# Today's State of Vulnerability Response: Patch Work Demands Attention

## Australia & New Zealand

## Sponsored by ServiceNow

Independently conducted by Ponemon Institute LLC

Publication Date: April 2018

**Today's State of Vulnerability Response: Patch Work Demands Attention**
**Australia & New Zealand**
Ponemon Institute, April 2018

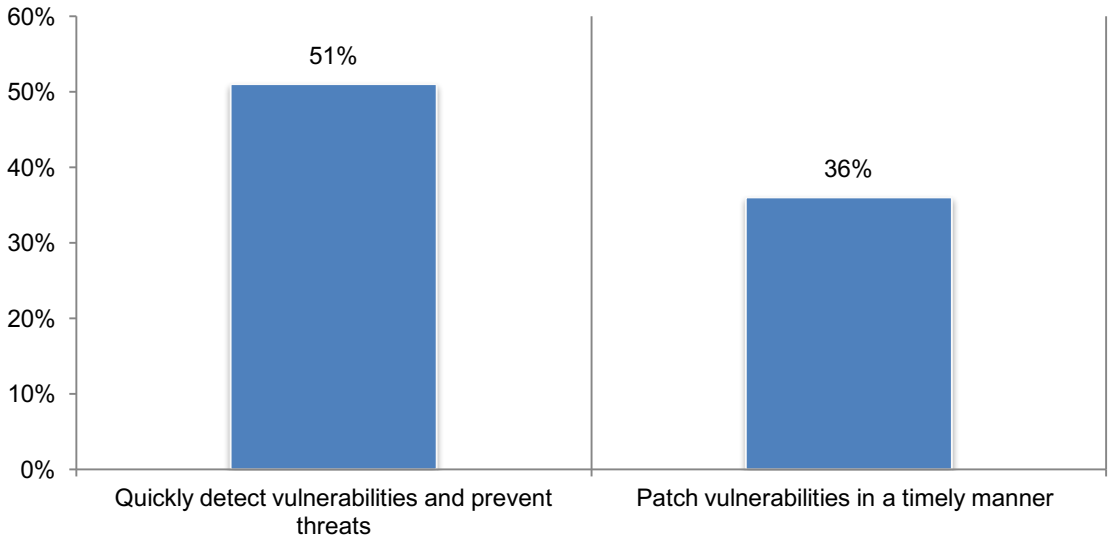
## Part 1. Introduction

For most companies it is a race against time to patch critical vulnerabilities and avoid a data breach. Based on the findings of *Today's State of Vulnerability Response: Patch Work Demands Attention*, sponsored by ServiceNow, the inability to patch in a timely manner is due to broken patch management processes. Specifically, many companies are relying upon manual processes and have difficulty in prioritising the vulnerabilities that need patching.

Ponemon Institute surveyed almost 3,000 IT security professionals in Australia/New Zealand, France, Germany, Japan, Netherlands, Singapore, United Kingdom and the United States to understand how organisations are responding to vulnerabilities and preventing hackers from exploiting attack vectors. In this report, we present the Australia and New Zealand findings.

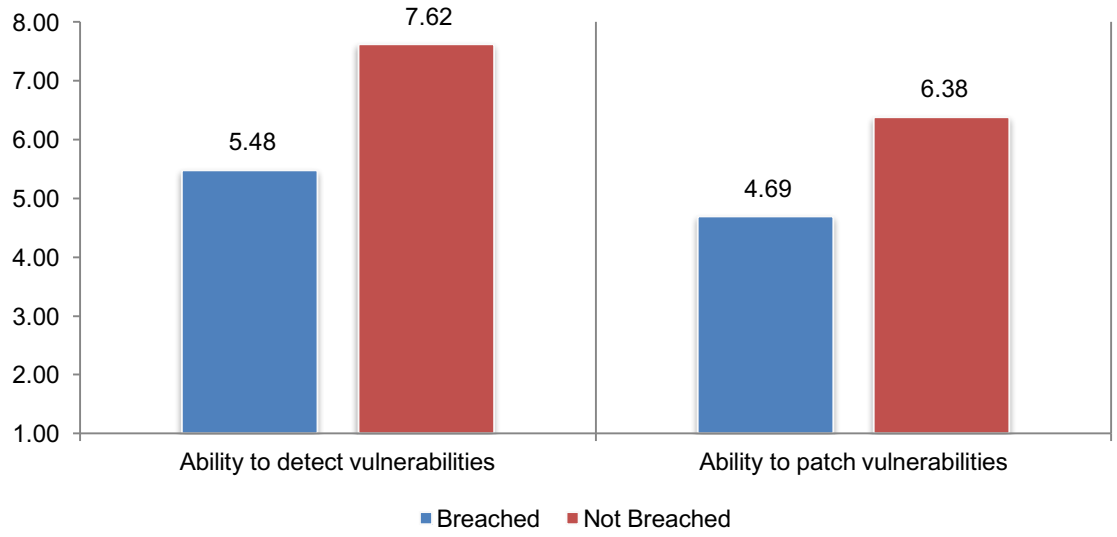
**More effective processes are required to close down attack vectors before hackers strike.** In this study we asked respondents to rate their organisations' ability to quickly detect vulnerabilities, prevent threats and patch vulnerabilities in a timely manner. Figure 1 presents the percentage of respondents who rate their ability as high (7+ on a scale of 1 to 10). Fifty-one percent of respondents rate the ability to quickly detect vulnerabilities and prevent threats as high. Only 36 percent rate their ability to patch in a timely manner as high.

**Figure 1. The ability to prevent threats and patch vulnerabilities in a timely manner**
1 = low ability to 10 = high ability, 7+ responses reported



In our analysis we looked at organisations that self-reported they had a data breach, and if companies that did not have a breach were better able to detect and patch vulnerabilities. As shown in Figure 2, organisations that avoided a data breach rated their ability to patch vulnerabilities in a timely manner 36 percent higher than those that had been breached, and they rated their ability to detect vulnerabilities 39 percent higher.

**Figure 2. Capability Gap Update**
1 = low ability to 10 = high ability, extrapolated value presented
Ability to detect: Percentage difference between 7.62 and 5.48 = 39%
Ability to patch: Percentage difference between 6.38 and 4.69 = 36%




**Following are other key takeaways:**

**More than half of respondents say their organisation had a breach.** Fifty-two percent of respondents say their organisations had a data breach in the past two years. Most breaches were caused by human error (55 percent of respondents) or a criminal external attack that exploited the organisations' vulnerabilities (52 percent of respondents). Thirty percent of respondents say a system glitch was the root cause.

**Patching could have prevented many of these data breaches**. Forty-eight percent of respondents say one or more of these breaches could have been caused by a vulnerability for which a patch was available but not applied. Thirty-seven percent of respondents say their organisations were actually aware that they were vulnerable prior to the data breach.

**New data breach laws could improve patch management.** Sixty-nine percent of respondents say their organisations 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. The steps most likely to be taken are an increase in automation (49 percent of respondents) and an increase in IT security staff (43 percent of respondents).

**Attackers are outpacing the ability of organisations to prevent cyberattacks.** According to respondents, the severity and volume of cyberattacks has increased an average of 24 percent and 15 percent in the past 12 months. Further, hackers are using such advanced technologies as machine learning/artificial intelligence to outpace organisations, according to 54 percent of respondents.

**In contrast, the reliance on manual processes is putting organisations at risk.** Sixty-five percent of respondents acknowledge that their organisation is at a disadvantage because of the reliance upon manual processes to respond to vulnerabilities. Fifty-six percent agree that security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable response backlog.

**The average window of time to patch is shorter**. Fifty-four percent of respondents say the average window of time has decreased in the past two years by an average of 28 percent.

**Siloed tools and the inability to take critical applications and systems off-line to patch them quickly are obstacles to timely patching.** Delays in vulnerability patching are primarily caused by not having a common view of applications and assets across security and IT teams (71 percent of respondents). On average, 12 days are lost coordinating with the responsible team before a patch is applied. Seventy percent say their organisations cannot take critical applications and systems off-line so they can be patched quickly.

**Patching is labour intensive, and timely patching is difficult because of insufficient staffing.** Most organisations represented in this research are using manual processes to deal with vulnerabilities, which affects the amount of time cybersecurity teams have to fulfill their other responsibilities**.** Organisations spend an average of 324 hours each week to prevent, detect and remediate vulnerabilities. This is the equivalent to about 8 full-time employees. Most time is allocated to patching applications and systems. On average, organisations are spending $1.05 million annually on patching activities.

Eighty-one percent of respondents say their companies do not have enough staff to patch fast enough to prevent a data breach. Sixty-four percent of respondents say their companies plan to hire an average of 3 staff members dedicated to patching in the next 12 months, an increase of 34 percent over today's staffing levels.

**IT operations and security operations are most responsible for patching.** Thirty-two percent of respondents say IT operations is most responsible for applying the majority of patches and 23 percent of respondents say it is IT security operations. Eighty-two percent of respondents say they have to coordinate with other areas of the organisation when patching vulnerabilities and this process results in an extra 12 days before a patch can be applied.

## Part 2. Key findings

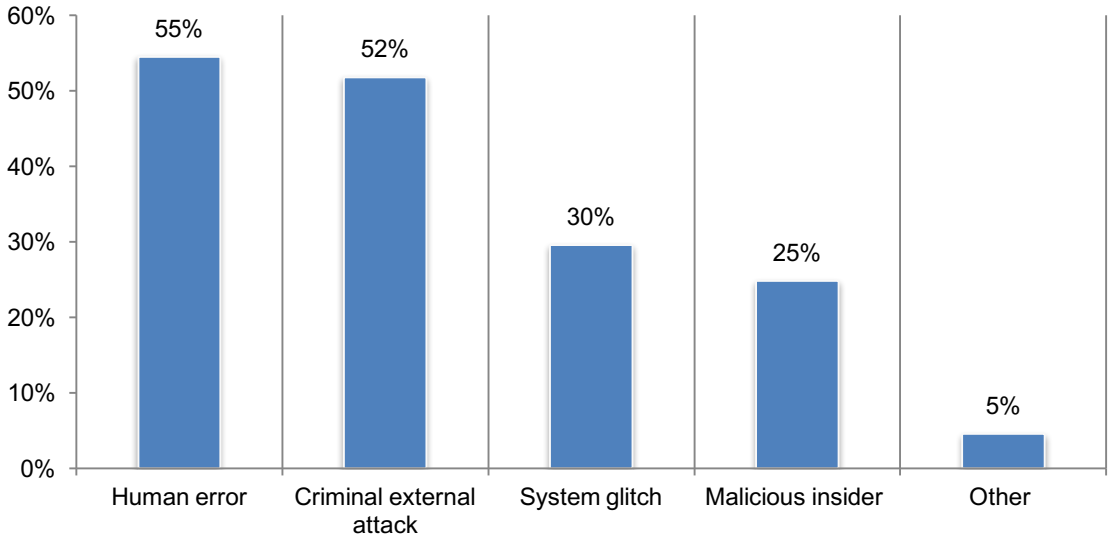
In this section we provide a deeper analysis of the research. The complete audited findings are presented in the Appendix of this report. The findings are organised according to the following topics:

- Data breaches occur because of poor patch management practices
- Bad guys are getting better because of broken processes
- Barriers to keeping ahead of the bad guys

### Data breaches occur because of poor patch management practices

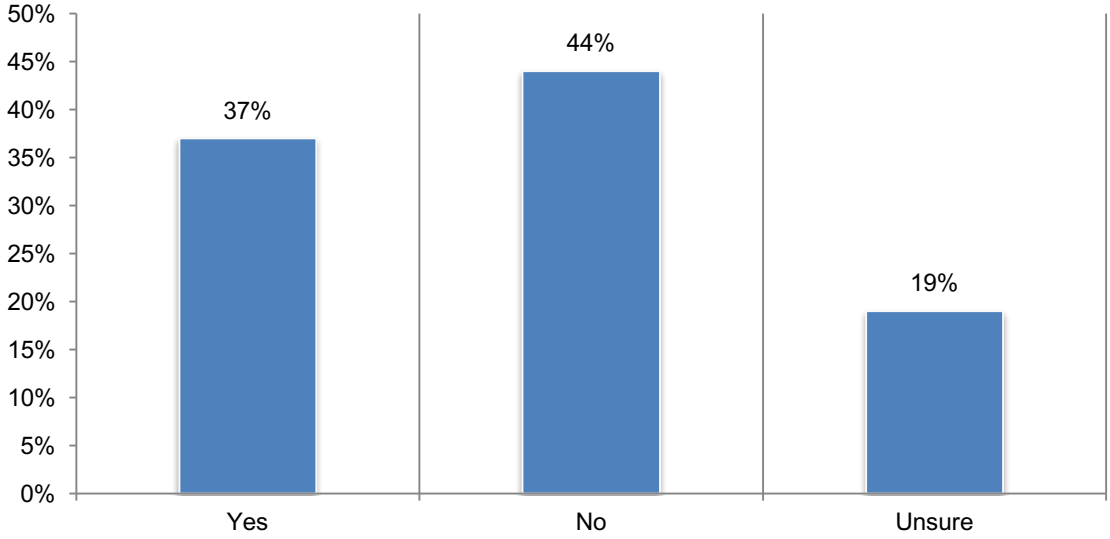
**More than half of respondents say their organisation had a breach.** Fifty-two percent of respondents say their organisations had a data breach in the past two years. As shown in Figure 3, most breaches were caused by human error (55 percent of respondents) or a criminal external attack that exploited the organisations' vulnerabilities (52 percent of respondents). Thirty percent of respondents say a system glitch was the root cause.

**Figure 3. What were the root causes of these data breaches?**



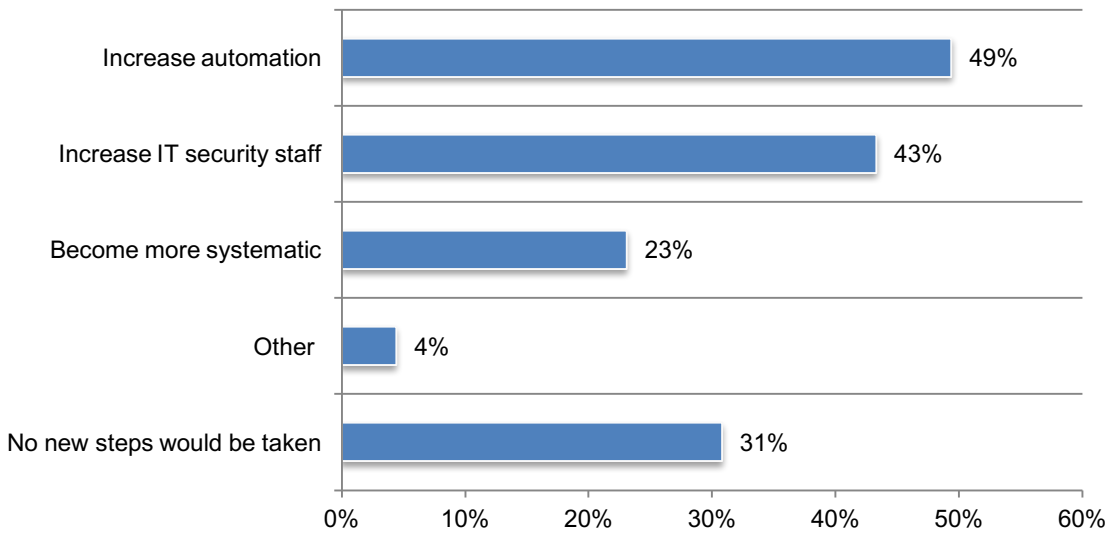
**Patching could have prevented many of these data breaches**. Forty-eight percent of respondents say one or more of these breaches could have been caused by a vulnerability for which a patch was available but not applied. According to Figure 4, 37 percent of respondents say their organisations were actually aware that they were vulnerable prior to the data breach.

**Figure 4. Was your organisation aware it was vulnerable prior to the data breach?**




**New data breach laws could improve patch management.** Sixty-nine percent of respondents say their organisations 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. The steps most likely to be taken are an increase in automation (49 percent of respondents) and an increase in IT security staff (43 percent of respondents), as shown in Figure 5.

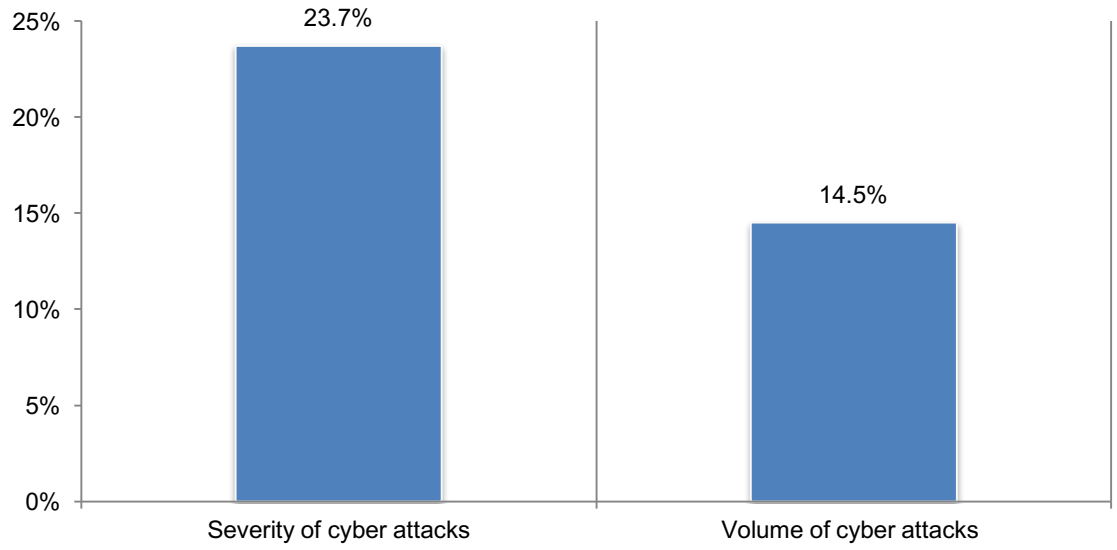
**Figure 5. What steps would you take to improve your organisation's patch management?**
More than one response permitted



**Bad guys are getting better because of broken processes**

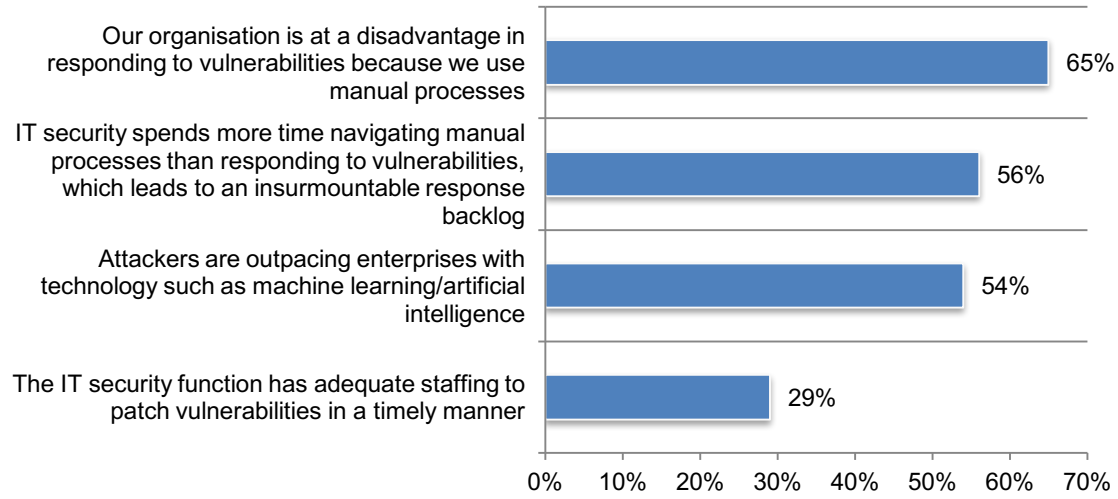
**Attackers are outpacing the ability of organisations to prevent cyberattacks.** According to Figure 6, the severity and volume of cyberattacks has increased an average of 24 percent and 15 percent in the past 12 months. Further, hackers are using such advanced technologies as machine learning/artificial intelligence to outpace organisations, according to 54 percent of respondents.

**Figure 6. How has the volume and severity of cyberattacks increased in the past 12 months?**
Extrapolated values



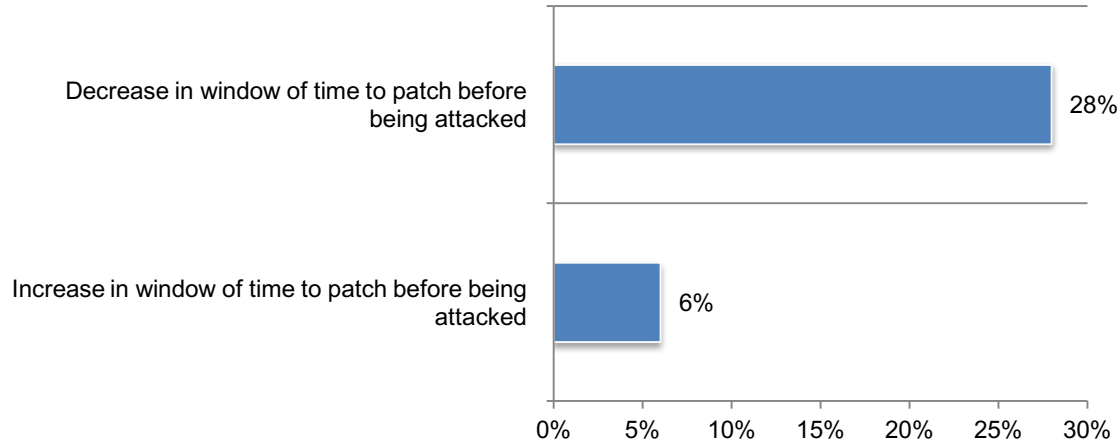
**In contrast, the reliance on manual processes is putting organisations at risk.** As shown in Figure 7, 65 percent of respondents acknowledge that their organisation is at a disadvantage because of the reliance upon manual processes to respond to vulnerabilities. Fifty-six percent agree that security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable response backlog.

**Figure 7. Perceptions about the broken processes in patch management**
Strongly agree and Agree responses combined




**The average window of time to patch is shorter**. Fifty-four percent of respondents say the average window of time has decreased in the past two years by an average of 28 percent, as shown in Figure 8.

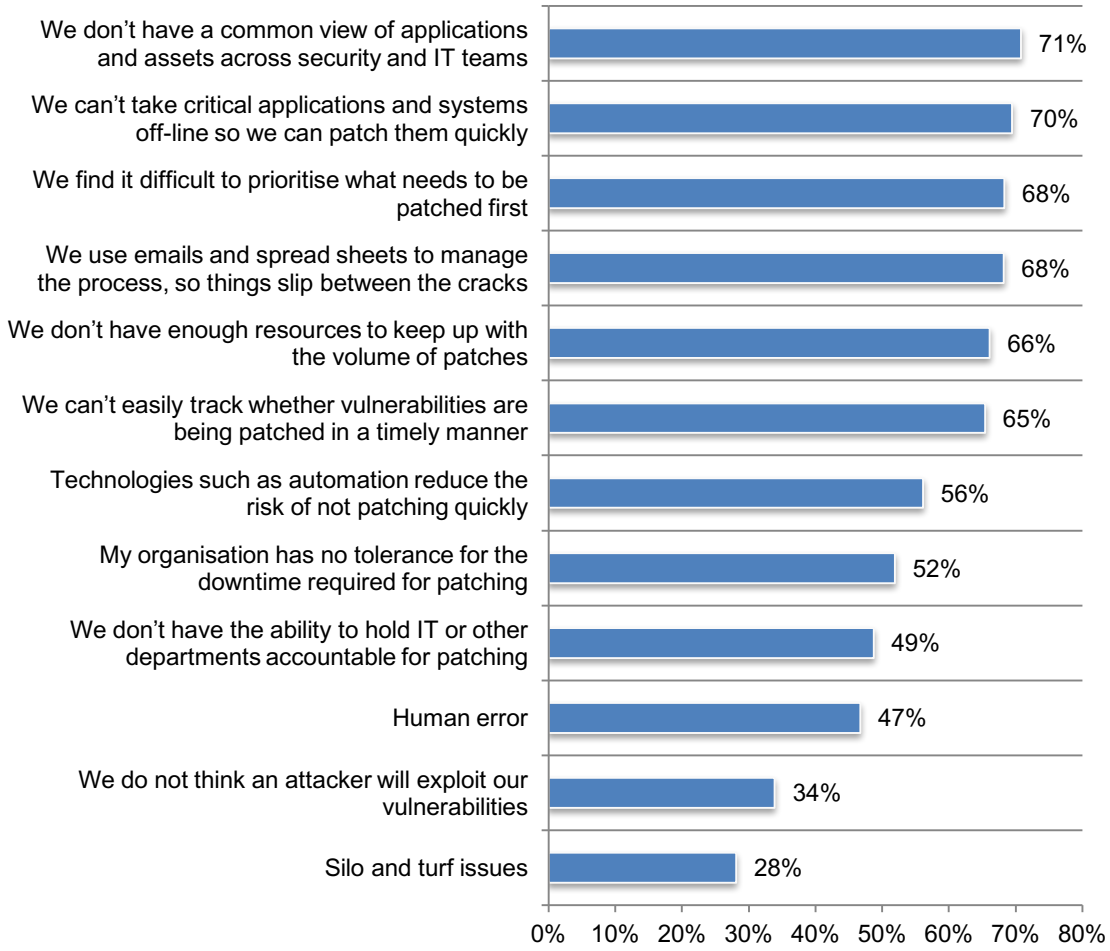
**Figure 8. By what percentage did the average window of time to patch increase or decrease?**
Extrapolated values



**Barriers to keeping ahead of the bad guys**

**Siloed tools and the inability to take critical applications and systems off-line to patch them quickly are obstacles to timely patching.** According to Figure 9, delays in vulnerability patching are primarily caused by not having a common view of applications and assets across security and IT teams (71 percent of respondents). On average, 12 days are lost coordinating with the responsible team before a patch is applied. Seventy percent say their organisations cannot take critical applications and systems off-line so they can be patched quickly.

**Figure 9. Why major delays occur in vulnerability patching**
More than one choice permitted



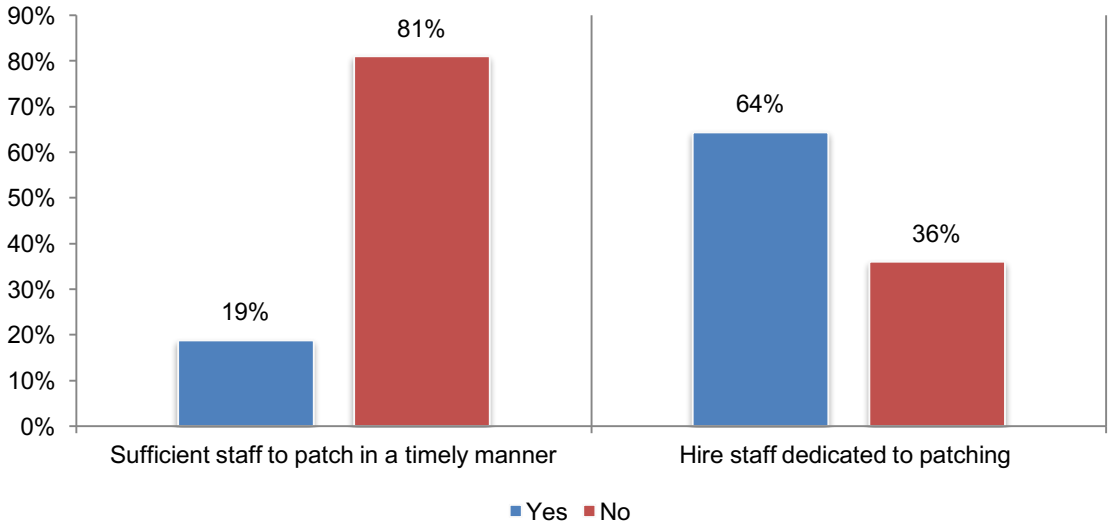
**Patching is labour intensive, and timely patching is difficult because of insufficient staffing.** Most organisations represented in this research are using manual processes to deal with vulnerabilities, which affects the amount of time cybersecurity teams have to fulfill their other responsibilities**.** Organisations spend an average of 324 hours each week to prevent, detect and remediate vulnerabilities. This is the equivalent to about 8 full-time employees. Most time is allocated to patching applications and systems. On average, organisations are spending $1.05 million annually on patching activities.

| **Table 1. Time spent preventing, detecting and remediating vulnerabilities** | **Average hours spent each week** | **Cost per hour*** |
|---|---|---|
| How many hours each week are spent monitoring systems for threats & vulnerabilities? | 122 | $7,625 |
| How many hours each week are spent patching applications and systems? | 147 | $9,188 |
| How many hours each week are spent documenting and/or reporting on the patch management process? | 26 | $1,625 |
| How much downtime occurs because of the patching of vulnerabilities? | 17 | $1,063 |
| How much time is lost coordinating with the responsible team before a patch is applied? | 12 | $750 |
| Total per week | 324 | $20,250 |
| Total per year | 16,848 | $1,053,500 |

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

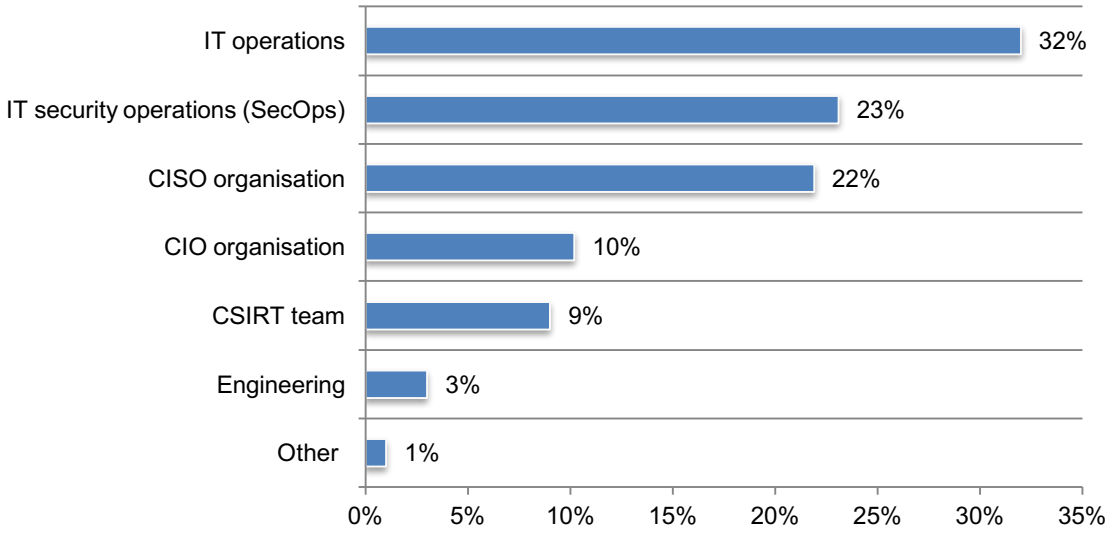
Eighty-one percent of respondents say their companies do not have enough staff to patch fast enough to prevent a data breach. Sixty-four percent of respondents say their companies plan to hire an average of 3 staff members dedicated to patching in the next 12 months, an increase of 34 percent over today's staffing levels, as shown in Figure 10.

**Figure 10. Is your staff sufficient and will you hire more staff dedicated to patching in the next 12 months?**




**IT operations and security operations are most responsible for patching.** According to Figure 11, 32 percent of respondents say IT operations is most responsible for applying the majority of patches and 23 percent of respondents say it is IT security operations. Eighty-two percent of respondents say they have to coordinate with other areas of the organisation when patching vulnerabilities and this process results in an extra 12 days before a patch can be applied.

**Figure 11. Which team in your organisation is responsible for applying the majority of patches?**
Only one choice permitted



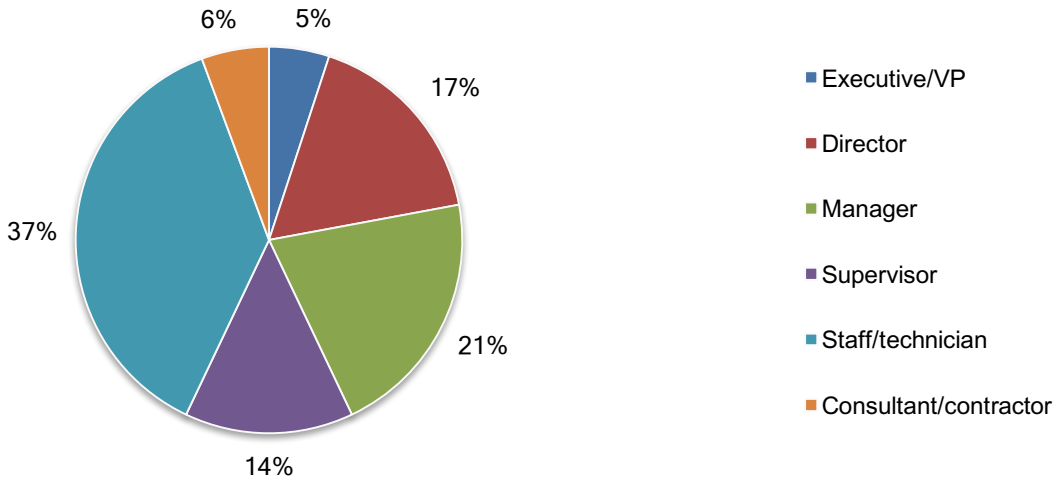
**Part 3. Methods Update**

A sampling frame of 6,780 IT and IT security practitioners located in Australia/New Zealand were selected as participants in this survey. Table 1 shows 263 total returns. Screening and reliability checks required the removal of 43 surveys. Our final sample consisted of 220 surveys or a 3.2 percent response.

| **Table 1. Sample response** | FY2017 | Pct% |
|---|---|---|
| Sampling frame | 6,780 | 100% |
| Total returns | 263 | 3.9% |
| Rejected or screened surveys | 43 | 0.6% |
| Final sample | 220 | 3.2% |

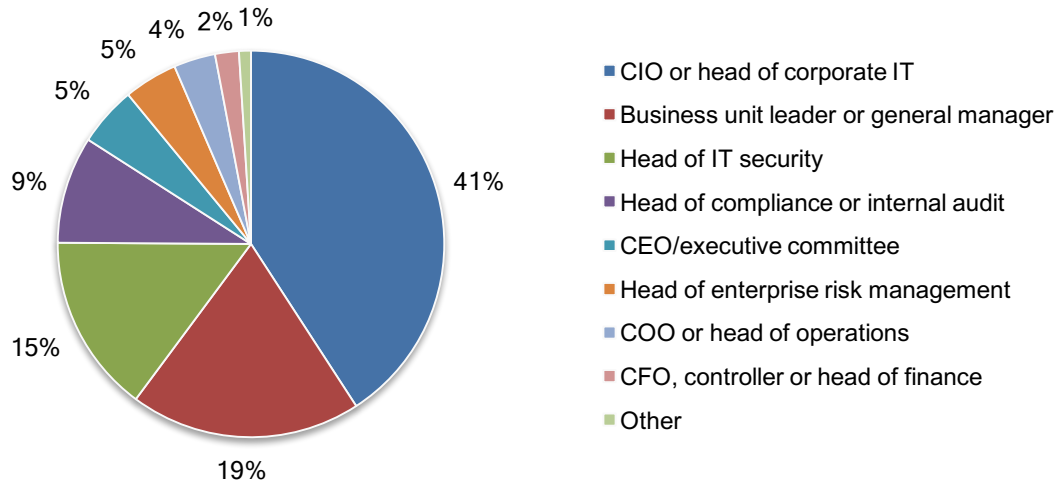
Pie Chart 1 reports the respondents' organisational levels within the participating organisations. Slightly more than half of the respondents (57 percent) are at or above the supervisory levels.

**Pie Chart 1. Current position within the organisation**



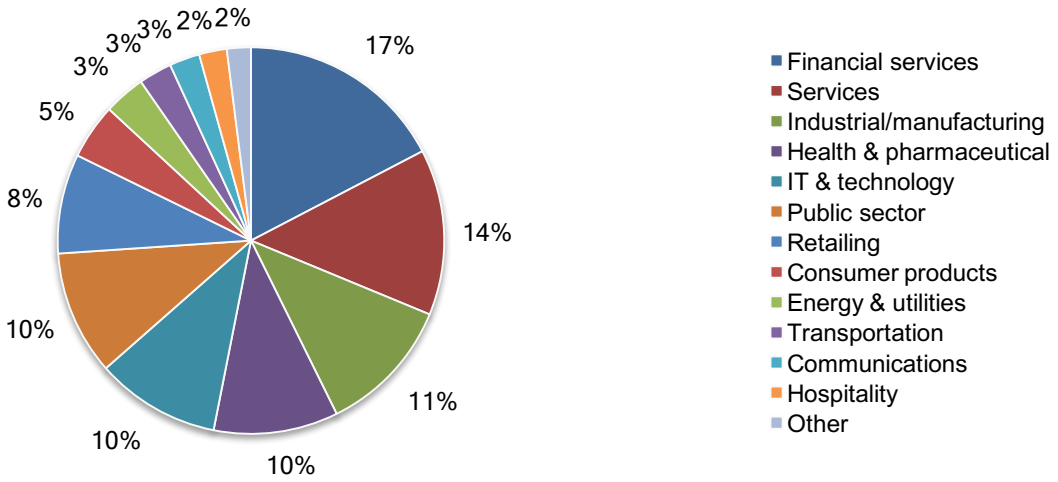
As shown in Pie Chart 2, 41 percent of respondents report to the chief information officer or head of corporate IT, 19 percent report to the business unit leader or general manager, and 15 percent indicated they report to the head of IT security.

**Pie Chart 2. Reporting channel or chain of command**



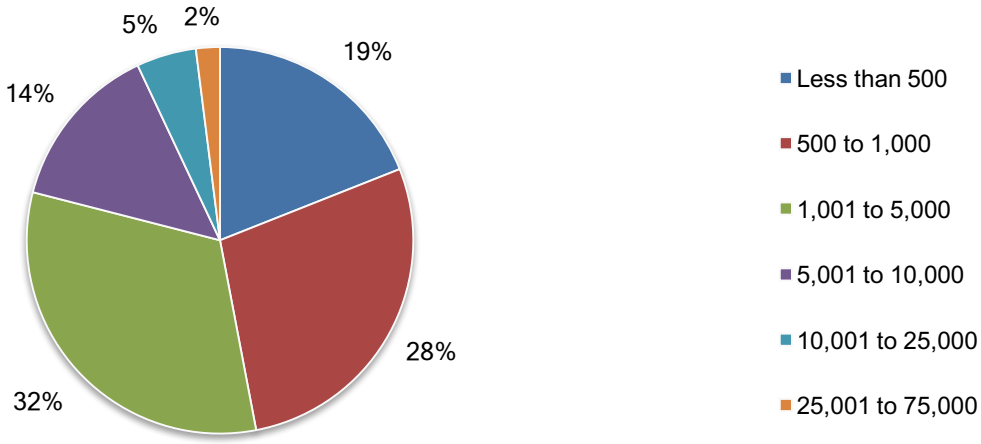

Pie Chart 3 reports the industry segments of respondents' organisations. This chart identifies financial services (17 percent of respondents) as the largest segment, followed by services sector (14 percent of respondents), industrial/manufacturing (11 percent of respondents) and health and pharmaceuticals (10 percent of respondents).

**Pie Chart 3. Industry distribution of respondents' organisations**



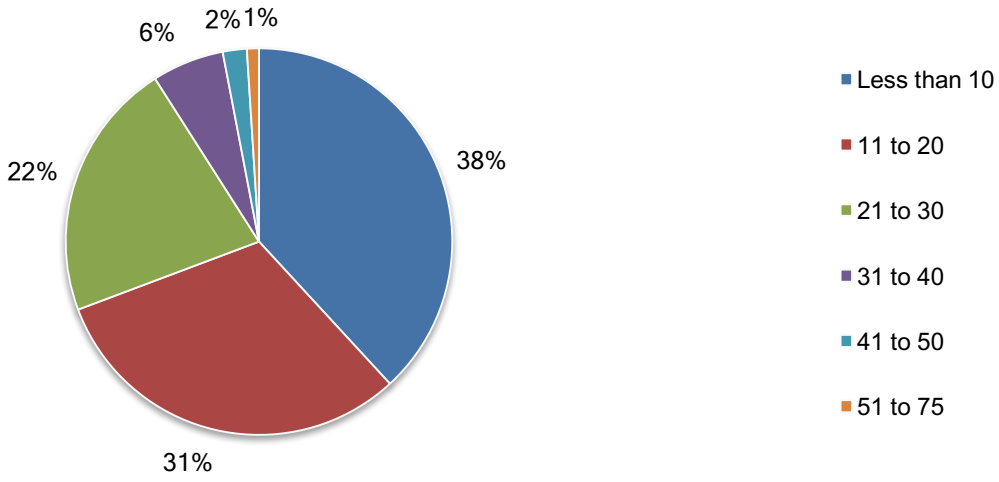
According to Pie Chart 4, more than half of the respondents (53 percent) are from organisations with a global headcount of more than 1,000 employees.

**Pie Chart 4. Distribution of respondents according to organisational headcount**




According to Pie Chart 5, more than half of the respondents (62 percent) reported their IT security function has a fulltime headcount of more than 10 employees.

**Pie Chart 5. Full-time headcount of the IT security function**



**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 organisations in Australia/New Zealand. 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.

**Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.**