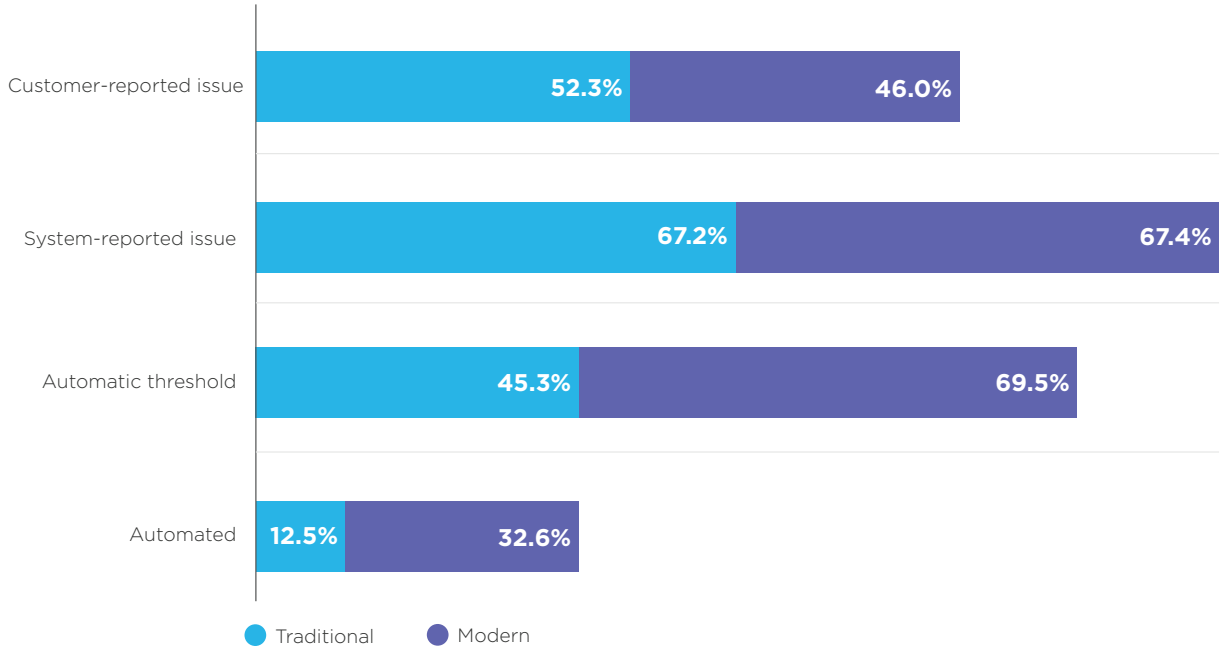
What role does executive leadership (technical or business) have in your organization's incident response and management process?



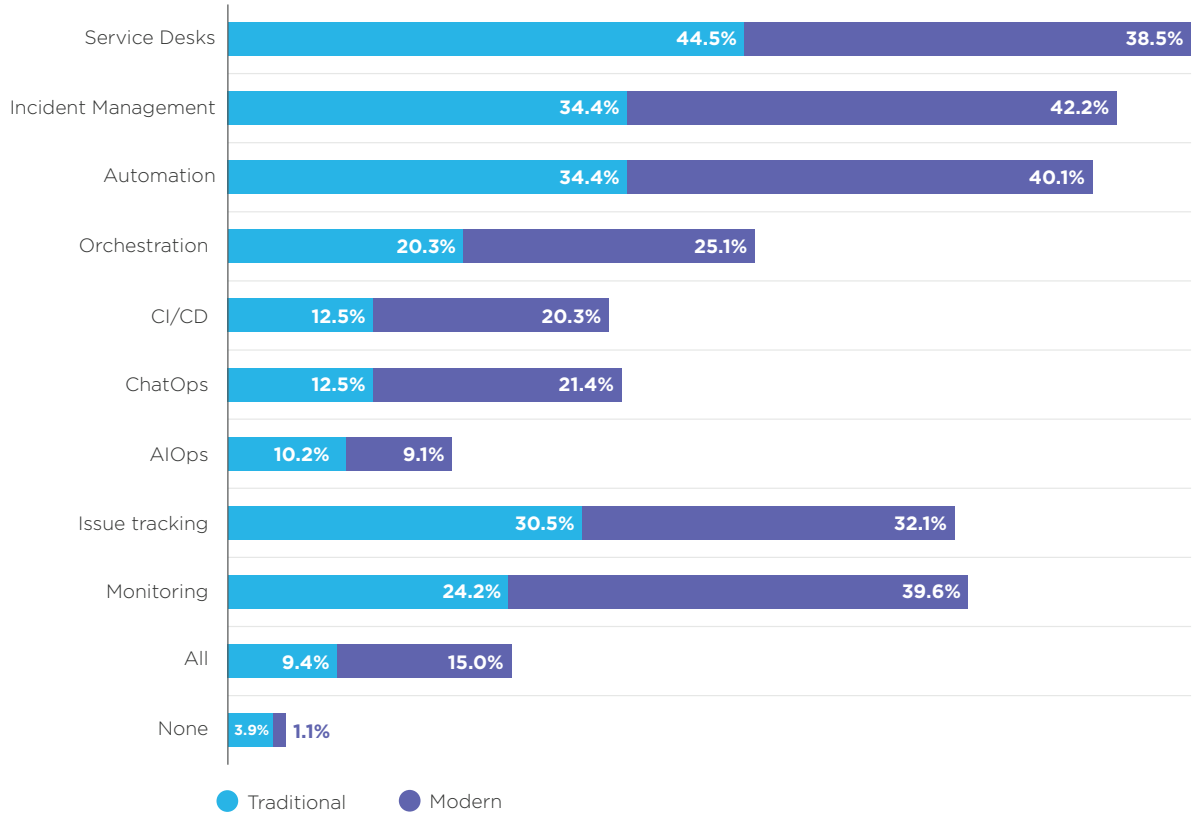
Approximately how much of your team's time is spent resolving incidents compared to time spent on innovation?



Which situations most commonly trigger incidents in your organization? Select those that apply.



What tools do you currently use for incident response and management? Select those that apply.



Spectrum: Ad Hoc and Adaptive

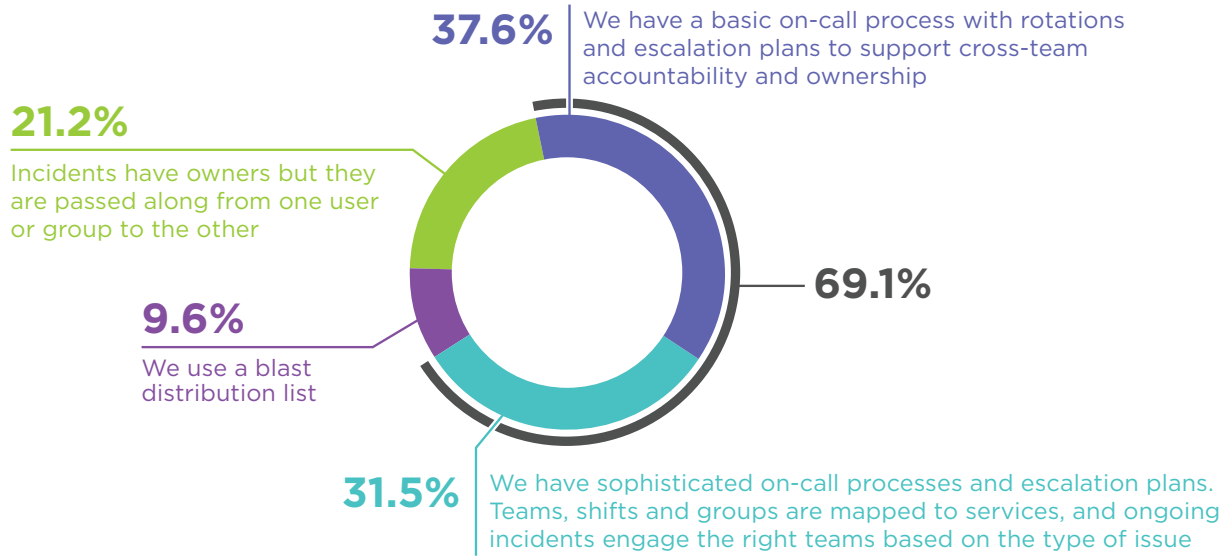
While only a small sample of respondents apply an ad hoc (.6%) or adaptive (.6%) approach to incident management, findings point to potential characteristics for organizations that fall in these categories.

Technology teams with an adaptive approach also have executive leadership who supports the process and sees it as less about firefighting and more about business development. Most of their team's time is spent on new features, delivering digital services and preventing recurring incidents.

Those who apply an ad hoc approach report that leadership does not have an active role in incident management. These organizations also don't typically measure the time they spend resolving incidents compared to innovation.

Trends: Collaboration, Constant Learning and Automation

More than two-thirds (69.1%) of respondents have team-oriented processes for incident management.



Despite the application of team-oriented processes by a majority of technology professionals surveyed, there are key areas for improvement.

Less than half of respondents (46.9%) reported that they use tools such as instant messaging, conference calling, SMS, and targeted emails to engage team members, stakeholders, and customers during an incident. Others deploy less sophisticated processes such as email blasts, conference bridges or manual setup and outreach, which typically delay incident resolution. A small proportion of respondents use automated chat channel creation, collaborator invitations, and chatbots to help engage.

Tools used for team communications

46.9%
instant messaging, conference calling, SMS and targeted emails

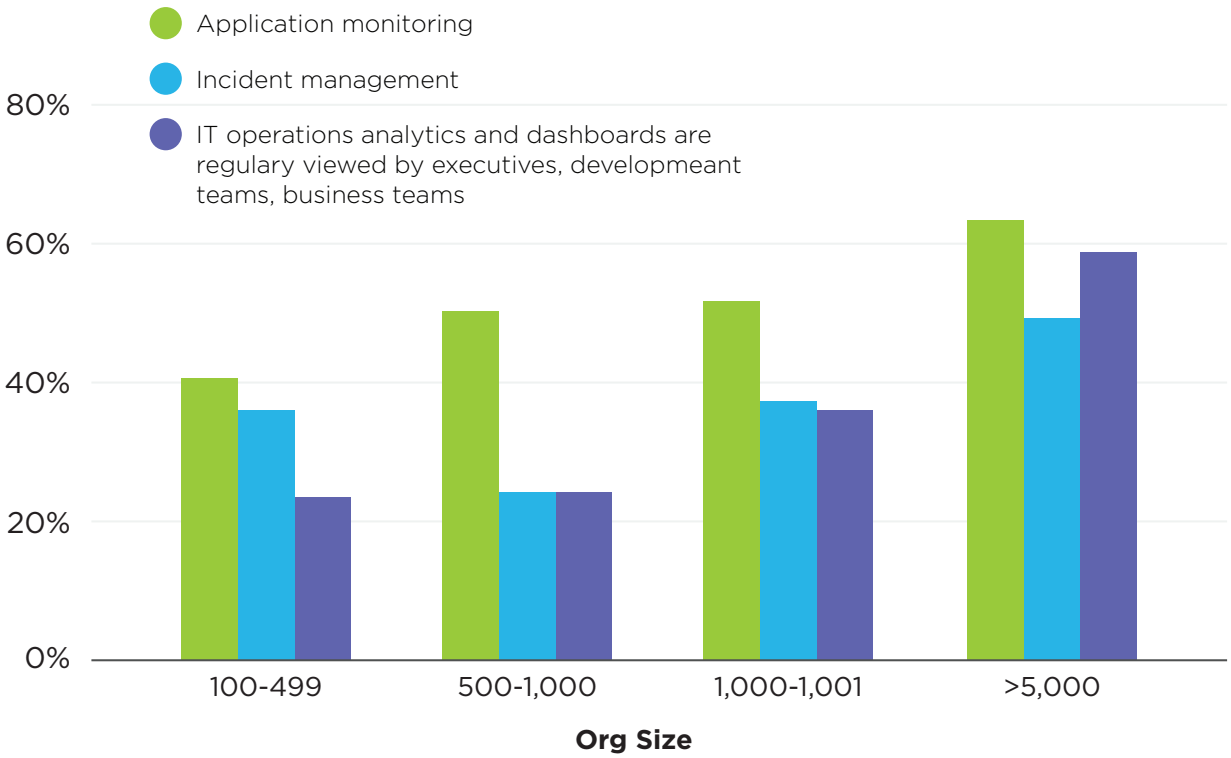
43.4%
email blasts or conference bridges or manual setup and outreach

9.6%
automated chat channel creation, collaborator invitations and chatbots

According to the November 2019 *Incident Management in the Age of Customer-Centricity* research, 91.6% of respondents reported that delivering a superior customer experience is a priority in their role. Companies are prioritizing customer experience and look to reliable digital services as an indicator of customer success.

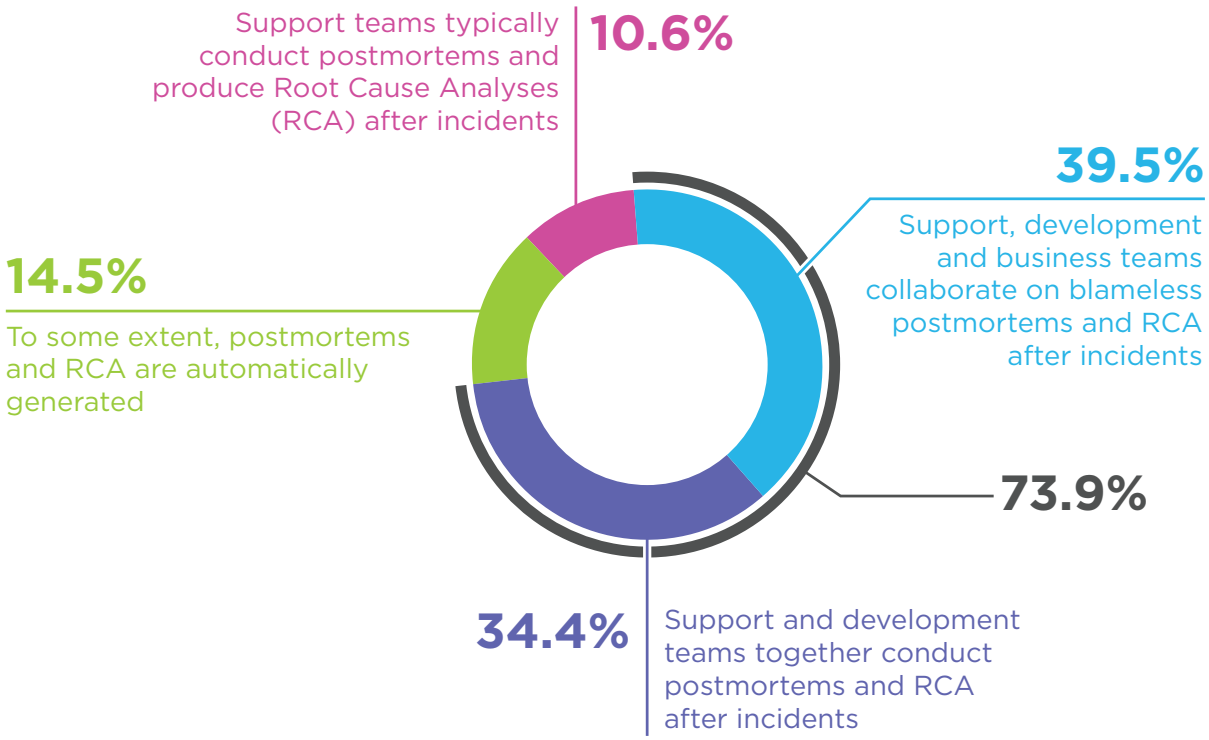
For example, there is an increase in importance of analytics and dashboards which are viewed regularly not just by development teams, but also by executives and business teams. Additionally, as the size of a company increases, so does its use of tools to enable automation of incident management processes.

Tools used to enable automation of incident management processes



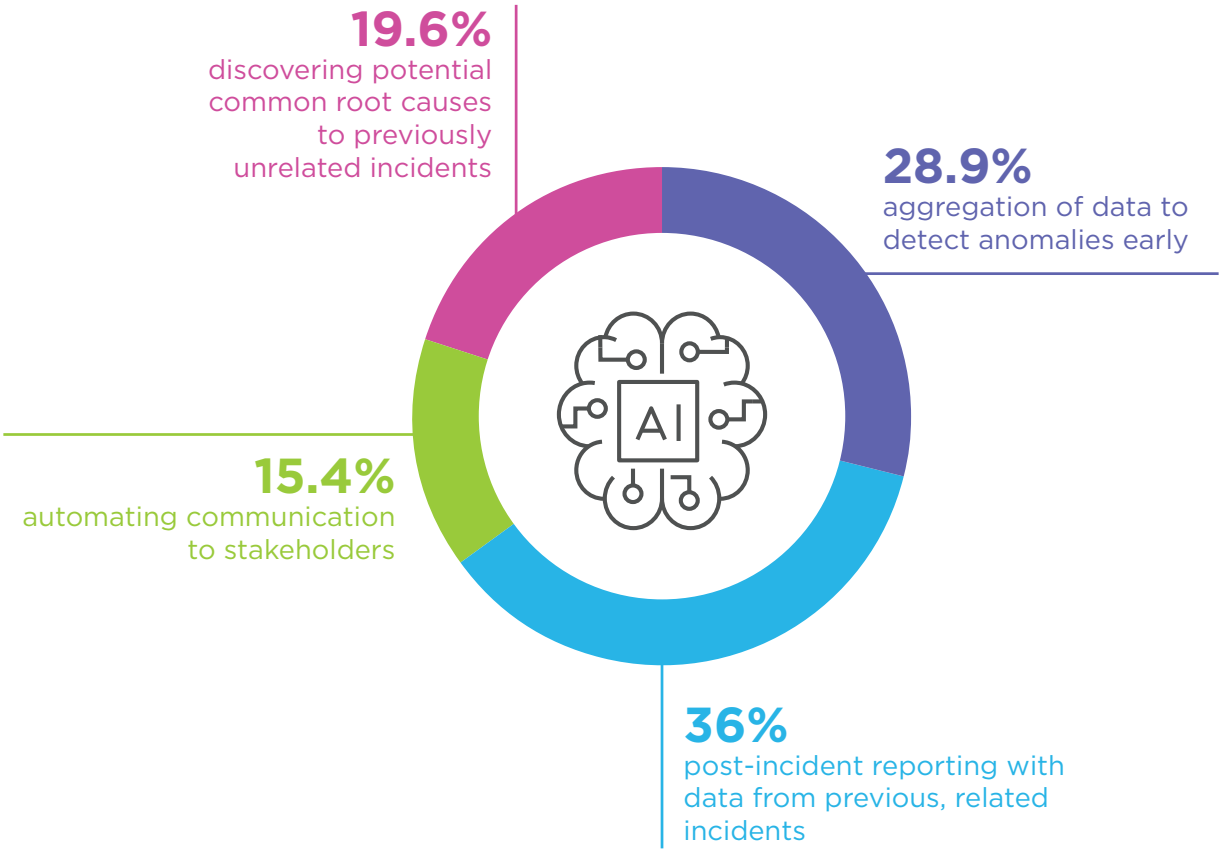
While a majority of respondents (73.9%) report that support and development teams collaborate to assess the cause of an incident, after an incident is identified, there is an opportunity to automate the postmortem process and introduce collaboration with business teams. Only 39.5% of respondents reported that support, development, and business teams collaborate on blameless postmortems and Root Cause Analyses (RCA) after incidents.

Postmortem automation



Automated post-incident reporting is essential for raising an organization's awareness about the things that can go wrong so that corrective and preventative actions can be taken promptly. When asked about using artificial intelligence or machine learning for incident management, top benefits identified by respondents relate to those that prepare technology teams for future customer-impacting incidents. These include using artificial intelligence and machine learning for aggregation of data to detect anomalies early and inform post-incident reporting with data from previous, related incidents.

Which of the following do you see as benefits of using artificial intelligence or machine learning for incident management?



A New Era for Incident Management

We are living and working in a technology forward world where the pace with which businesses introduce new, reliable digital services will transform the customer experience and determine business success. Rapid migration to digital services enables the next generation of innovation. While the ingenuity is exciting, the pace often compromises the customer experience.

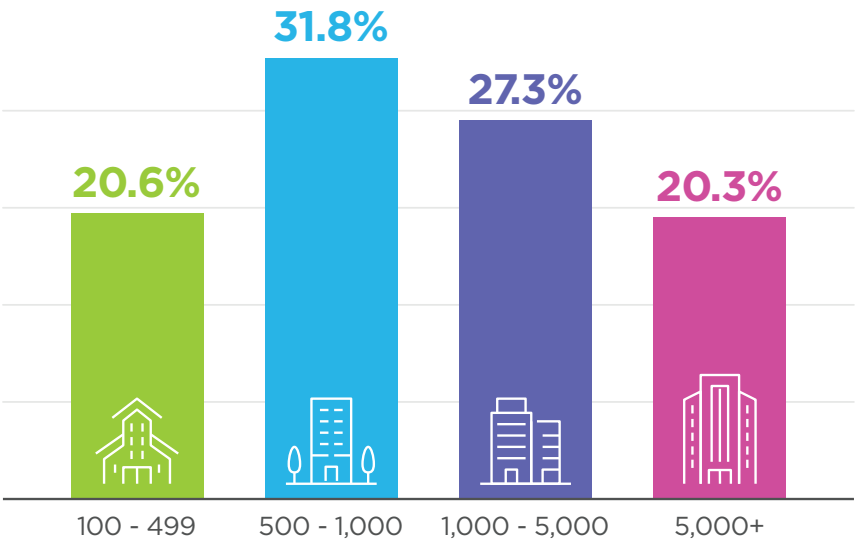
Today's digital, fast moving, competitive environment requires teams to spend less time supporting operations and more time innovating. Achieving digital service resilience requires an approach that fosters greater alignment between teams and tools as companies grow. As evidenced across various organizations, there is an opportunity for technology practitioners to take a giant leap forward and realize a higher level of customer delight through automation, collaboration, and constant learning, so more of their time can be spent on creating business value.

Given the speed of digital innovation and infrastructure complexity, advancing an organization's position in the Incident Management Spectrum is essential for building resiliency. A commitment to continuous automation is required to ensure organizations can meet the demand for digital service reliability and innovation. Automation efforts should be applied in areas of the software development cycle where friction in the process impedes an engineer from completing a task and ensuring an uninterrupted customer experience.

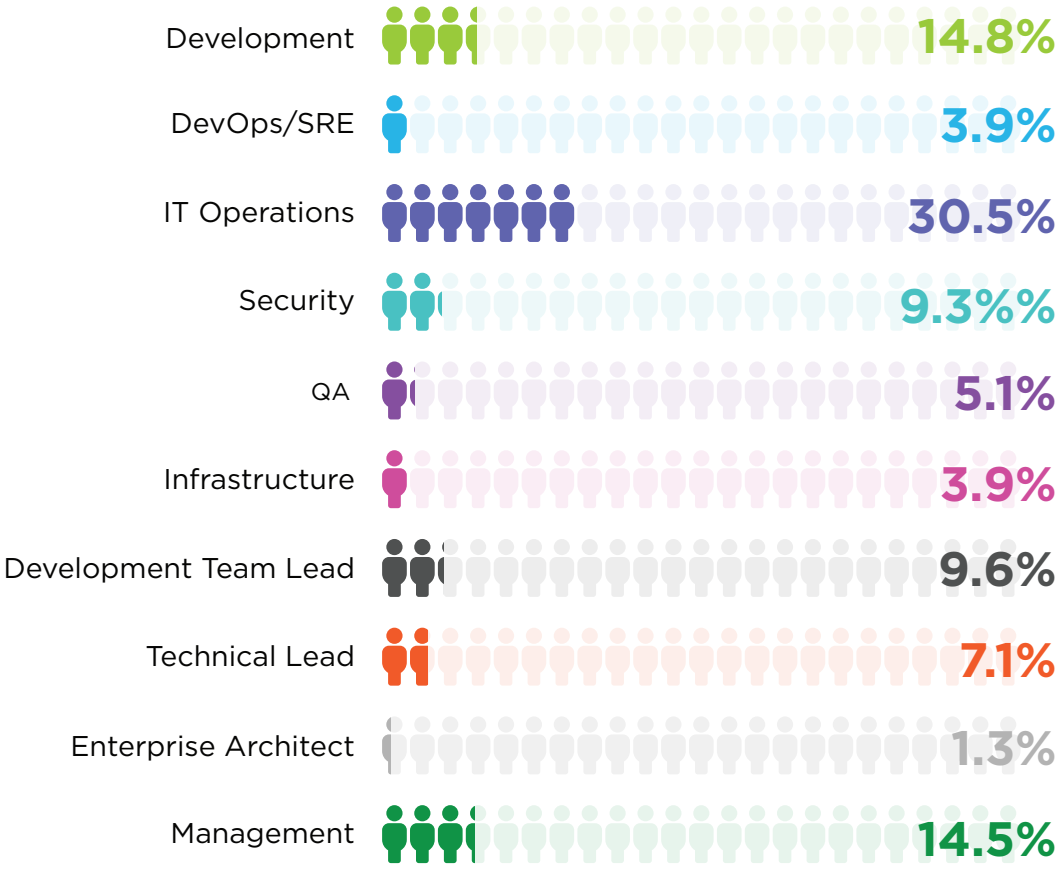
Once an organization understands its place on the Incident Management Spectrum it can evolve its position to better achieve digital service resilience.

Survey Respondent Demographics

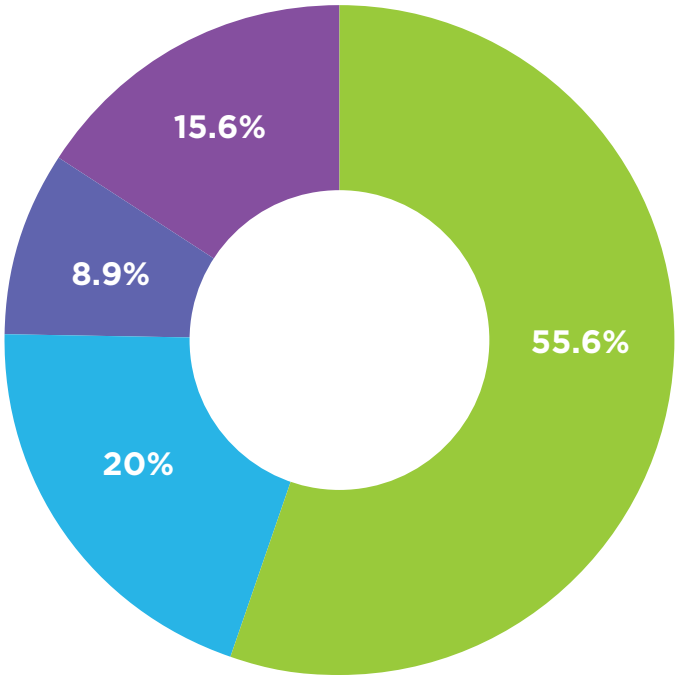
Number of employees in a company



Primary role

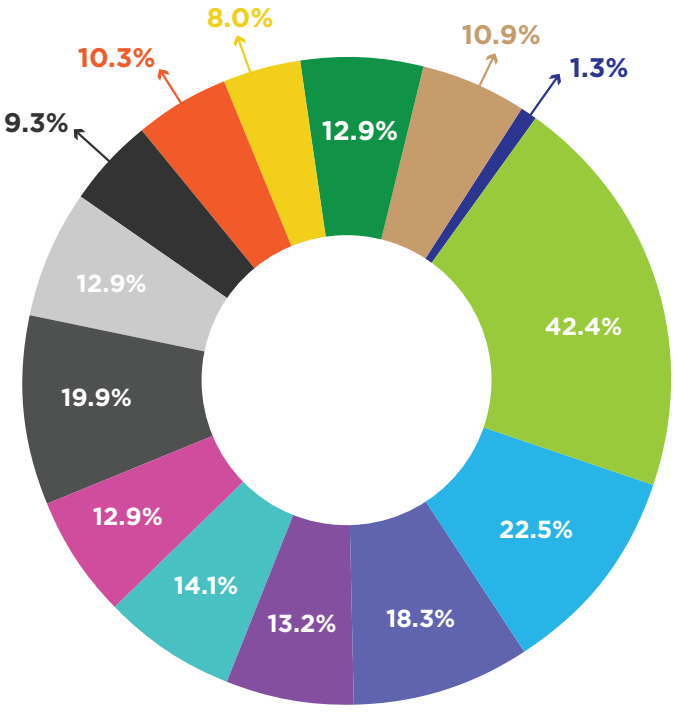


Role in Management



- Manager / Supervisor
- Director (e.g., Director of IT, Director of Engineering, etc.)
- Vice President (e.g., Vice President of IT, Vice President of Engineering, General Manager, etc.)
- Executive (e.g., CIO, CTO, etc.)

Industry



- Information Technology
- Financial Services
- Telecommunications
- Media & Broadcasting / Entertainment
- Manufacturing
- Public Administration / Government
- Healthcare
- Retail
- Transportation / Travel
- Legal Services
- Property / Real Estate
- Retail
- General Public
- Other

About xMatters

xMatters helps enterprises prevent, manage and resolve technology incidents. xMatters industry-leading Digital Service Availability platform prevents technical issues from becoming big business problems. Large enterprises, agile SREs and innovative DevOps teams rely on its proactive incident response, automation and management service to maintain operational visibility and control in today's highly fragmented technology environment. xMatters provides toolchain integrations to hundreds of IT management, security and DevOps tools. xMatters is the primary incident response and management platform trusted by leading global companies and innovative challengers including BMC Software, Credit Suisse, Danske Bank, DXC technology, Experian, NVIDIA, ViaSat and Vodafone. xMatters is headquartered in San Ramon, California and has offices worldwide. For more information, **please visit www.xMatters.com.**

(x) matters®

www.xmatters.com