servicenow | Ponemon INSTITUTE

SPONSORED BY SERVICENOW:
INDEPENDENTLY CONDUCTED BY PONEMON INSTITUTE LLC

COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE

TABLE OF CONTENTS

PART 1. INTRODUCTION 1

PART 2. KEY FINDINGS 4

Timely patching is critical to preventing data breaches 4

Gaps in vulnerability and patch management 7

The race to outpace the attackers continues 17

Automation and sufficient staff enable more timely patching 20

SPECIAL ANALYSIS:

How the size of an organization affects vulnerability management 24

How maturity of vulnerability management practices affects patching 31

Industry differences in vulnerability and patch management 35

PART 3. METHODS 40

PART 4. CAVEATS 44

PART 1. INTRODUCTION

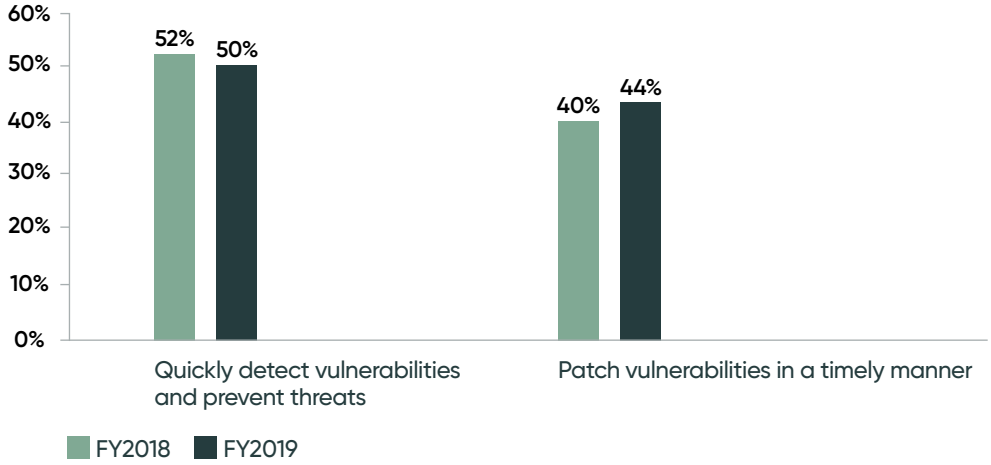
Ponemon Institute is pleased to present the findings of the second study on vulnerability and patch management. As shown in this research, the severity and volume of cyberattacks is increasing. However, most organizations are not comparably enhancing their abilities to prevent hackers from exploiting attack vectors. In fact, it's taking longer to detect and longer to patch critical vulnerabilities than last year. The cost and consequences of this failure are myriad. Thirty-nine percent of respondents say their organizations were aware that actual breaches were linked to known vulnerabilities, an increase from 34 respondents in last year's study. This indicates that more focus should be paid to vulnerability response for business-critical assets. On the upside, organizations that are using automation are getting better at patching.

With sponsorship from ServiceNow, Ponemon Institute surveyed almost 3,000 IT security professionals in the United States, United Kingdom, Germany, France, Netherlands, Australia/New Zealand, Singapore and Japan to understand how organizations are responding to vulnerabilities. In this report, we present the consolidated findings and comparisons to the 2018 study.[1]

According to the findings, organizations seem to be keeping to the status quo in their approaches to patching. As a consequence, they are not achieving significant improvements in their ability to quickly detect and patch vulnerabilities and keep ahead of the attackers. Respondents were asked to rate their organizations' ability to quickly detect vulnerabilities, prevent threats and patch vulnerabilities in a timely manner on a scale from 1 = low ability to 10 = high ability. Figure 1 shows the high ability responses (7+ on the 10-point scale). This year, 50 percent of respondents rate their detection capabilities as very high and only 44 percent say they have a high ability to patch in a timely manner, a very slight increase from last year's research.

[1] Individual country reports are available.

FIGURE 1. The ability to prevent threats and patch vulnerabilities in a timely manner
On a scale of 1 = low ability to 10 = high ability, 7+ responses presented



THE FOLLOWING ARE REASONS VULNERABILITY AND PATCH MANAGEMENT PRACTICES ARE NOT IMPROVING.

- Most organizations are unaware of vulnerabilities that could lead to a data breach.
- On average, it takes 43 days to see a cyberattack once a patch is released for a critical or high priority vulnerability, an increase from 36 days in the 2018 study.
- Organizations' patching process is under greater pressure because they have less time to patch vulnerabilities before being attacked.
- Silo and turf issues delay patching. Eighty-eight percent of respondents say their team is not fully responsible for patching vulnerabilities and they have to coordinate with other teams. As a result, patching is delayed an average of 12 days.
- CVSS scoring is often the only metric of patch prioritization, and leaves out asset criticality and systems as a part of vulnerability response.
- Vulnerability patching is delayed because of a lack of resources, no common view of applications and assets and no ability to take critical applications and systems off-line so they can be patched quickly.
- Respondents believe attackers are outpacing their organizations with such technologies as machine learning/artificial intelligence.
- Too much time is spent navigating manual processes rather than responding to vulnerabilities.

THE FOLLOWING ARE TAKEAWAYS FROM THE RESEARCH

The cost of doing nothing. Since last year's study, more resources are being spent on preventing, detecting and remediating vulnerabilities, but organizations are not able to minimize the risk of an attack. On average, organizations are spending $1.4 million annually based on vulnerability management activities, an increase of an average of $282,750 from 2018 when organizations spent an average of $1.16 million.

This finding indicates the importance of improving the efficiency of the vulnerability management process through automation and more resources. Currently, only 44 percent of respondents say their organizations use automation to assist with vulnerability management and patching. The steps most often automated are prioritization and patching.

Patching prevents data breaches. Almost half of respondents (48 percent) report that their organizations had one or more data breaches in the past two years. Sixty percent of these respondents say these breaches could have occurred because a patch was available for a known vulnerability but not applied. Of these respondents, 62 percent were unaware that their organizations were vulnerable prior to the data breach.

Threat intelligence, incident response platforms and security automation are the preferred tools for improving vulnerability response. Despite the benefits of automation in responding to vulnerabilities, less than half of respondents (46 percent) say they use this technology.

PART 2. KEY FINDINGS

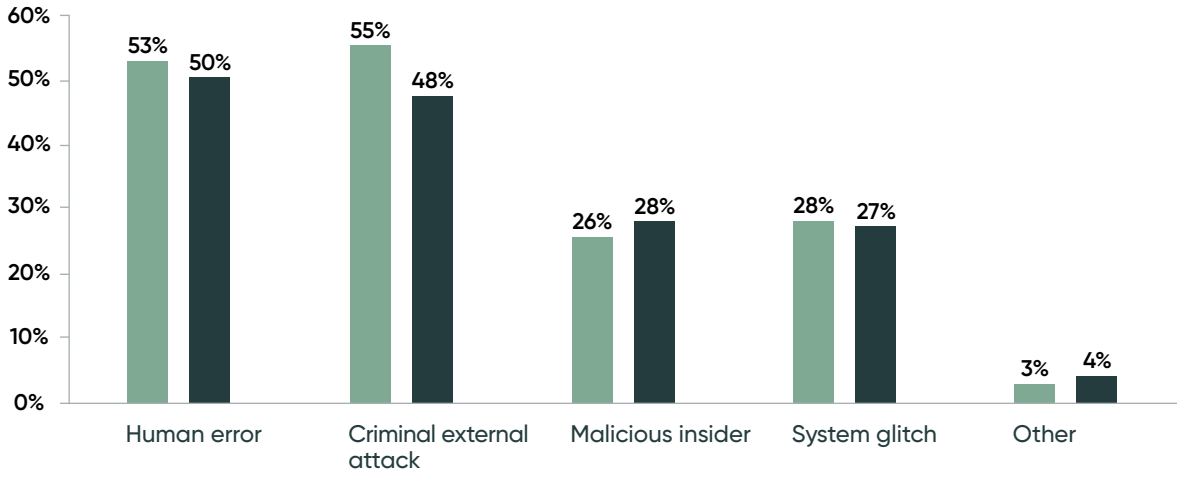
In this section we provide a deeper analysis of the research. The complete audited findings are presented in the Appendix of this report. The findings are organized according to the following topics:

- Timely patching is critical to preventing data breaches
- Gaps in vulnerability and patch management
- The race to outpace the attackers continues
- Automation and sufficient staff enable more timely patching
- How the size of an organization affects vulnerability management
- How maturity of vulnerability management practices affects patching
- Industry differences in vulnerability and patch management

TIMELY PATCHING IS CRITICAL TO PREVENTING DATA BREACHES

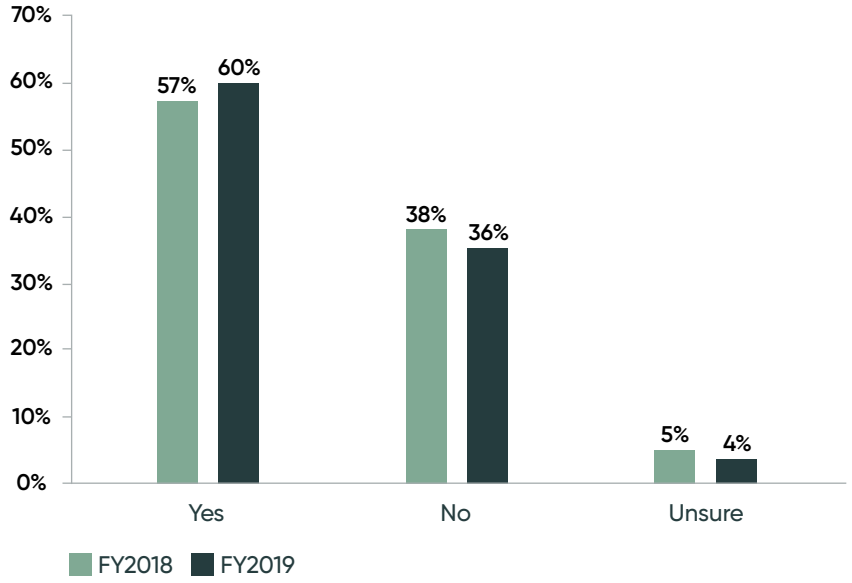
Most data breaches are due to human error and criminal attacks. Same as last year, almost half of respondents (48 percent) say their organizations had a data breach in the past two years. The root causes of these breaches are shown in Figure 2. This year, most breaches were caused by human error (50 percent of respondents). In 2018, the number one root cause was criminal external attacks.

FIGURE 2. What were the root causes of these data breaches?
More than one response permitted



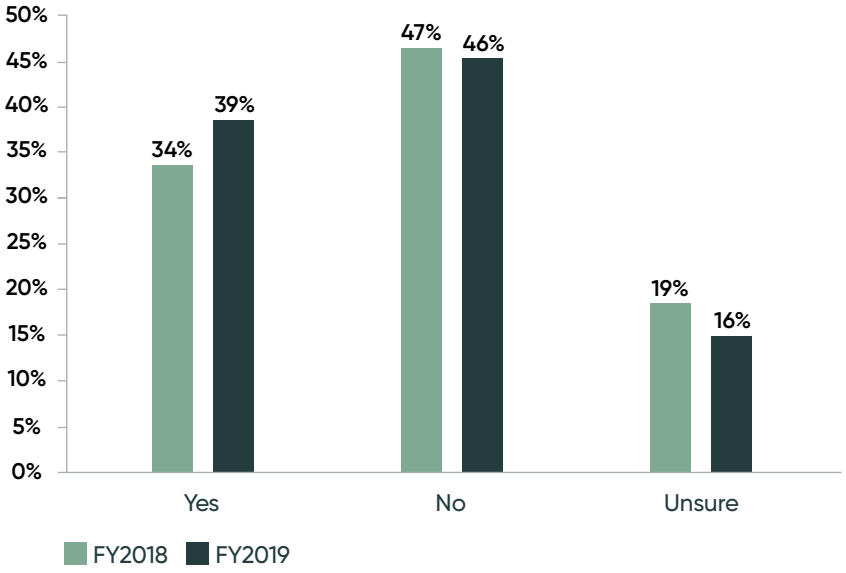
Patching could have prevented many of these data breaches. As shown in Figure 3, 60 percent of these respondents say one or more of these breaches could have occurred because a patch was available for a known vulnerability but not applied.

FIGURE 3. Did any of these breaches occur because a patch was available for a known vulnerability but not applied?



Of the 60 percent of respondents who say a patch was available, 62 percent of respondents (46 percent + 16 percent) were unaware that their organizations were vulnerable to a data breach, as shown in Figure 4. Only 39 percent of respondents say their organizations were actually aware that their organizations were vulnerable prior to the data breach, a slight increase since last year.

FIGURE 4. **Was your organization aware it was vulnerable prior to the data breach?**

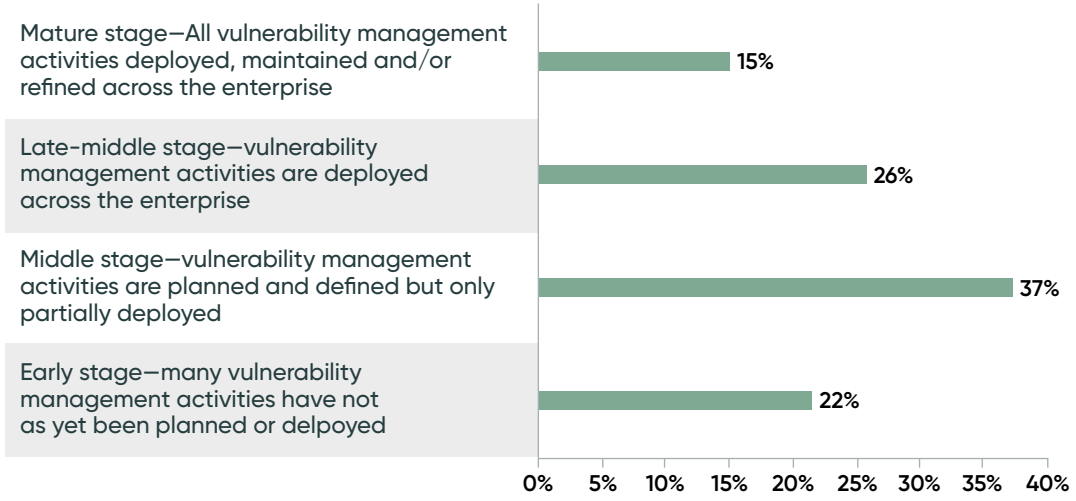


GAPS IN VULNERABILITY AND PATCH MANAGEMENT

Most vulnerability management programs are not mature. In the context of this research, vulnerability management is the process of making certain vulnerabilities are effectively and frequently fixed. A characteristic of a mature vulnerability management program is the ability to prioritize vulnerabilities that pose the most immediate risk to the network.

As shown in Figure 5, 59 percent of respondents (22 percent + 37 percent) say their vulnerability management programs are in the early or middle stage which means that many activities are only partially deployed or have not been planned or deployed. As a result, only 40 percent of respondents have a single view of the full vulnerability management lifecycle, including exception handling.

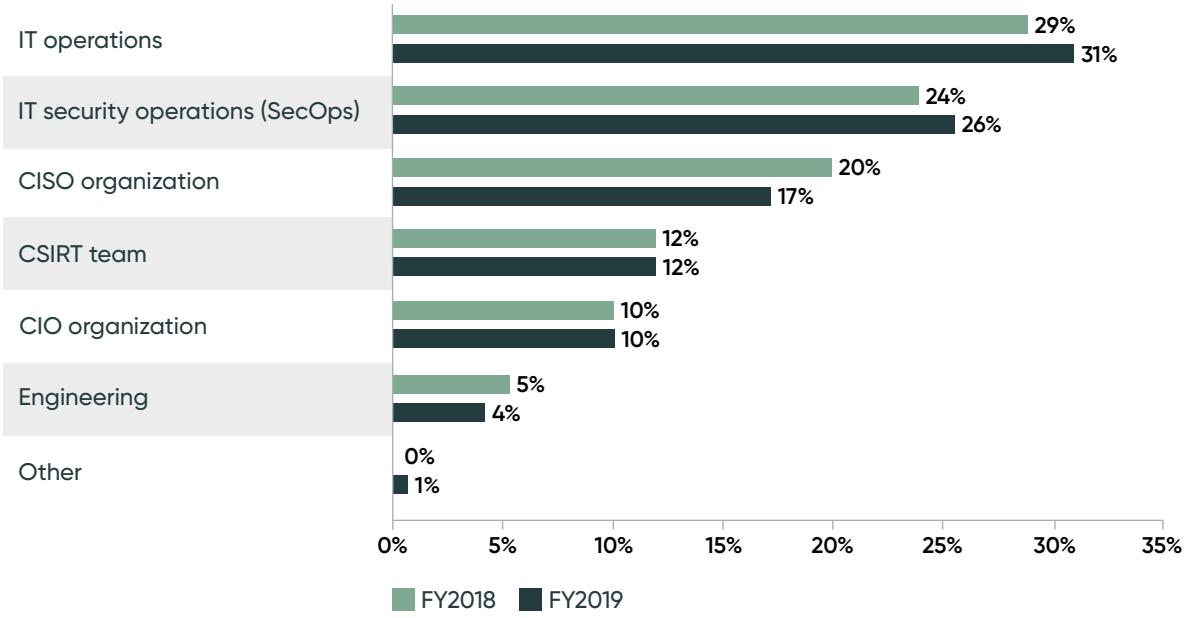
FIGURE 5. What best describes the maturity level of your organization's vulnerability management lifecycle?



IT operations and IT security operations are most responsible for patching. As shown in Figure 6, 31 percent of respondents say IT operations is most responsible for applying the majority of patches and 26 percent of respondents say it is IT security operations.

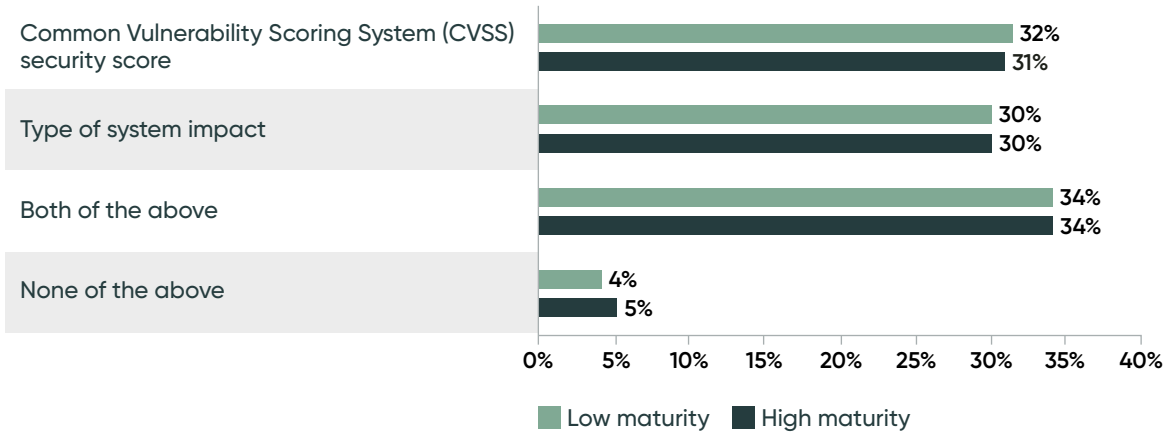
Eighty-eight percent of respondents say they have to coordinate with other areas of the organization when patching vulnerabilities and this results in taking an extra 12 days before a patch can be applied.

FIGURE 6. Which team in your organization is responsible for applying the majority of patches?
Only one choice permitted



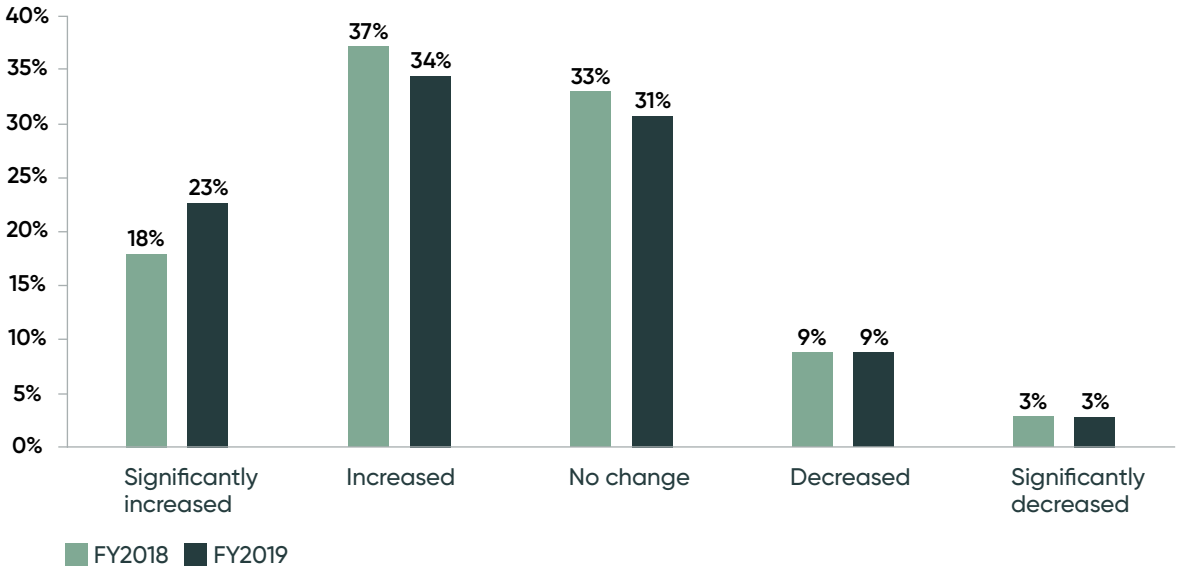
CVSS scoring, as shown in Figure 7, is often the only metric of patch prioritization and leaves out asset criticality and systems as part of vulnerability response.

FIGURE 7. How do you prioritize vulnerabilities?



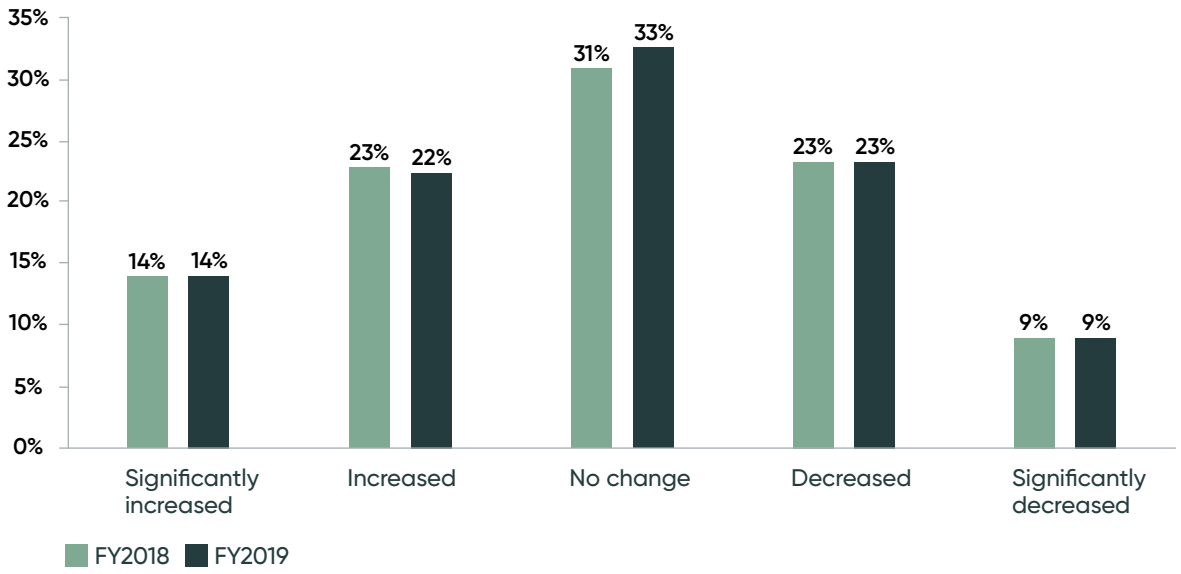
It takes more time to detect a cyberattack against a critical vulnerability following the release of a patch. On average, it takes 43 days to see a cyberattack once a patch is released for a critical or high priority vulnerability, an increase from 36 days in the 2018 study. As shown in Figure 8, 57 percent of respondents (23 percent + 34 percent) say the time between when they become aware of a cyberattack and a patch is available has increased.

FIGURE 8. How has the time changed to see a corresponding cyberattack after a patch is released for a critical vulnerability?



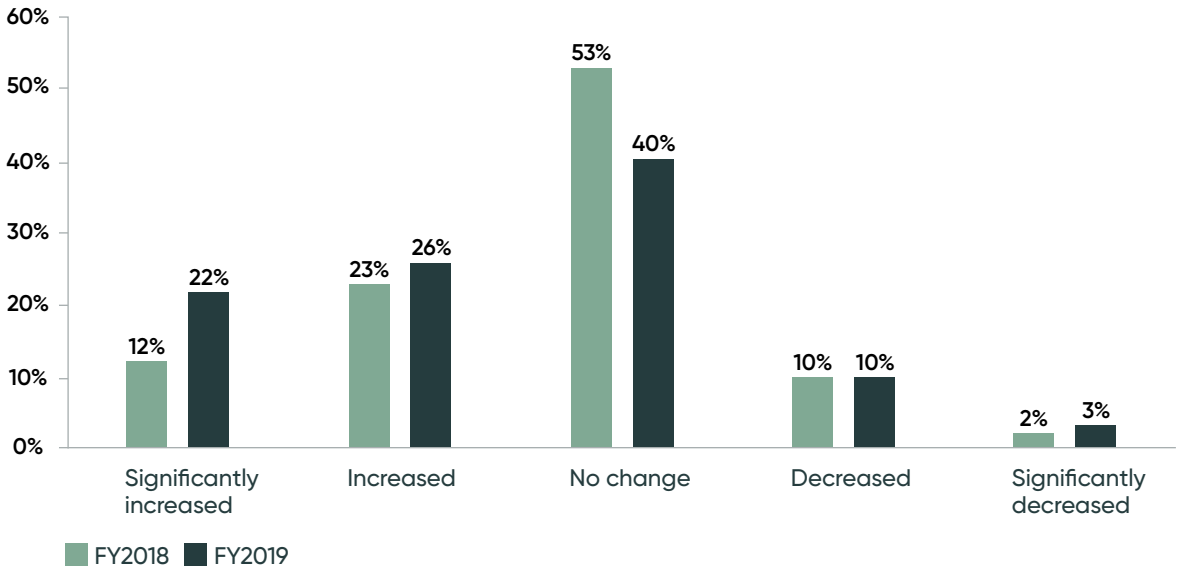
It takes more time to patch critical vulnerabilities. On average, it takes 16 days to patch a critical vulnerability after it has been detected. According to Figure 9, the time to patch a critical vulnerability has significantly increased or increased, according to 36 percent of respondents. One-third of respondents say there has been no improvement in being able to patch quickly.

FIGURE 9. In the past two years, how has the time changed to patch a critical vulnerability once detected?



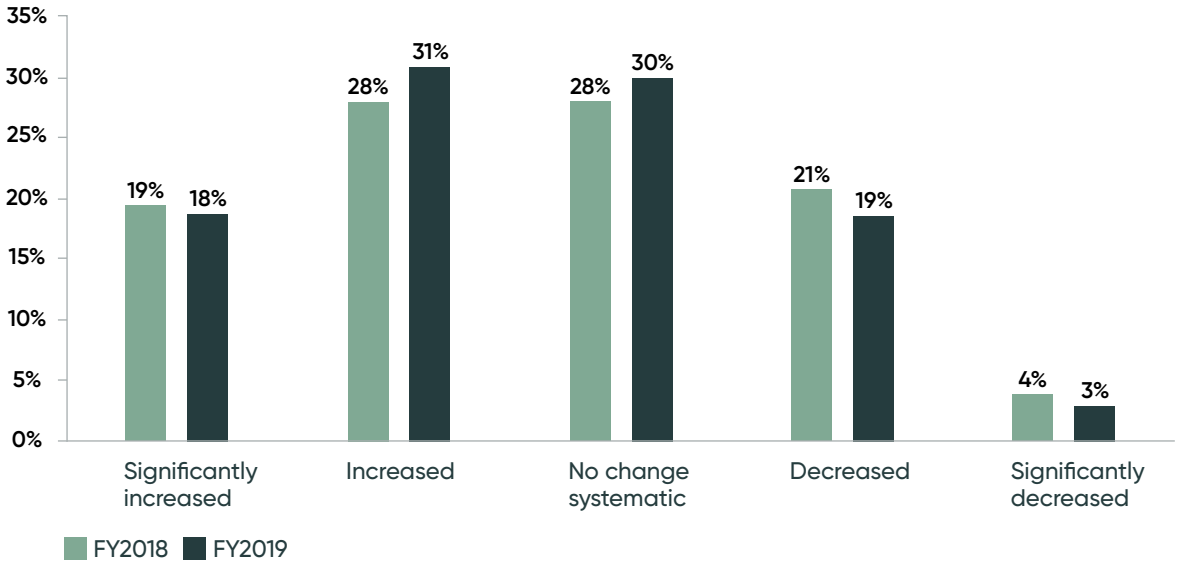
Organizations have less time to prevent an attack against a low priority vulnerability. On average it takes 169 days to see a cyberattack once a patch is released for a medium or low vulnerability. According to 48 percent of respondents (22 percent + 26 percent), it takes longer to patch a medium or low priority as shown in Figure 10.

FIGURE 10. How has the time changed to see a corresponding cyberattack after a patch is released for a low priority vulnerability?



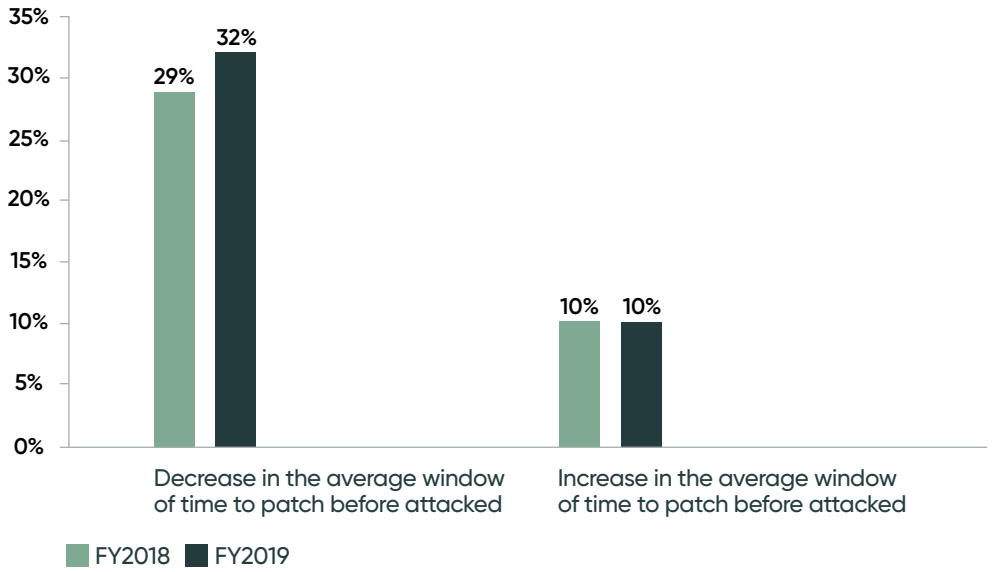
On average, it takes 151 days to patch a medium or low priority vulnerability, an increase from 125 days in 2018. According to 49 percent of respondents (18 percent + 31 percent), as shown in Figure 11, the time to patch a medium or low priority vulnerability has increased and is similar to last year's research.

FIGURE 11. In the past two years, how has the time changed to patch a low priority vulnerability once detected?



Organizations' patching process is under greater pressure because they have less time to patch a vulnerability before being attacked. Fifty percent of respondents say the window of time has decreased in the past two years. Only 20 percent of respondents say they have more time and 30 percent of respondents say there has been no improvement. Figure 12 shows the average percentage decrease and increase in the average window of time to patch in the past two years.

FIGURE 12. By what percentage did the average window of time to patch increase or decrease? Extrapolated values presented



Year over year, more time is spent on prevention, detection and remediation of vulnerabilities with no improvements in reducing the risk of an attack. As shown in Table 1, since last year, there was a 30 percent increase in downtime due to patching of vulnerabilities, meaning a higher impact on service outcomes. The biggest increase (35 percent) is in patching applications and systems.

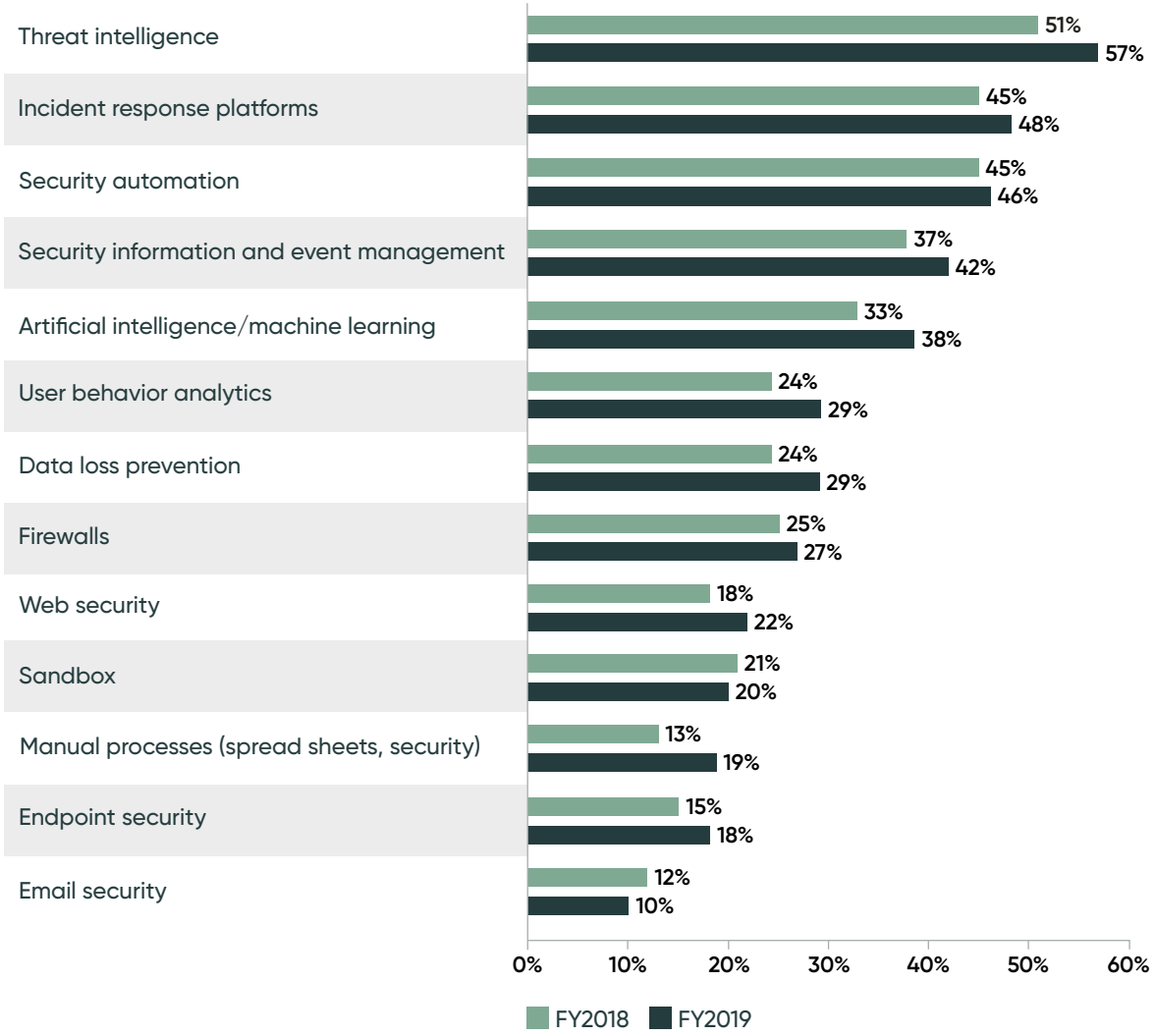
With the exception of lost time coordinating with the responsible team before a patch is applied, since last year's study more time is being spent on preventing, detecting and remediating vulnerabilities each week. Based on an average pay rate per hour of $62.50, an average of $1.4 million is spent annually on these vulnerability management activities, an increase of an average of $282,750 from last year.

TABLE 1. Time spent preventing, detecting and remediating vulnerabilities each week	Average hours (2019)	Average hours (2018)	Cost per week* (2019)	Cost per week* (2018)
How many hours each week are spent monitoring systems for threats & vulnerabilities?	139	127	$8,688	$7,938
How many hours each week are spent patching applications and systems?	206	153	$12,875	$9,563
How many hours each week are spent documenting and/or reporting on the patch management process?	56	41	$3,500	$2,563
How much downtime occurs because of the patching of vulnerabilities?	30	23	$1,875	$1,438
How much time is lost coordinating with the responsible team before a patch is applied?	12	12	$750	$750
Total per week	443	356	$27,688	$22,250
Total per year	23,036	18,512	$1,439,750	$1,157,000

*IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)

Threat intelligence, incident response platforms and security automation are the preferred tools for improving vulnerability response. Figure 12, shows trending with almost universal increases in tool usage. Despite the benefits of automation in responding to vulnerabilities, less than half (46 percent of respondents) say they use this technology.

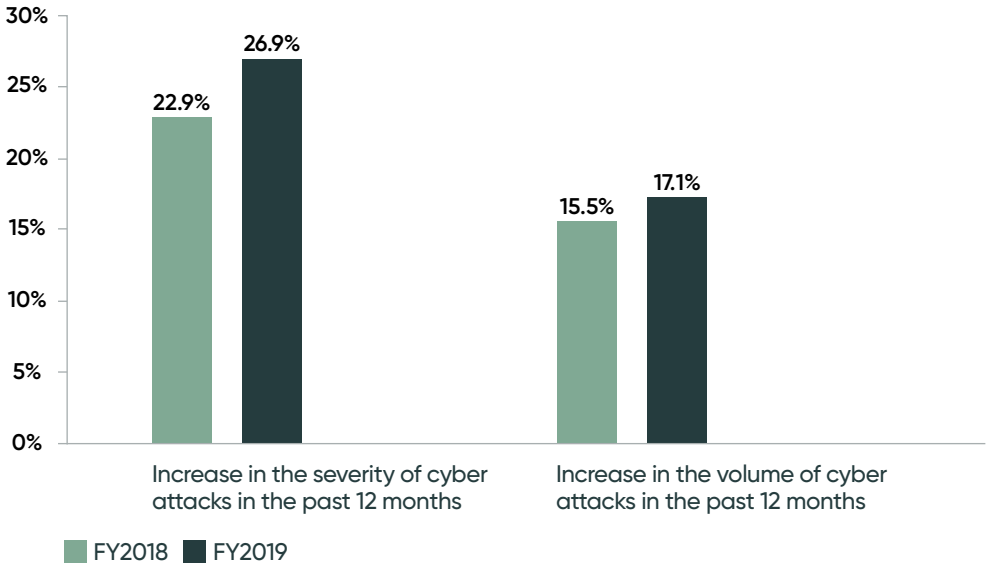
FIGURE 13. Tools used to respond to vulnerabilities. More than one response permitted



THE RACE TO OUTPACE THE ATTACKERS CONTINUES

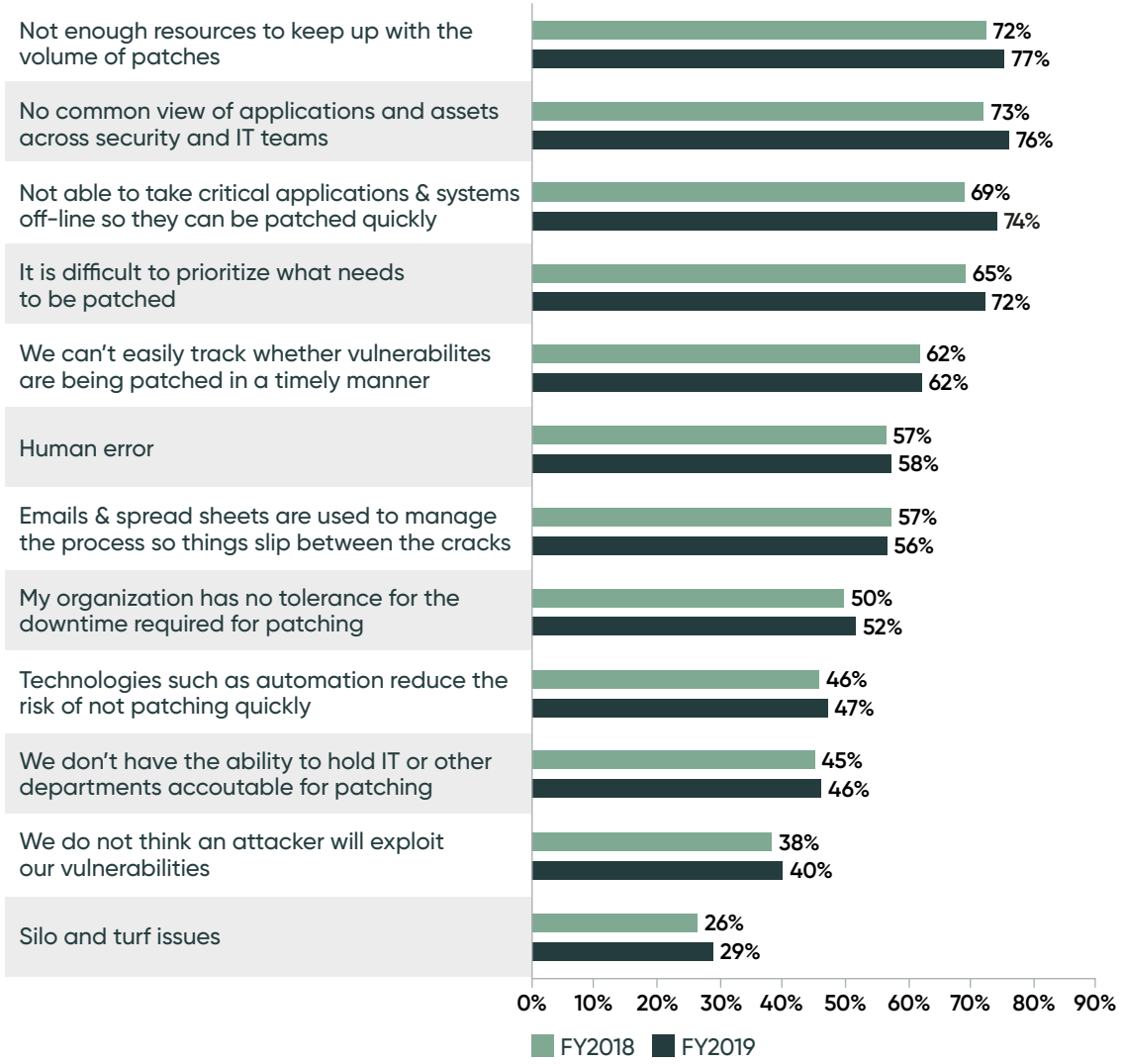
Stopping the bad guys continues to be a daunting task. As shown in Figure 14, the severity and volume of cyberattacks has increased an average of 27 percent and 17 percent in the past 12 months, respectively

FIGURE 14. How has the volume and severity of cyberattacks increased in the past 12 months? Extrapolated values presented



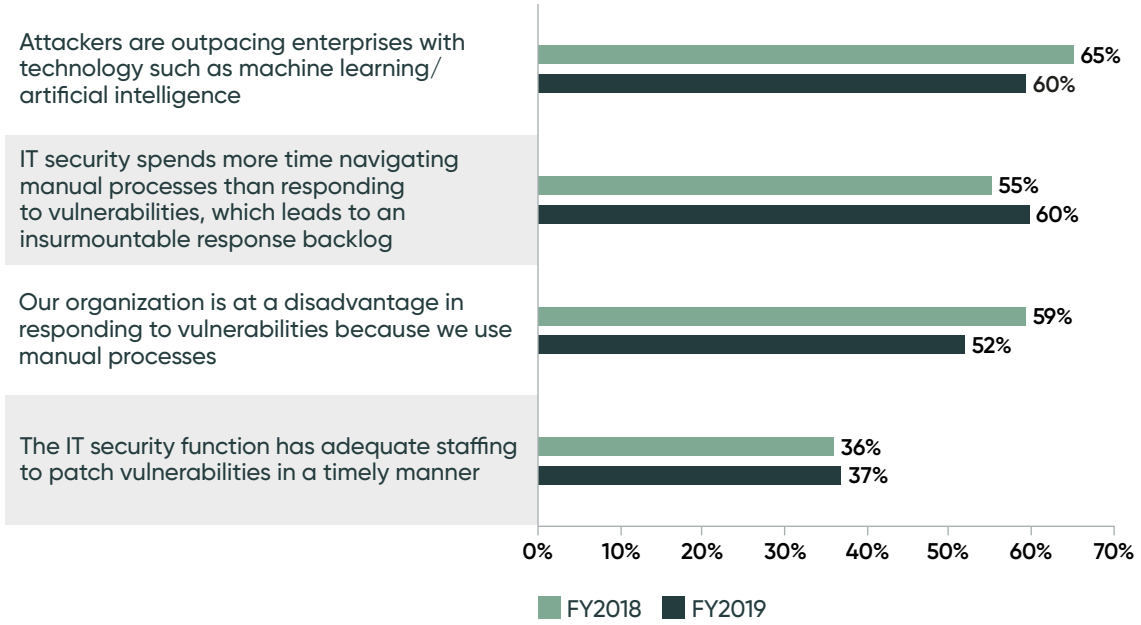
Delays in vulnerability patching are getting worse. Organizations are not able to conquer the delays that occur in vulnerability patching. As shown in Figure 15, more respondents since last year are reporting delays in vulnerability patching caused by not having enough resources to keep up with the volume of patches (77 percent of respondents), not having a common view of applications and assets across security and IT teams (76 percent of respondents), not able to take critical applications and systems off-line so they can be patched quickly (74 percent of respondents) and difficulty in prioritization (72 percent of respondents).

FIGURE 15. Why major delays occur in vulnerability patching. More than one response permitted



Organizations are not keeping up with the hackers. As shown in Figure 16, concerns that attackers are outpacing enterprises because of their use of machine learning/artificial intelligence have decreased from 65 percent to 60 percent of respondents who still agree that attackers are using these technologies. More respondents (60 percent) agree that IT security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable response backlog. Fifty-two percent of respondents say their organizations are at a disadvantage in responding to vulnerabilities because they use manual processes.

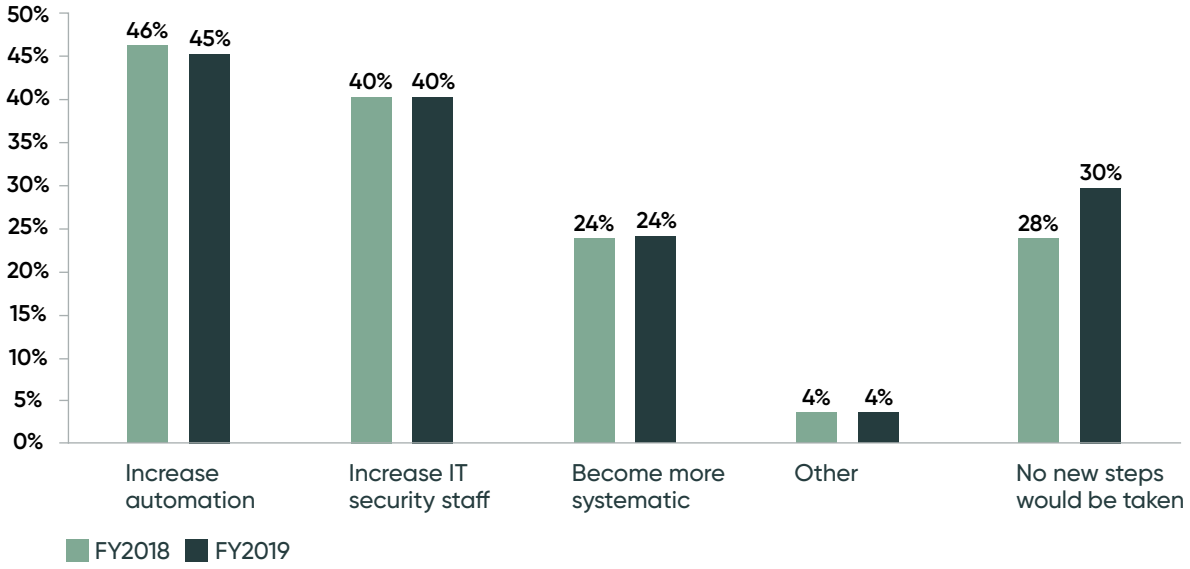
FIGURE 16. Perceptions about the broken processes in patch management
Strongly agree and Agree responses combined



AUTOMATION AND SUFFICIENT STAFF ENABLE MORE TIMELY PATCHING

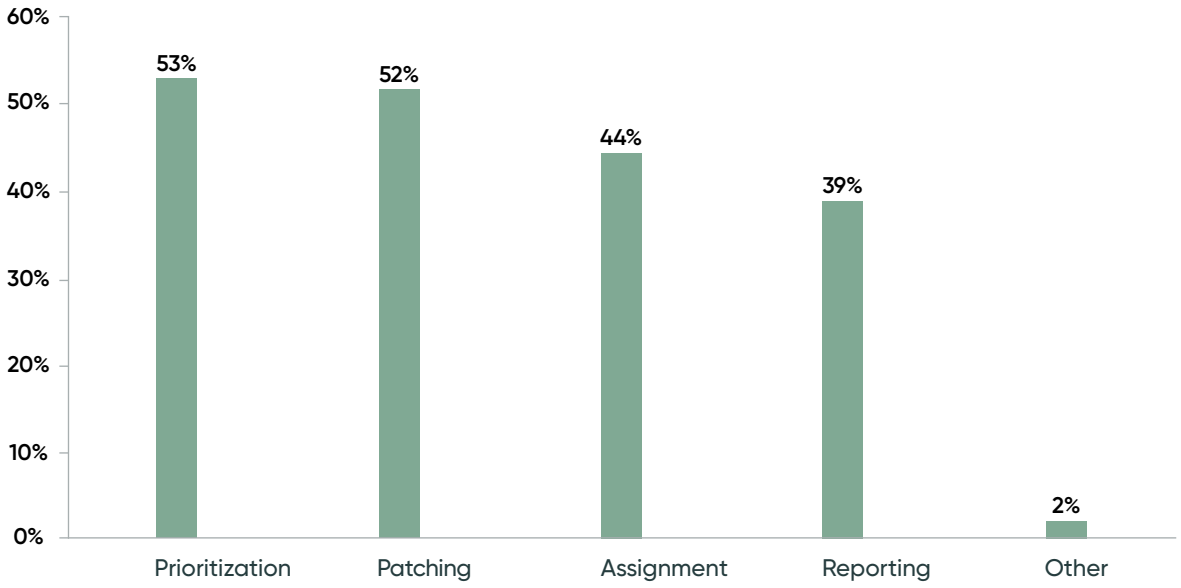
Automation and more staff are steps organizations believe would improve patching. Seventy percent of respondents say their organizations would take measures to improve their patch management if strict new data breach laws holding companies accountable for data breaches involving customer information were passed. According to Figure 17, the steps most likely to be taken are an increase in automation (45 percent of respondents) and an increase in IT security staff (40 percent of respondents).

FIGURE 17. What steps would you take to improve your organization's patch management?
More than one response permitted



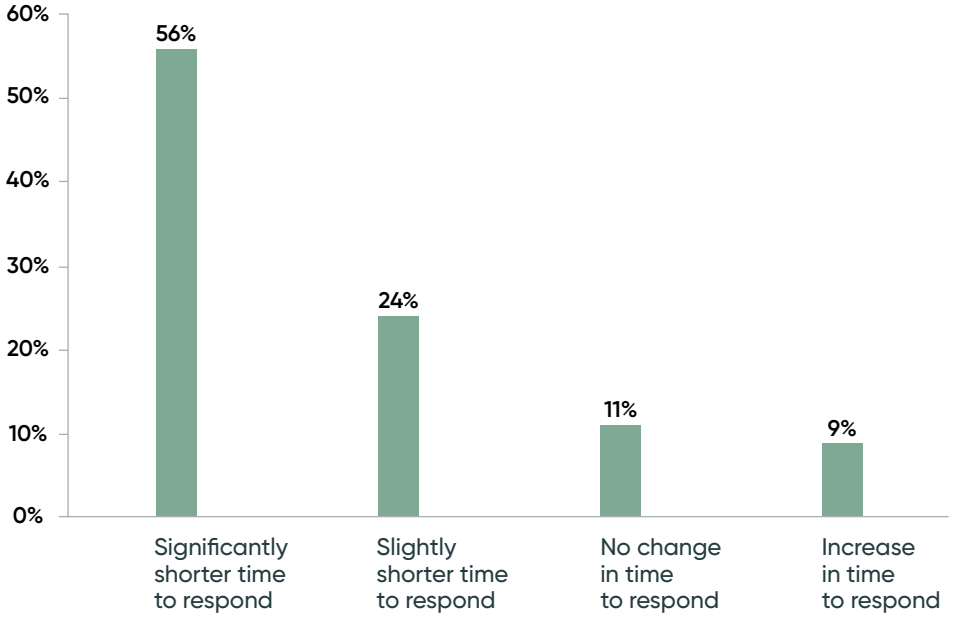
Forty-four percent of respondents say their organizations use automation to assist with vulnerability management and patching. According to Figure 18, the steps most often automated are prioritization and patching.

FIGURE 18. **What steps do you automate?**
More than one response permitted



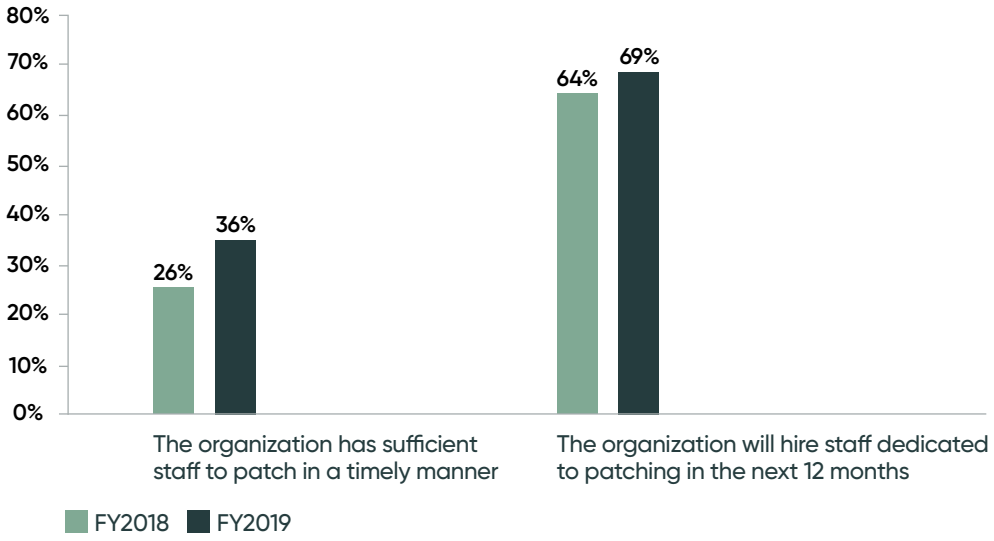
Automation reduces the time to respond to vulnerabilities. According to Figure 19, 80 percent of organizations (56 percent + 24 percent) that use automation say they have the ability to respond to vulnerabilities in a shorter timeframe.

FIGURE 19. How automation impacted the time to respond to vulnerabilities



Timely patching is difficult because of insufficient staffing. Only 36 percent of respondents, as shown in Figure 20, say their companies have enough staff to patch fast enough to prevent a data breach. Sixty-nine percent of respondents say their companies plan to hire an average of 5 staff members dedicated to patching in the next 12 months.

FIGURE 20. **Is your staff sufficient and will you hire more staff dedicated to patching in the next 12 months?**
Yes responses presented

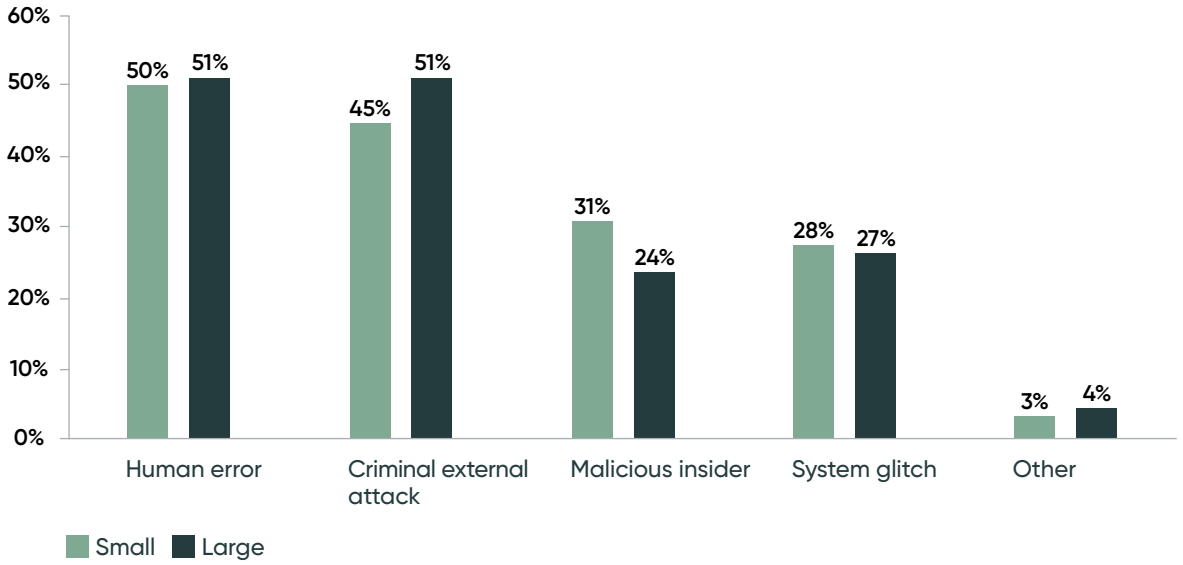


HOW THE SIZE OF AN ORGANIZATION AFFECTS VULNERABILITY MANAGEMENT

In this section, we present a special analysis of the findings based on organizational size. Fifty-eight percent of respondents are employed in organizations with less than a 5,000 headcount (small organizations) and 42 percent of respondents are in organizations with greater than a 5,000 headcount (large organizations).

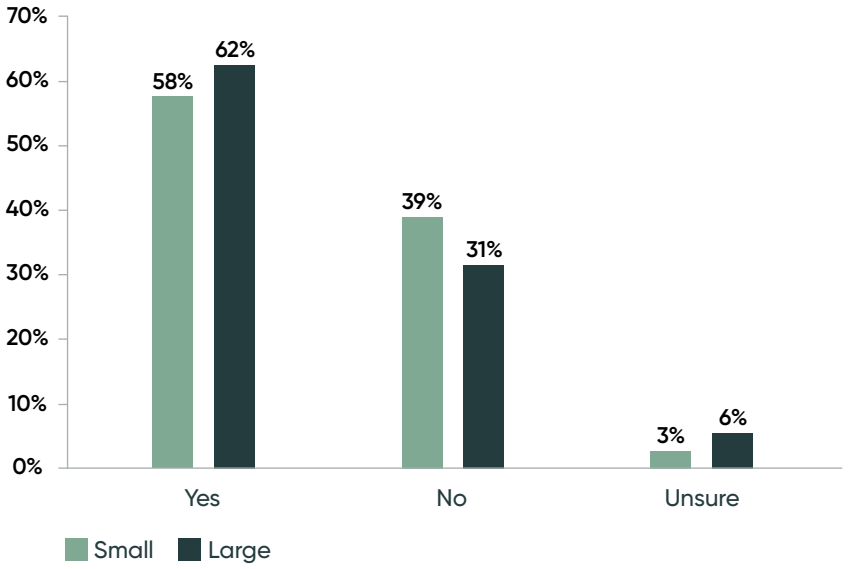
Small or large, all organizations faced similar types of a data breach. According to Figure 21, organization size generally did not affect root cause, except for malicious insider. Almost one-third of respondents in smaller organizations say it was a malicious insider who caused the data breach vs. 24 percent of respondents in larger organizations.

FIGURE 21. What were the root causes of these data breaches?



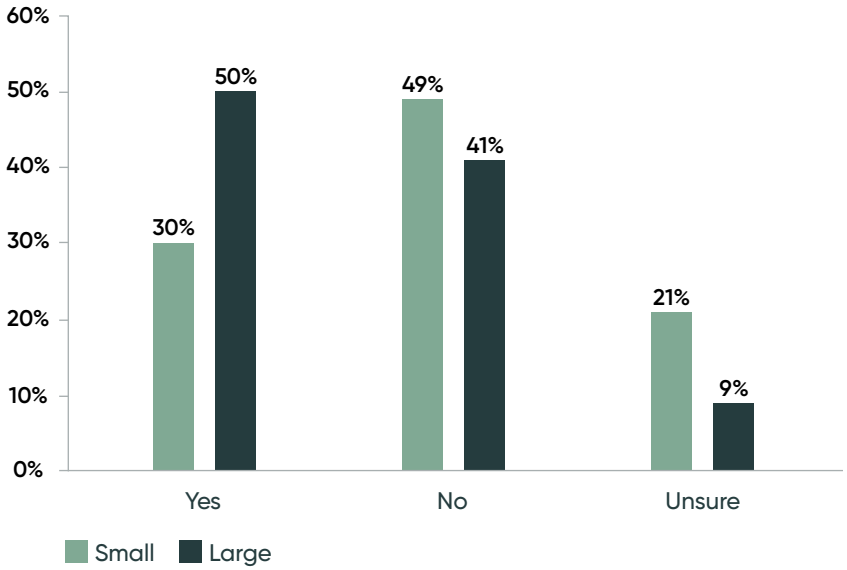
Larger organizations were slightly more likely to be aware that the data breach could have been caused due to having an available patch that was not applied. As shown in Figure 22, 62 percent of respondents in large organizations say they could link the data breach to their inability to patch a known vulnerability.

FIGURE 22. Did any of these data breaches occur because a patch was available for a known vulnerability but not applied?



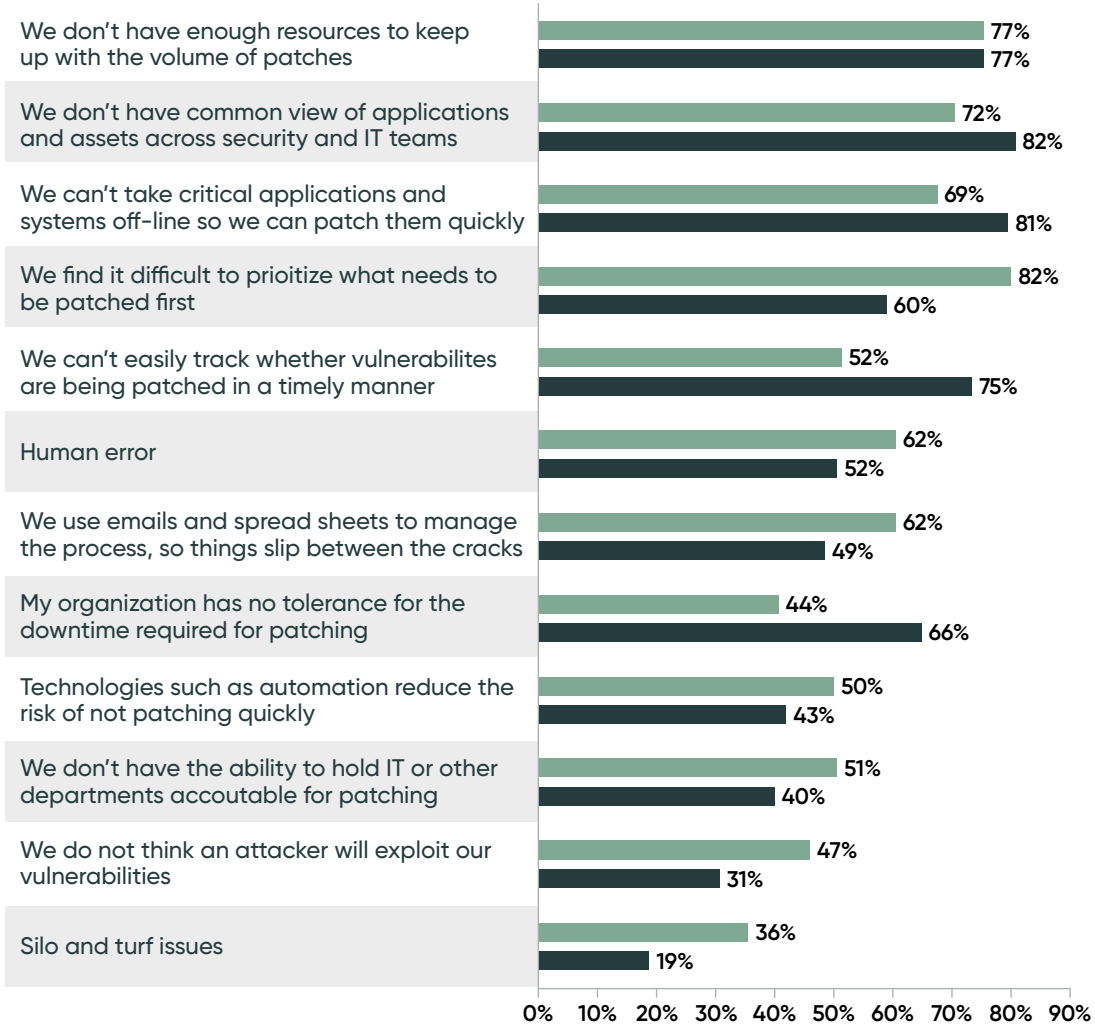
However, visibility did not translate into effective action. Fifty percent of respondents in large organizations were aware of their vulnerability to a data breach. Only 30 percent of respondents in small organizations were aware that their organization was vulnerable.

FIGURE 23. If yes, was your organization actually aware that it was vulnerable prior to the data breach?



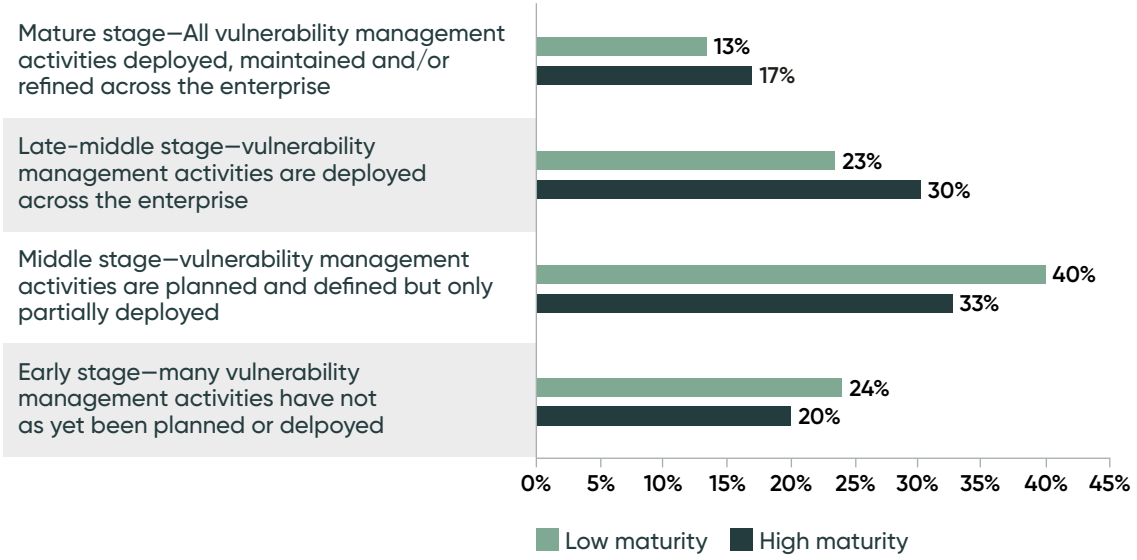
Both large and small organizations do not have enough resources to keep up with the volume of patches. As shown in Figure 24, respondents in large organizations are more likely than small organizations to say delays are caused by not having a common view of applications and assets across security and IT teams, inability to take critical applications and systems off-line to be able to patch quickly and the difficulty in tracking whether vulnerabilities are being patched in a timely manner. Small organizations find it more difficult to prioritize what needs to be patched first, experience human error and use emails and spreadsheets to manage the process so things slip between the cracks.

FIGURE 24. Which factors below cause major delays in your vulnerability patching process?
More than one response permitted



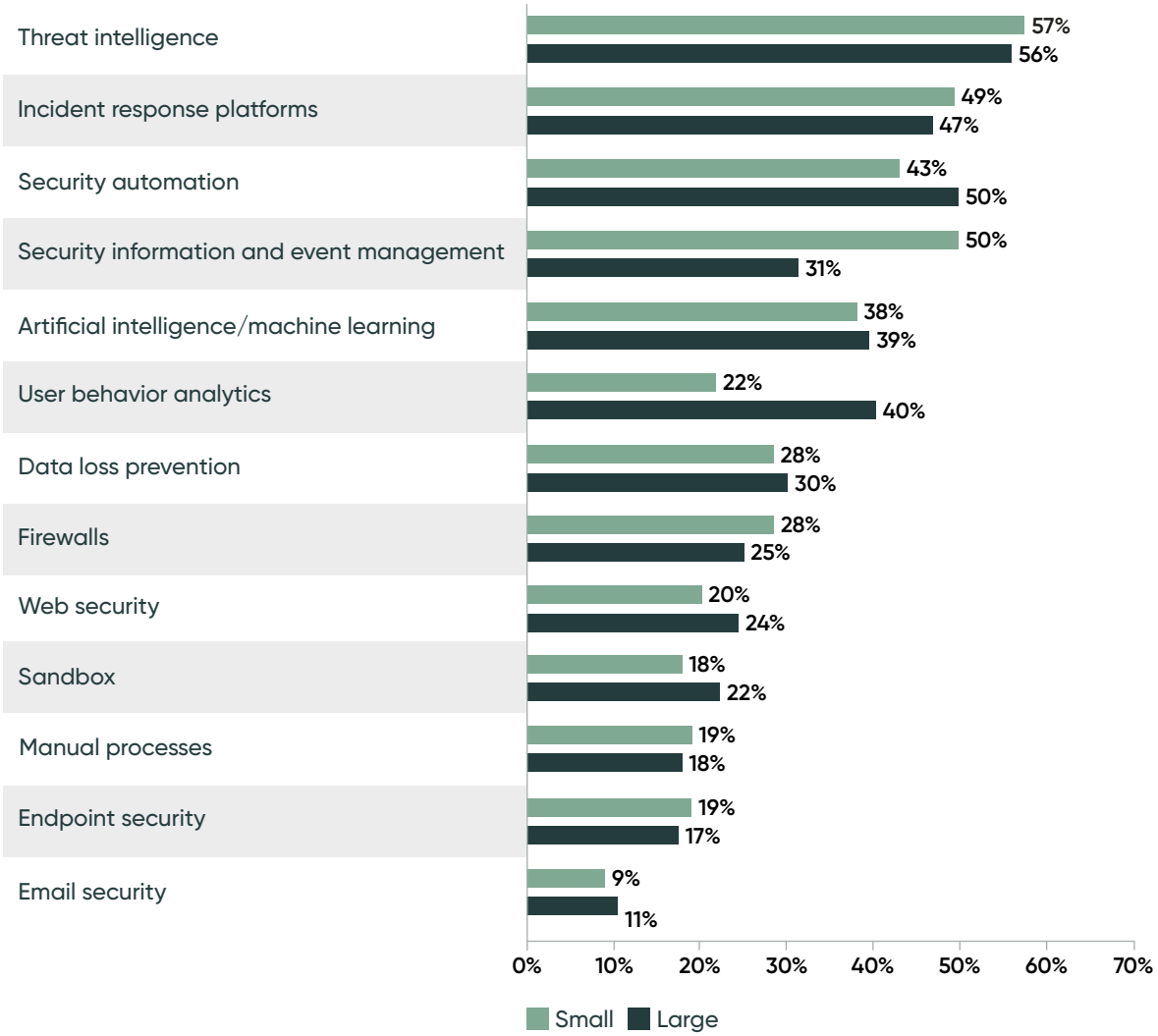
Large companies have more mature vulnerability management programs. Forty-seven percent of respondents in larger organizations say they have all or many vulnerability management activities deployed, maintained and/or refined across the enterprise. Only 36 percent of respondents in smaller organizations say they are in the mature or late stage of the vulnerability management lifecycle.

FIGURE 25. What best describes the maturity level of your organization's vulnerability management lifecycle?



Large and small organizations most likely use threat intelligence, incident response platforms and security automation to respond to vulnerabilities. Figure 26 lists the tools large and small organizations use to respond to vulnerabilities. The top three tools are threat intelligence, incident response platforms and security automation. However, small organizations are more likely to use SIEM. Large organizations are more likely to use security automation and user behavior analytics.

FIGURE 26. What tools does your organization use for the respond function?
More than one response permitted



Small organizations are spending more time and money on vulnerability management activities. As shown in Table 2, with the exception of lost time coordinating with the responsible team before a patch is applied, most time is spent by small and large organizations monitoring systems, patching applications and systems, documenting and reporting on the patch management process. Small organizations also experience more downtime than large organizations. Based on an average pay rate per hour of $62.50, small organizations spend an average of $1.2 million annually on vulnerability management and large organizations spend an average of $1.1 million annually.

TABLE 2. Time spent preventing, detecting and remediating vulnerabilities each week	Small organizations	Small organization Costs	Large organizations	Large organizations costs
How many hours each week are spent monitoring systems for threats & vulnerabilities?	142	$8,875	133	$8,313
How many hours each week are spent patching applications and systems?	213	$13,313	195	$12,188
How many hours each week are spent documenting and/or reporting on the patch management process?	56	$3,500	56	$3,500
How much downtime occurs because of the patching of vulnerabilities?	34	$2,125	25	$1,563
How much time is lost coordinating with the responsible team before a patch is applied?	12	$750	13	$813
Total per week	457	$28,563	422	$26,375
Total per year	23,764	$1,235,728	21,944	$1,141,088

*IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)

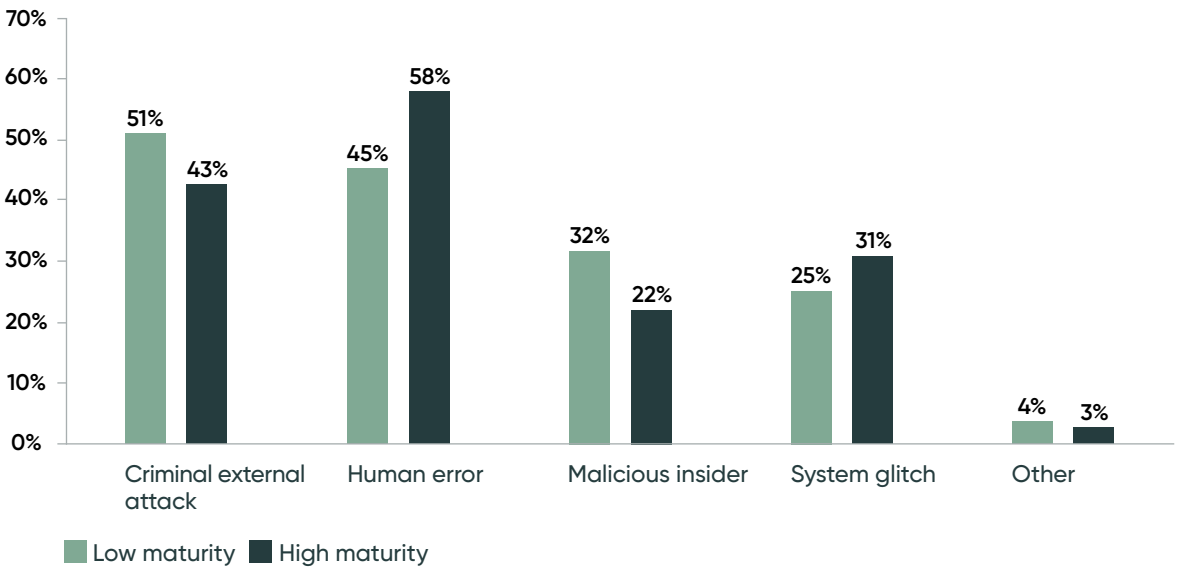
HOW MATURITY OF VULNERABILITY MANAGEMENT PRACTICES AFFECTS PATCHING

In this section, we show the differences between respondents who self-report their organizations are in the early or middle stage (low mature) and those respondents who are in the late-middle or mature stage (high mature) in their vulnerability management activities. Fifty-nine percent of respondents say their vulnerability management programs are low maturity, which means that many vulnerability management activities are only partially deployed or have not been planned or deployed. Forty-one percent of respondents are in organizations that have achieved high maturity and have many or all vulnerability management activities deployed, maintained and/or refined across the enterprise.

According to the research, organizations that have achieved a high maturity in their vulnerability process are most likely to have adequate staffing and other resources to be able to patch in a timely manner, to not rely upon manual processes, to have a single view of the full vulnerability management lifecycle and more likely to use automation to assist with vulnerability management.

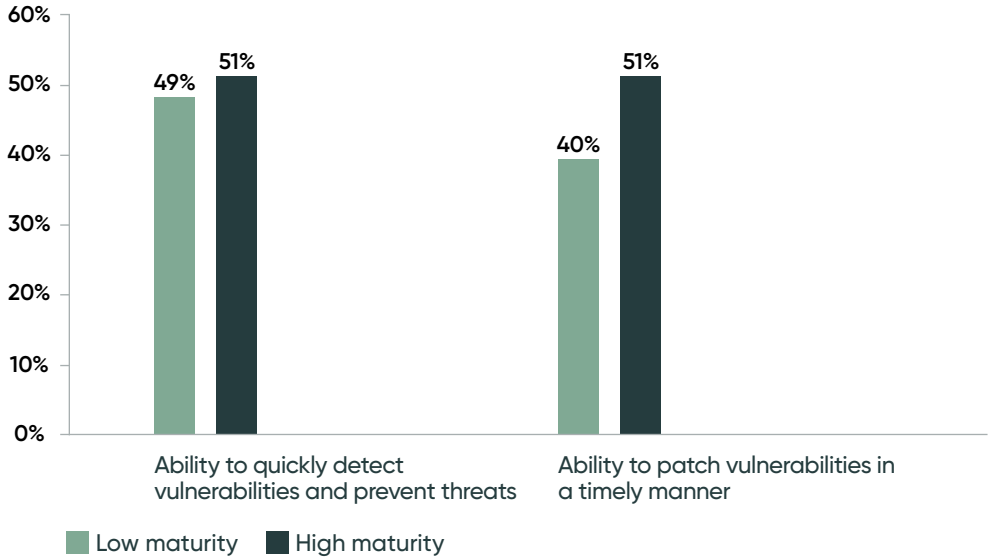
Low maturity organizations are more likely to have had one or more data breaches in the past two years (52 percent of respondents vs. 43 percent of respondents) that was caused by a criminal attack. As shown in Figure 27, Fifty-one percent of respondents say the breach was caused by a criminal attack. Mature organizations were more likely to have a breach caused by a human error.

FIGURE 27. What were the root causes of these data breaches?



High maturity organizations are better able to quickly detect and patch in a timely manner. Respondents were asked to rate the ability to quickly detect vulnerabilities and prevent threats and patch in a timely manner from a scale of 1 = low ability to 10 = high ability. Figure 28 shows the high ability responses (7+ on a scale of 1 to 10). According to Figure 28, more than half of respondents in mature organizations (51 percent) rate their ability as very high to quickly detect vulnerabilities and patch in a timely manner. In contrast, only 40 percent of low maturity organizations rate their ability to patch in a timely manner as very high.

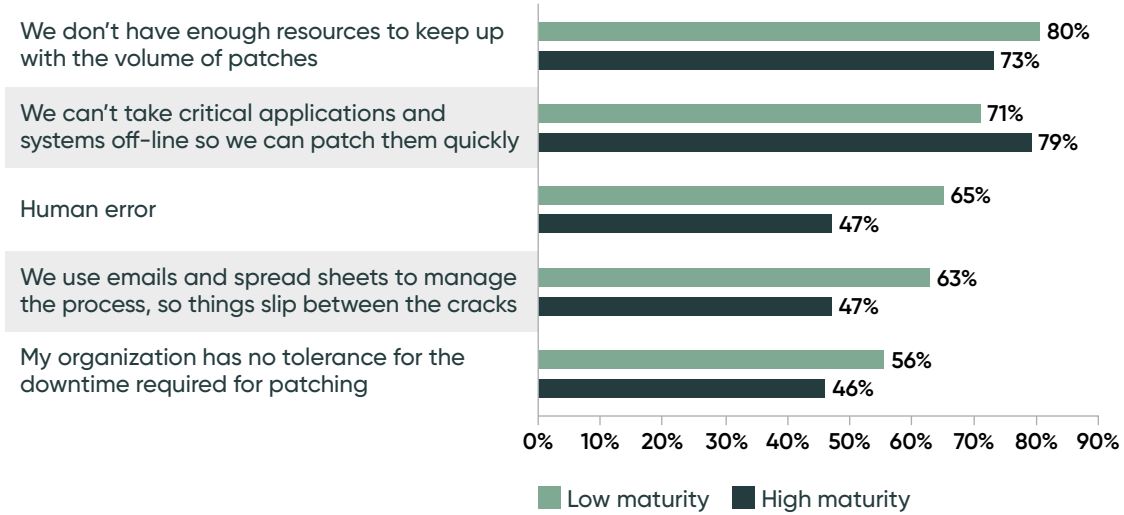
FIGURE 28. The ability to quickly detect vulnerabilities and patch in a timely manner
From 1 = low ability to 10 = high ability, 7+ responses presented



Delays in low maturity organizations are more often to be caused by human error, the use of manual processes and no tolerance for the downtime required for patching. According to Figure 29, the biggest differences between low and high maturity organizations with respect to delays are the following:

- Human error (65 percent of respondents vs. 47 percent of respondents)
- The inability to take critical applications and systems off-line so they can be patched quickly (71 percent of respondents vs. 79 percent of respondents)
- The use of emails and spread sheets to manage the process, so things slip between the cracks (63 percent of respondents vs. 47 percent of respondents)
- Not enough resources to keep up with the volume of patches (80 percent of respondents vs. 73 percent of respondents)
- The organization has no tolerance for the downtime required for patching (56 percent of respondents vs. 46 percent of respondents)

FIGURE 29. Which factors cause the most delays in vulnerability patching?
More than one response permitted



Low maturity organizations spend more time and money on vulnerability management activities. As shown in Table 3, with the exception of lost time coordinating with the responsible team before a patch is applied, most time is spent patching applications and systems and monitoring systems for threats and vulnerabilities. Based on an average pay rate per hour of $62.50, low maturity organizations spend an average of $1.3 million annually and high maturity organizations spend $1.1 million.

TABLE 3. Time spent preventing, detecting and remediating vulnerabilities each week	Low Maturity	Low Maturity Costs	High Maturity	High Maturity Costs
How many hours each week are spent monitoring systems for threats & vulnerabilities?	162	$10,125	105	$6,563
How many hours each week are spent patching applications and systems?	205	$12,813	207	$12,938
How many hours each week are spent documenting and/or reporting on the patch management process?	56	$3,500	55	$3,438
How much downtime occurs because of the patching of vulnerabilities?	28	$1,750	34	$2,125
How much time is lost coordinating with the responsible team before a patch is applied?	14	$875	10	$625
Total per week	465	$29,063	411	$25,688
Total per year	24,180	$1,257,360	21,372	$1,111,344

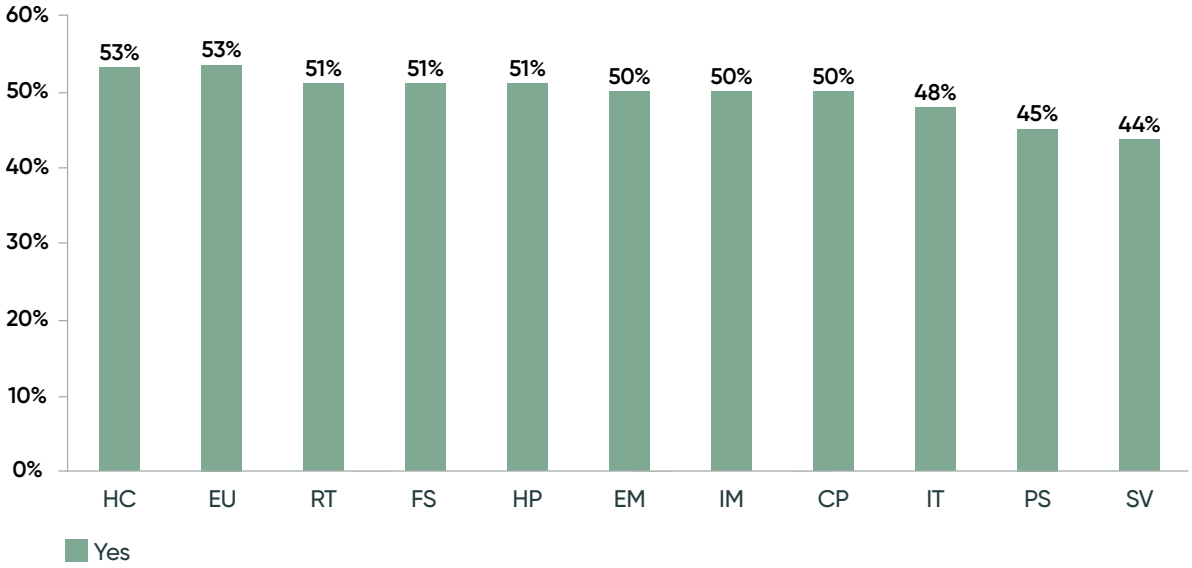
*IT and IT security fully loaded pay rate per hour is $62.50 (source: Ponemon Institute)

INDUSTRY DIFFERENCES IN VULNERABILITY AND PATCH MANAGEMENT

In this section, we present the most salient differences for the following industries: Financial services (FS), Industrial/manufacturing (IM), Public sector (PS), Services (SV), IT & technology (IT), Health & pharmaceutical (HC), Retailing (RT), Energy & utilities (EU), Consumer products (CP), Hospitality (HP) and Entertainment & media (EM).

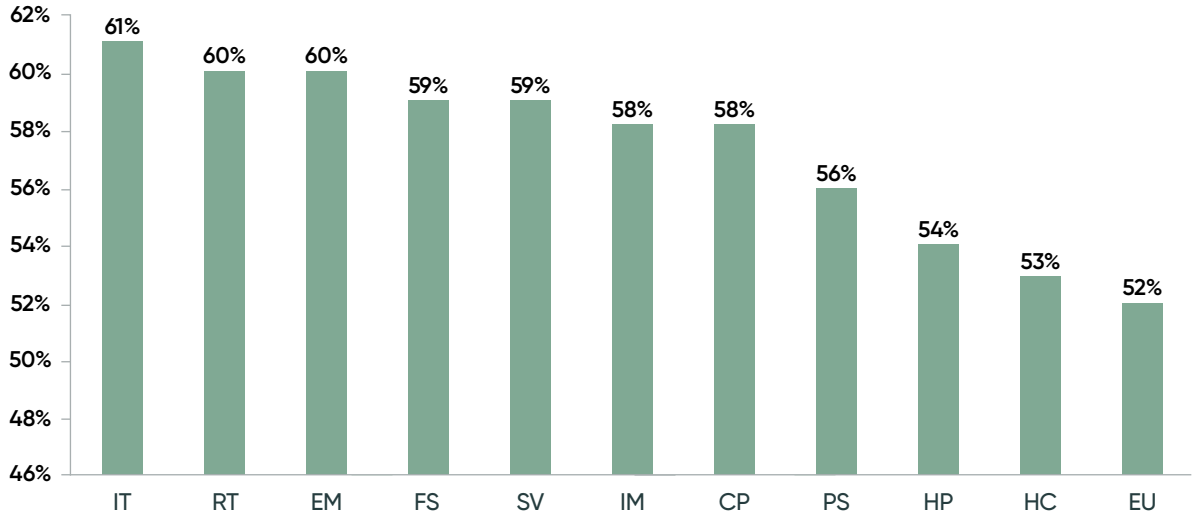
The majority of industries have experienced one or more data breaches in the past two years. Healthcare and Energy & Utilities experienced the most (53 percent of respondents). Public Sector and Services experienced the least (45 percent of respondents and 44 percent of respondents, respectively), as shown in Figure 30.

FIGURE 30. Did your organization have one or more data breaches in the past two years?
Yes responses presented



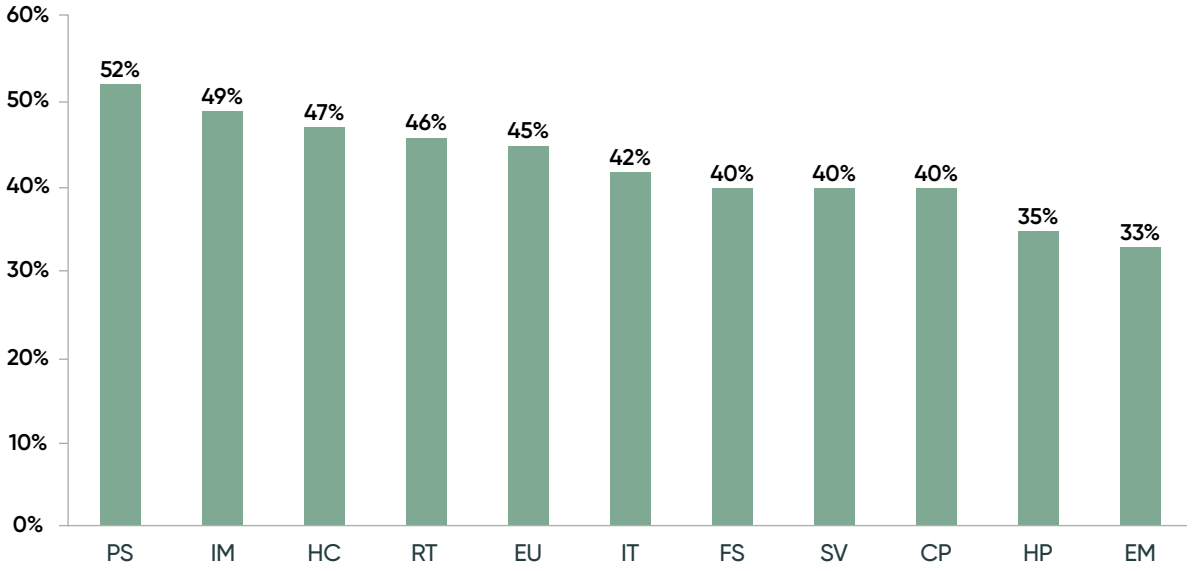
IT & Technology and Retailing were most aware that the data breach occurred because a patch was available but not applied. According to Figure 31, 61 percent of respondents in IT & Technology and 60 percent of respondents in Retailing say a patch was available but not applied and the data breach occurred. Healthcare and Pharma and Energy and Utilities were least aware (53 percent of respondents and 52 percent of respondents, respectively).

FIGURE 31. **Did any of these data breaches occur because a patch was available for a known vulnerability but not applied**
Yes responses presented



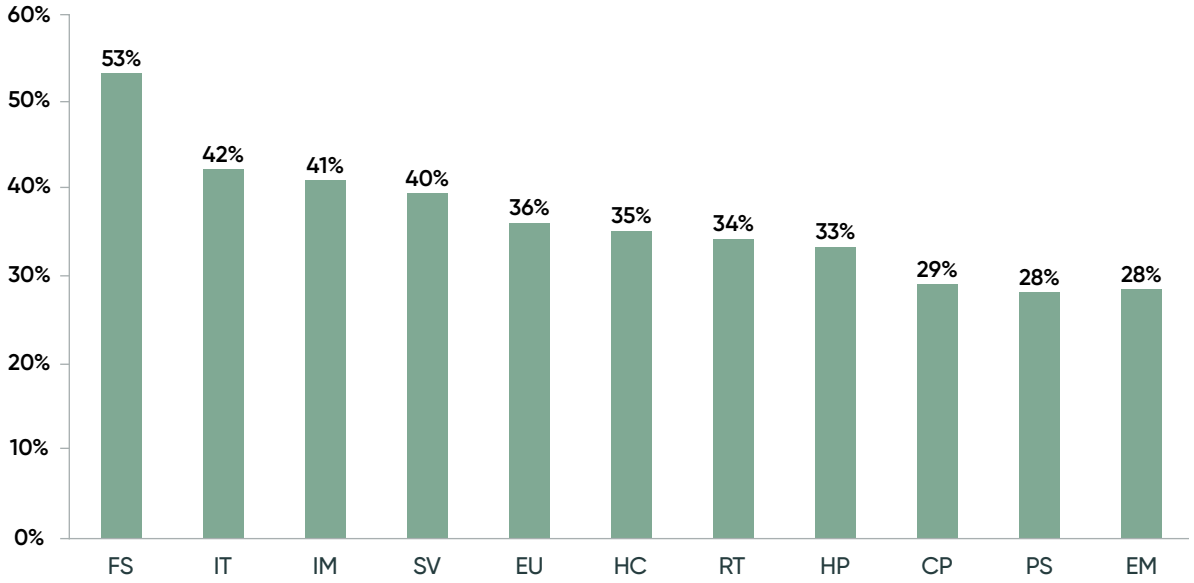
Public Sector and Industrial/Manufacturing are best able to patch in a timely manner. As shown in Figure 32, Hospitality and Entertainment & Media are least likely to patch in a timely manner.

FIGURE 32. The ability to patch vulnerabilities in a timely manner
From 1 = low ability to 10 = high ability, 7+ responses presented



By far, Financial Services use automation. As shown in Figure 33, 53 percent of respondents in Financial Services say their organizations use automation to assist with vulnerability management. Public Sector and Entertainment & Media are least likely to use automation (28 percent of respondents for both industries).

FIGURE 33. Does your organization use automation to assist with vulnerability management?
Yes responses presented



CONCLUSION

Automation, according to those organizations that use this technology (44 percent of respondents), reduces the time to respond to vulnerabilities. In fact, one of the biggest delays in patching vulnerabilities quickly is because the organization relies upon manual processes. The research also reveals that organizations that invest in automation experience the following benefits: reducing downtime, patching in a timely manner, being able to prioritize the most critical vulnerabilities and increasing the efficiency and effectiveness of the IT staff.

In addition to automation, organizations should invest in staffing. This is essential to keeping up with the volume of patches and making vulnerability management activities more efficient in order to reduce the cost of patch management. Both of these investments will strengthen the organization's security posture by improving their ability to prevent threats and patch vulnerabilities in a timely manner.

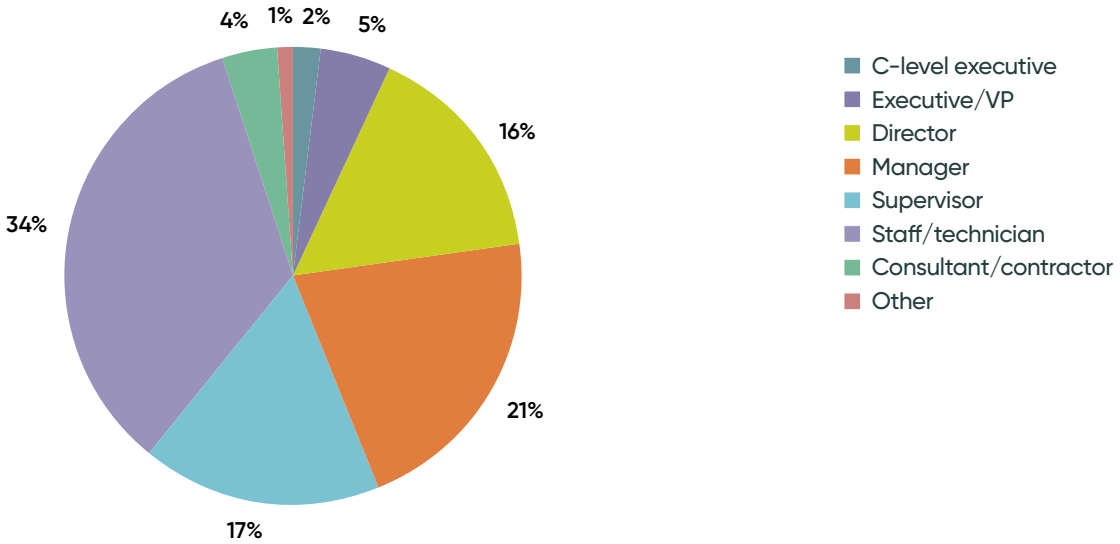
PART 3. METHODS

A sampling frame of 80,987 IT and IT security practitioners located in the United States, the United Kingdom, Germany, France, Netherlands, Australia/New Zealand, Singapore and Japan were selected as participants in this survey. Table 4 shows 3,251 total returns. Screening and reliability checks required the removal of 351 surveys. Our final sample consisted of 2,900 surveys or a 3.6 percent response.

TABLE 4. Sample response	FY2019	Pct%
Sampling frame	80,987	100%
Total returns	3,251	4.0%
Rejected or screened surveys	351	0.4%
Final sample	2,900	3.6%

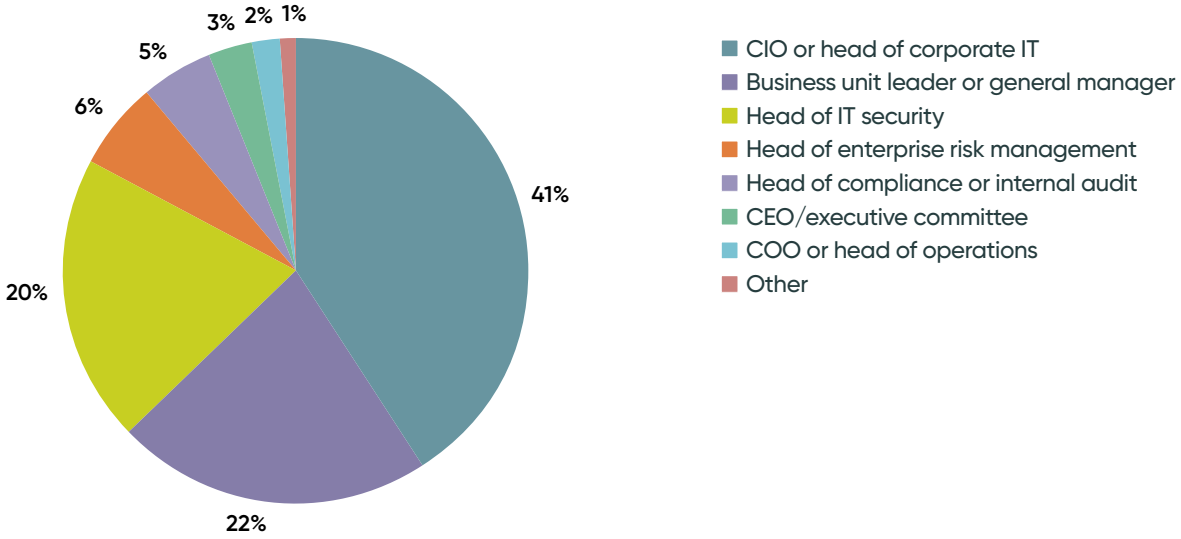
Pie Chart 1 reports the respondents' position within the participating organizations. Slightly more than half of the respondents (61 percent) are at or above the supervisory levels.

PIE CHART 1. Current position within the organization



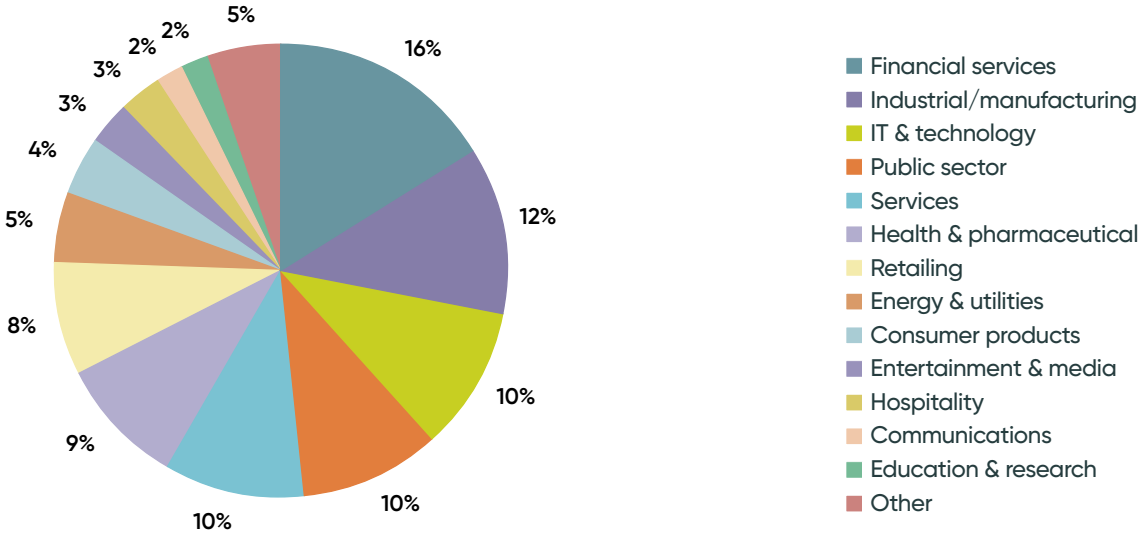
As shown in Pie Chart 2, 41 percent of respondents report to the chief information officer or head of corporate IT, 22 percent of respondents report to the business unit leader or general manager, 20 percent of respondents report to the head of IT security and 6 percent indicated they report to the head of enterprise risk management.

PIE CHART 2. Reporting channel or chain of command



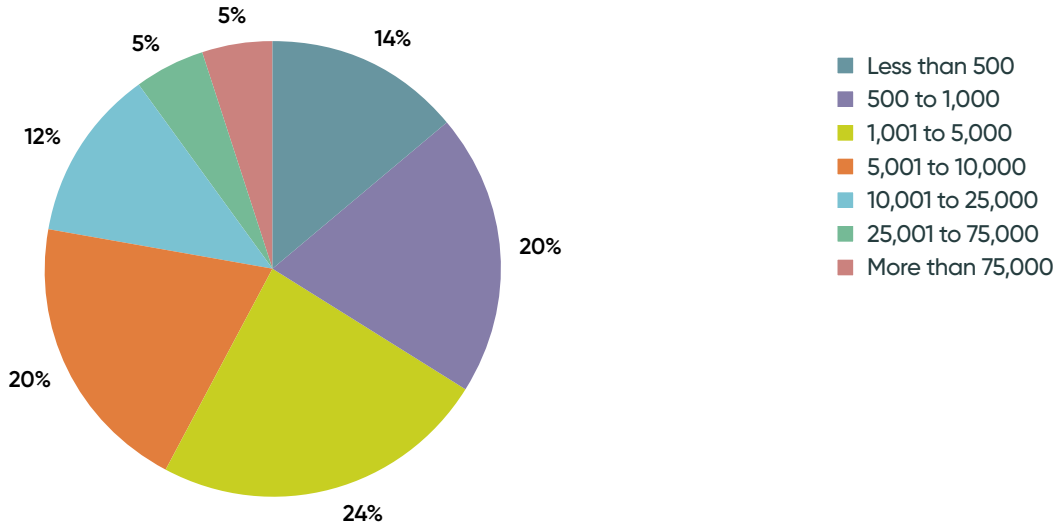
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial/manufacturing (12 percent of respondents), IT and technology, public sector and services (each at 10 percent of respondents).

PIE CHART 3. Industry distribution of respondents' organizations



According to Pie Chart 4, more than half of the respondents (66 percent) are from organizations with a global headcount of more than 1,000 employees.

PIE CHART 4. Distribution of respondents according to organizational headcount



PART 4. CAVEATS TO THIS STUDY

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

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in various organizations. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.