



Understanding the depth of the Ransomware problem in Small and Mid-sized business in Australia





Who Am I?



Over 18 years history in security community
across ANZ

Heads Malwarebytes' expansion into Oceania

jcook@malwarebytes.com

Jim Cook, Regional Director, Australia and New Zealand



ABOUT THE SURVEY

- A total of 175 surveys were conducted with SMEs
- The median number of employees at the SMEs surveyed was 401; they have a median of 269 email users
- 50% of respondent organizations have up to 500 employees, 50% have 501-1,000 employees
- All of the surveys were conducted by telephone
- The survey was conducted during June 2017



KEY TAKEAWAYS

- Ransomware can cause SMEs enormous damage, including cessation of business operations
- Downtime is a much more serious problem with ransomware than the extortion itself
- Many SMEs don't know the source of their ransomware infection
- In many cases, ransomware spreads well beyond the initial point of infection
- Most decision makers are opposed to paying ransom demands
- Not paying ransomware can result in significant file loss
- Dealing with ransomware is a high priority, but confidence in solving the problem is low
- The primary focus for dealing with ransomware is technology, not user training
- Most SMEs are not satisfied with their current anti-ransomware technology



ABOUT THE SURVEY AUDIENCE

Industry	%
Manufacturing	14%
Engineering/Construction	12%
Retail/E-commerce	11%
High tech	9%
Education	7%
Food/Agriculture	7%
Transportation	7%

Industry	%
Financial services/Banking/Insurance	6%
Healthcare	6%
Government	4%
Hospitality	3%
Pharmaceutical	3%
Law enforcement	<1%
Other	11%

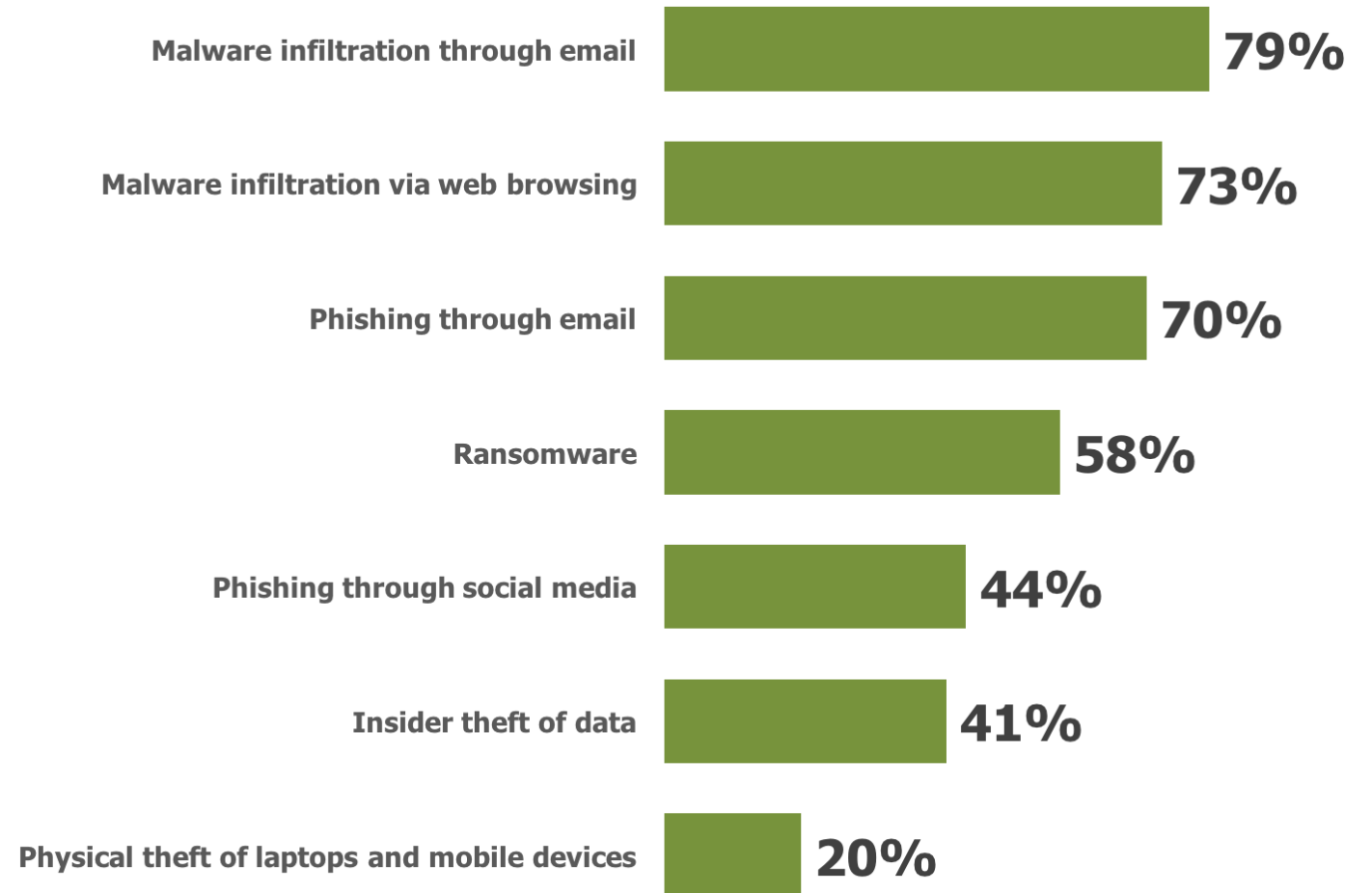


RANSOMWARE IS A CRITICAL PROBLEM

Percentage indicating “concern” or “extremely concerned”

Ransomware is a “top four” problem, second only to the general malware problem and email phishing

Nearly six in 10 SMEs is “concerned” or “extremely concerned” about ransomware

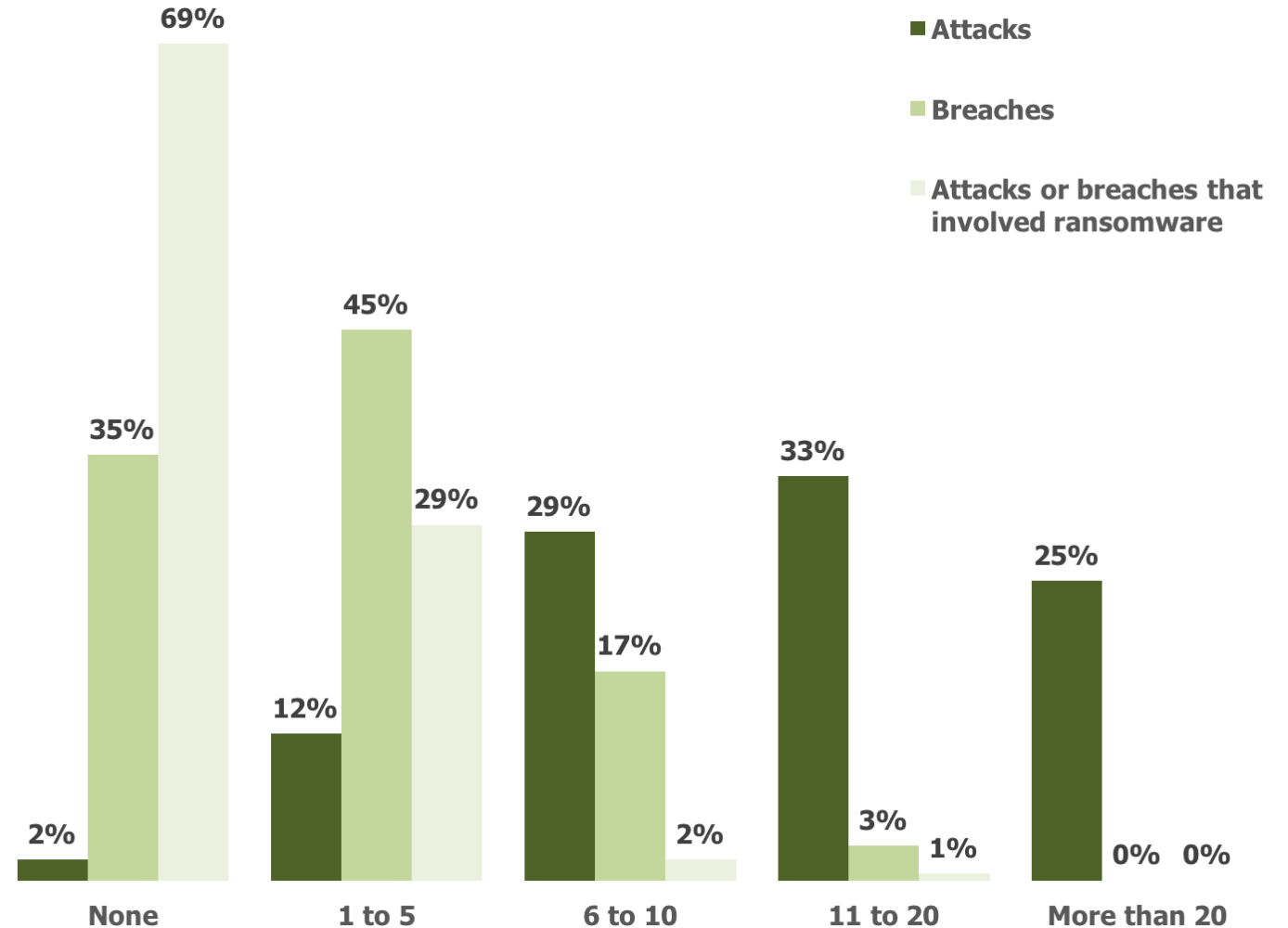


HOW COMMON IS RANSOMWARE?

Incidents during the past 12 months

Most SMEs have experienced attacks and breaches during the past year

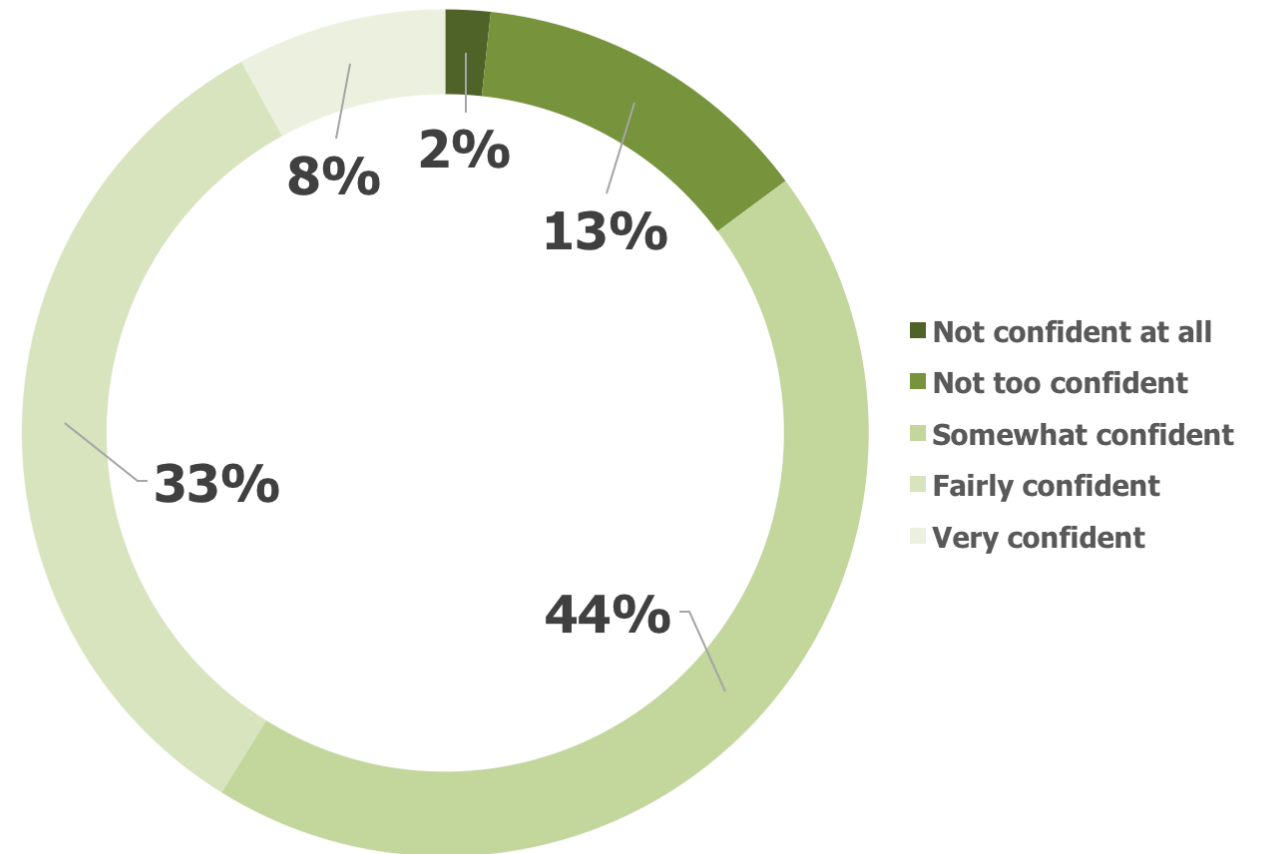
31% of SMEs have had a ransomware attack during the past year



CONFIDENCE IN ADDRESSING RANSOMWARE

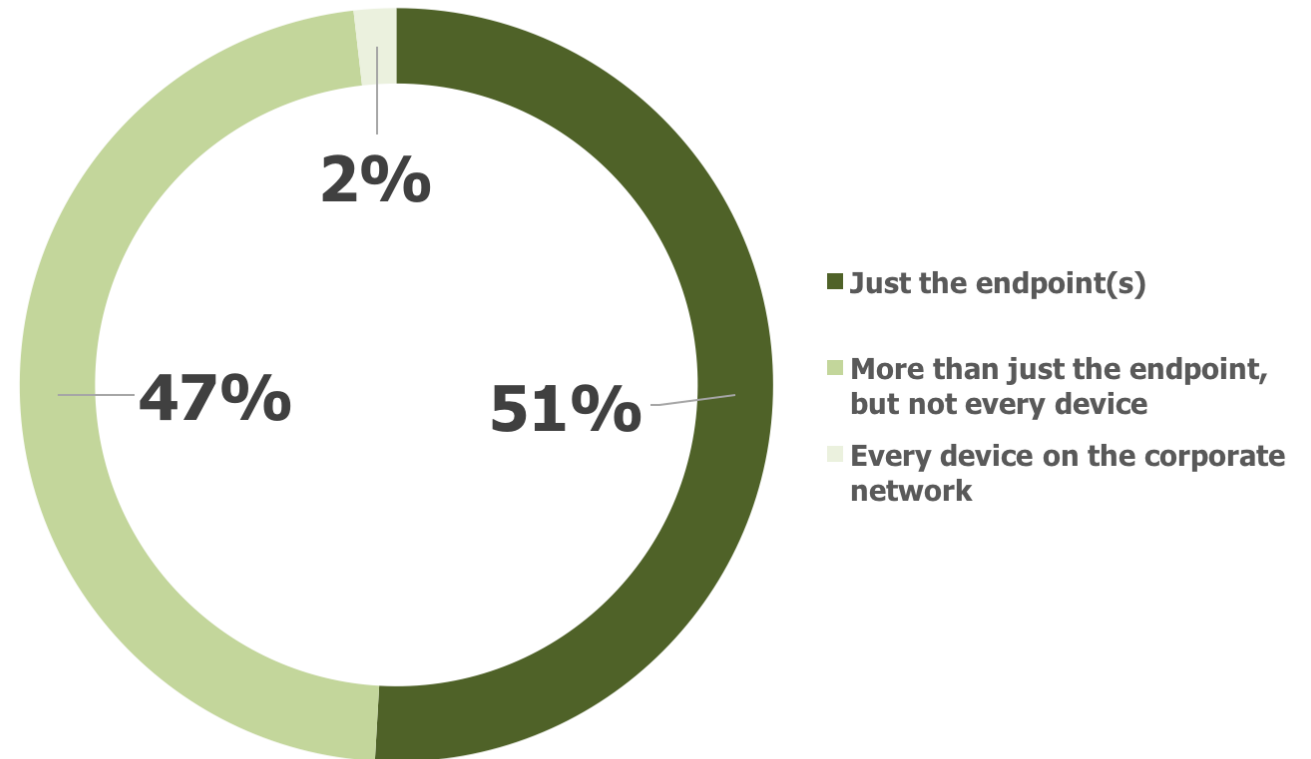
Most SMEs are not confident in their ability to stop ransomware attacks

Only one in 12 is “very confident”



RANSOMWARE COMMONLY SPREADS

In nearly one-half of SMEs, ransomware infections spread beyond just the initial point of infection



THE IMPACT OF RANSOMWARE

The most common impact of ransomware is on people...

....but for more than one in five SMEs the business ground to a halt...

....and 18% of SMEs lost revenue as a result

People were personally impacted (customers, students, vendors, staff, etc.)



It stopped business immediately



We lost revenue



Employees used personally owned smartphones, tablets or laptops because corporate systems were down



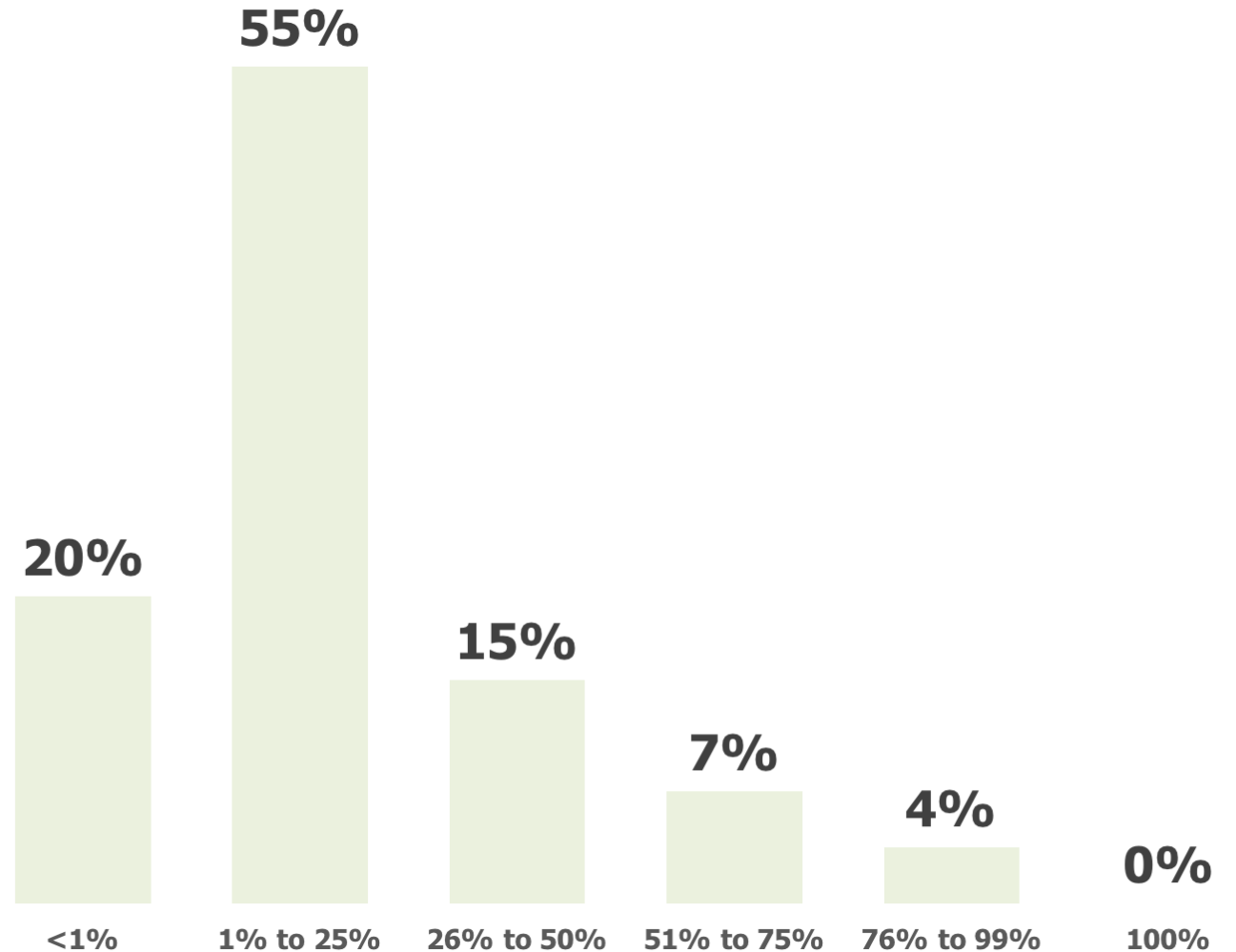
Lives were endangered



ENDPOINTS IMPACTED

In 25% of SMEs, more than one-quarter of endpoints were impacted by ransomware

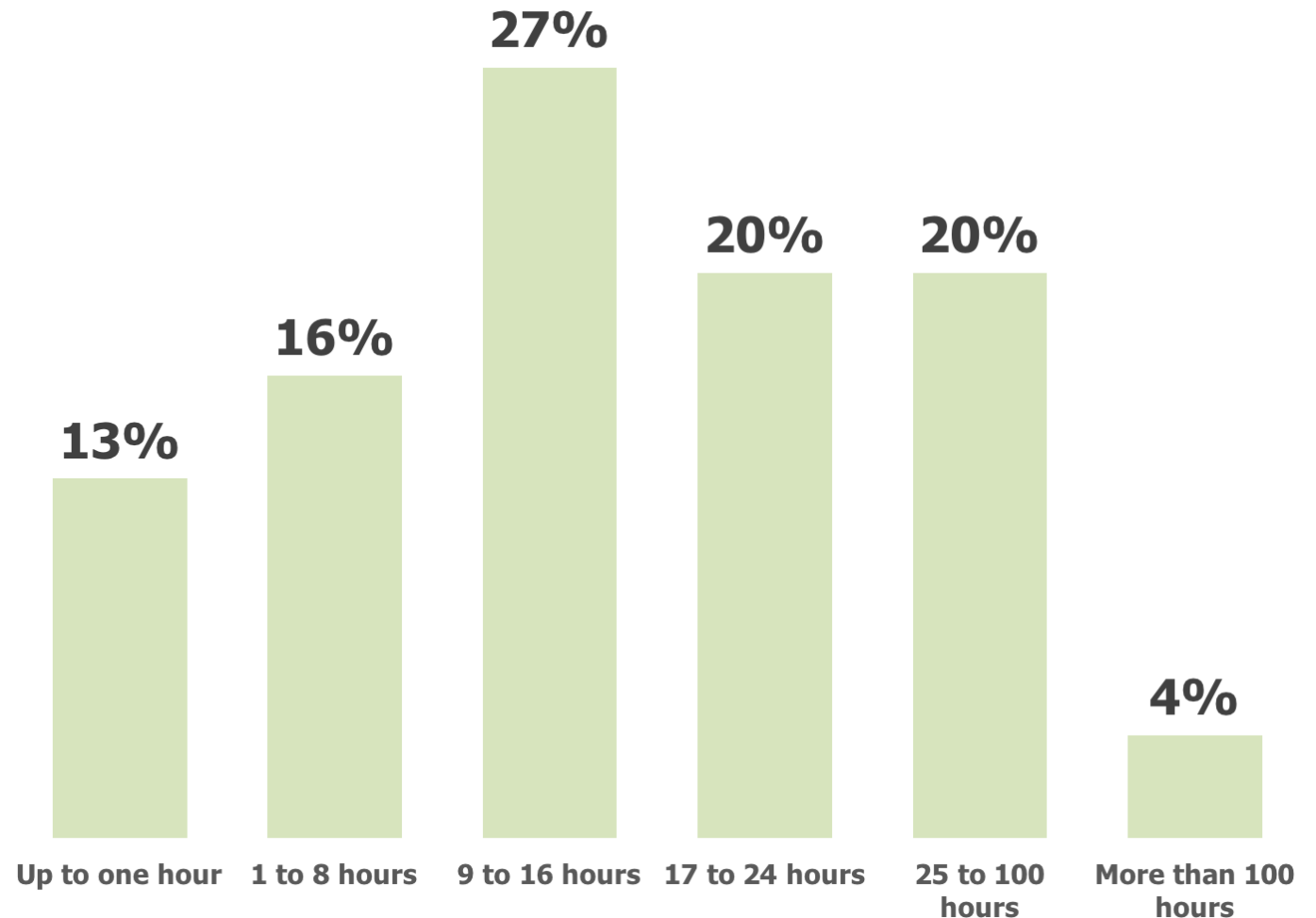
In some cases, every endpoint became infected



DOWNTIME IS A SERIOUS CONSEQUENCE

The extortion from ransomware is bad, but the downtime it causes is commonly a much bigger problem

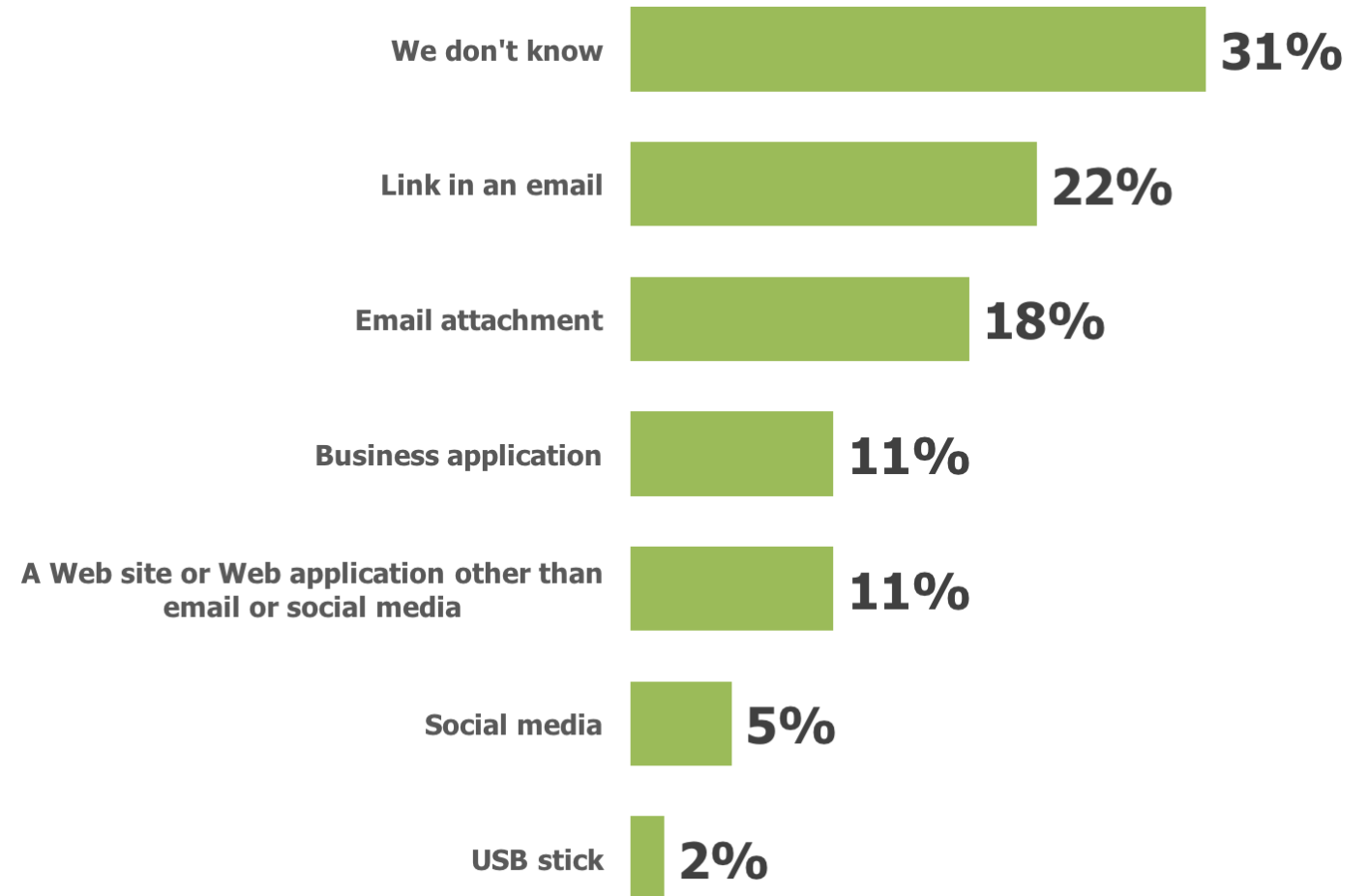
Nearly one in four organizations experienced more than 24 hours of downtime as a result of ransomware



HOW DID RANSOMWARE ENTER?

A plurality of SMEs infected with ransomware don't know how they became infected

Not knowing how the infection started makes remediation longer and keeps decision makers from plugging the gaps in their ransomware defenses

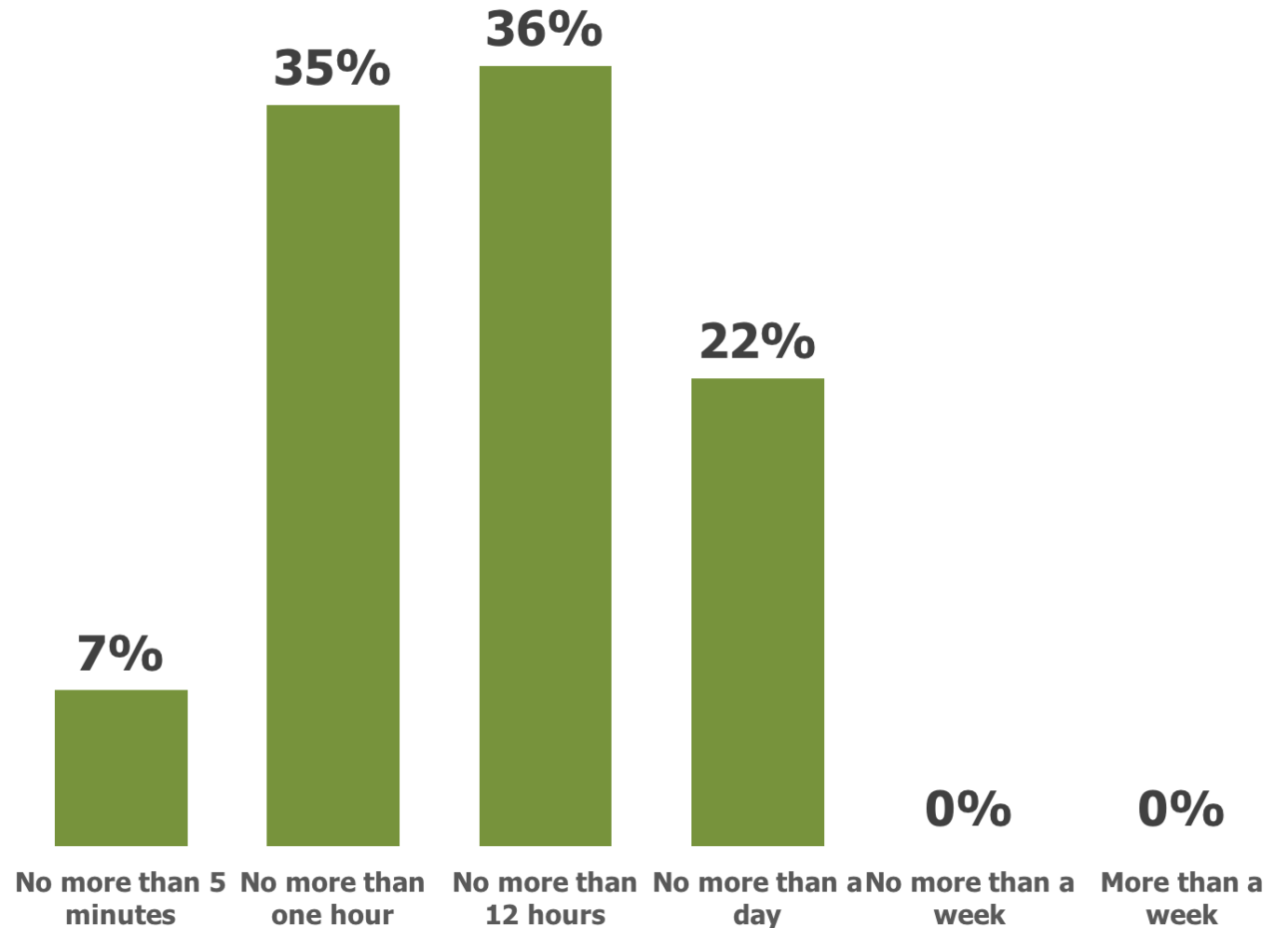


HOW DOES IT RESPOND TO RANSOMWARE?

Time elapsed before the ransomware was detected

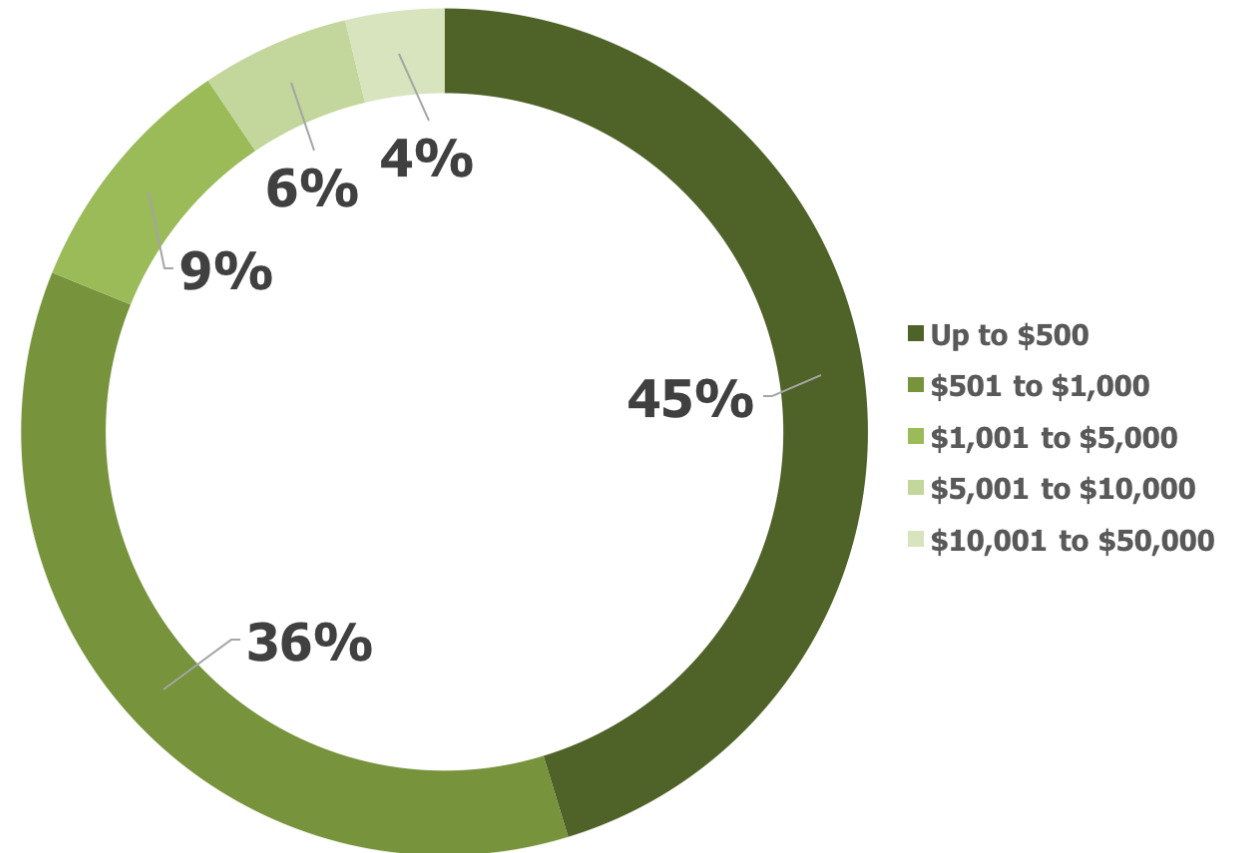
Most SMEs took more than one hour before they knew they had been victimized by ransomware

Some organizations didn't know they were infected for up to a week



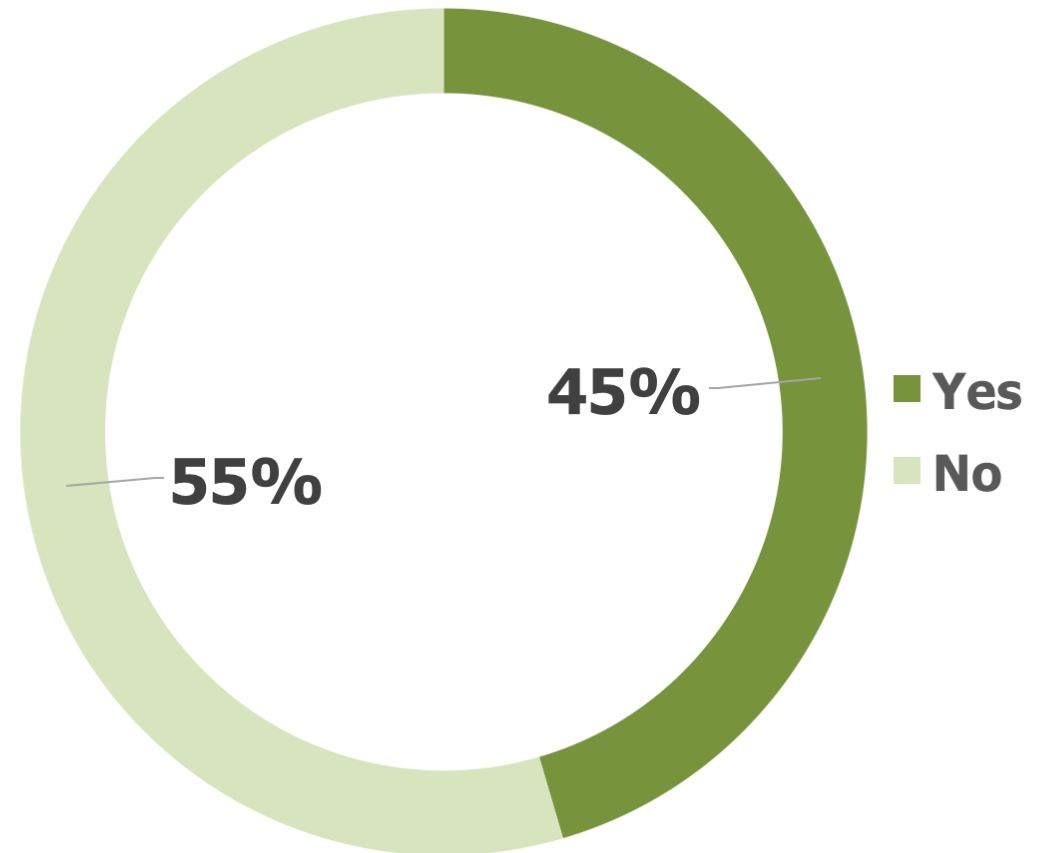
AMOUNTS DEMANDED

Most ransomware demands that strike SMEs are for relatively small sums



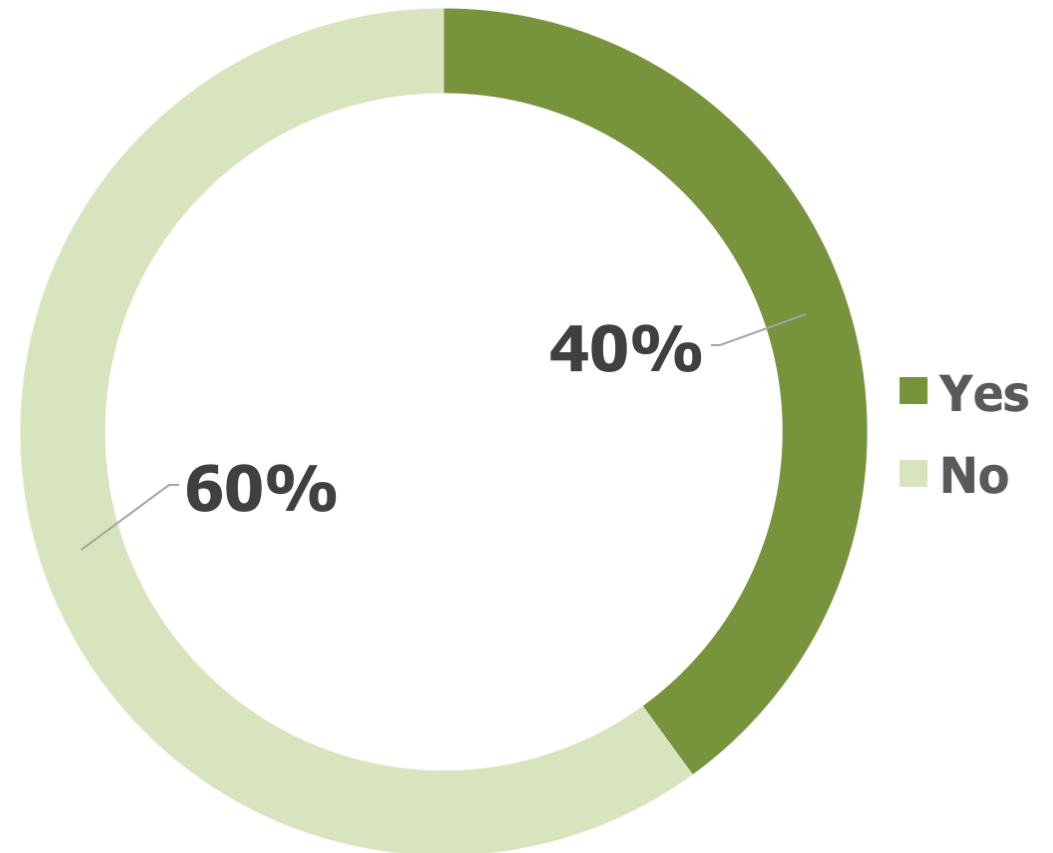
WAS THE RANSOM PAID?

Most SMEs chose not to pay the ransom that was demanded of them



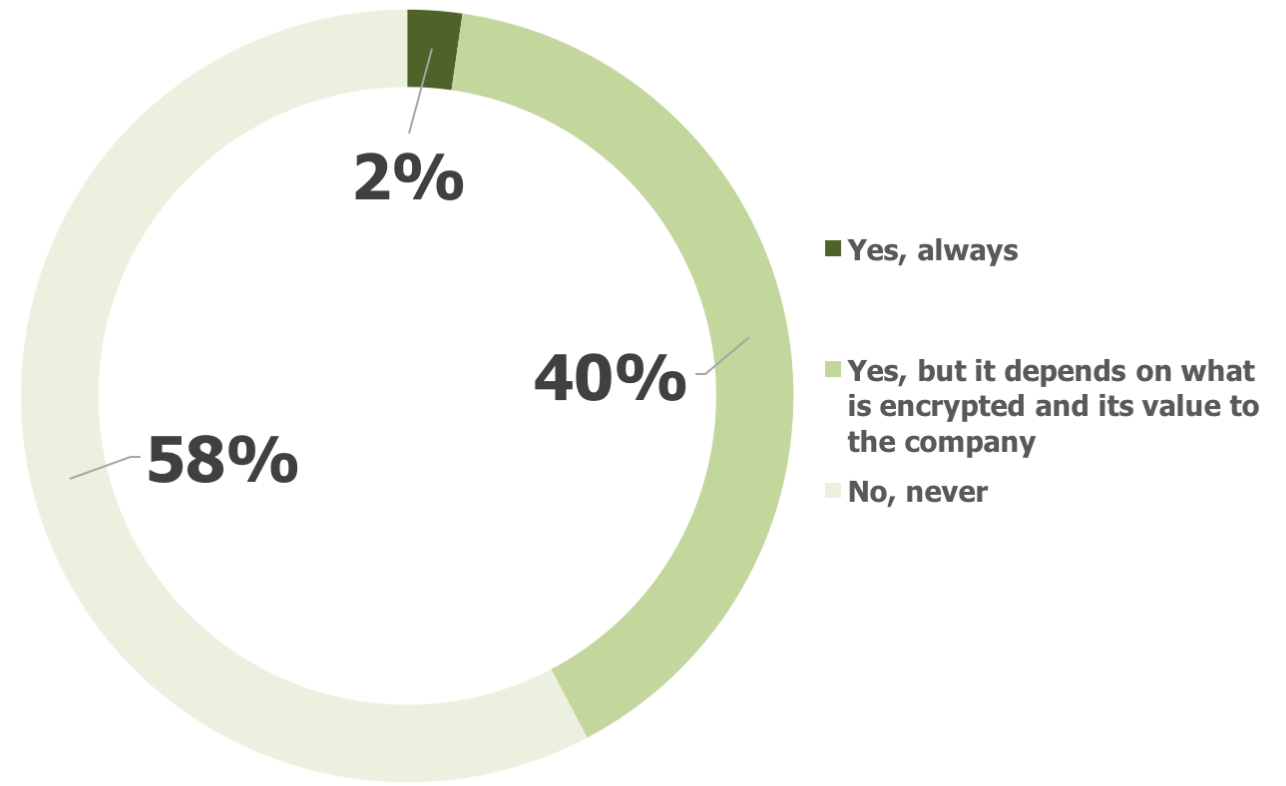
WERE FILES LOST IF THE RANSOM WASN'T PAID?

Among organizations that chose not to pay the extortion demands, about two in five lost files as a result



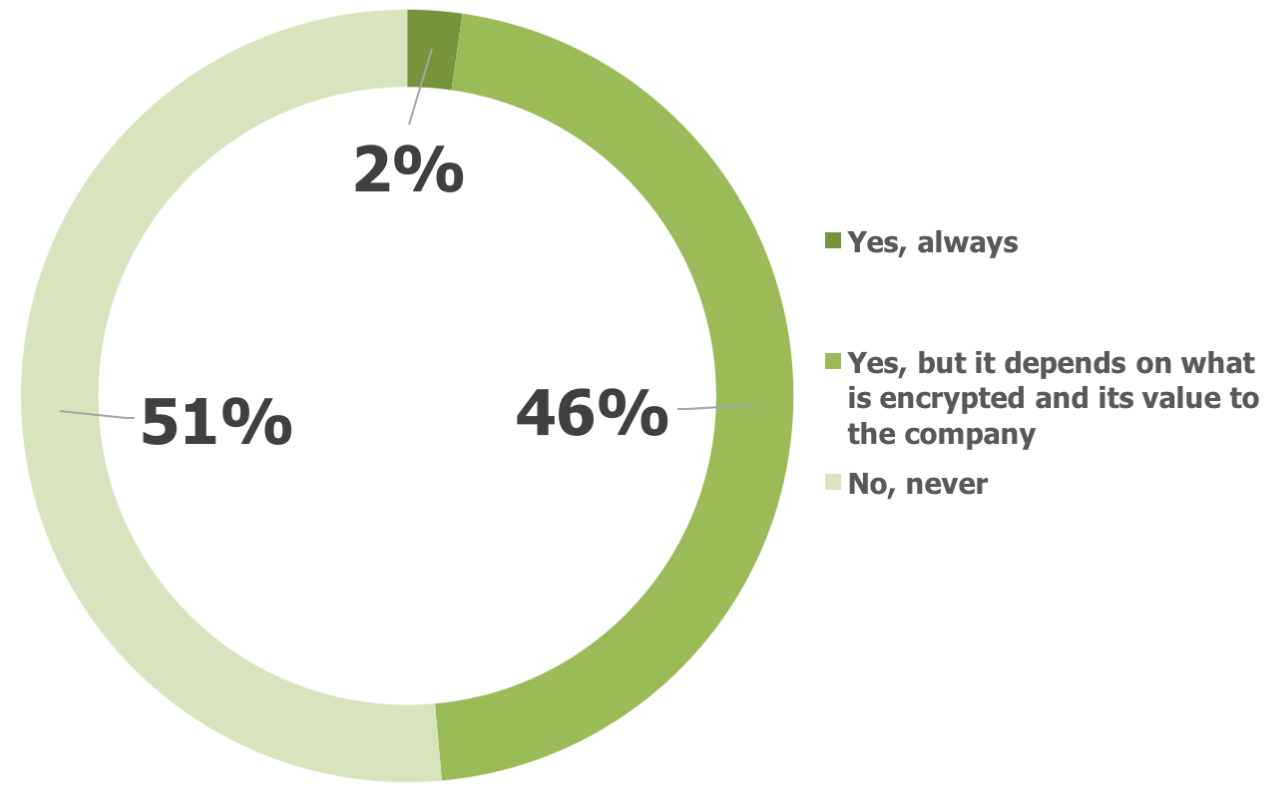
SHOULD COMPANIES PAY RANSOM?

Only about two in five believe that ransomware demands should be paid



SHOULD YOUR COMPANY PAY THE RANSOM?

SMEs are fairly consistent in their views about paying ransom, even when it's their own company that gets victimized



THE NEED TO ADDRESS RANSOMWARE

Percentage indicating a “high priority” or “very high priority”

The vast majority of SMEs view addressing the ransomware problem in general as a high priority

They are less enthused about making investments to do so, however

Addressing the ransomware problem

61%

Investing in resources, technology and funding to address ransomware

54%

Investing in education and training about ransomware for your end users

47%



A HUMAN OR TECHNOLOGY ISSUE?

SMEs view solving the ransomware issue as both a technology and a training problem

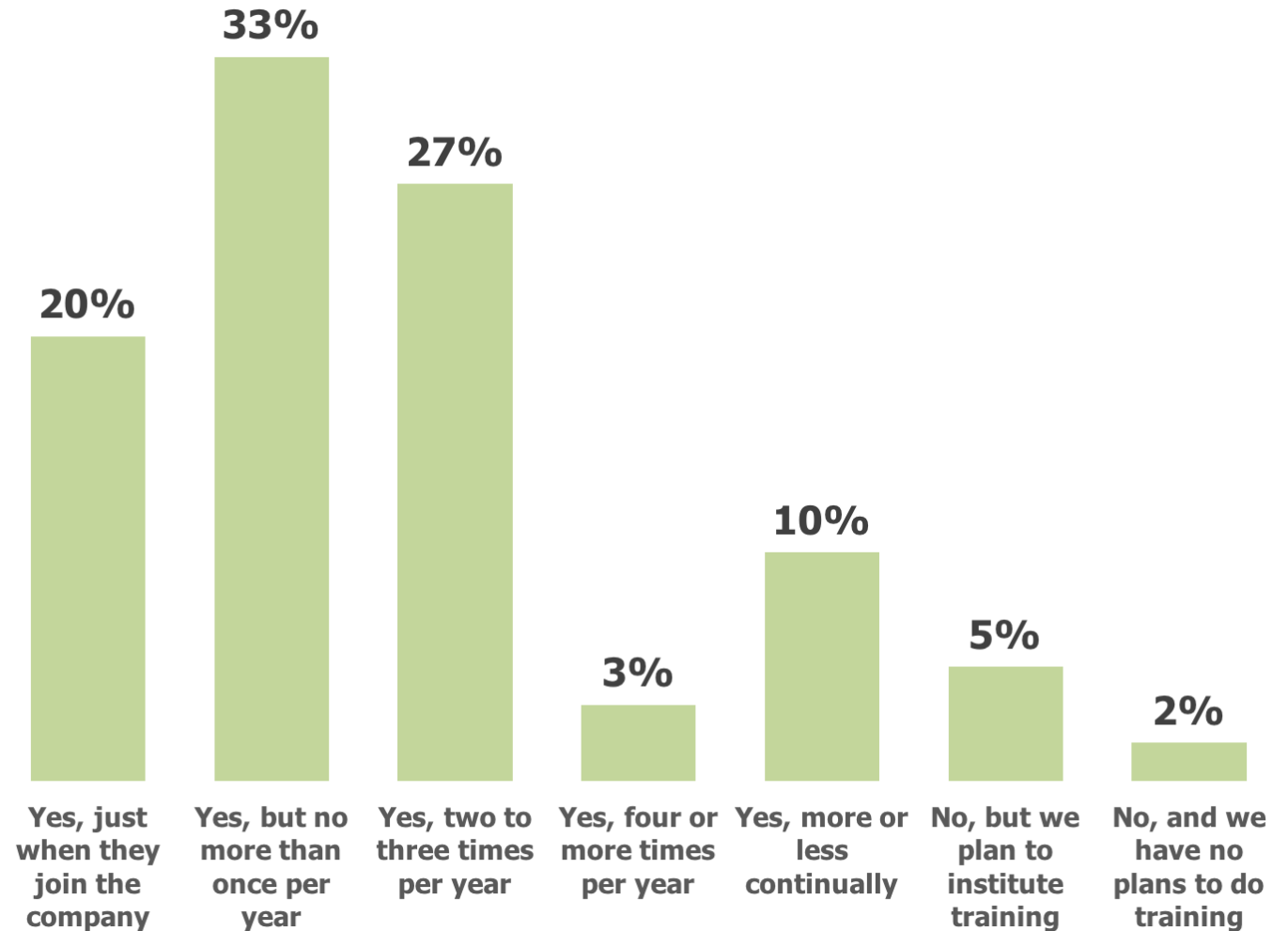
However, they lean toward technology-based solutions as the best way to solve ransomware



THE ROLE OF SECURITY TRAINING

Only about one in 14 organizations does not conduct security awareness training that specifically addresses ransomware

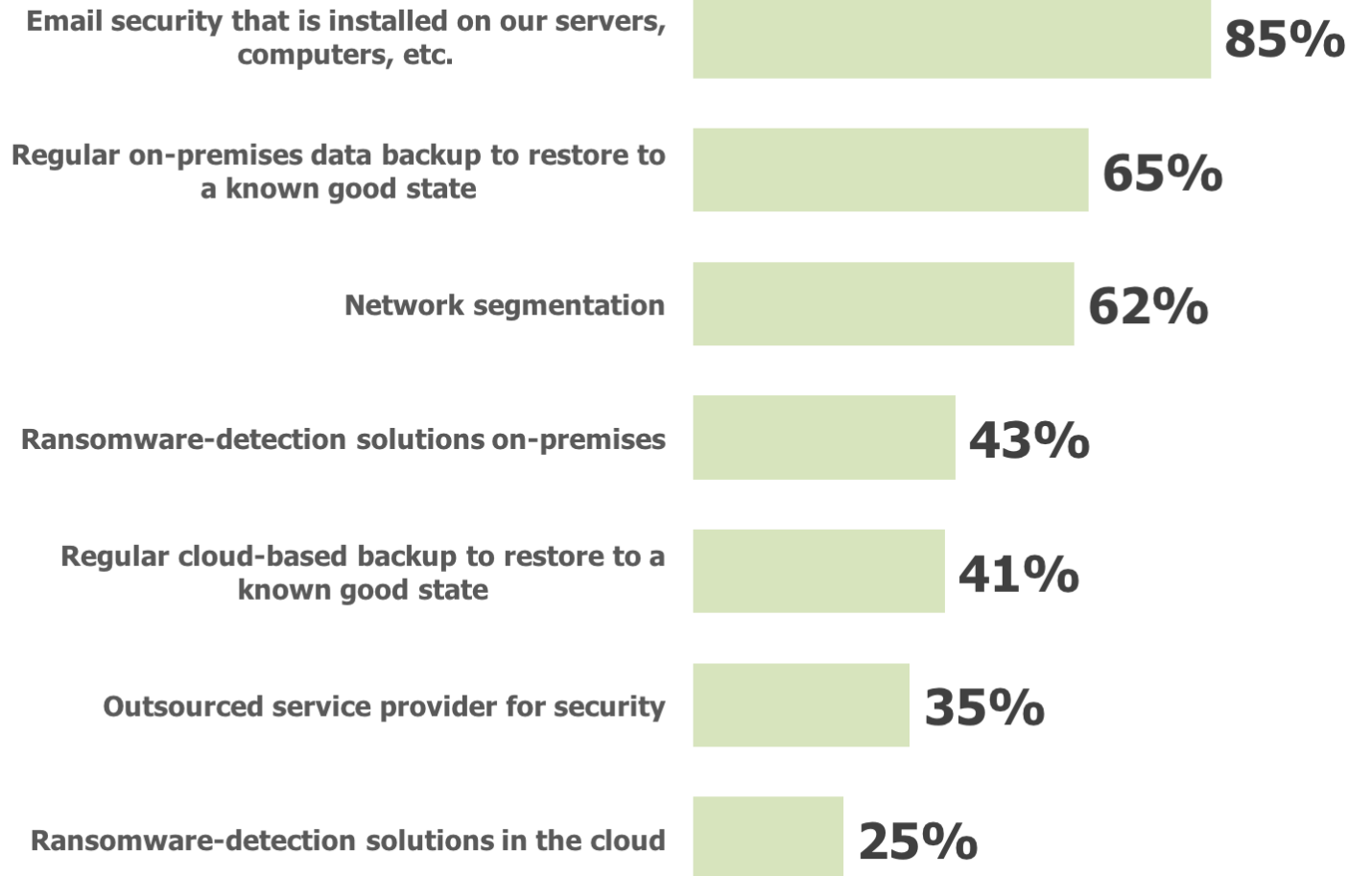
However, training is not as frequent or as comprehensive as it needs to be



TECHNOLOGIES AND PROCESSES IN PLACE

Most SMEs used email security solutions and backups as their ways of preventing or recovering from ransomware

Most do not yet have anti-ransomware technologies in place



Thanks and Questions?

