SAN FRANCISCO, 2018

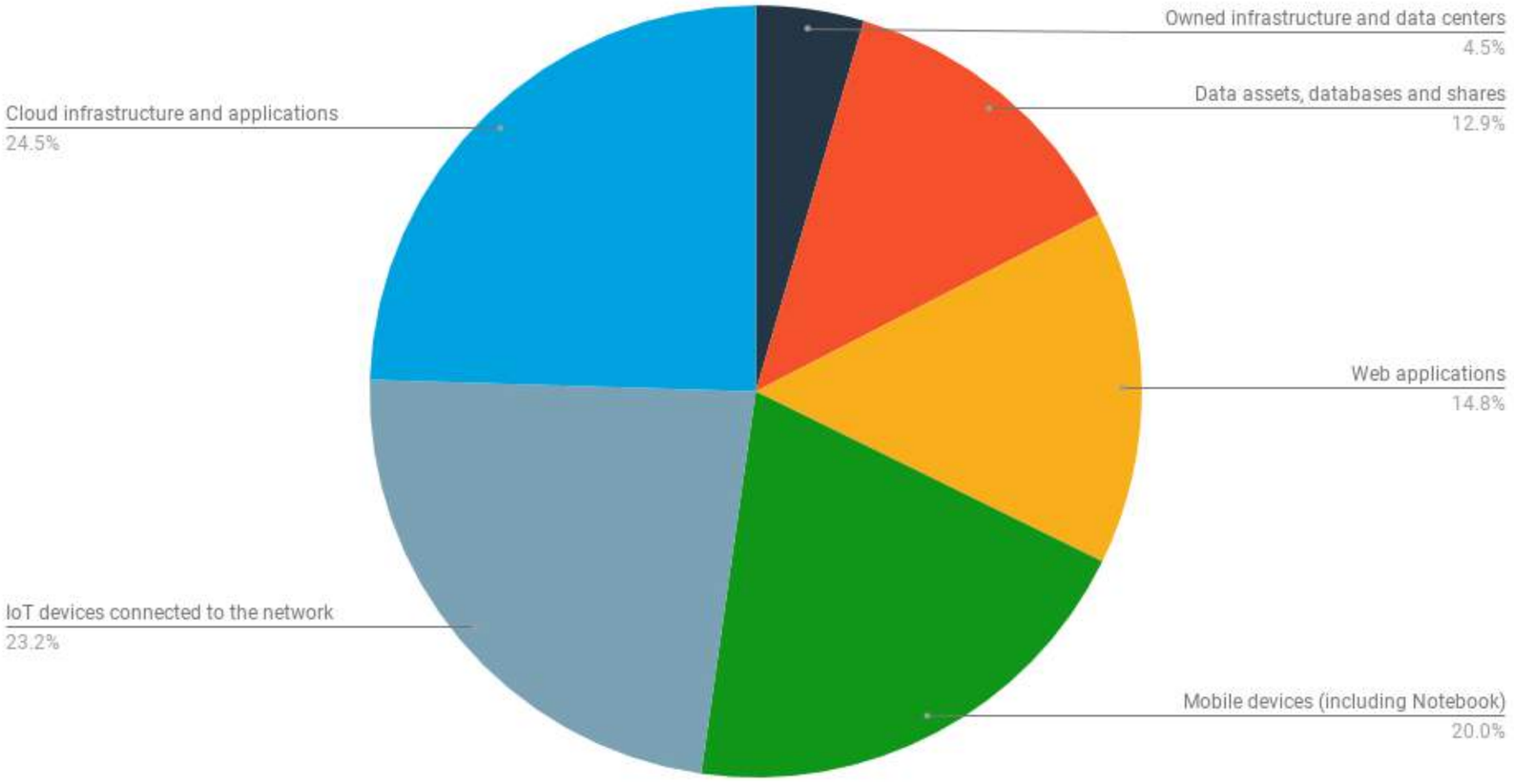
RSA SURVEY

Outpost24

SURVEY HIGHLIGHTS

- Cloud infrastructure, IoT and mobile devices are perceived as the biggest security problems for organizations surveyed
- Only **47 percent** of organizations patch vulnerabilities as soon as they are known, 16 percent wait for one month, while eight percent admit to only applying patches once or twice a year.
- **16 percent** of organizations have ignored a critical security flaw because they didn't have the skills to rectify it, while **26 percent** have ignored a critical security flaw because they didn't have time to fix it
- Only **15 percent** run security testing to understand the assets on their network and their relative security posture, **85 percent** don't, or don't know if their organization does
- **Only 17 percent** of organizations have hired a penetration tester to assess the security of their network, of those **46 percent** found a critical flaw which could have put their organization at risk. However, **35 percent** believe that if they were to hire a penetration testing services they wouldn't surface any new risks
- **15 percent** of IT professionals believe their web applications are least secure
- **25 percent** believe cloud infrastructure and applications are least secure
- **23 percent** believe IoT devices connected to the network are least secure
- **20 percent** believe mobile devices (including Notebook) used by mobile/remote workers are least secure
- When asked what route they'll take to hack their companies, **21 percent** said they would enter through our public Cloud Hosted compute, while **34 percent** said they would use social engineering
- When asked if their attack would be successful, **71 percent** said it was likely or highly likely that it would be. Only **9%** said it is very unlikely their attack would succeed
- Only **4 percent** of organizations use a commercial cloud
- **40% percent** say they use the same security for their cloud environments as they do for their owned assets or data centres.

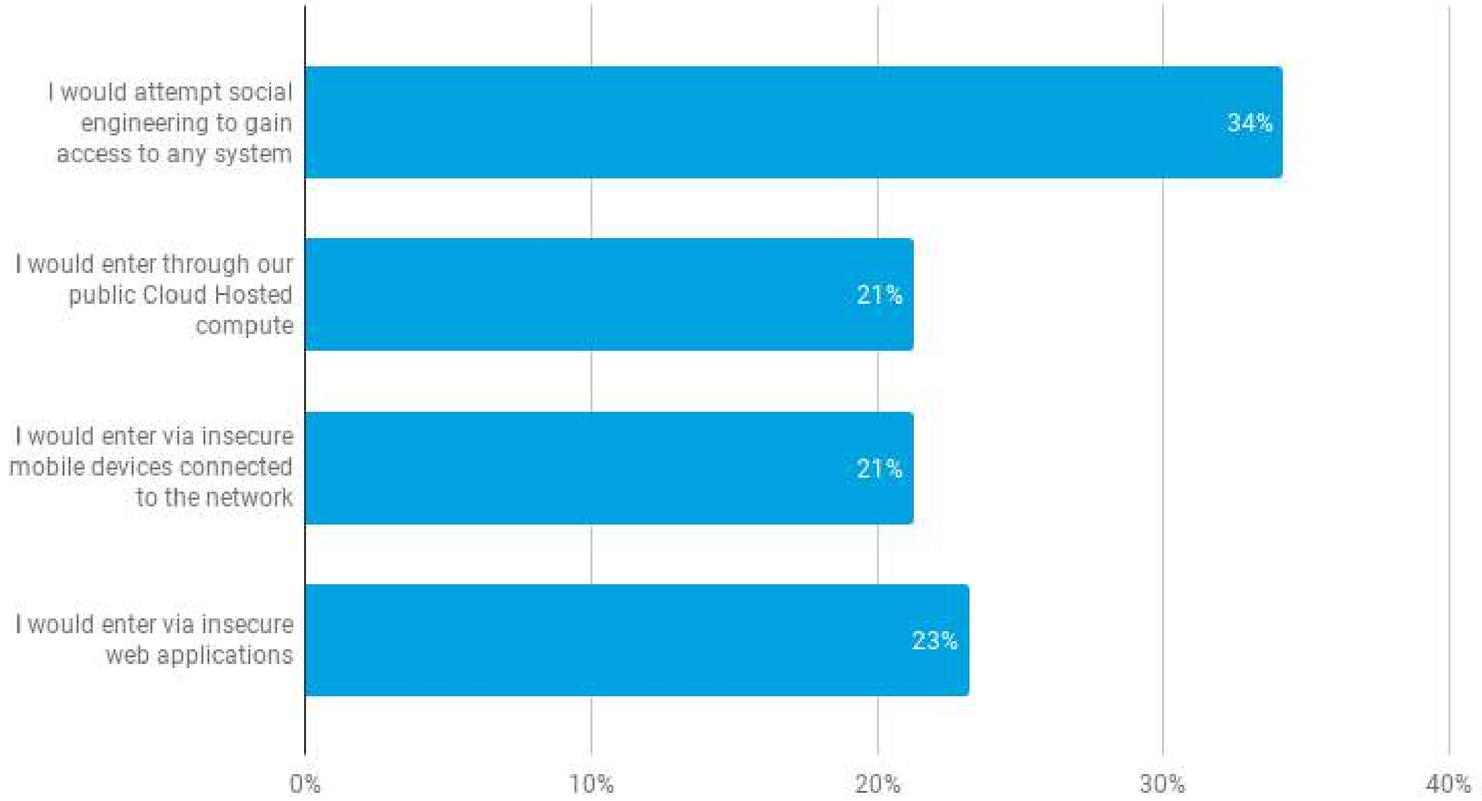
Q1. In your opinion, what area of your organization's technology is the least secure?



Source: Based on a survey of 155 security professionals during RSA 2018

Outpost24
Vulnerability Management made easy

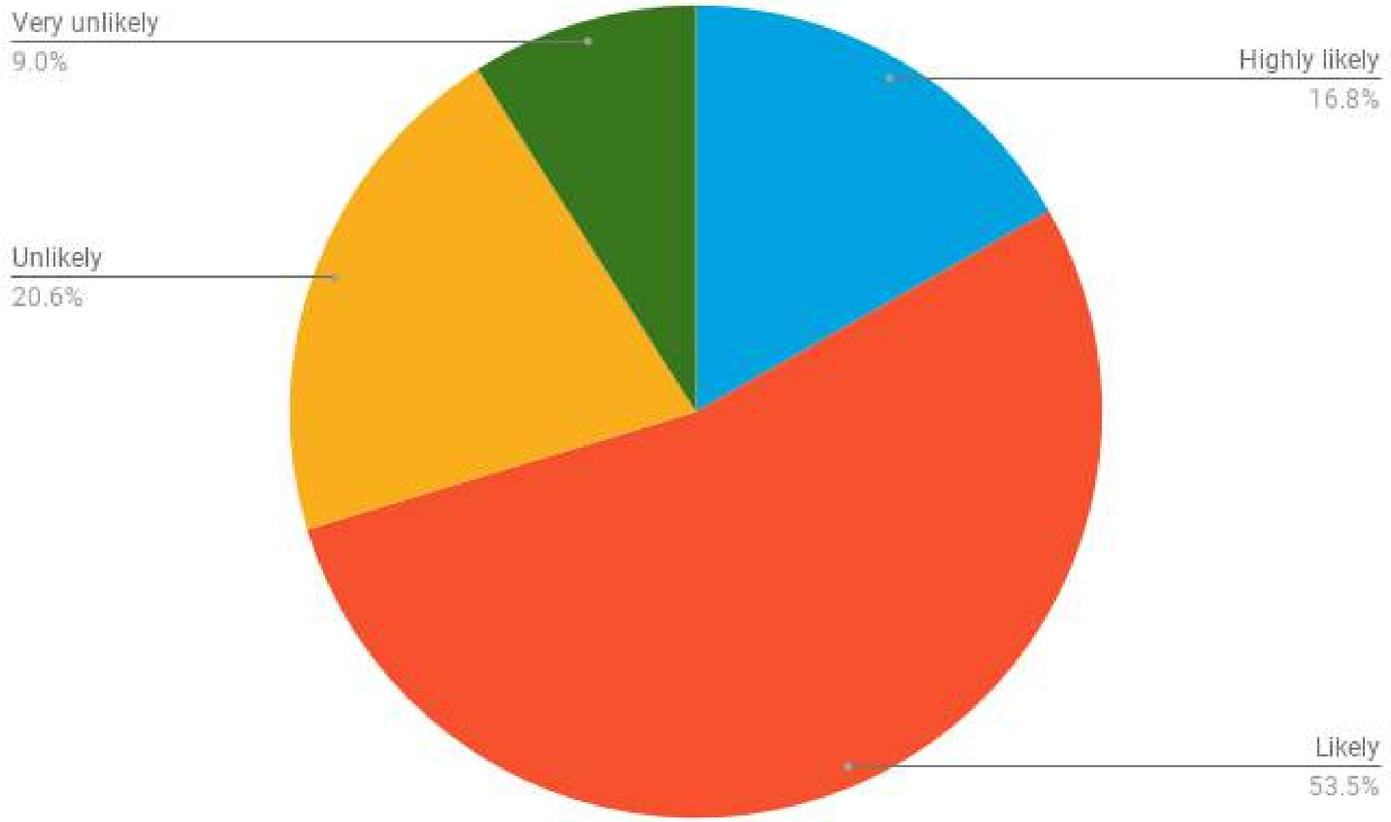
Q2. From your knowledge of hacking and recent cyber attacks, what route would you take to infiltrate an organization with the highest chance of success?



Outpost24
Vulnerability Management made easy

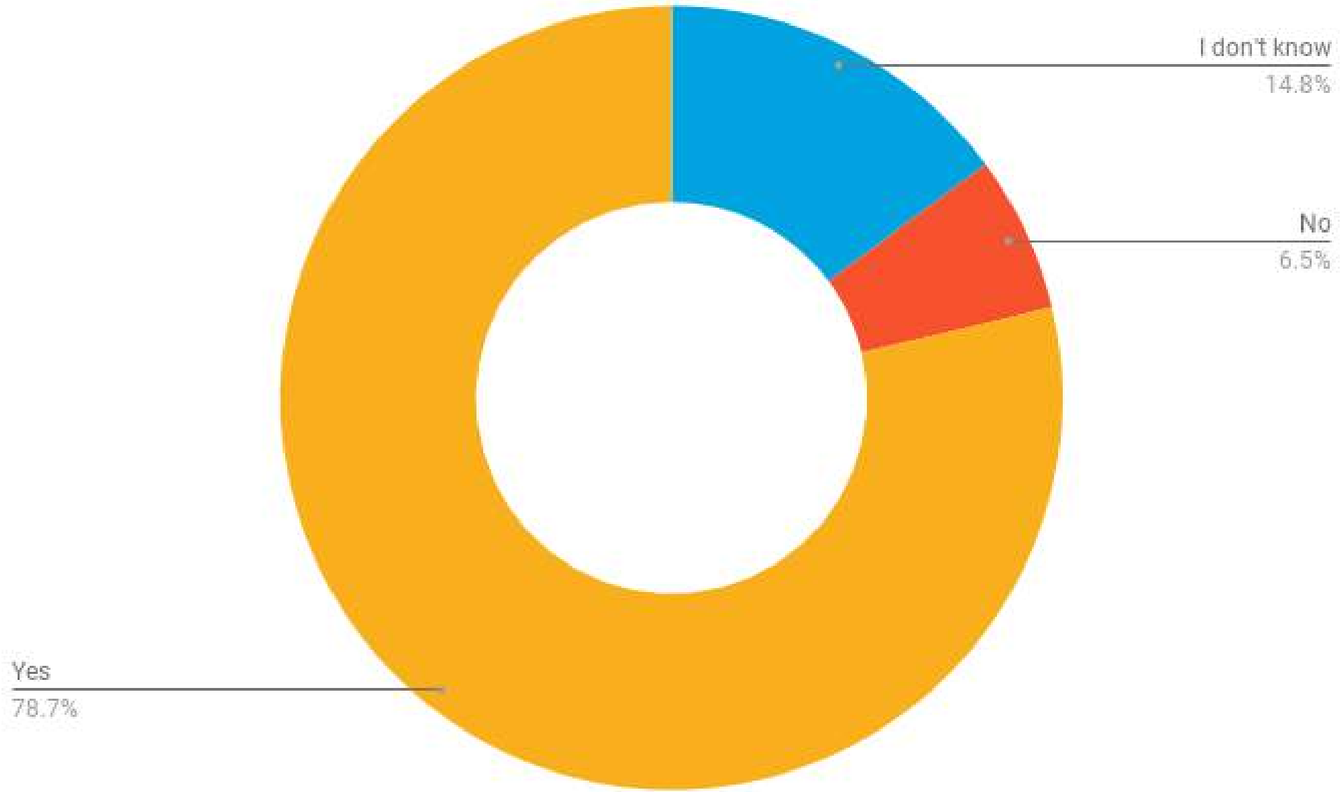
Source: Based on a survey of 155 security professionals during RSA 2018

Q2a. What are the chances of your attack being successful?



Outpost24
Vulnerability Management made easy

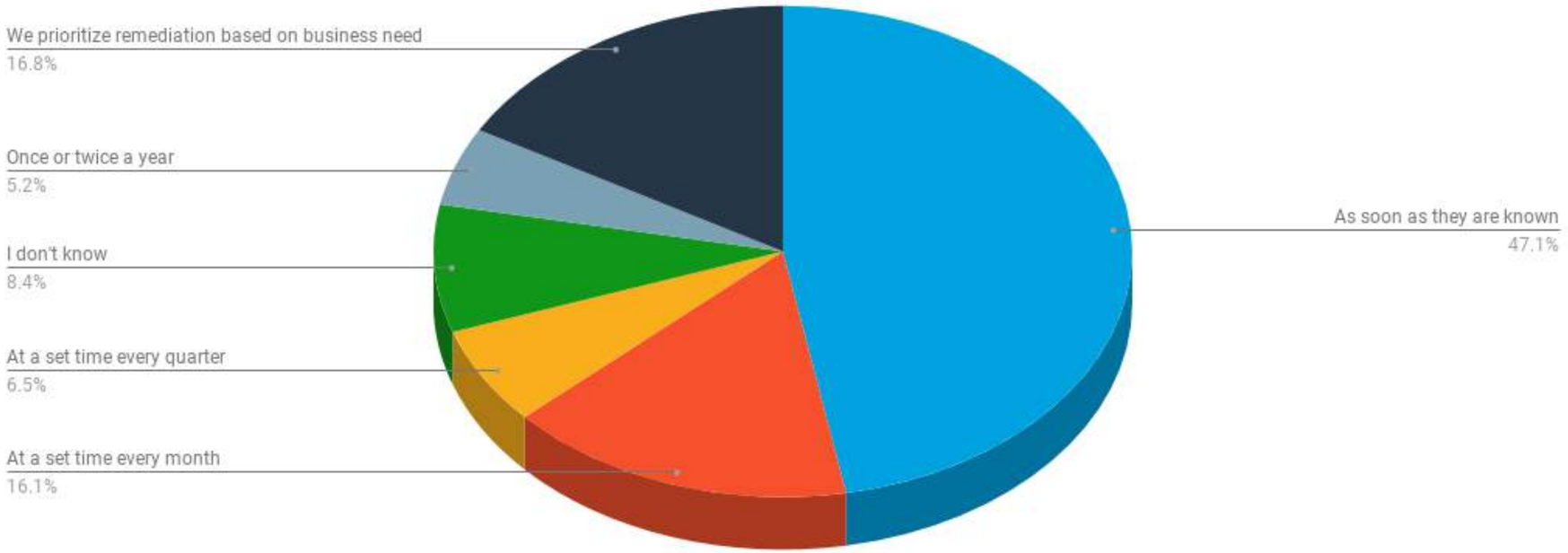
Q3. Does your organization run any security testing to understand the assets you own and their relative security posture?



Source: Based on a survey of 155 security professionals during RSA 2018

Outpost24
Vulnerability Management made easy

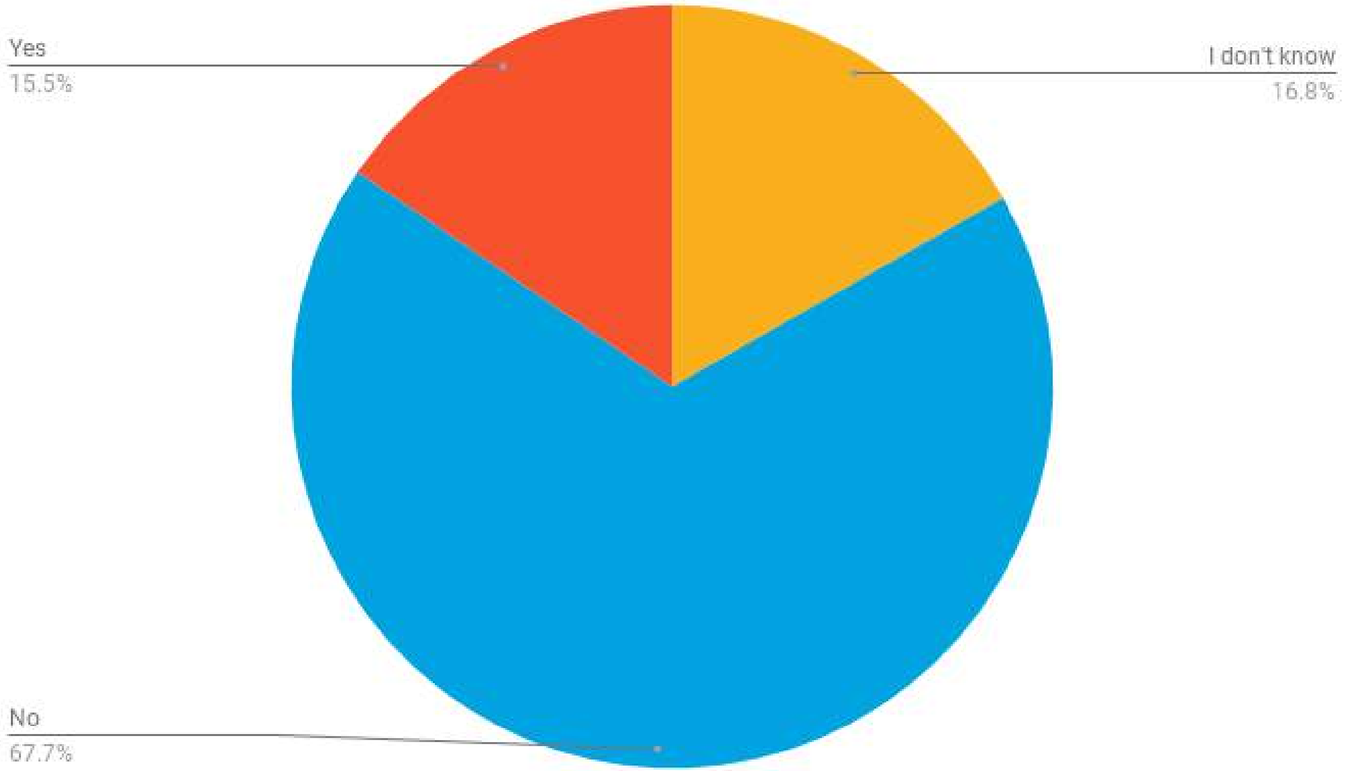
Q4. How quickly does your organization remediate known vulnerabilities of any type configuration, hardening, patching, access controls, etc?



Outpost24
Vulnerability Management made easy

Source: Based on a survey of 155 security professionals during RSA 2018

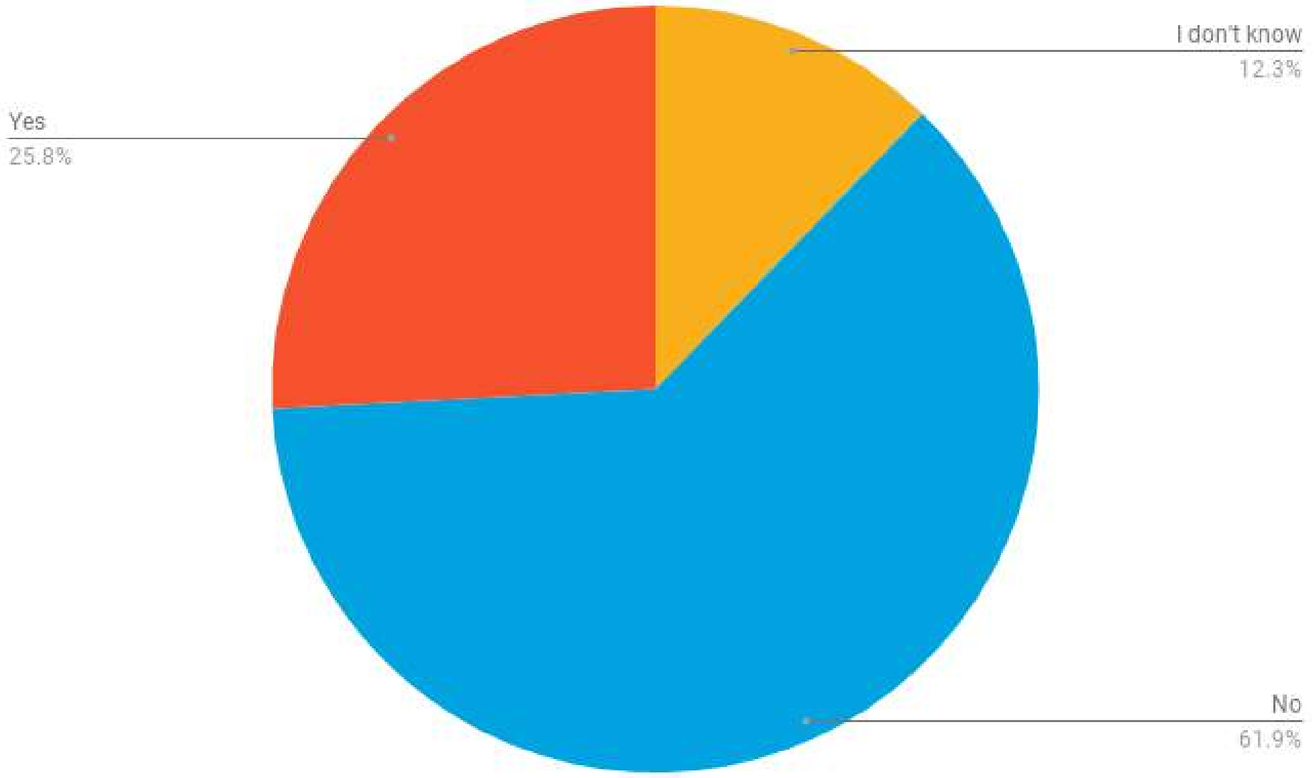
Q5. Has your organization ever ignored a critical security problem because it didn't know how to rectify it?



Outpost24
Vulnerability Management made easy

Source: Based on a survey of 155 security professionals during RSA 2018

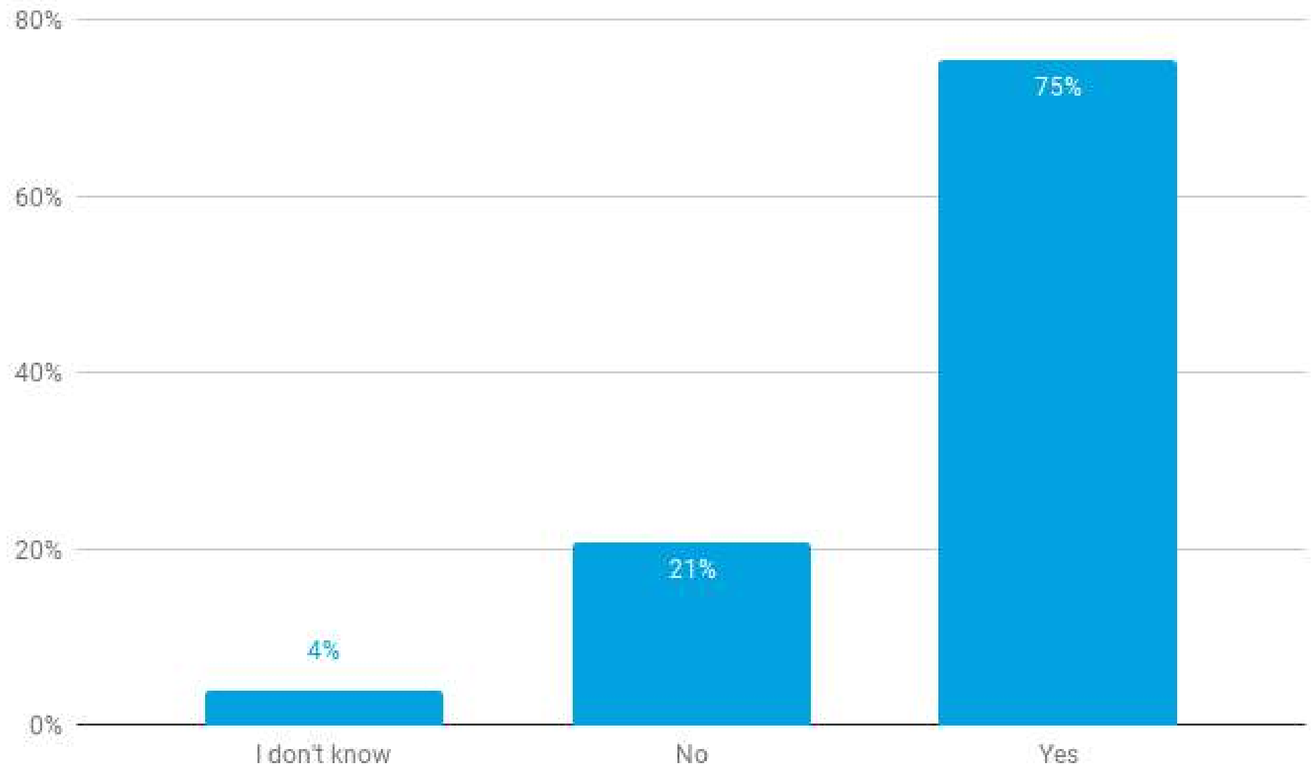
Q6. Has your organization ever ignored a critical security problem because it didn't have time or resources to rectify it?



Outpost24
Vulnerability Management made easy

Source: Based on a survey of 155 security professionals during RSA 2018

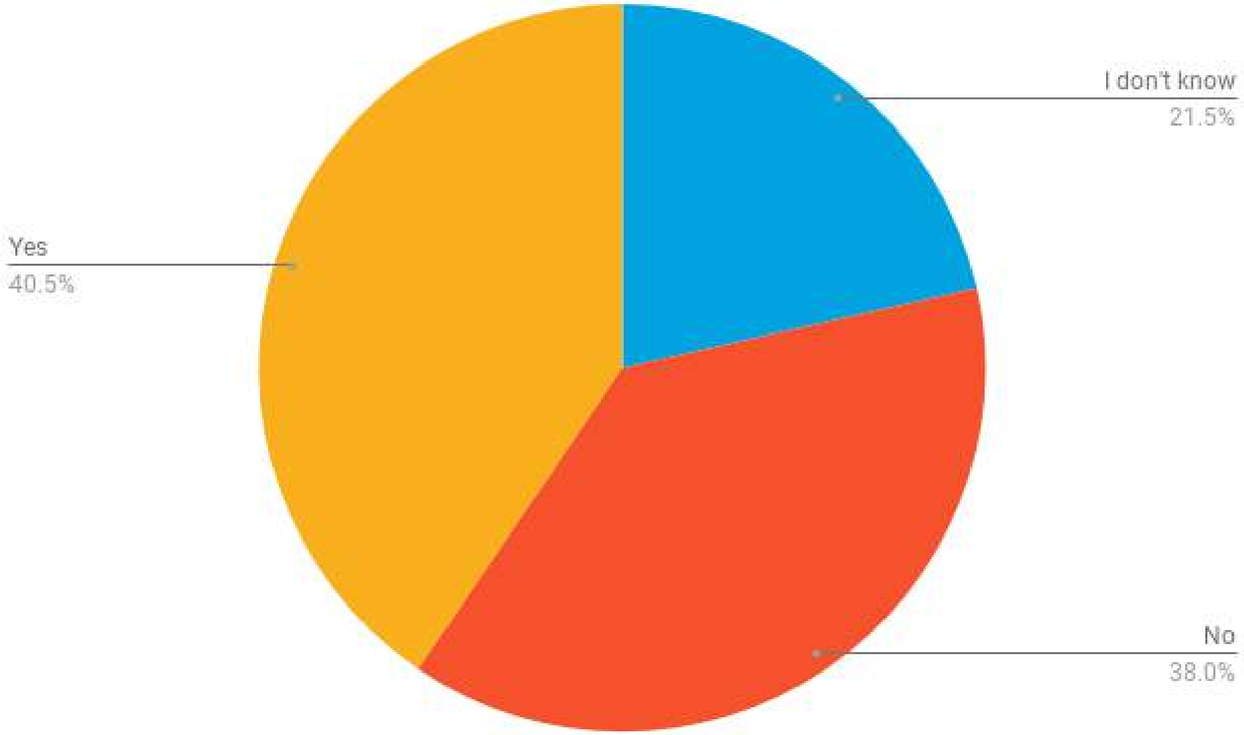
Q7. Does your organization use any infrastructure in a commercial cloud, such as Amazon AWS or Microsoft Azure?



Source: Based on a survey of 155 security professionals during RSA 2018

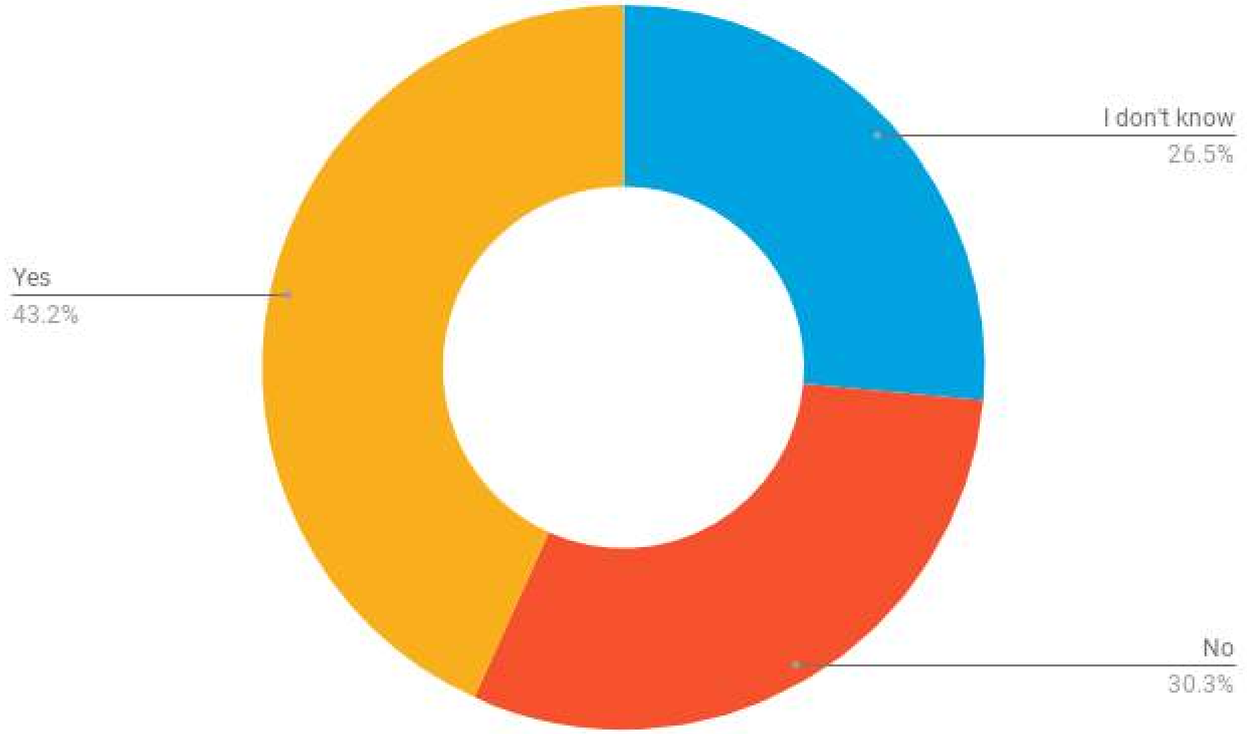
Outpost24
Vulnerability Management made easy

Q7a. If yes to question 7, do you use the same security technologies for your cloud environments as you use for your owned assets or data centers?



Outpost24
Vulnerability Management made easy

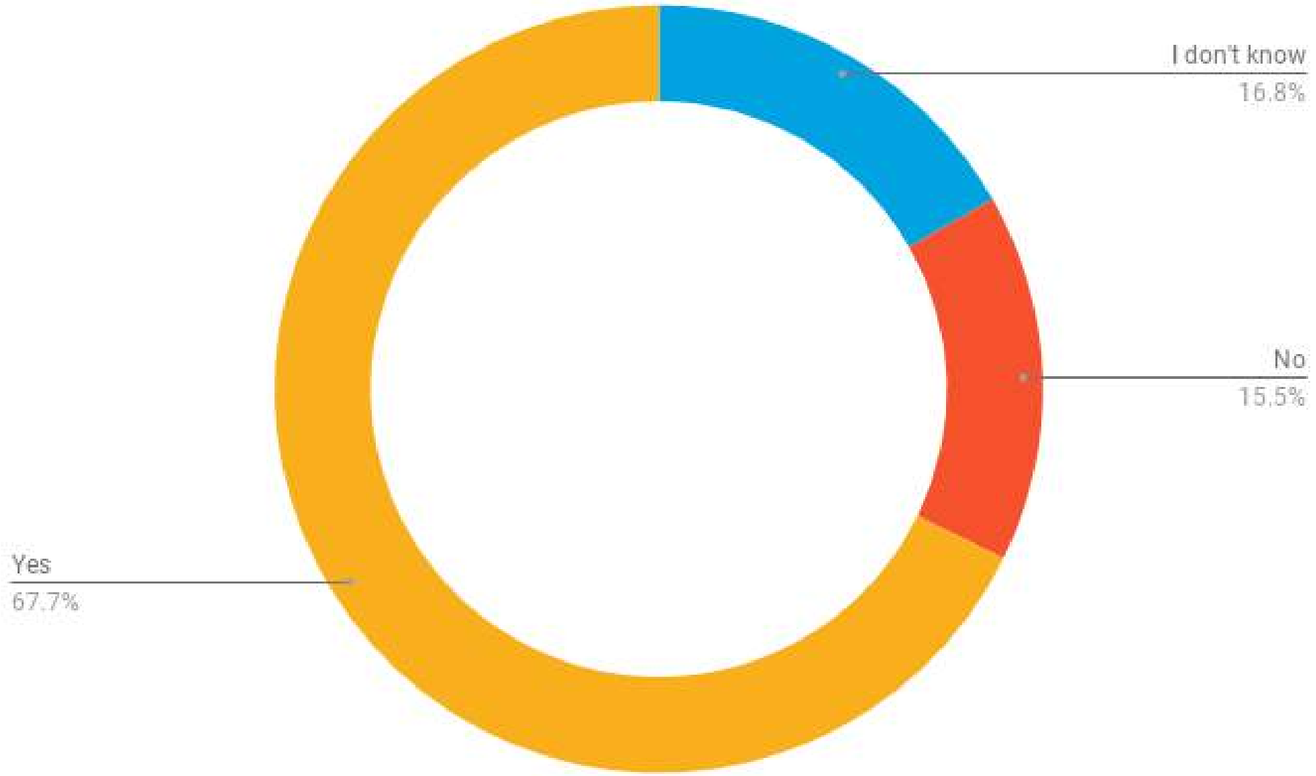
Q8. Do you think a penetration test on your technology stack would uncover a lot of risks you are not aware of?



Source: Based on a survey of 155 security professionals during RSA 2018

Outpost24
Vulnerability Management made easy

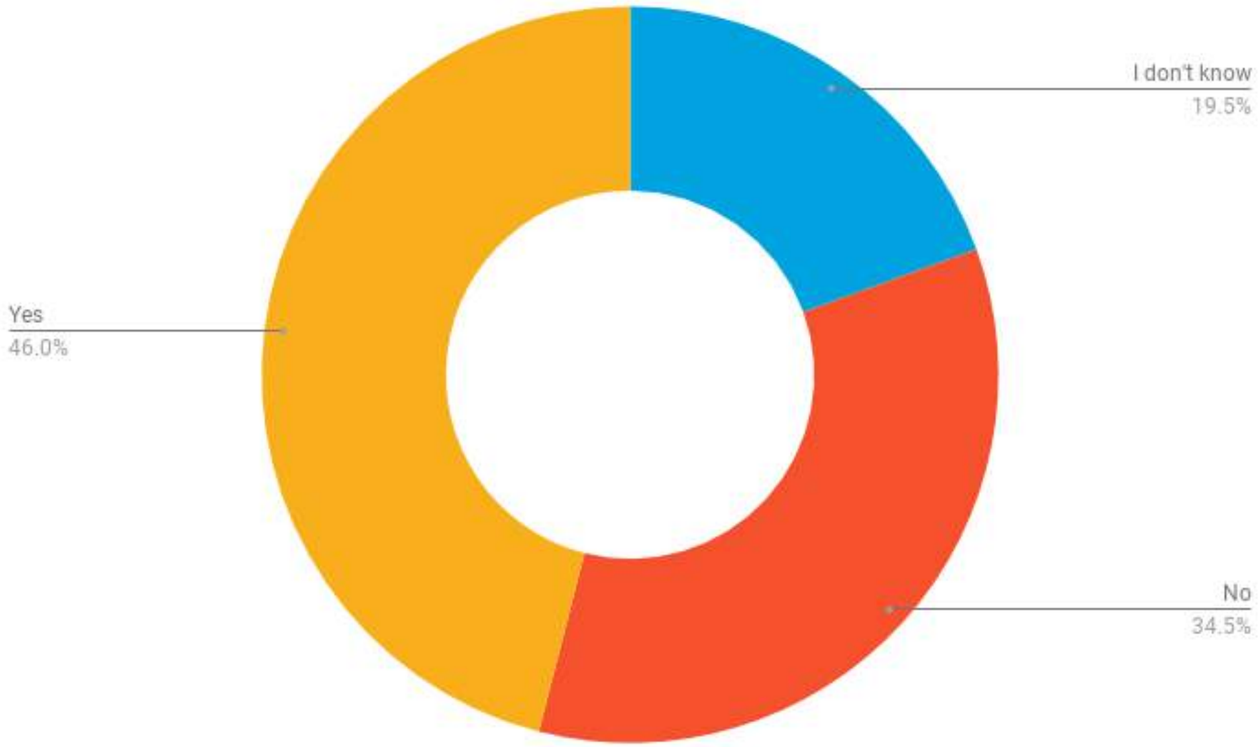
Q9. Has your company ever hired a penetration tester to carry out a security assessment on your organization's network?



Source: Based on a survey of 155 security professionals during RSA 2018

Outpost24
Vulnerability Management made easy

Q9a. If yes to question 9, did they discover anything critical which could have put your organization at risk?



Outpost24
Vulnerability Management made easy

Outpost24 provides security software that helps companies identify where they might be attacked before it happens. We don't think it's fair that businesses are targets of cyber criminals, so our ethical hackers have built tools that help our customers seek out vulnerabilities and fix them before their business is disrupted.

Over 2,000 customers in more than 40 countries trust Outpost24 to inspect their devices, networks, cloud infrastructure and web applications and report compliance status to government, industry sector, or internal regulations.

Outpost24.com