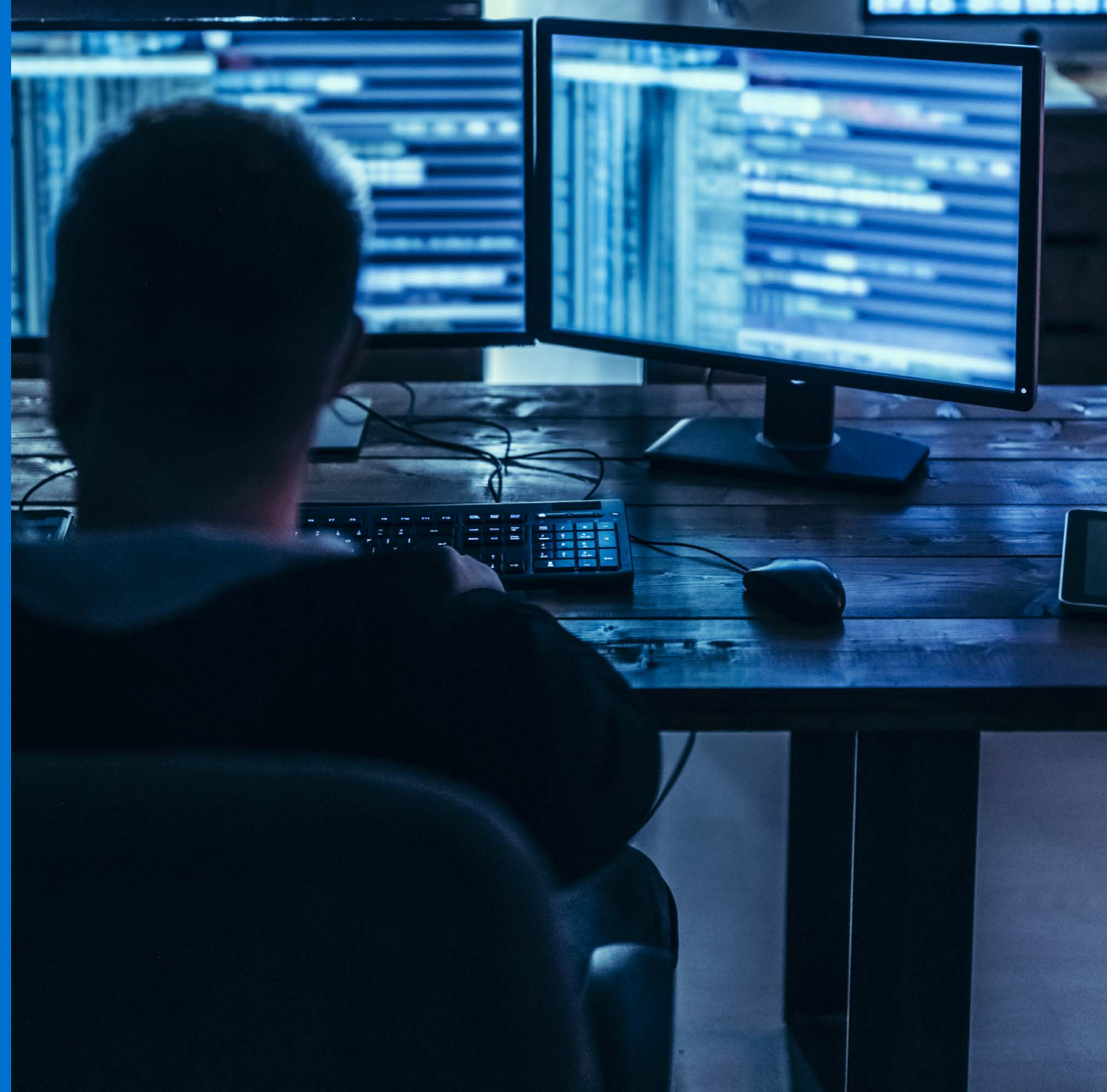# Cyber security protect checklist

How prepared are you to respond to a cyber-attack?

mazars

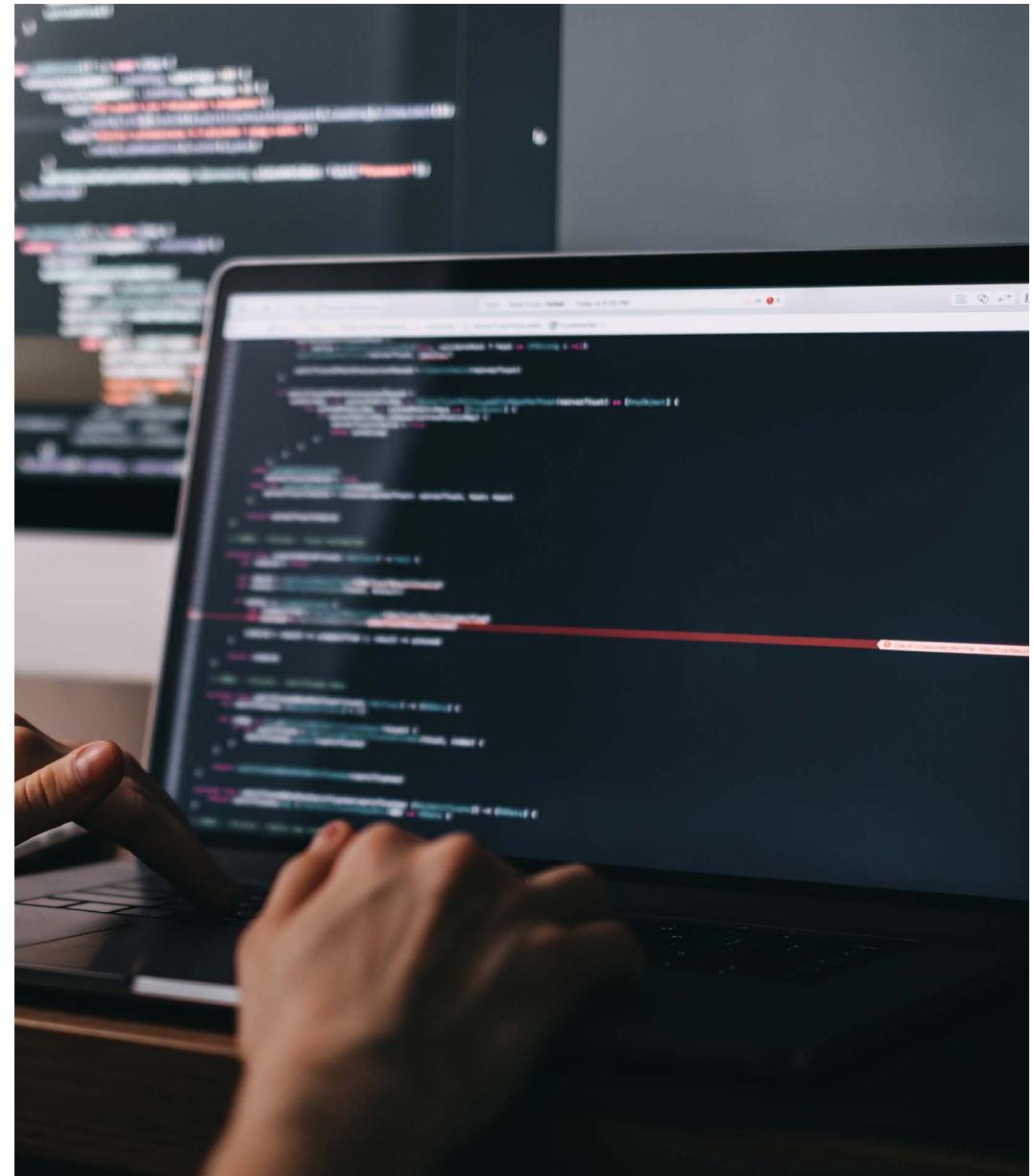# How prepared are you to respond to a cyber-attack?

In the shadow of what has been suggested as Ireland's most significant ransomware cyber-attack, bringing the HSE to a near standstill, organisations should now be asking themselves: how prepared are we for a cyber-attack?

Organisations of all sizes are under the continuous threat of becoming the next victim of a cyber-attack that may significantly impact their ability to operate effectively or, in extreme circumstances, operate in the same way ever again. Without a structured approach to cyber security it is more a case of when, as opposed to if a cyber-attack may occur.
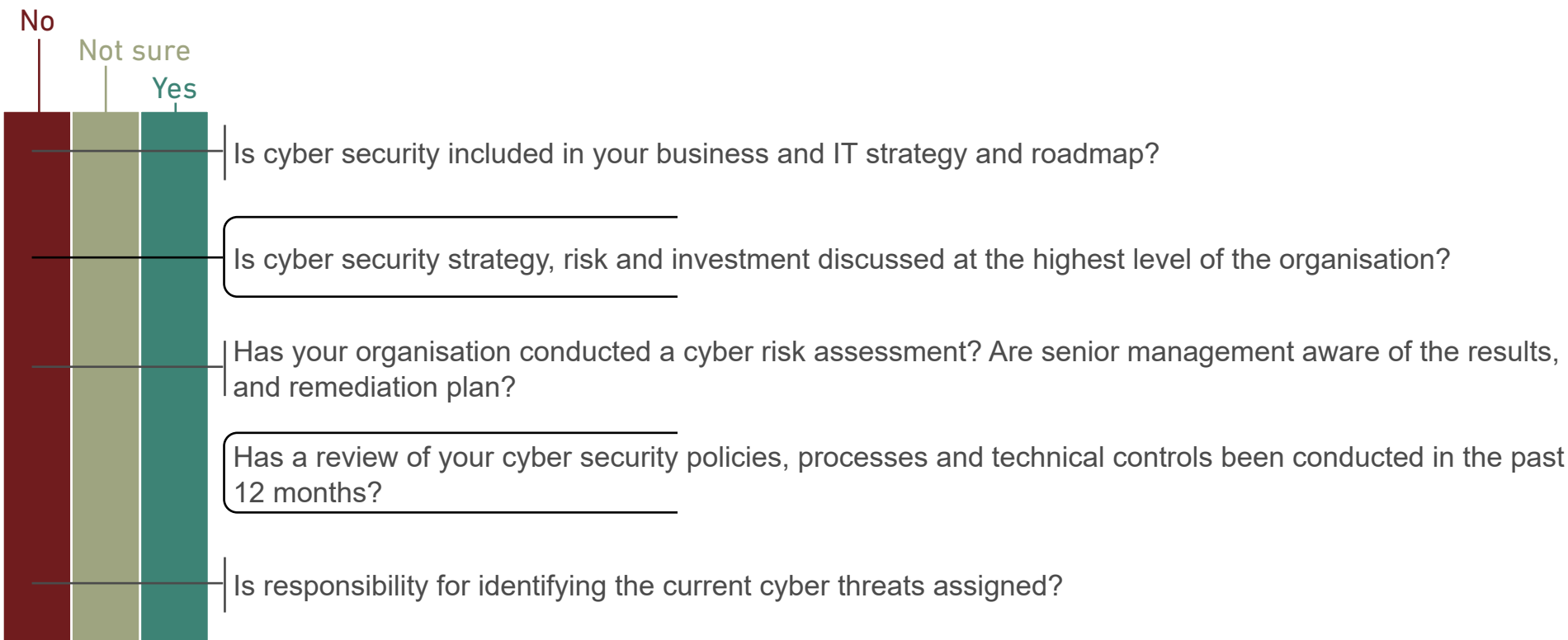
Technical detection and prevention solutions are no longer enough to reduce the risk of a becoming a victim of cyber-crime. Simple actions such as opening an email attachment or a link that a member of staff was not expecting can bring an organisation to a standstill. Cyber security awareness, culture and incident response are now an essential part of an organisation's arsenal to manage cyber security risk.

The aim of this document is to provide senior managers of organisations of all sizes with a checklist of key questions that they should now be asking their IT and Security Managers and/or outsourced IT service providers.

If you are answering **no** or **not sure** to any of these questions you may need to review your organisations current approach to cyber security:

mazars

Cyber governance and risk management

No

Not sure

Yes

Is cyber security included in your business and IT strategy and roadmap?

Is cyber security strategy, risk and investment discussed at the highest level of the organisation?

Has your organisation conducted a cyber risk assessment? Are senior management aware of the results, and remediation plan?

Has a review of your cyber security policies, processes and technical controls been conducted in the past 12 months?

Is responsibility for identifying the current cyber threats assigned?

mazars

Cyber security policies, training and awareness

No

Not sure

Yes

Have cyber security policies been updated to reflect working from home changes?

Is cyber security training provided to staff on a periodic basis?

Is training provided as part of the staff induction process?

Has your senior management team received targeted cyber security training?

Are your staff kept aware of the latest cyber threats on a continual basis?

Have you tested your staff's cyber awareness e.g., mock phishing training?
This is probably one of 'value for money' and best ways to get a return on your investment, based on human risk profile.

Are outsourced IT service providers made aware of their security responsibilities?

mazars

Cyber security incident management

No

Not sure

Yes

Has responsibility for the management of a cyber incident within your organisation been clearly defined?

Do you have an adequate level of internal knowledge to manage a cyber security incident? If not, you will need to identify how you will obtain these services in the event of an incident.

Does your organisation have a detailed cyber incident response plan, that interacts with your crisis management and/or business continuity plans?

Have you tested your incident response plan?

Cyber governance and risk management

Cyber security policies, training and awareness

Cyber security incident management

Cyber resilience

Cyber monitoring

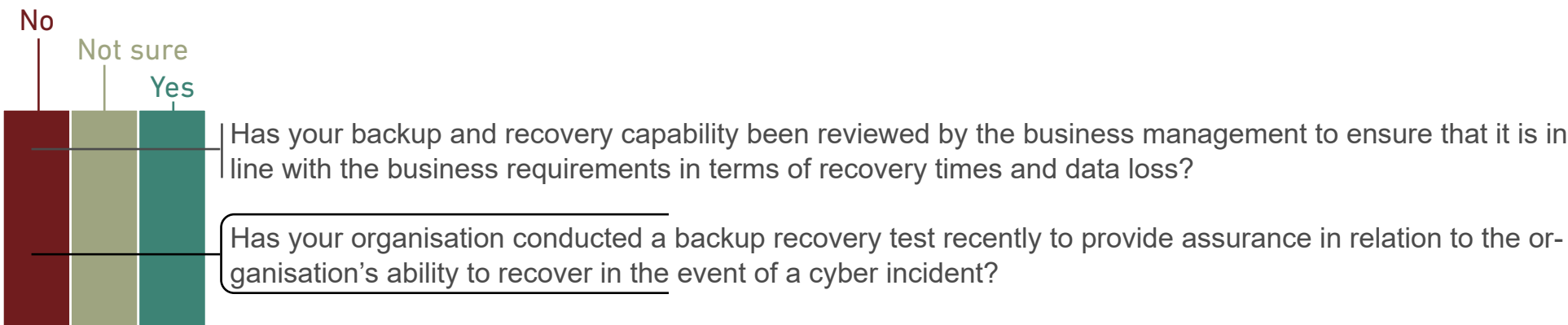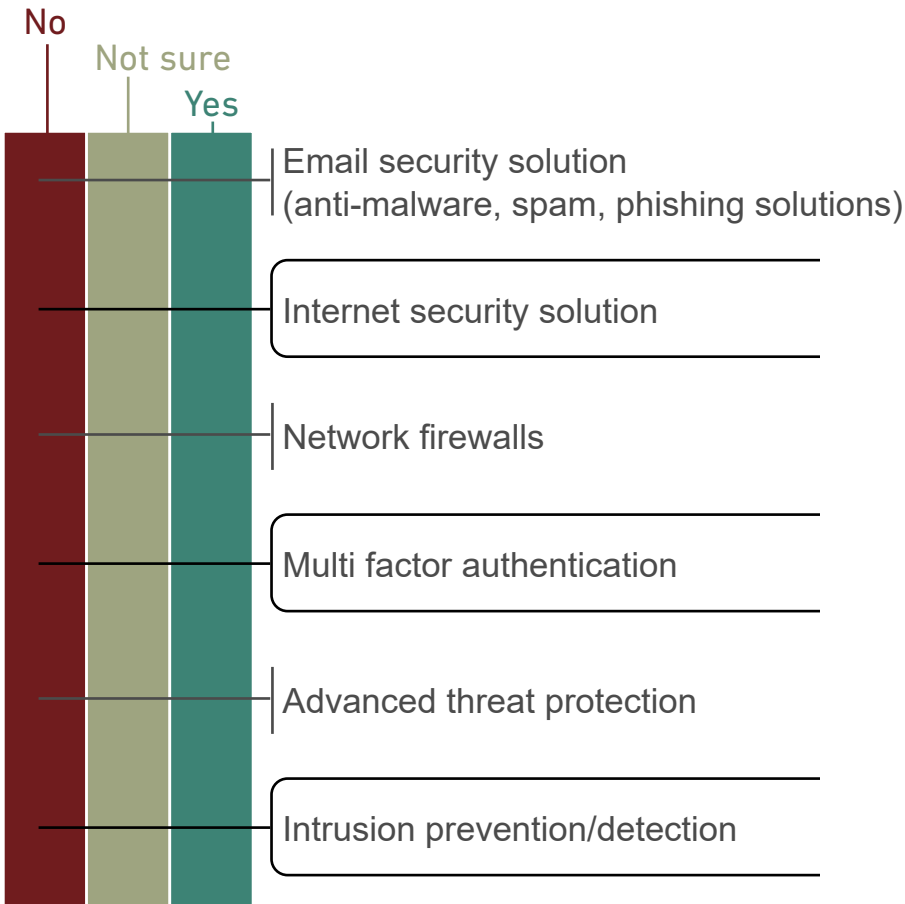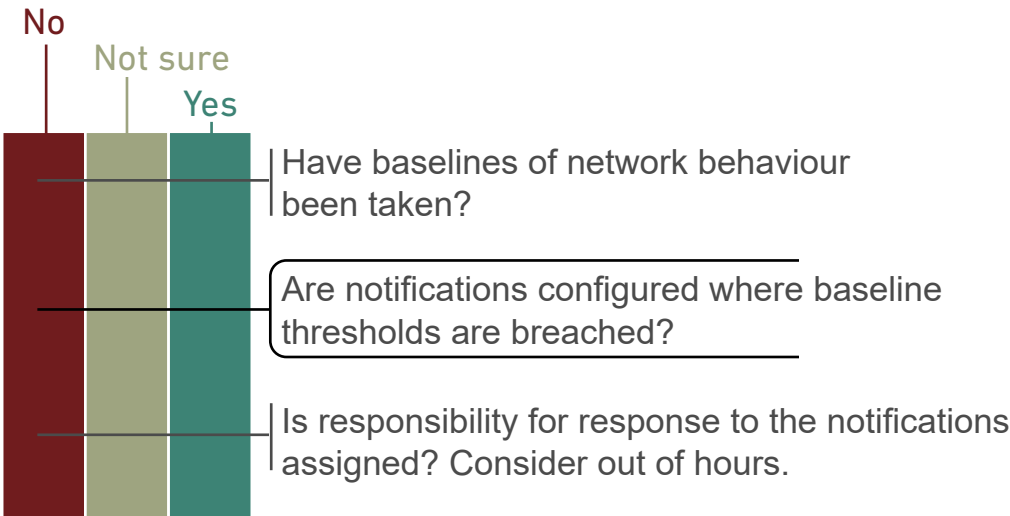Vulnerability management

IT outsourced service providers

mazars

Cyber resilience

Is all of your data and systems being backed up?

No

Not sure

Yes

Has your backup and recovery capability been reviewed by the business management to ensure that it is in line with the business requirements in terms of recovery times and data loss?

Has your organisation conducted a backup recovery test recently to provide assurance in relation to the organisation's ability to recover in the event of a cyber incident?

mazars

Cyber monitoring

Does your organisation have an adequate level of network security tools in operation? At minimum:

No

Not sure

Yes

Email security solution
(anti-malware, spam, phishing solutions)

Internet security solution

Network firewalls

Multi factor authentication

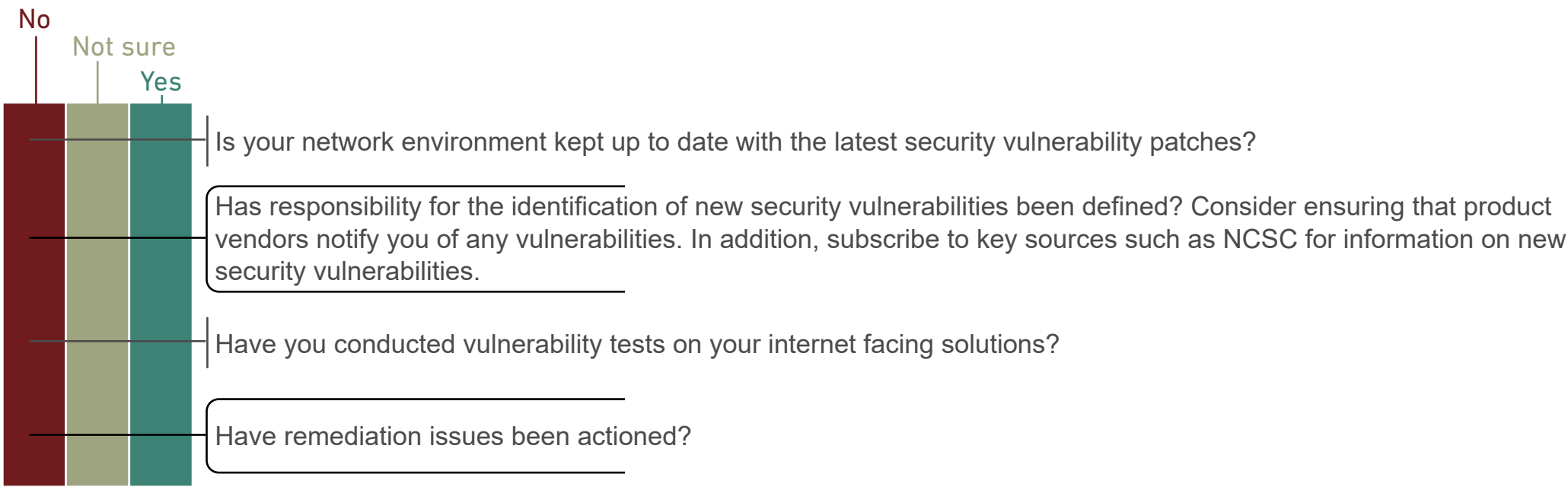Advanced threat protection

Intrusion prevention/detection

Endpoint security solution.
Are your security and infrastructure monitoring tools adequately configured to detect and notify the relevant staff members and/or outsourced IT third parties of suspicious and/or abnormal network behaviour?

No

Not sure

Yes

Have baselines of network behaviour been taken?

Are notifications configured where baseline thresholds are breached?

Is responsibility for response to the notifications assigned? Consider out of hours.

mazars

Vulnerability management

No

Not sure

Yes

Is your network environment kept up to date with the latest security vulnerability patches?

Has responsibility for the identification of new security vulnerabilities been defined? Consider ensuring that product vendors notify you of any vulnerabilities. In addition, subscribe to key sources such as NCSC for information on new security vulnerabilities.

Have you conducted vulnerability tests on your internet facing solutions?

Have remediation issues been actioned?

Cyber governance and risk management

Cyber security policies, training and awareness

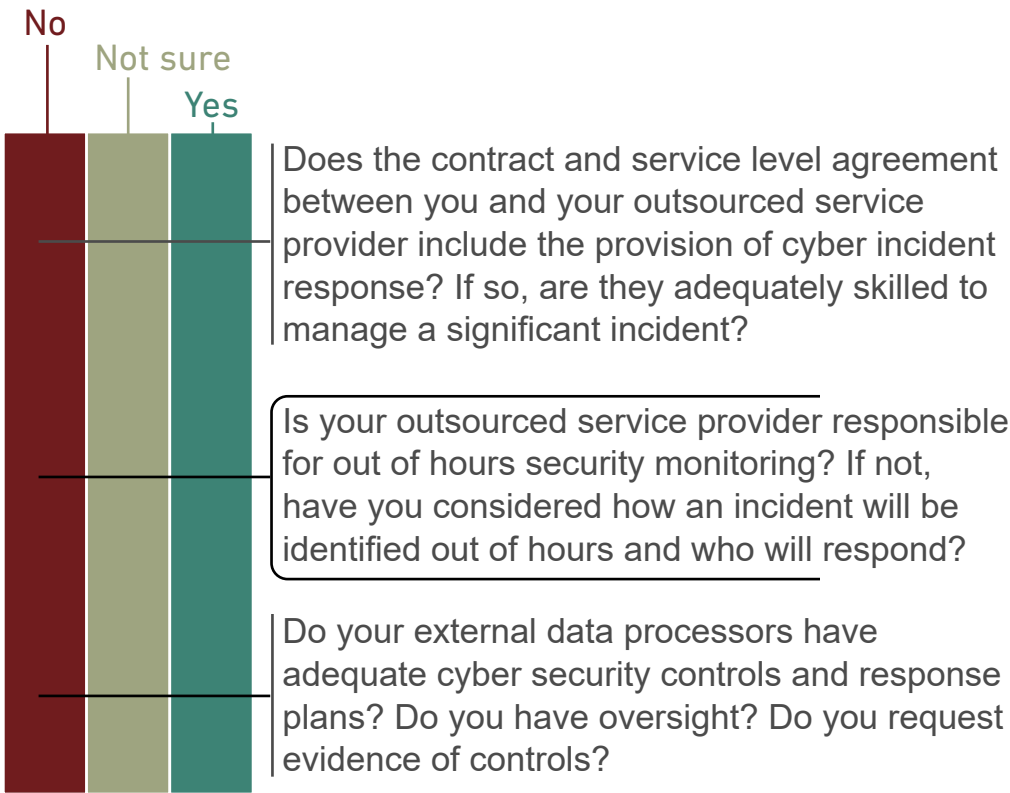Cyber security incident management

Cyber resilience

Cyber monitoring

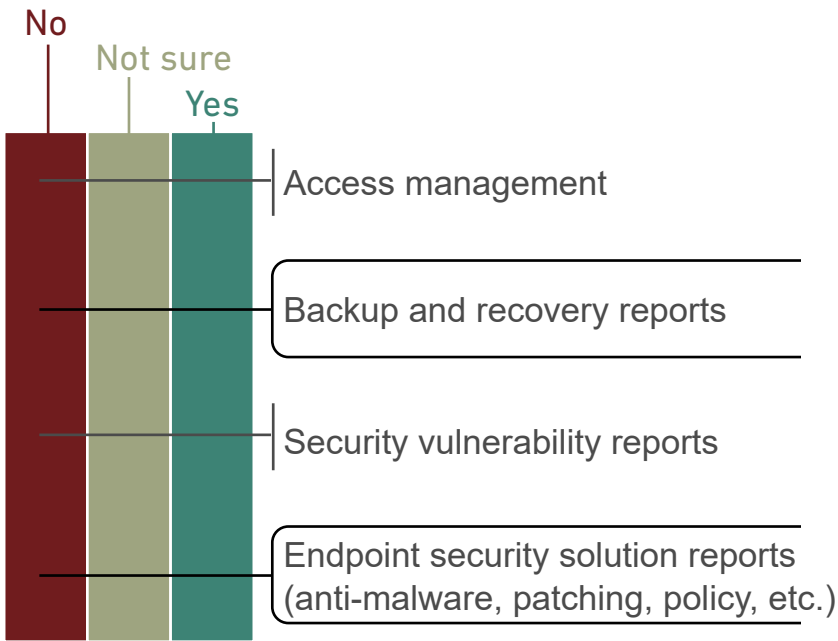Vulnerability management

IT outsourced service providers

mazars

IT outsourced service providers

Does your organisation rely on outsourced services providers? If yes, please answer:

No
Not sure
Yes

Does the contract and service level agreement between you and your outsourced service provider include the provision of cyber incident response? If so, are they adequately skilled to manage a significant incident?

Is your outsourced service provider responsible for out of hours security monitoring? If not, have you considered how an incident will be identified out of hours and who will respond?

Do your external data processors have adequate cyber security controls and response plans? Do you have oversight? Do you request evidence of controls?

Does your IT outsourced service provider issue your organisation with weekly or monthly oversight security reports?

No
Not sure
Yes

Access management

Backup and recovery reports

Security vulnerability reports

Endpoint security solution reports (anti-malware, patching, policy, etc.)

Cyber governance and risk management

Cyber security policies, training and awareness

Cyber security incident management

Cyber resilience

Cyber monitoring

Vulnerability management

IT outsourced service providers

mazars

LinkedIn:
www.linkedin.com/company/Mazars-in-Ireland

Twitter:
www.twitter.com/MazarsIreland

Facebook:
www.facebook.com/MazarsIreland

Instagram:
www.instagram.com/MazarsIreland

www.mazars.ie

mazars