CIP-OAS CYBER SURVEY RESULTS

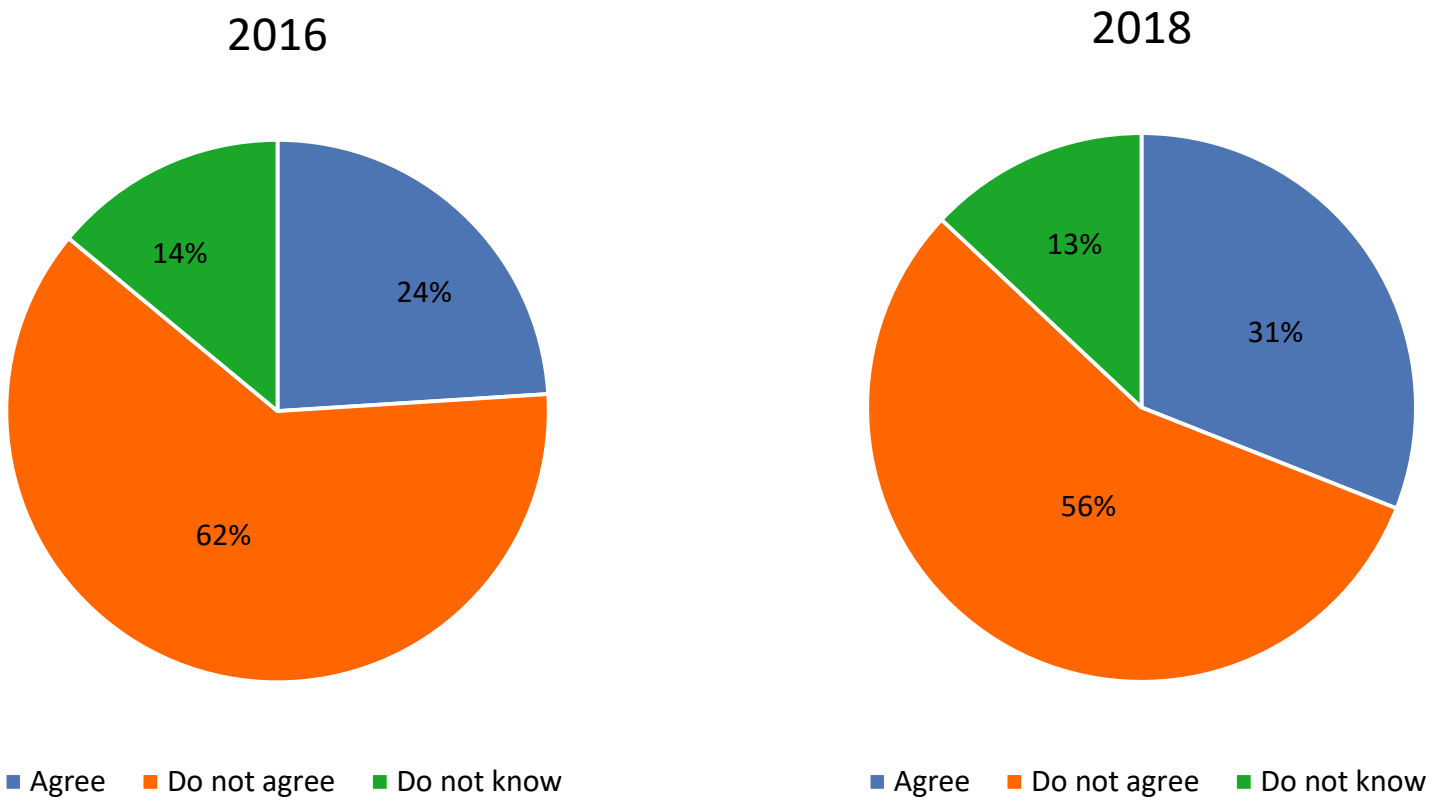
Positive

1. More awareness of previous cyber events and ongoing vulnerability
2. More confidence about what to do if compromised
3. More understanding of why a hacker might attack an individual employee
4. Limited formal cybersecurity training programs

Room for improvement

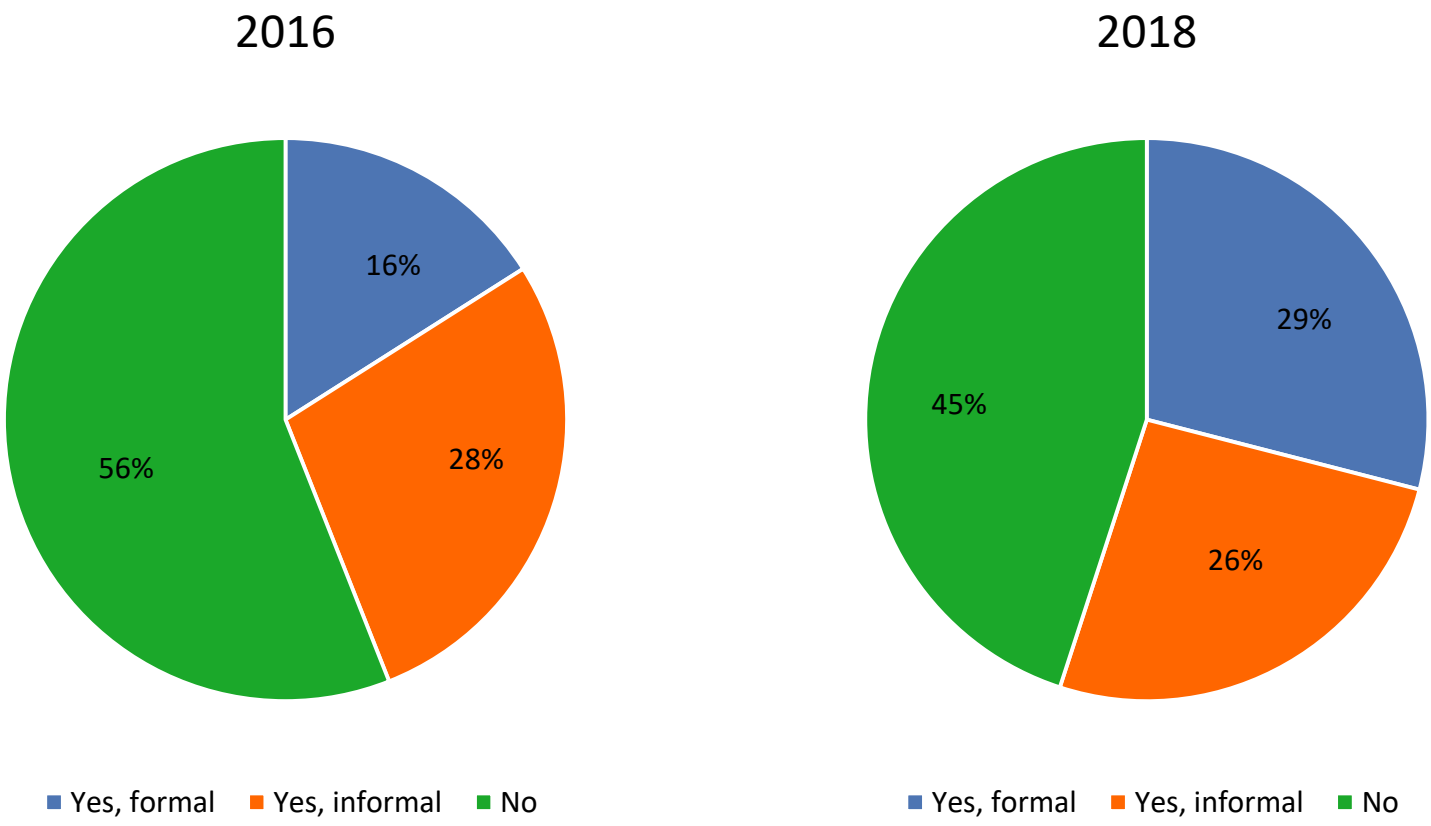
1. Many instances of shared passwords
2. Low confidence that the organization's IT and other networked assets are secure
3. Continued uncertainty regarding cyber insurance coverage gaps

1. To the best of my knowledge, my organization has suffered a successful cyber attack



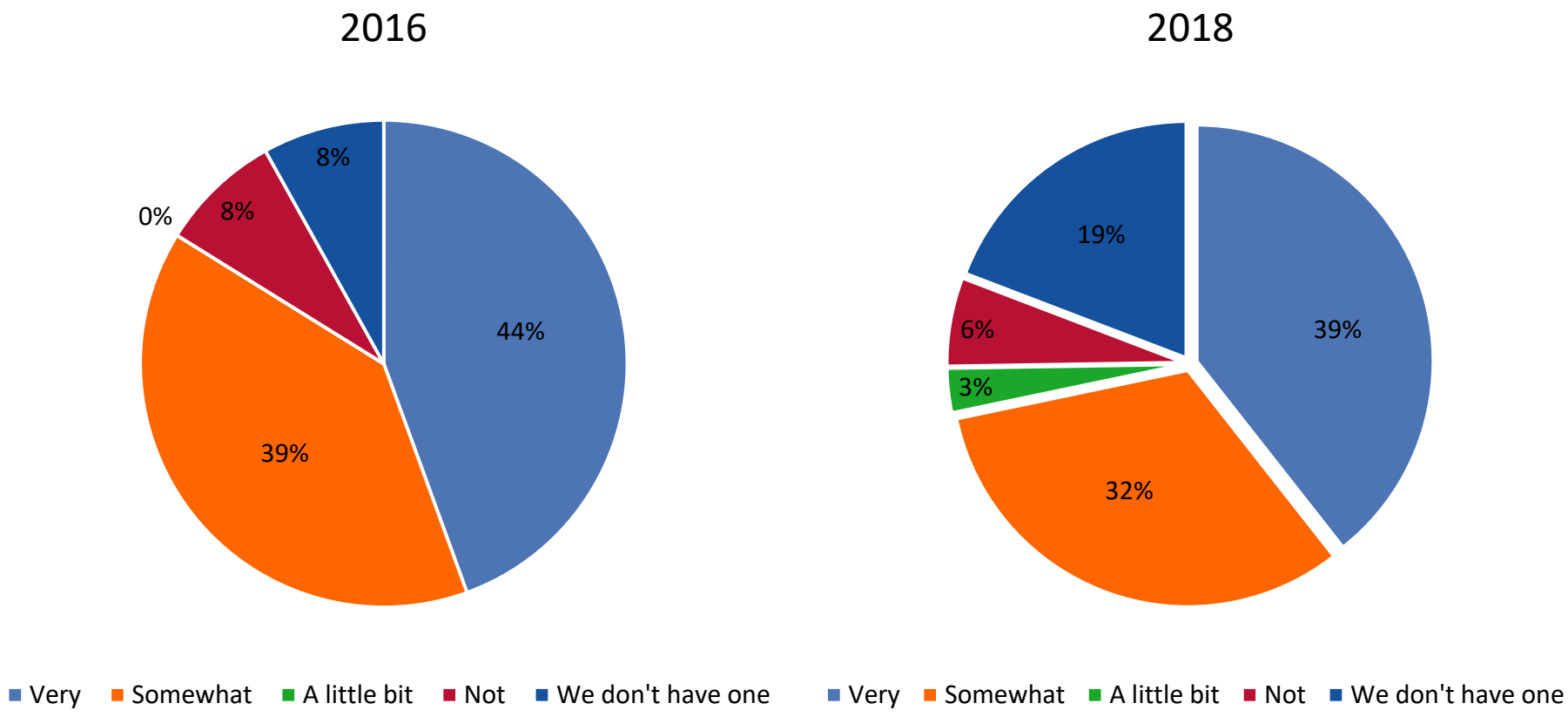
Although estimates vary, it is estimated that roughly half of organizations have suffered a successful cyber attack. Increasing awareness is important!

2. Does your organization provide any training on cyber risk awareness?



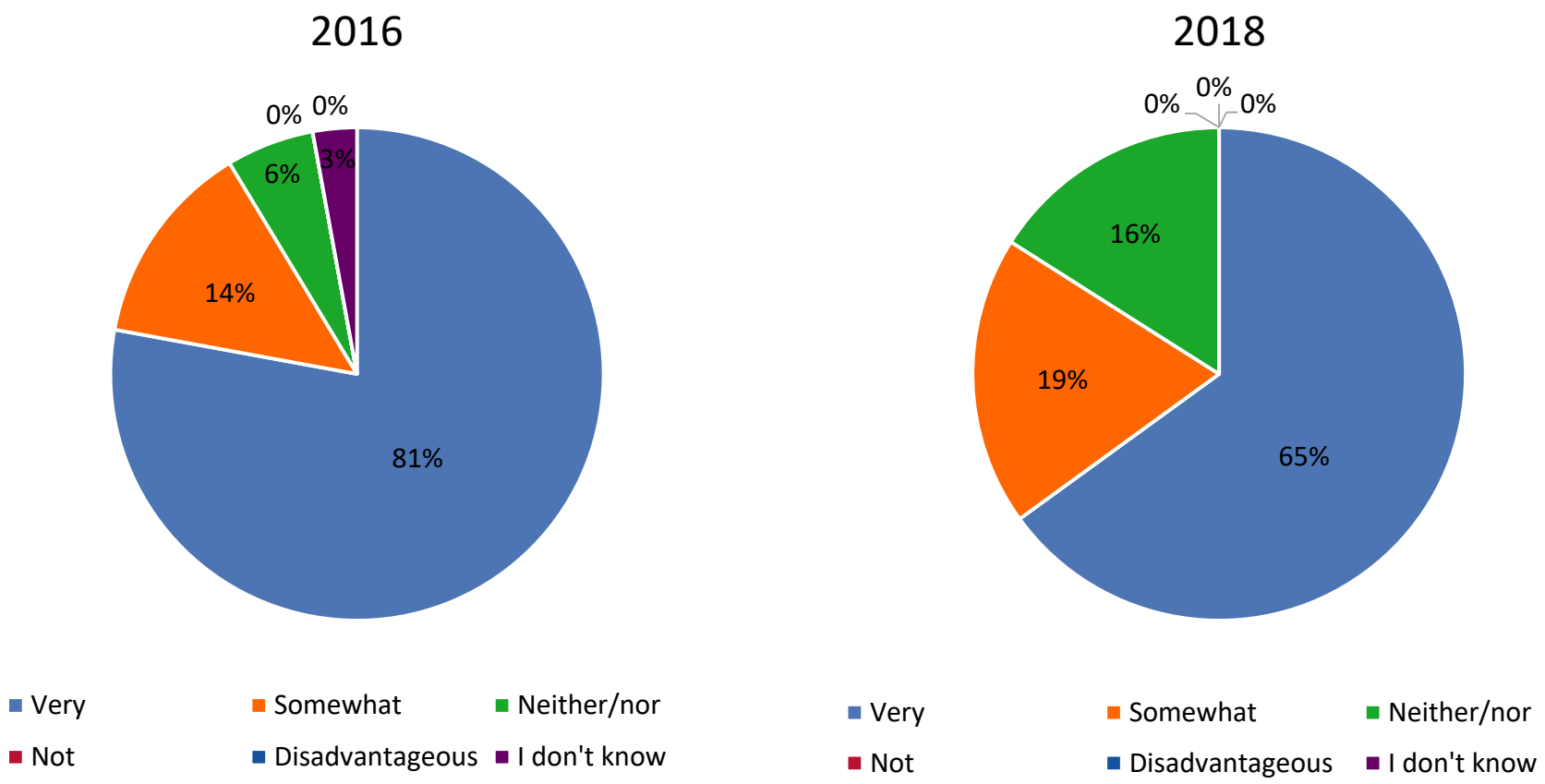
It is important that organizations provide cybersecurity training, and OAS CIP members are increasingly providing formalized training.

3. How aware are you of your organization's information security team's responsibilities?



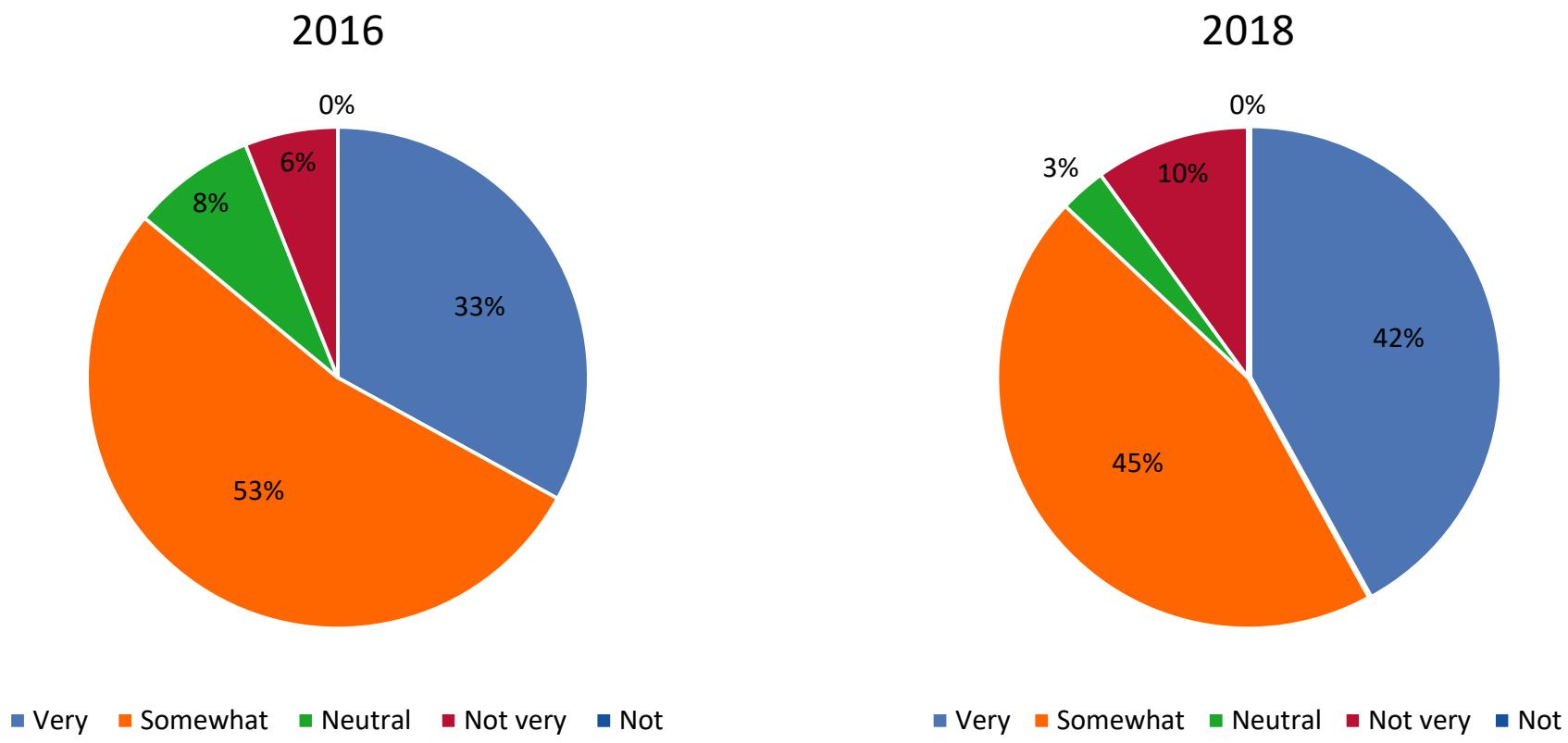
We can all work to increase familiarity with internal information security infrastructure. Knowing who to contact in the event of a cyber incident is critical to the security team's ability to identify, respond to, and recover from an attack.

4. How important is information security to your organization and its daily activities?



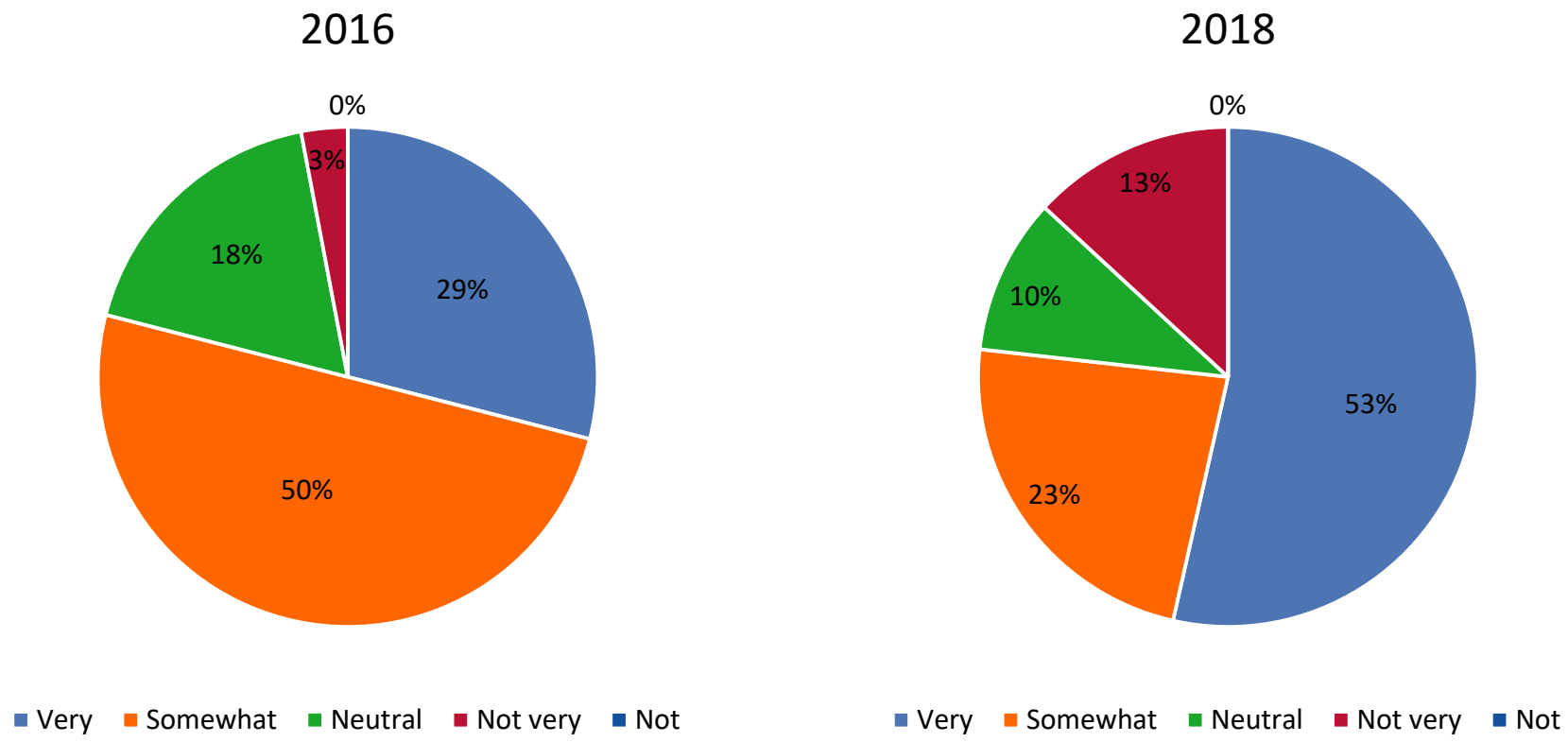
A decrease in perception that information security is important to our organizations is something we can seek to improve via awareness and training.

5. How confident are you that you can recognize the symptoms or indications of a cyber security incident?



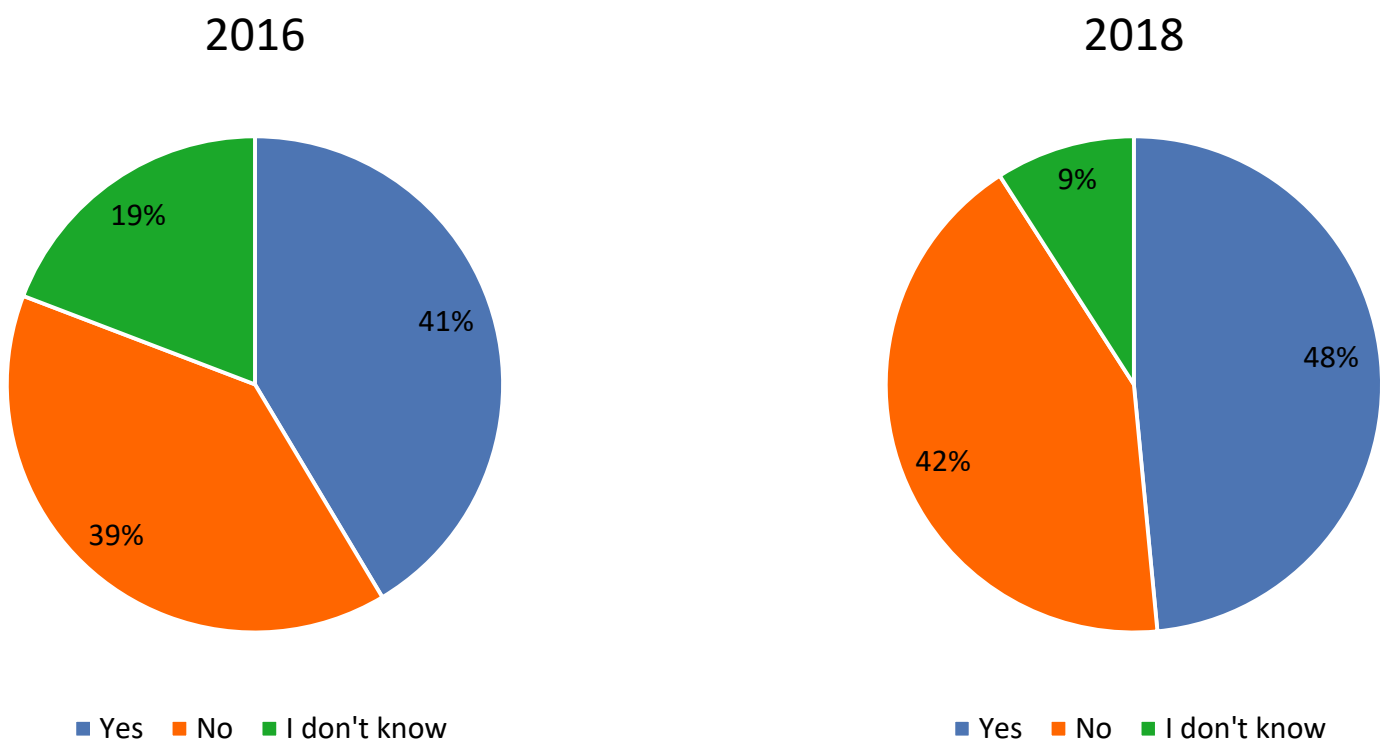
It is good that organizations are confident that they can recognize indications of a cyber attack. Continued awareness-building and training will enable organizations to maintain appropriate levels of vigilance.

6. If you suspect your desktop/laptop computer, smartphone, or other connected/connectable device (such as a tablet or USB drive) has been compromised, how confident are you that you know what to do?



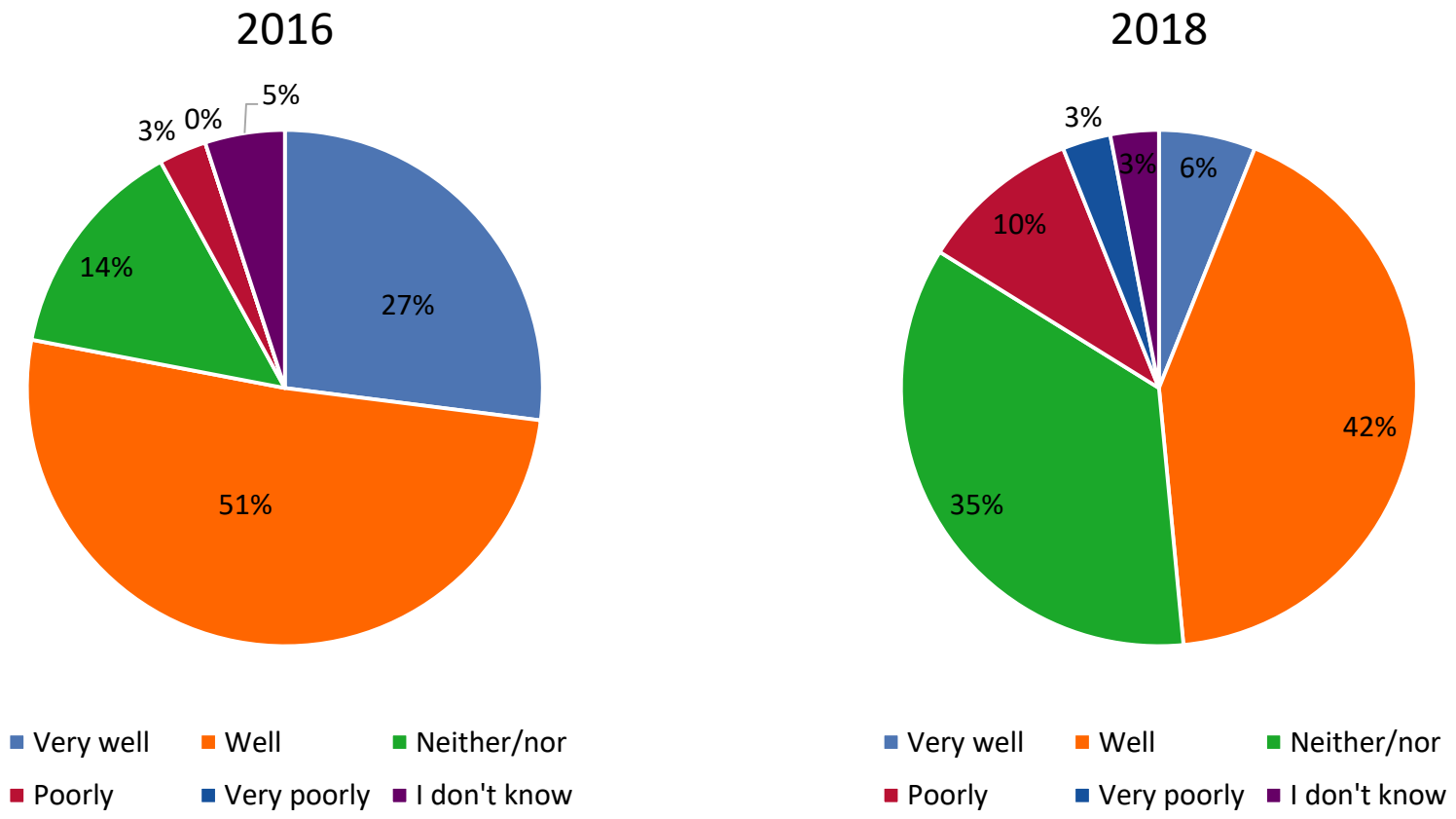
It is good that individuals within organizations are confident that they know what to do in the event of a cyber attack. Continued awareness-building and guidance will enable individuals to maintain appropriate levels of vigilance.

7. Without being specific, do you know of any situation where two or more people in the organization share the same password for a software application, IT system, equipment operating system using a software interface, or other networked device/infrastructure?



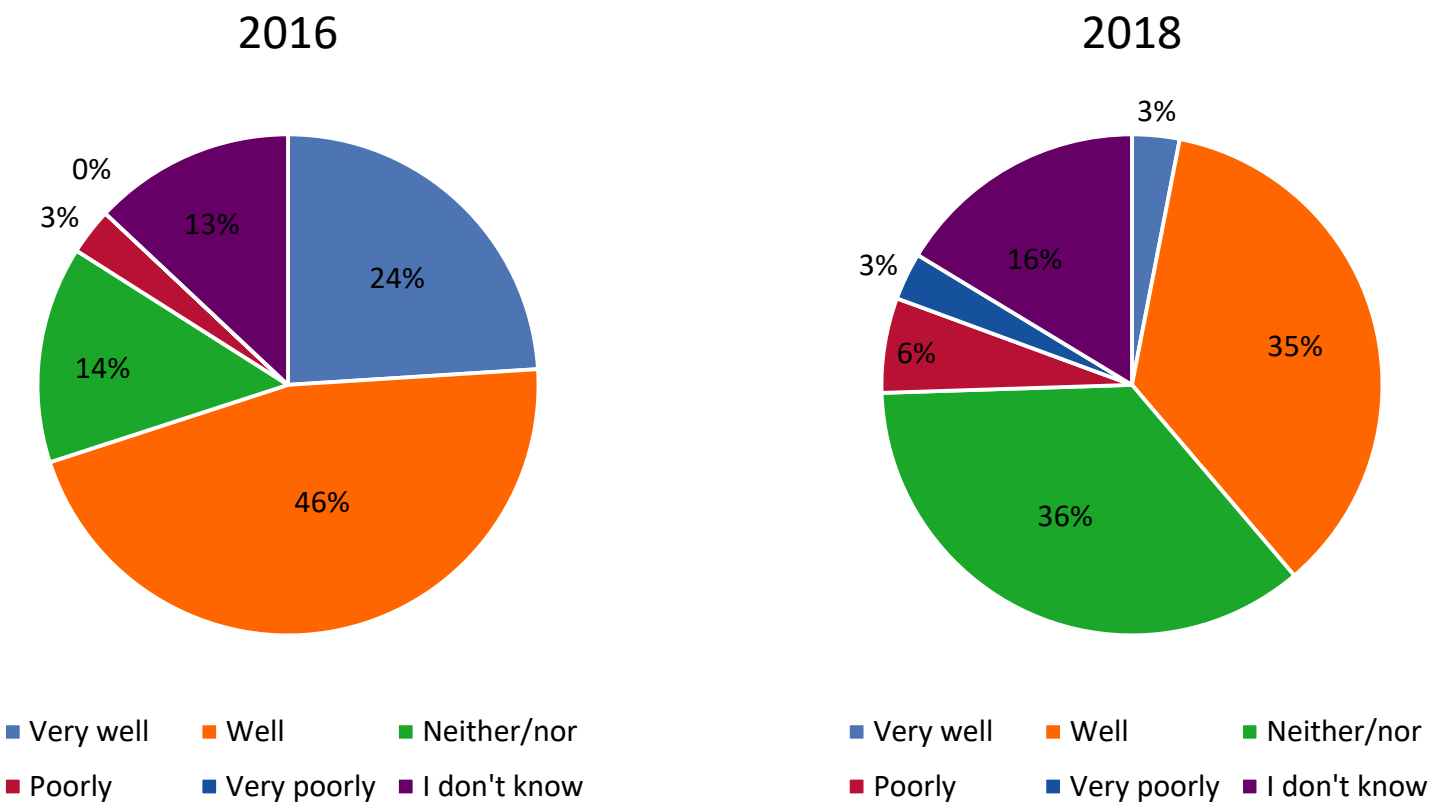
Sharing passwords is a common vulnerability. Training should include the threats posed by password-sharing.

8. How well do you feel your organization secures its office-based IT assets, such as office computers, phones and other network connected devices, from cyber attackers?



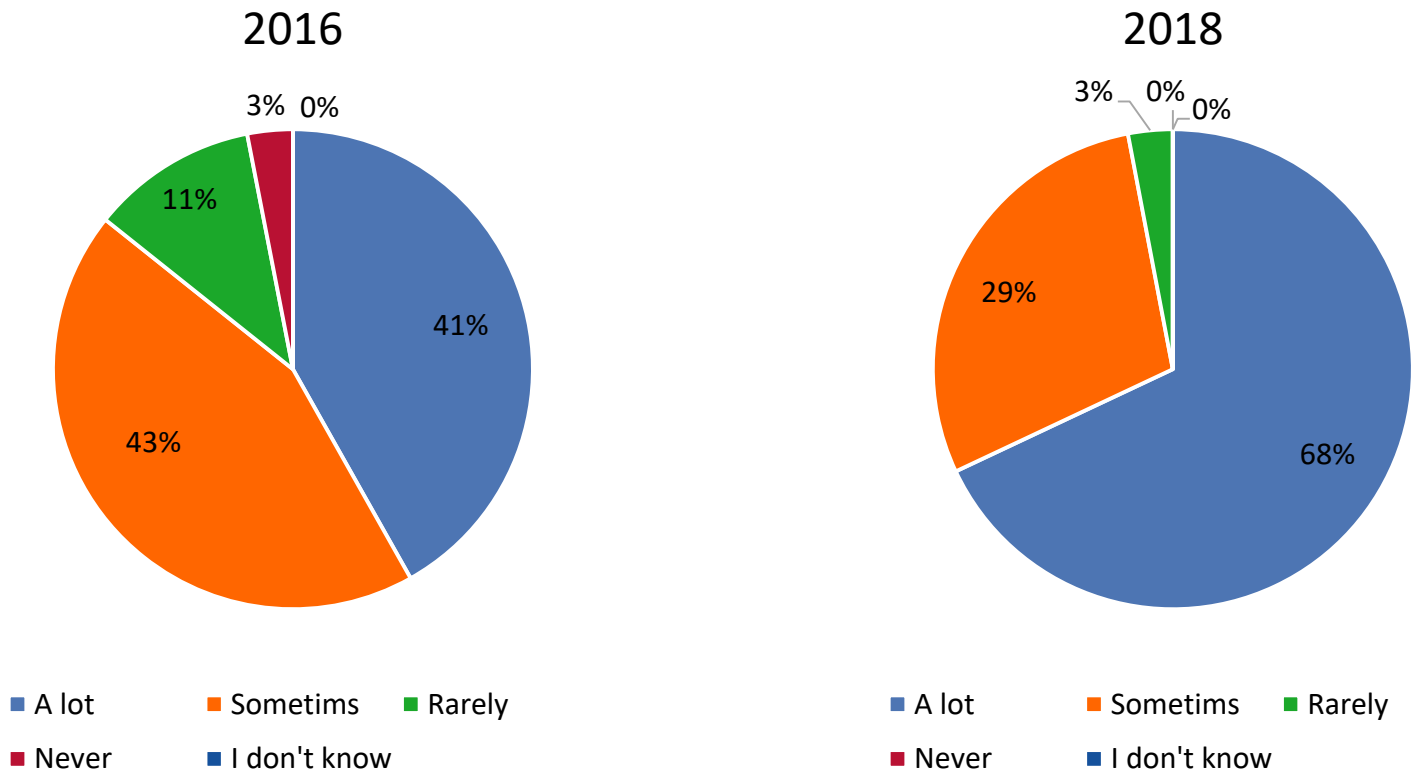
Perceptions of how an organization protects its IT assets have declined. Creating a culture of cyber risk management across the entire organization will help all staff feel empowered and are an an active part of the first line of cyber defense.

9. How well do you feel the organization secures its operational networked assets, such as terminal operating systems, security systems, RFID systems, cranes, and other network connected devices from cyber attackers?



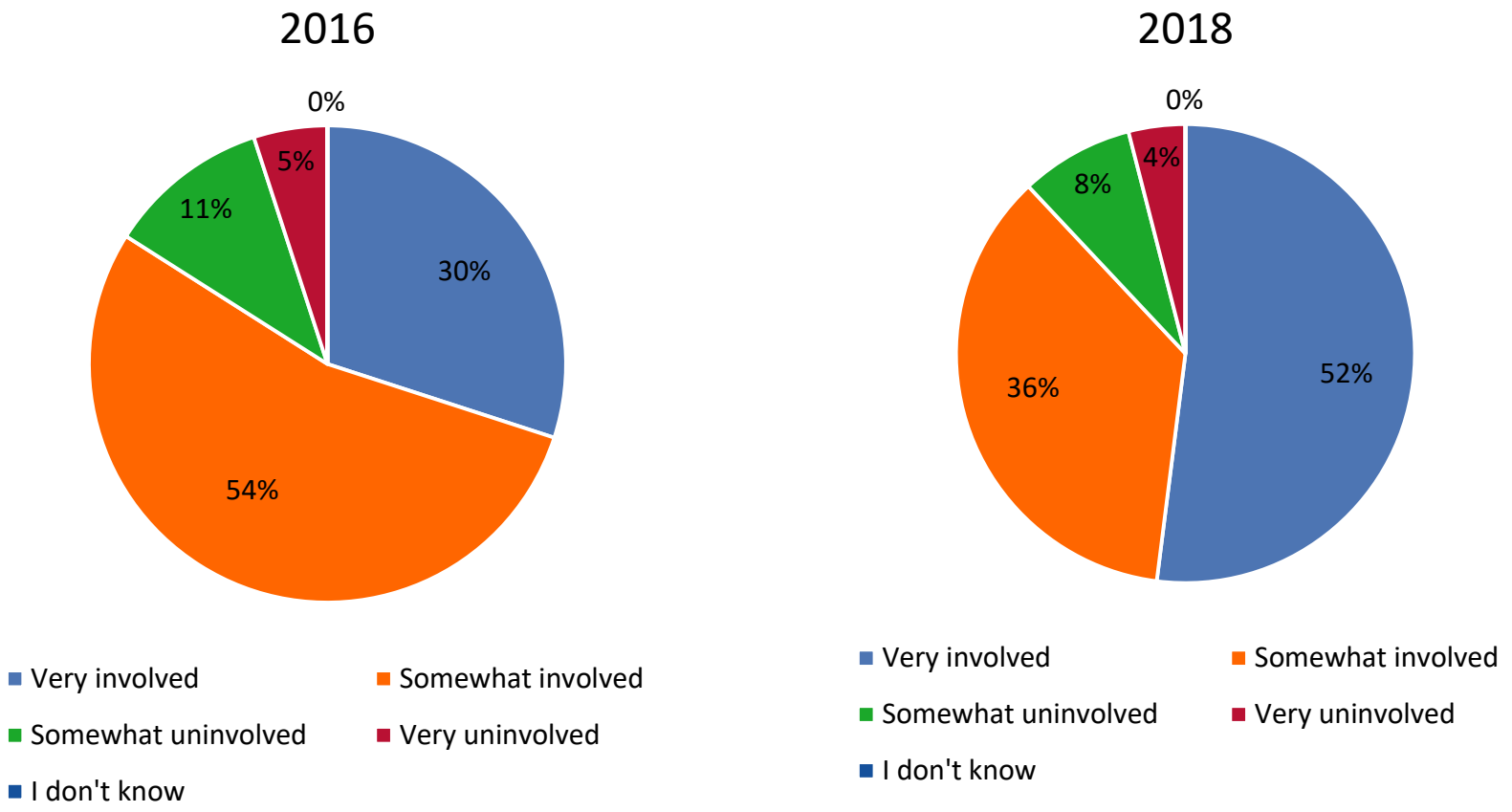
Perceptions of how an organization protects its operational networked assets have declined. Creating a culture of cyber risk management across the entire organization will help all staff feel empowered and are an an active part of the first line of cyber defense.

10. How often do you worry about the cybersecurity risks of using the organization's IT assets, such as computers, phones, and other network connected devices inside the company?



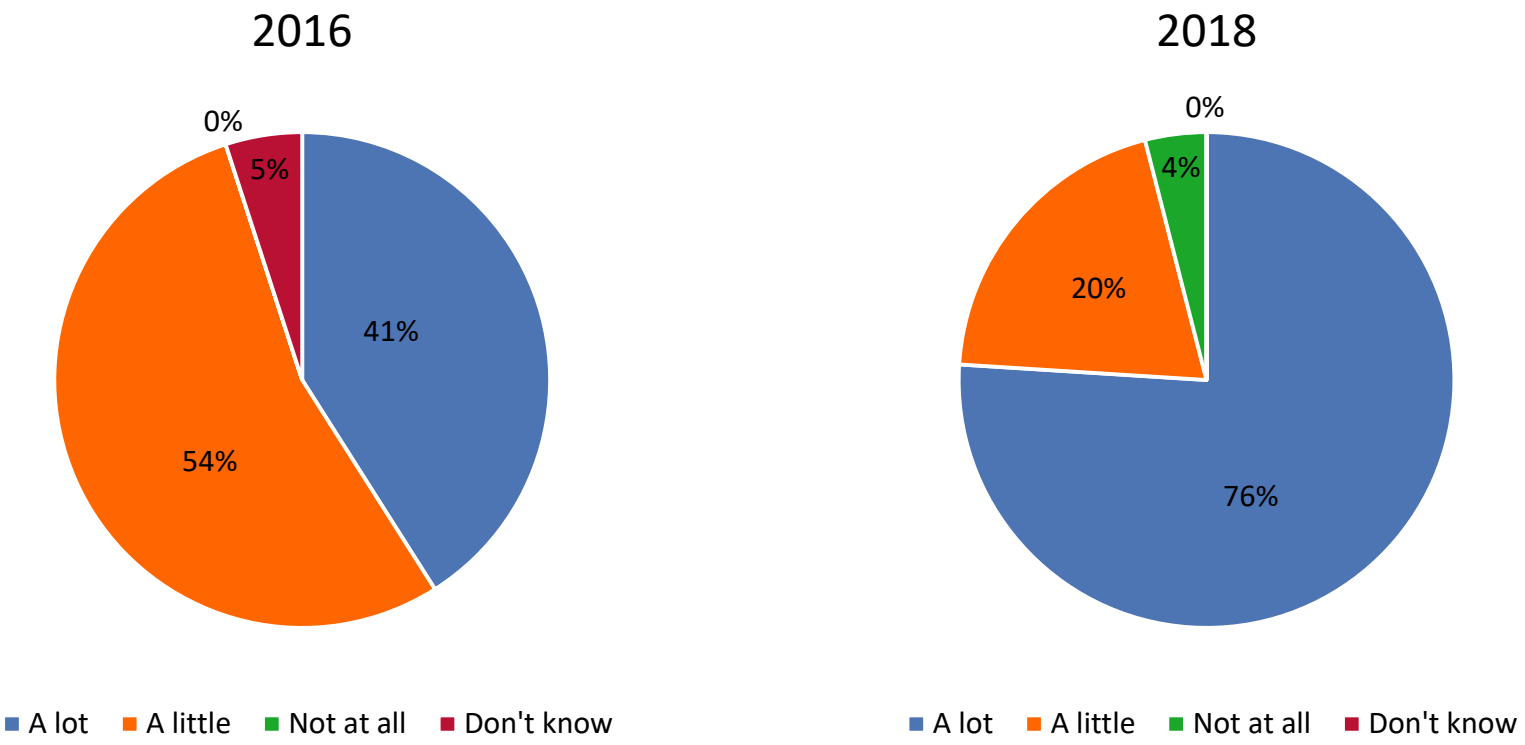
It is good that organizations are concerned with cybersecurity risks – this shows that cybersecurity awareness is increasing!

11. How engaged do you feel in the daily process of cyber security/cyber risk management and protecting the organization's information and protecting the organization's information and networked assets?



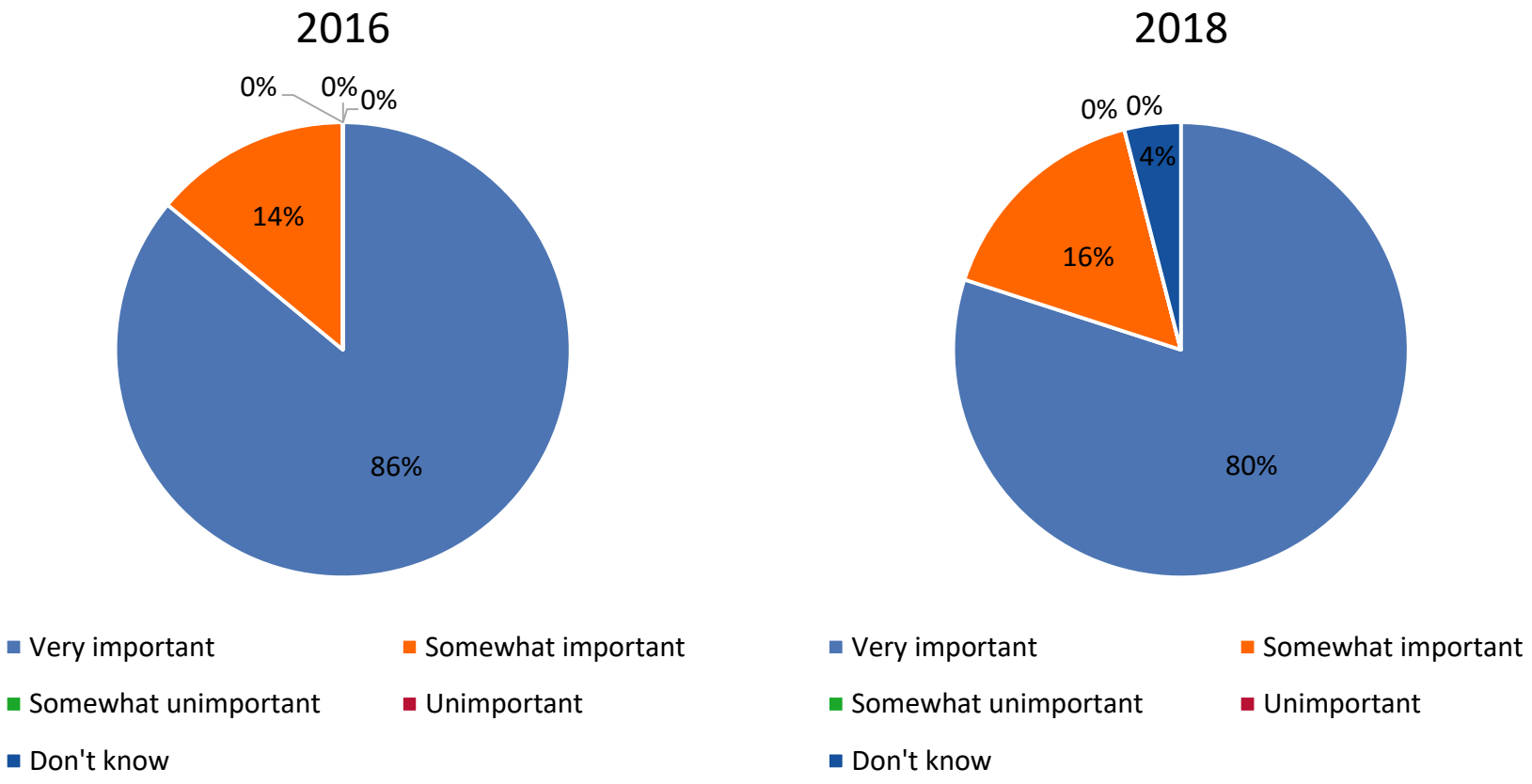
Great news - increasing the number of staff that feel empowered as an active part of the first line of cyber defense is critical to effective cyber risk management!

12. How much do you worry about becoming the victim of a spearphishing attack at work?



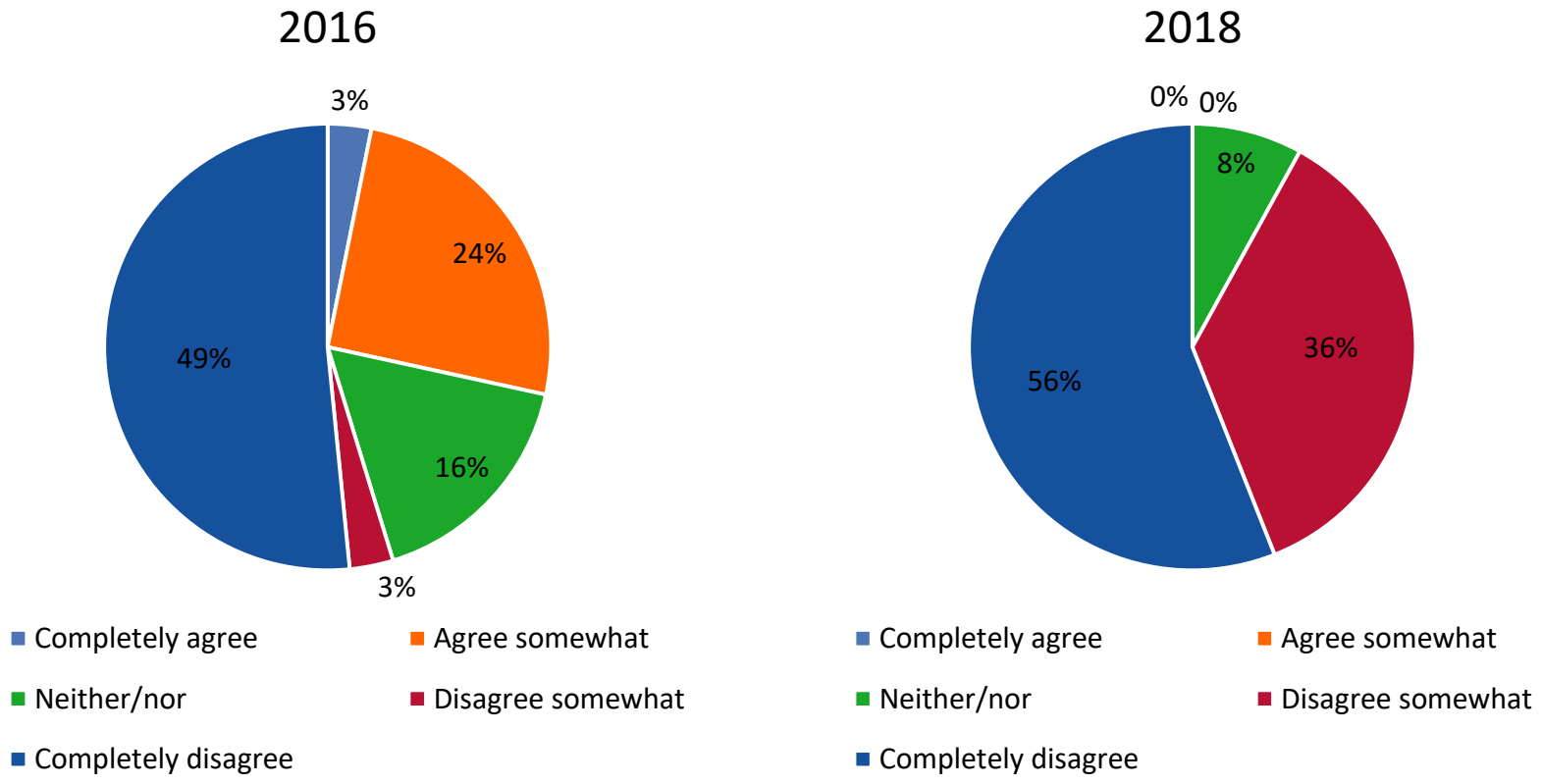
This increase in the concern about the prevalence of spearphishing attacks demonstrates an increased awareness about cybersecurity risks.

13. How important do you feel it is to keep your computers, mobile devices, smartphones, and software programs updated and current?



Ensuring that devices are updated and current is a basic tenet of effective cyber risk management – organizations should continue to ensure that staff understand this important point.

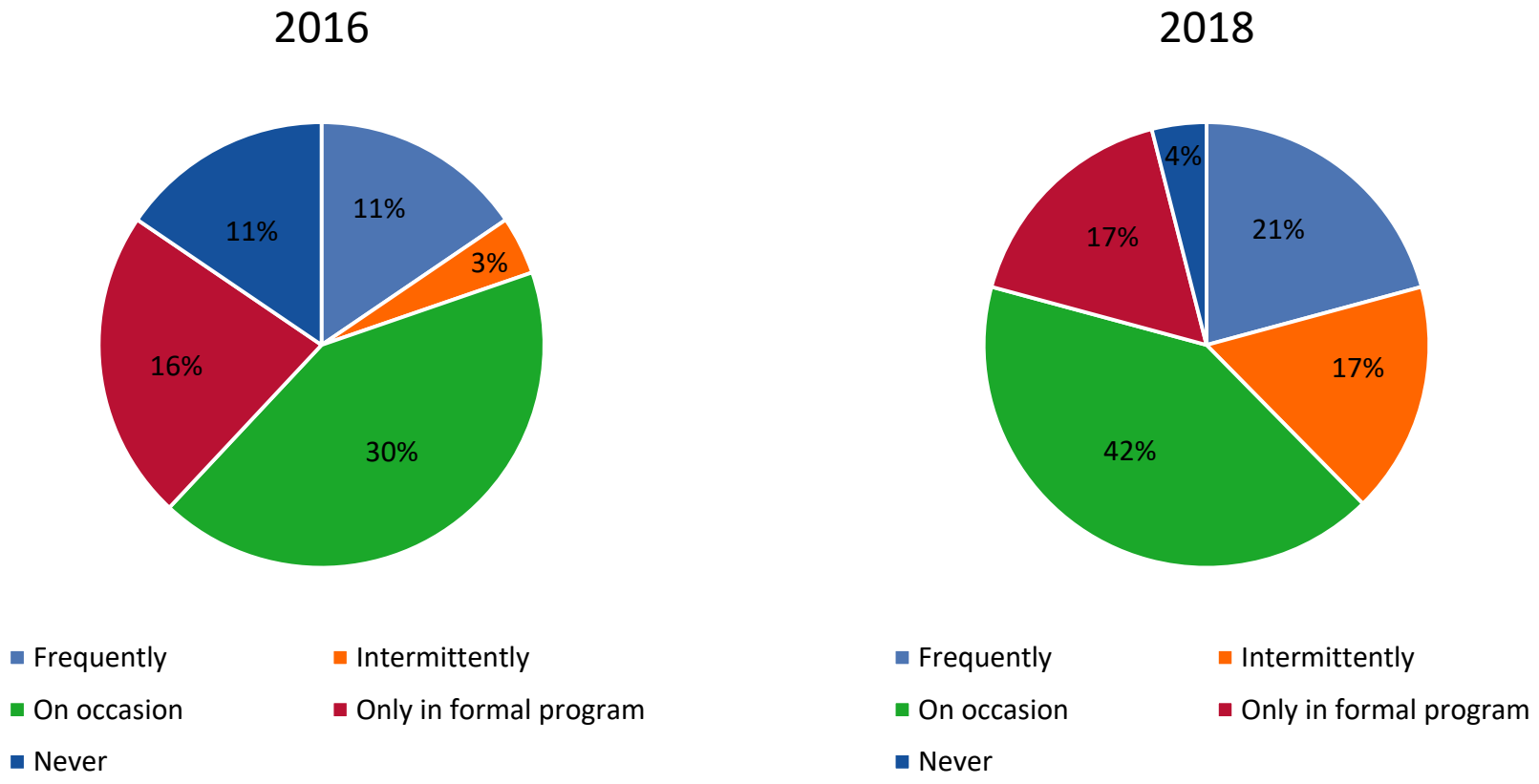
14. To what extent would you agree to the following statement: “No hacker would attack me or my computer. I don’t have anything they would want…”



All staff can be entry points for cyber attacks. This is why it is important that all staff receive cyber awareness training.

15. Over the last 12 months, how many times have you heard cybersecurity discussed in a formal setting outside of specific security training exercises?

Over the last 12 months, how many times have you heard cybersecurity discussed in a formal setting outside of specific security training exercises?



Pending any new regulatory mandates issued by either the IMO and/or national port state control directives addressing cyber risk factors, how motivated will your organization be in the coming year to invest in cybersecurity practices and/or solutions?