Jersey Financial Services Commission

JFSC Cyber-Security Survey

2017 Results

Issued: September 2017

Contents

JFSC Cyber-Security Survey Results 2017

129 financial services firms completed the Jersey Financial Services Commission's (JFSC) Cyber-Security Survey. Some of the main findings are illustrated below.

Top five threats selected by survey respondents:

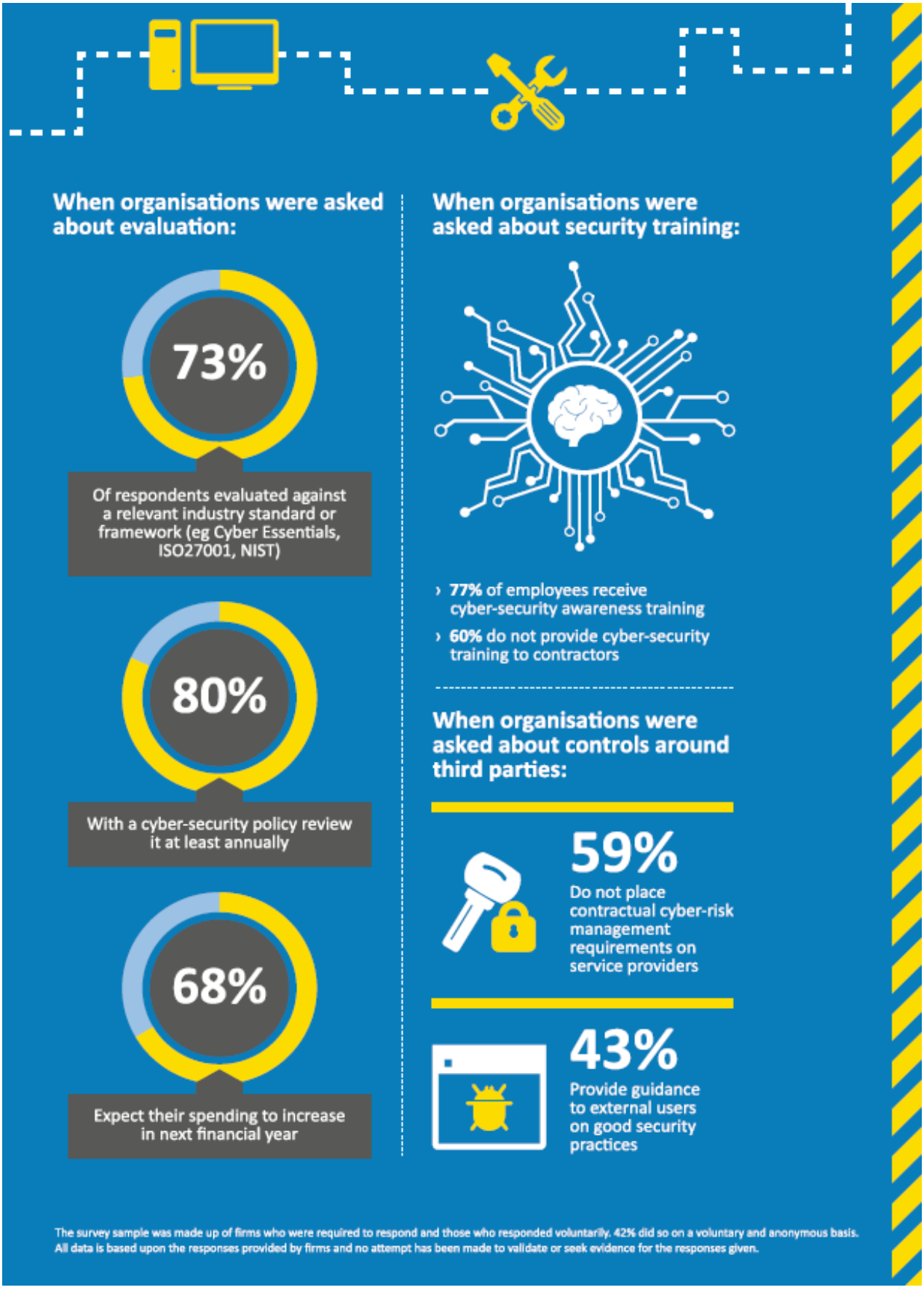
- Unintentional leakage of information
- Fraud
- Deliberate leakage of information
- Malicious code
- Social engineering attacks

The incidents experienced by most organisations surveyed were:

- **59%** Fraudulent emails
- **58%** Malware

When organisations were asked about their cyber policies:

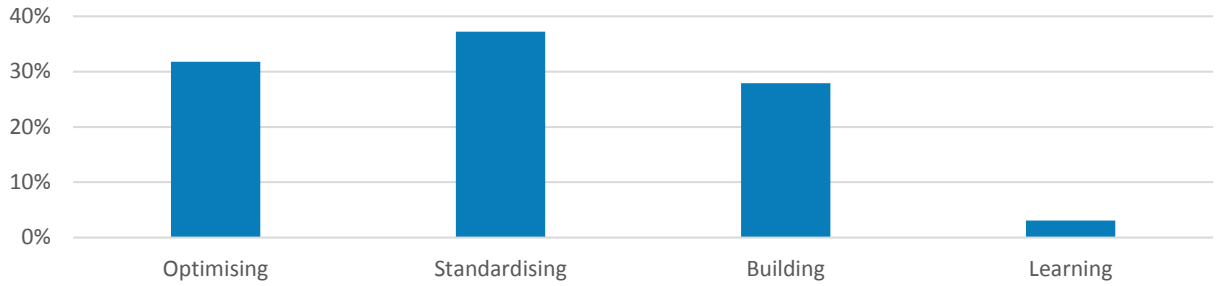
- **32%** Did not have a documented risk-assessment of cyber-security risks
- **57%** Did not have a documented risk appetite for cyber-security risks
- **32%** Did not have a cyber incident response plan
- **40%** Did not include cyber-security incidents in disaster recovery and contingency arrangements
- **63%** Did not have a dedicated cyber-security insurance policy
- **73%** Do not share information on cyber-security with other bodies / organisations


When organisations were asked about evaluation:
73%
Of respondents evaluated against a relevant industry standard or framework (eg Cyber Essentials, ISO27001, NIST)
80%
With a cyber-security policy review it at least annually
68%
Expect their spending to increase in next financial year
When organisations were asked about security training:
› 77% of employees receive cyber-security awareness training
› 60% do not provide cyber-security training to contractors
When organisations were asked about controls around third parties:
59%
Do not place contractual cyber-risk management requirements on service providers
43%
Provide guidance to external users on good security practices
The survey sample was made up of firms who were required to respond and those who responded voluntarily. 42% did so on a voluntary and anonymous basis. All data is based upon the responses provided by firms and no attempt has been made to validate or seek evidence for the responses given.

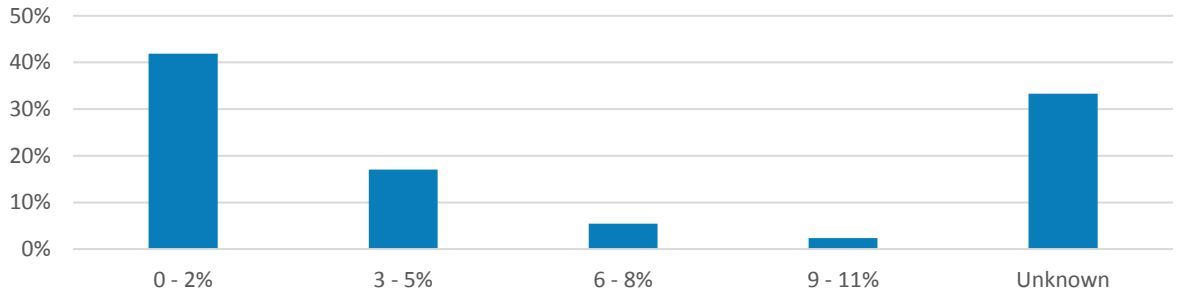
Survey Tables[1]

Introduction

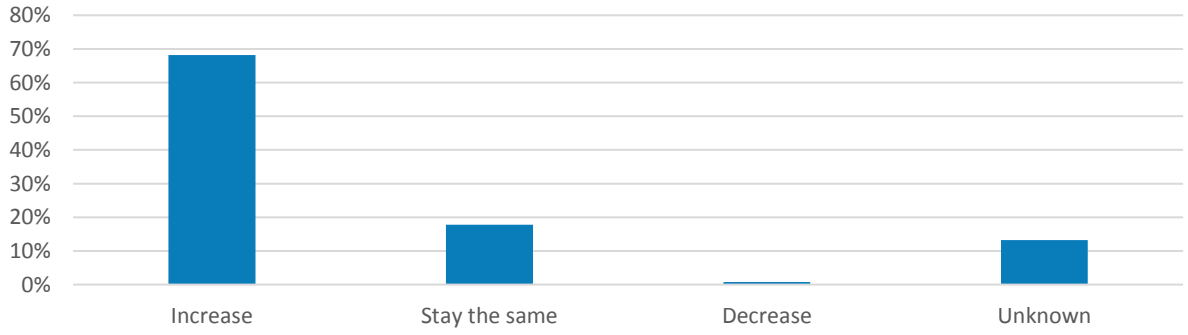
Q. Please select the option which you consider best describes the maturity of your firm's approach to cyber-security



Q. How much of your firm's budgeted annual expenditure is allocated to cyber-security?



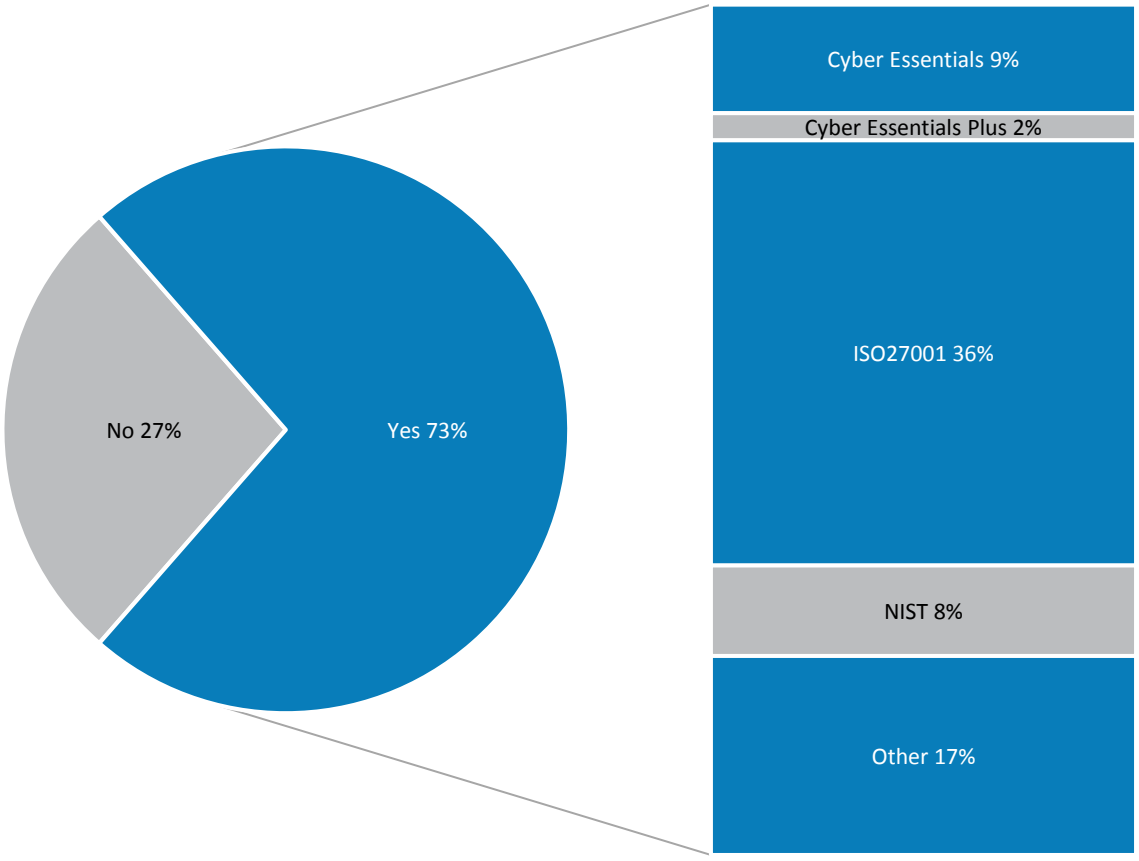
Q. In your firm's next financial year do you expect your cyber-security budget to decrease, increase, stay the same or is it unknown?



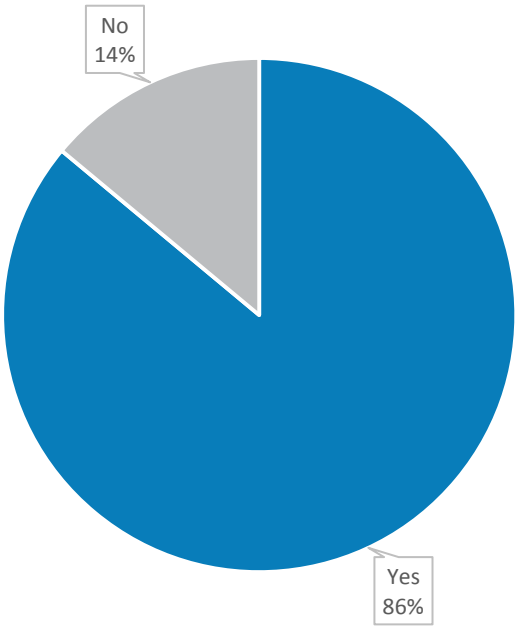
[1] Unless stated otherwise all charts show the % of respondents. Not all answers add up to 100% due to rounding of percentages or because questions permitted more than one response.

Identify - Governance

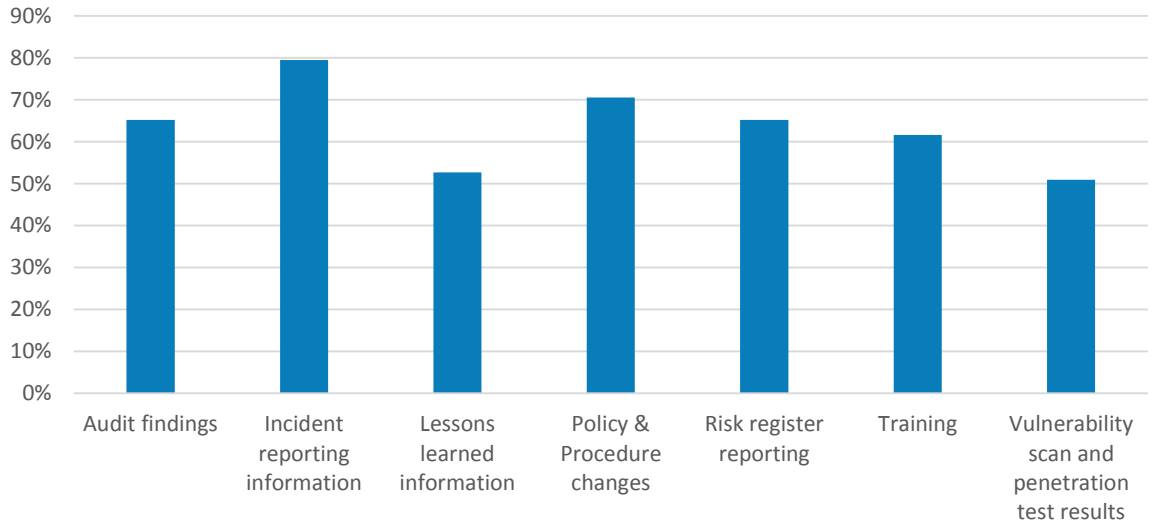
Q. Does your firm evaluate its cyber-security measures against a relevant industry standard or framework, if so, which?



Q. Does the Board receive regular reporting on cyber-security risks and controls?

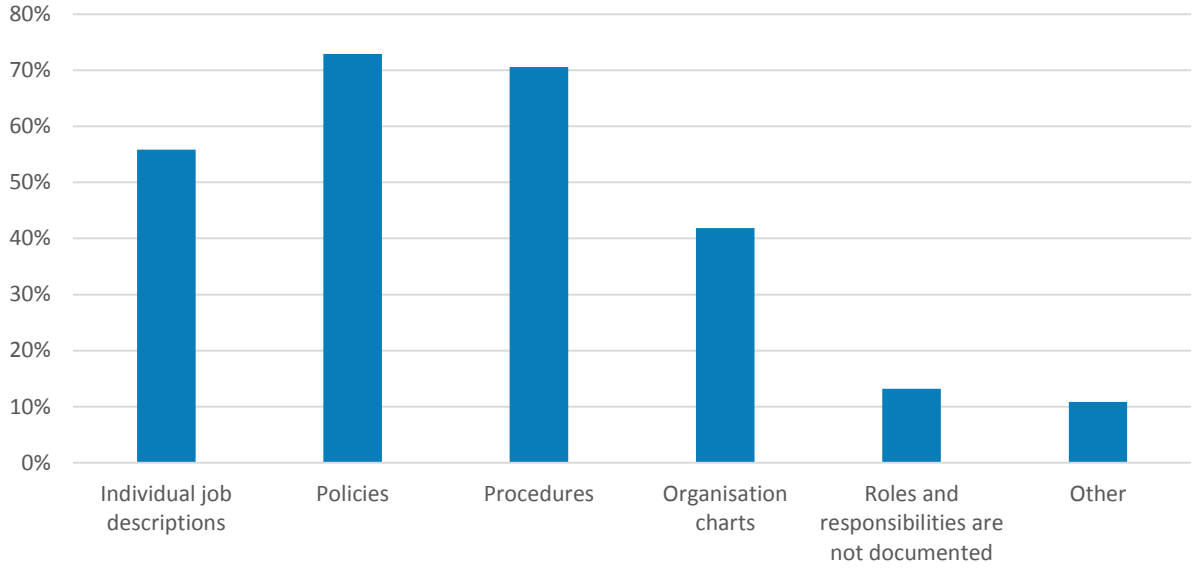


% of Boards receiving regular reporting on cyber-security that receive the following types of information

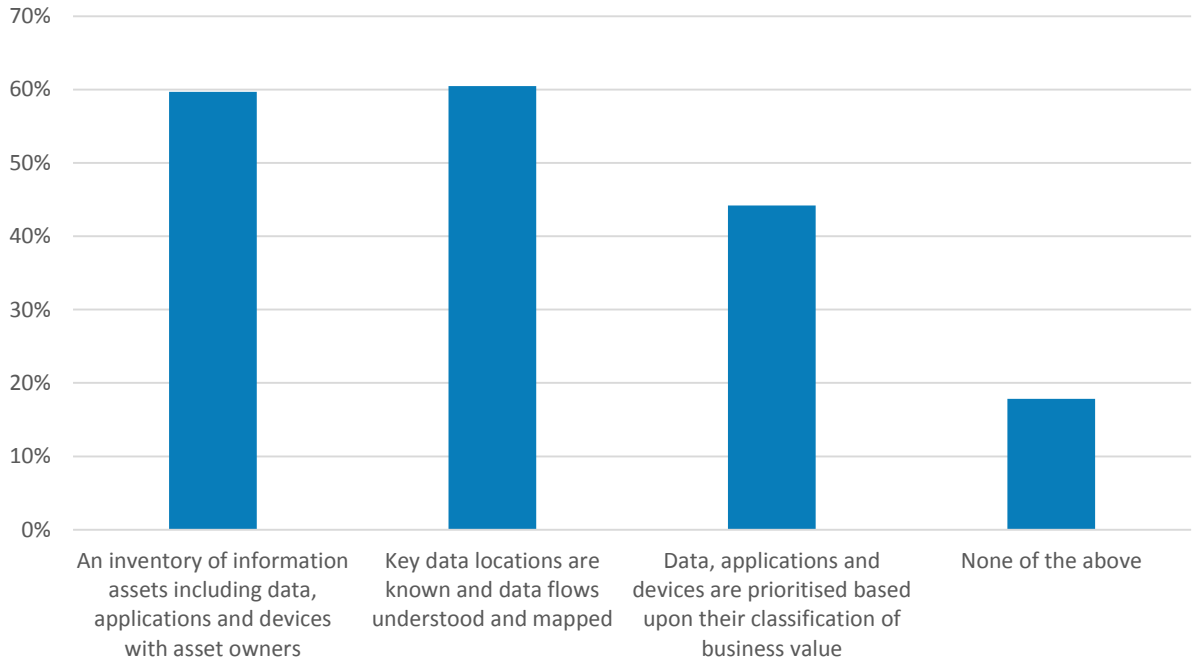


Budget reporting **29%** / Other **20%**

Q. Are any of the following used by your firm to document cyber-security roles and responsibilities?

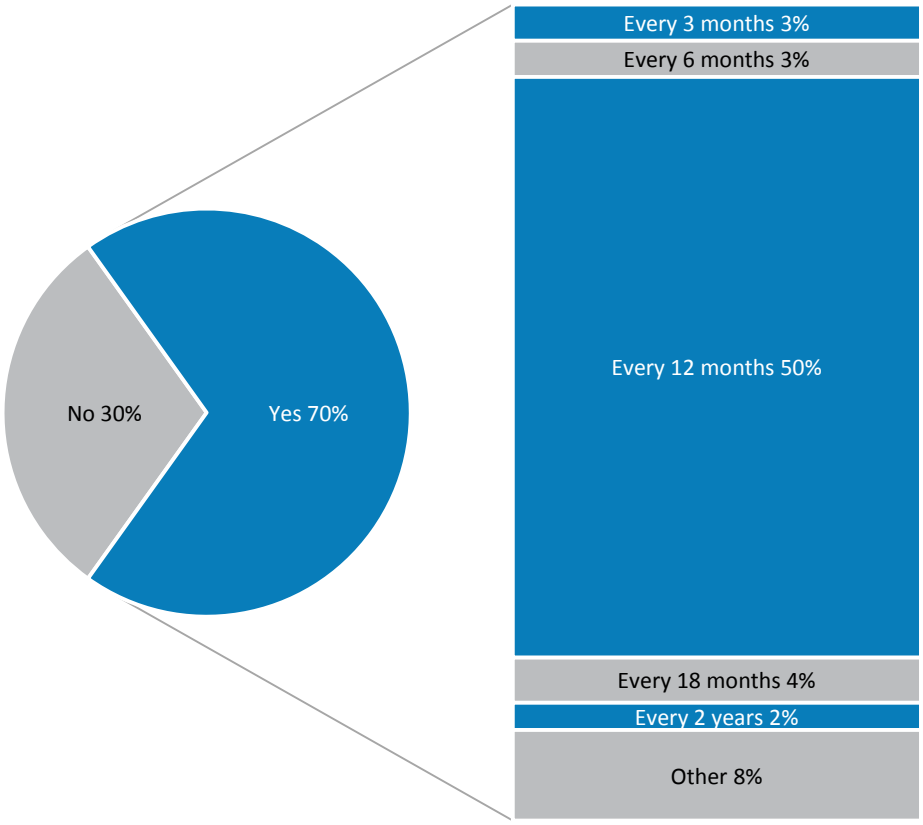


Q. Have any of the following been adopted by your firm to manage information assets?

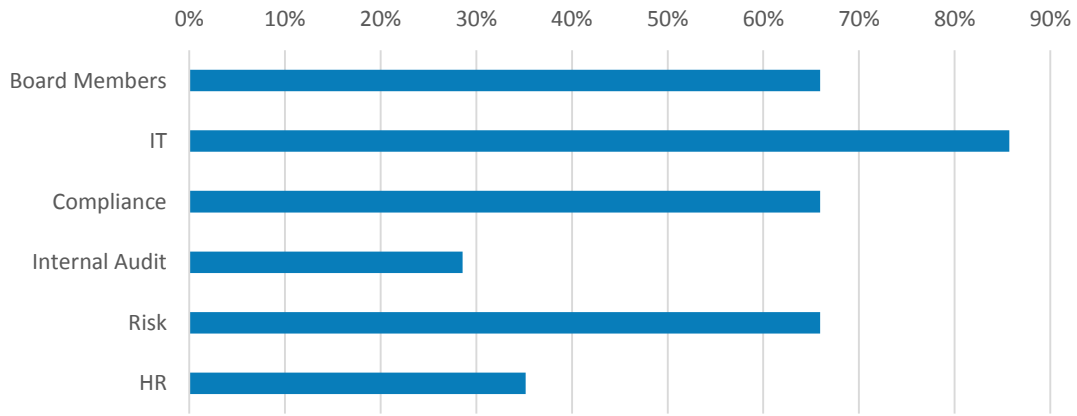


Identify – Cyber-Security Policy

Q. Does your firm have an over arching cyber-security policy or equivalent which has been signed off by the Board, if so, how often is it reviewed by the Board?



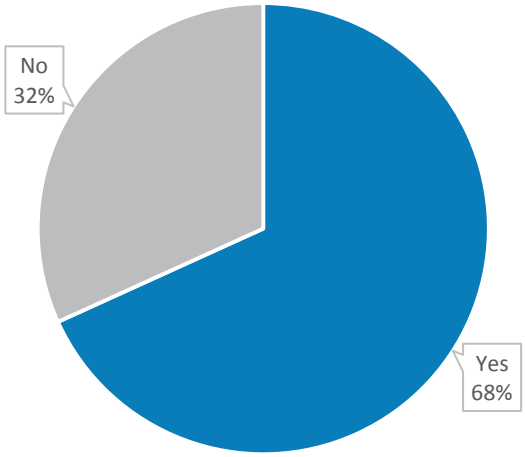
% of firms with a cyber-security policy or equivalent that involved the following areas of their business in its development



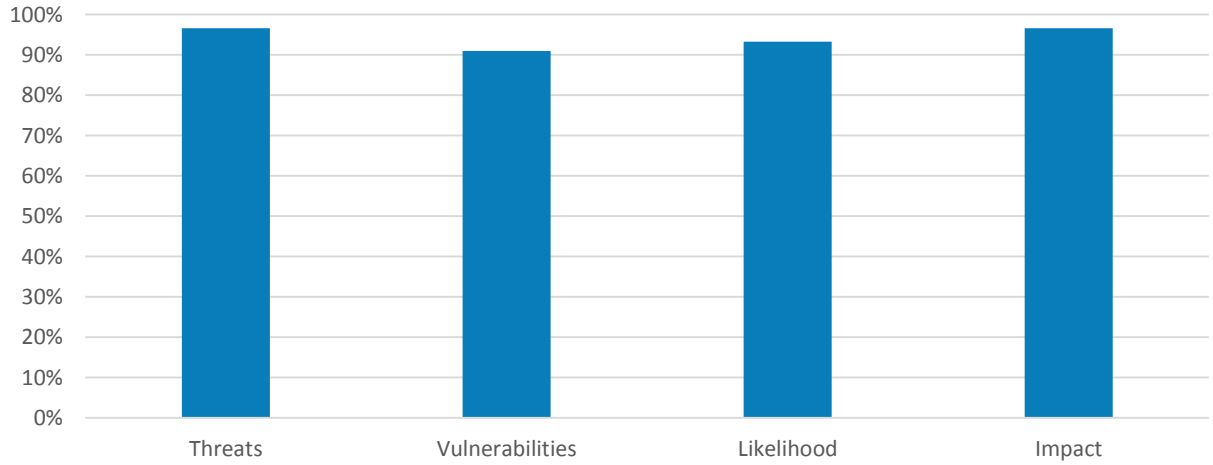
Customer facing units **22% /** Facilities **14% /** Marketing **8% /** Holding, subsidiary or sister company **16% /** Other **24%**

Identify – Risk Assessment

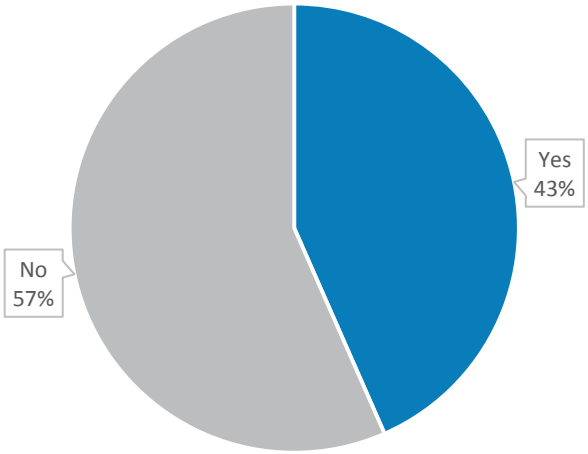
Q. Does your firm have a documented risk assessment process for assessing cyber-security risks?



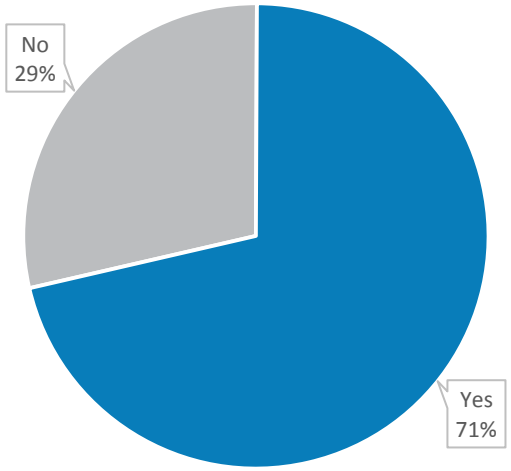
% of firms with a documented risk assessment process that utilise one or more of the following



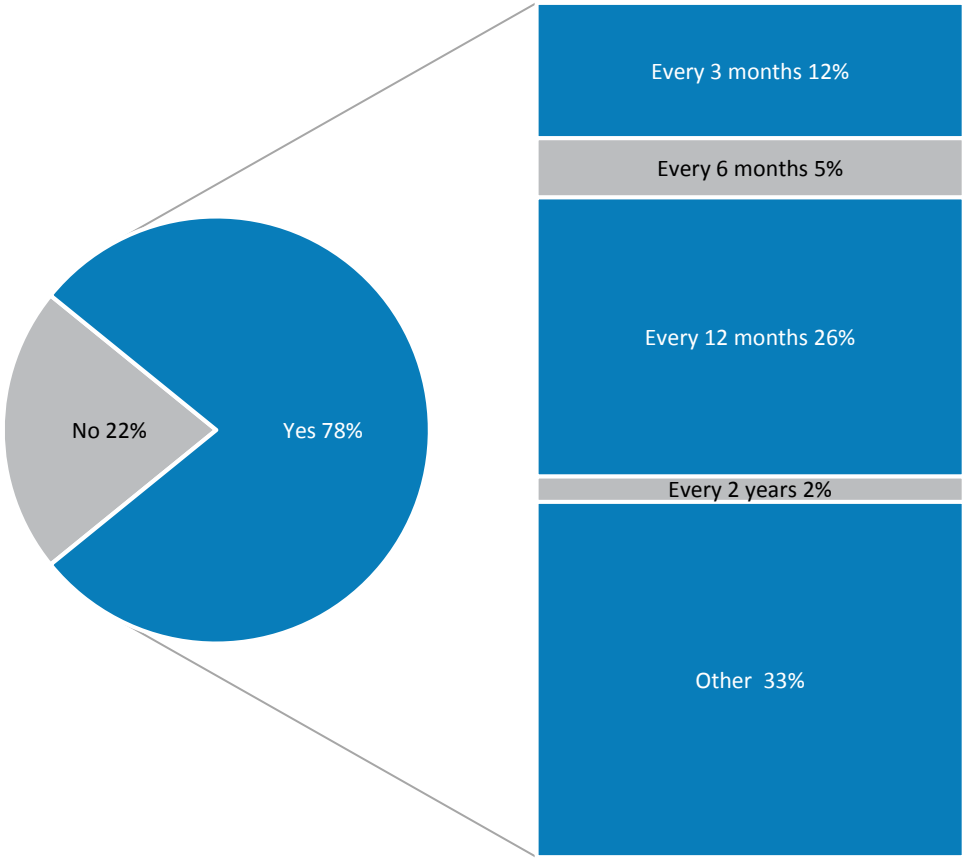
Q. Does your firm have a documented risk appetite for cyber-security risks?



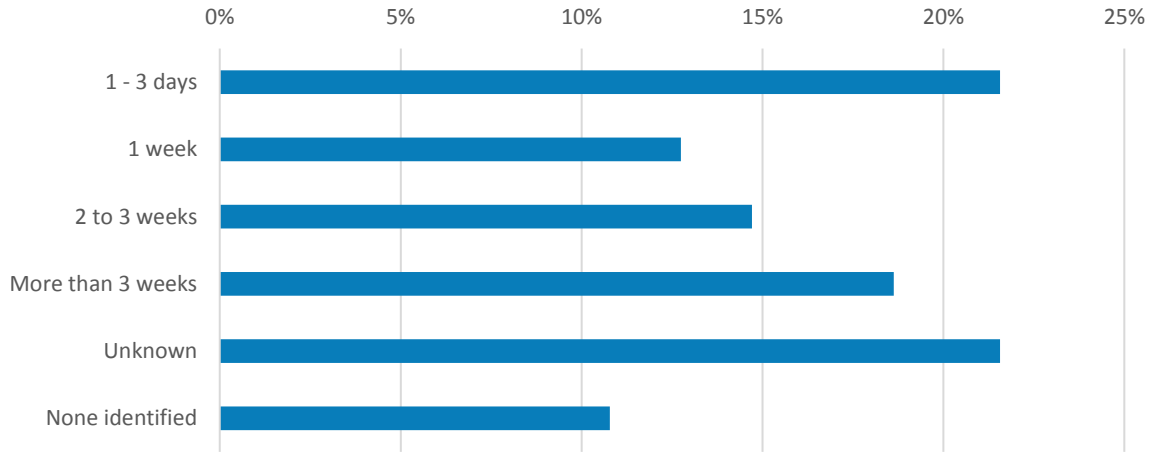
Q. Does your firm monitor external threat and vulnerability intelligence sources to identify cyber-security threats and vulnerabilities?



Q. Are automated vulnerability scanning and penetration testing (internal and external) performed regularly to identify vulnerabilities, if so, with what frequency?

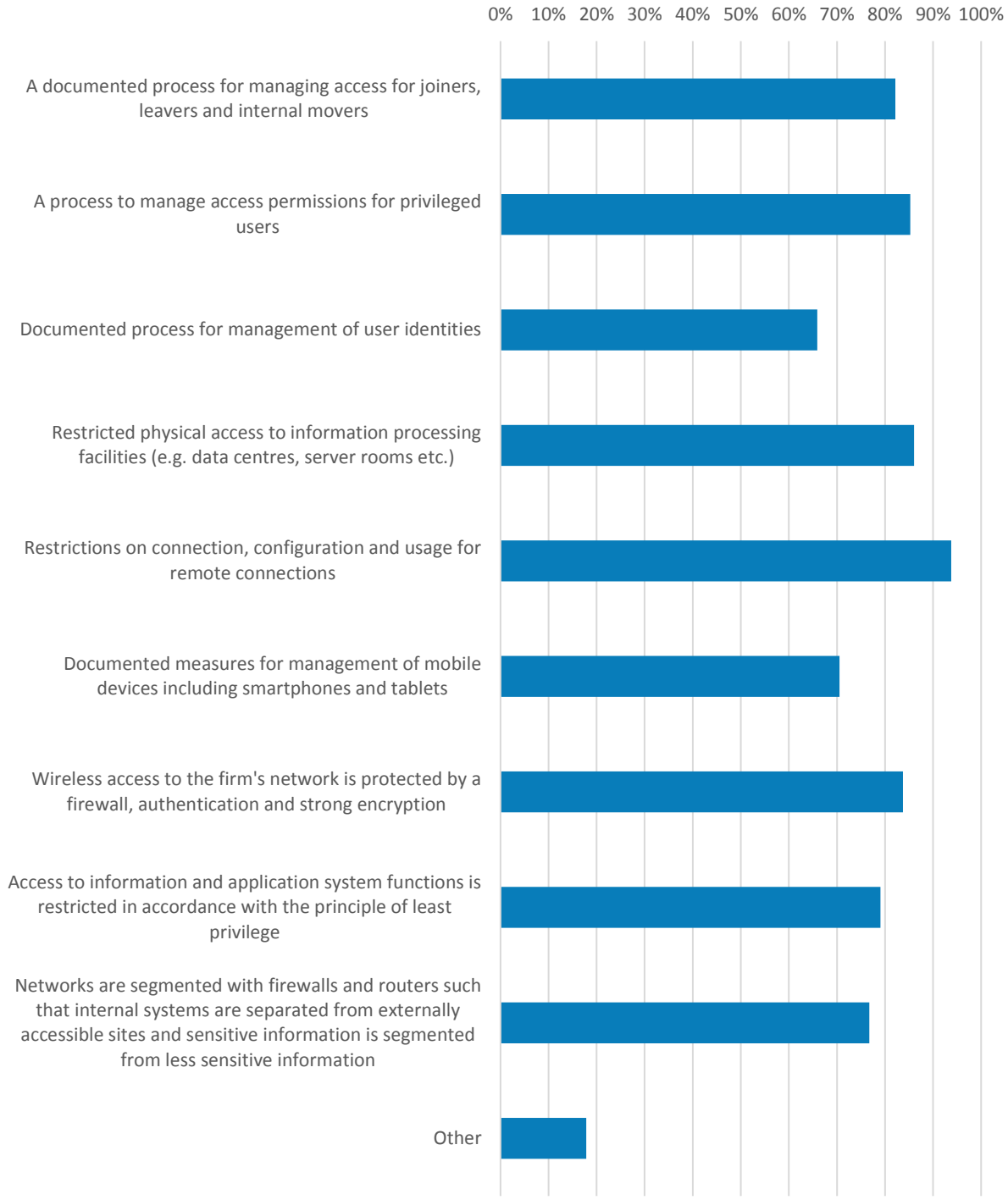


Average time taken by firms conducting automated vulnerability scanning and penetration testing from discovery of vulnerabilities to their resolution

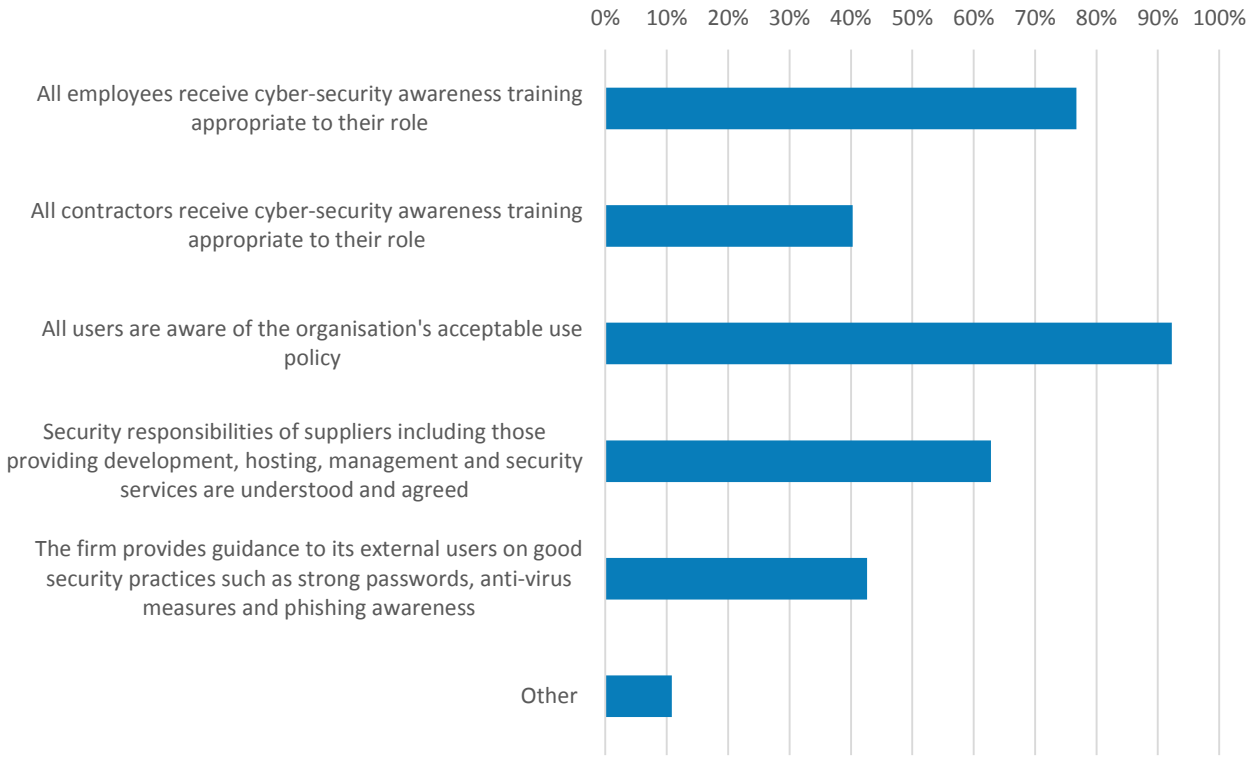


Protect

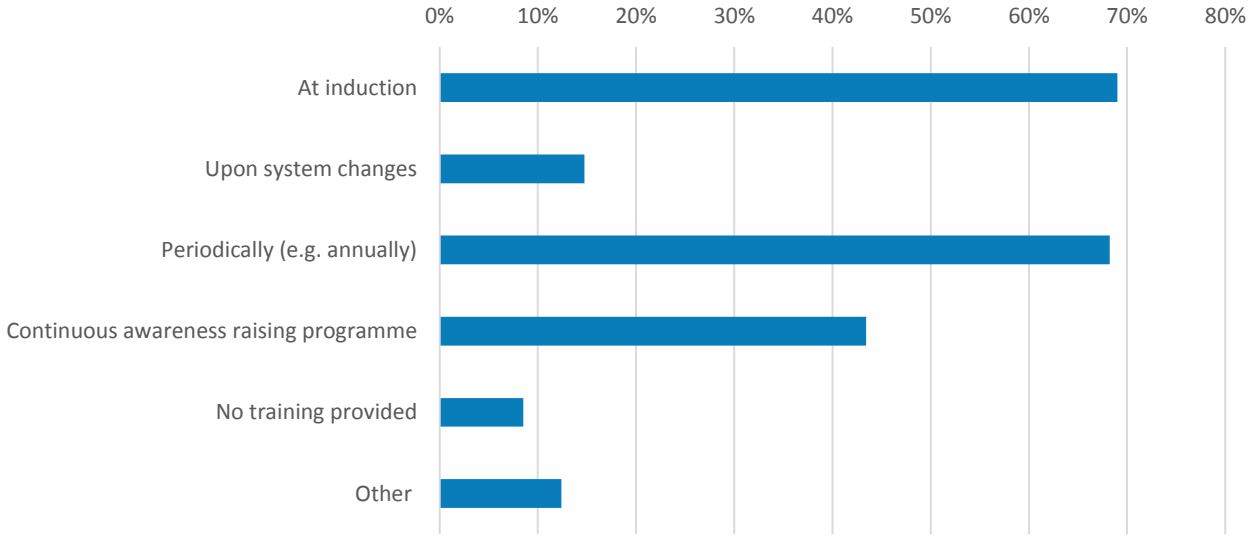
Q. Have any of the following access controls been adopted by your firm to manage cyber-security?



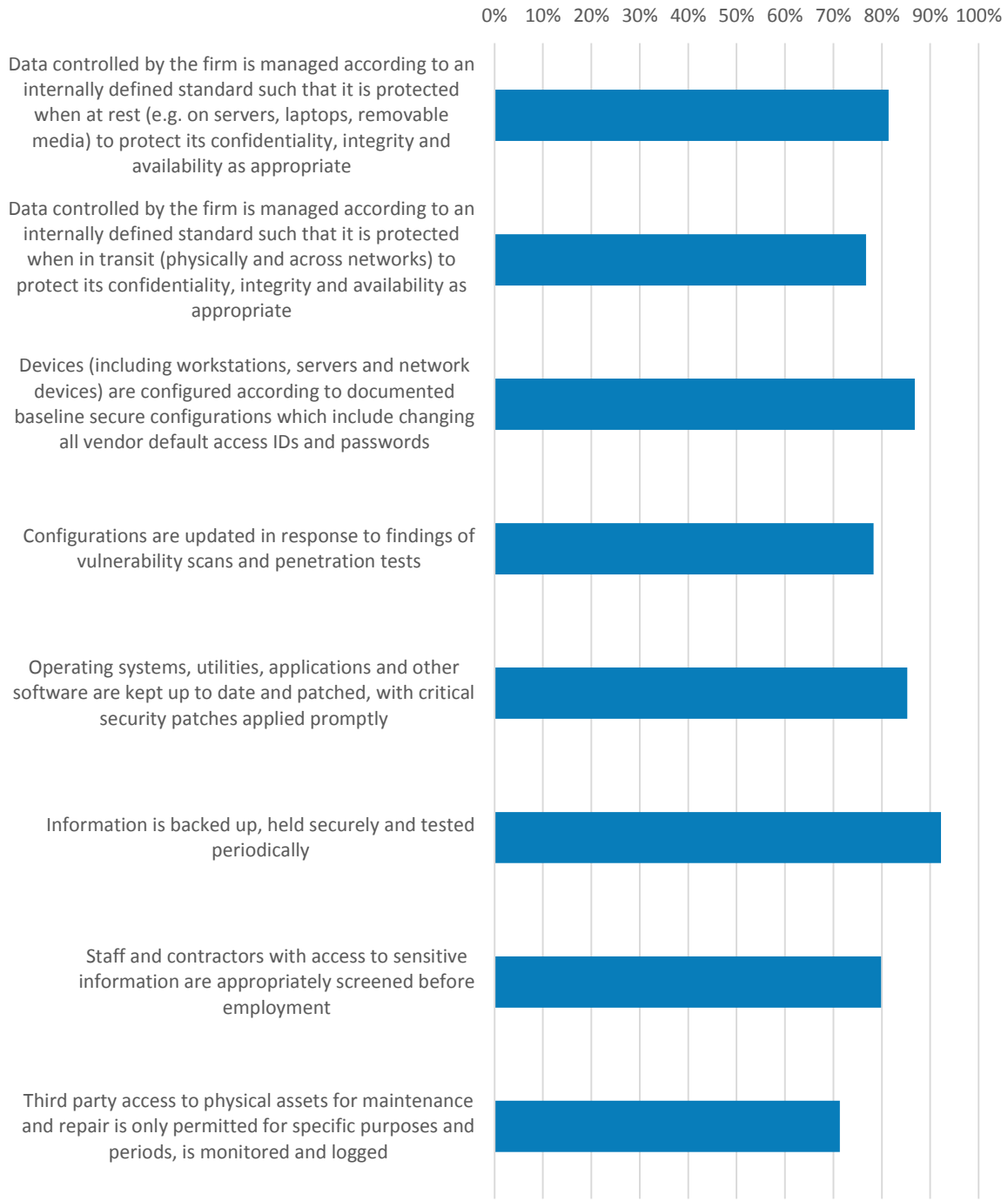
Q. Have any of the following been adopted by your firm to make employees and third parties aware of cyber-security issues?



Q. When does your firm provide cyber-security awareness training to employees?

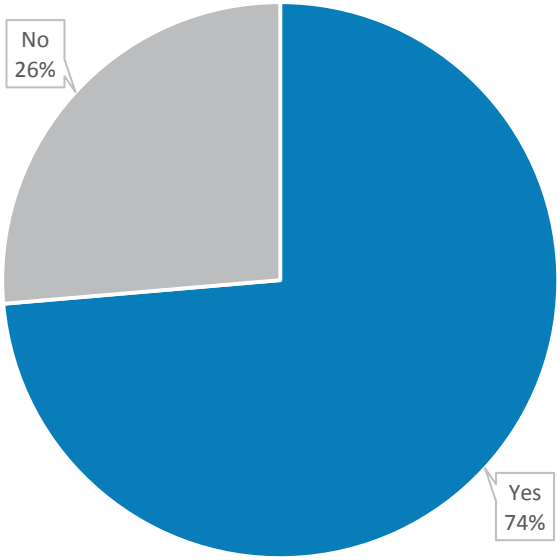


Q. Have any of the following information protection processes and procedures been adopted by your firm?

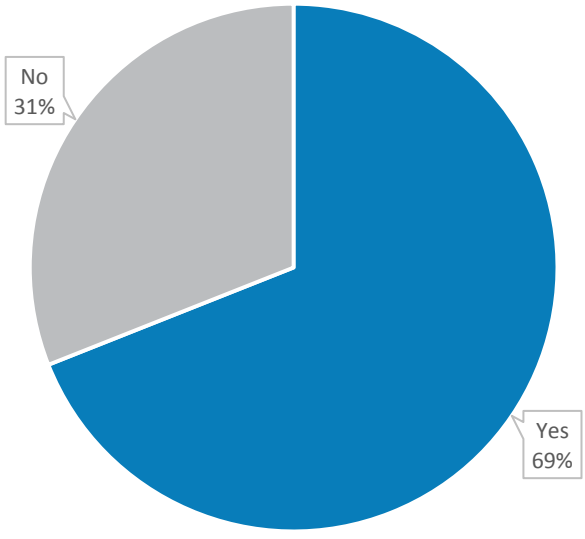


There is a system development lifecycle that incorporates security throughout the development process **43% /** Development, test and production environments are adequately separated and best practices followed e.g. not using live data in production and test environments **64% /** Software development, including that undertaken by third parties, ensures that secure coding practice is followed, taking account of at least 'OWASP top 10' **28% /** Change control for configurations and applications is managed through a formal change control process **68% /** Other **12%**

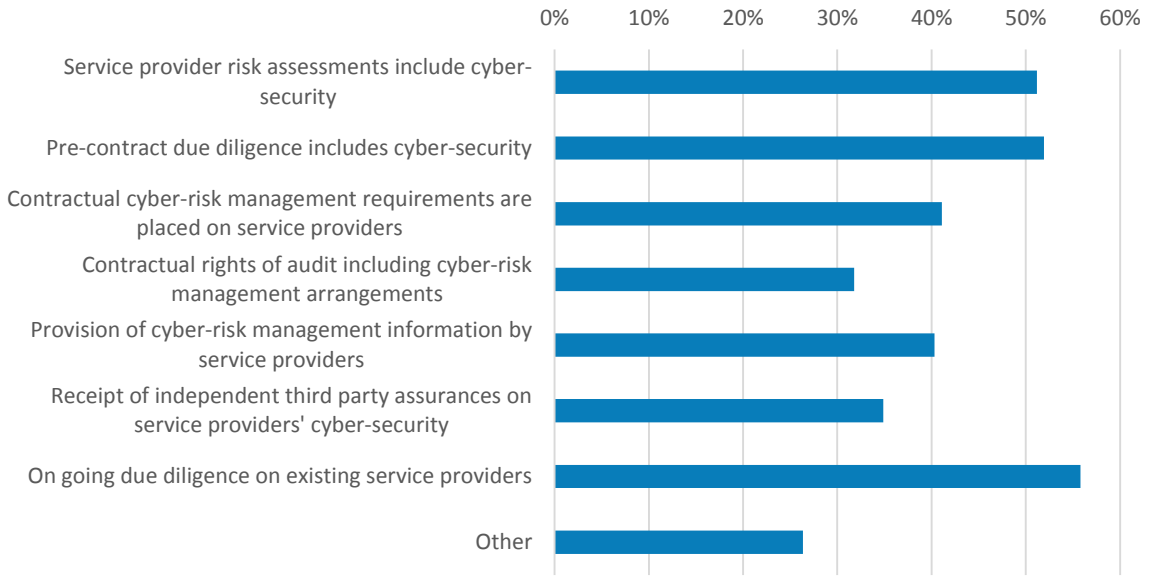
Q. Does your firm encrypt data on hard drives of mobile devices (e.g. laptops)?



Q. Does your firm have a policy covering the use of personal devices ('BYOD') by employees?

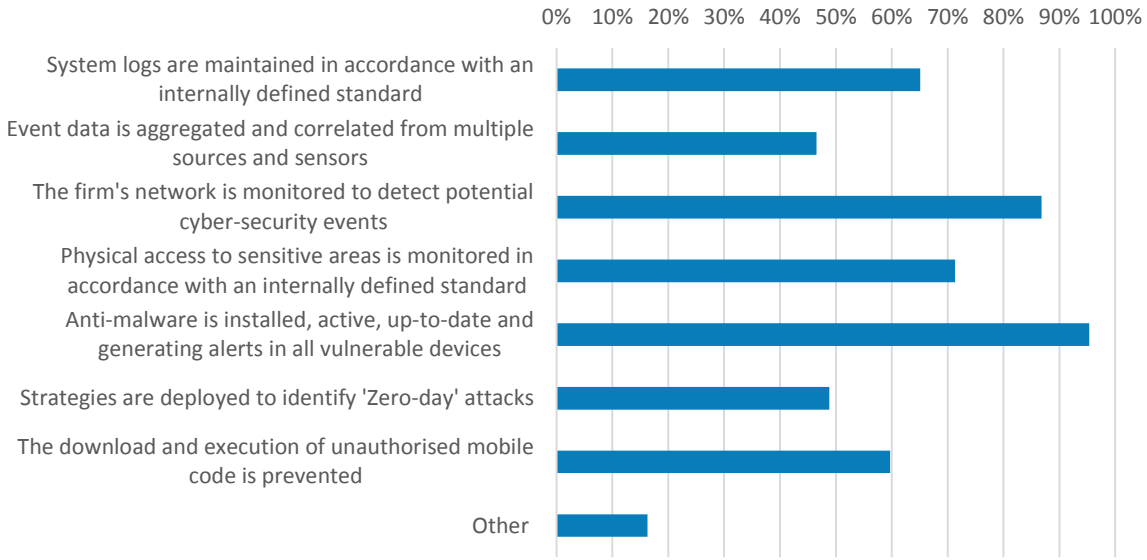


Q. Have any of the following been adopted by your firm to assess whether third party service providers are managing cyber-security appropriately?



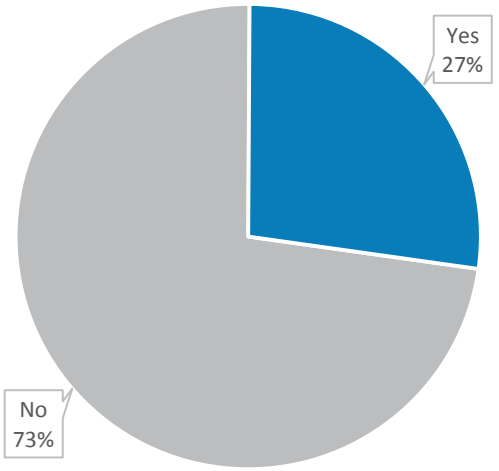
Detect

Q. Have any of the following continuous monitoring techniques been adopted by your firm to detect cyber-security issues?

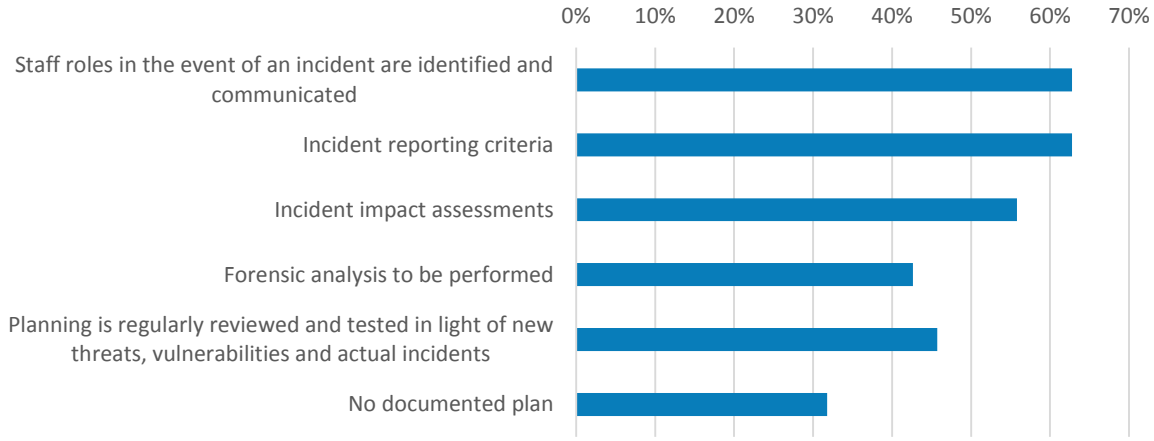


Respond

Q. Does your firm share information on cyber-security threats and vulnerabilities with other bodies or organisations such as industry alliances and 'CERTS'?

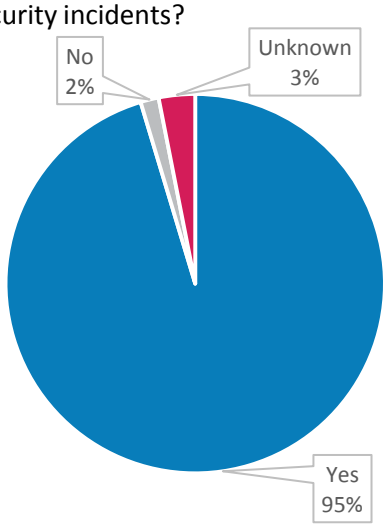


Q. If your firm has a documented cyber-security incident response plan which of the following does it contain?

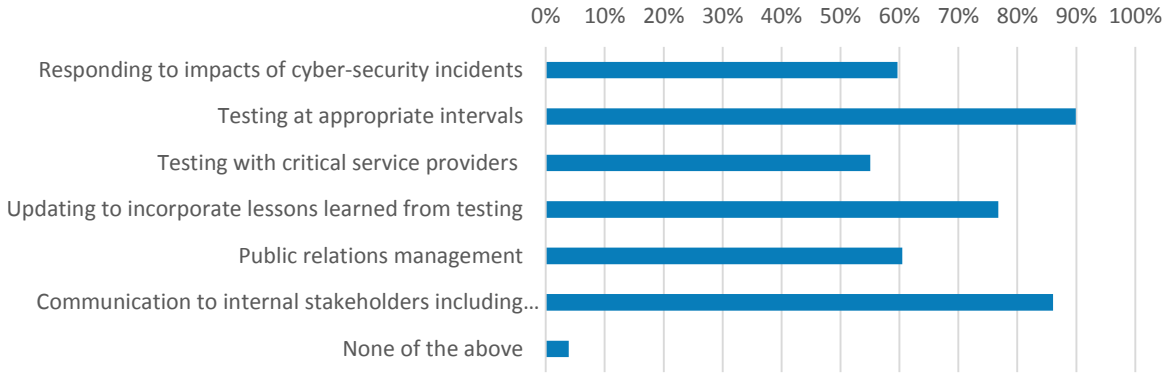


Recover

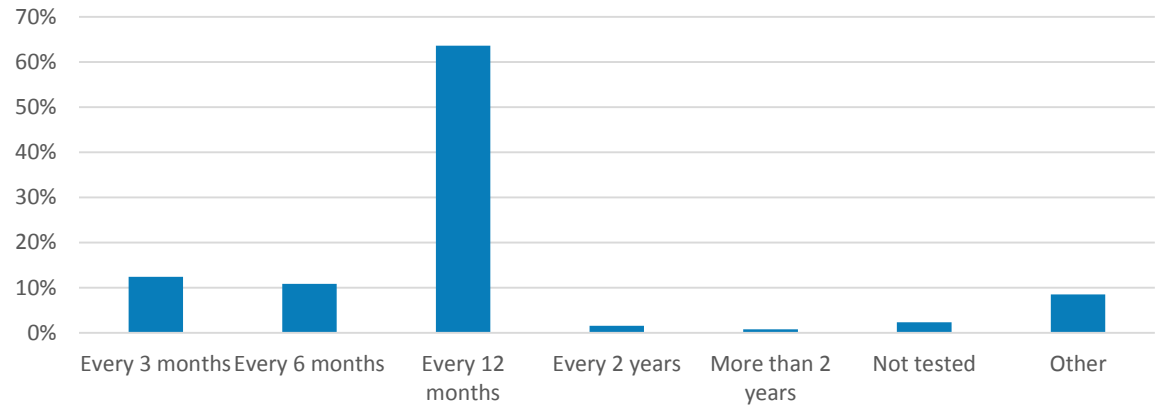
Q. Does your firm have appropriately skilled staff or ready access to resources to contain and mitigate cyber-security incidents?



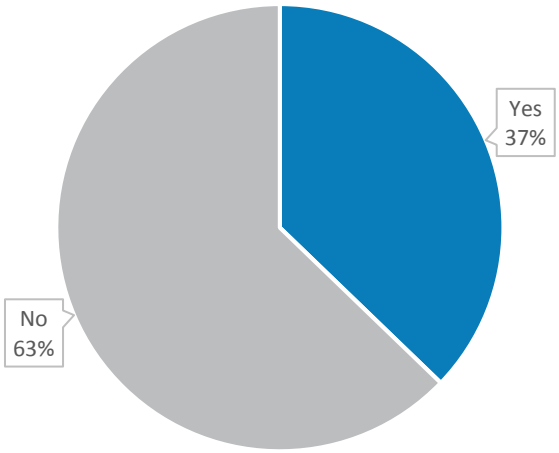
Q. Are any of the following included in your firm's business resumption, disaster recovery and contingency arrangements?



Q. How often are your firm's business resumption, disaster recovery and contingency arrangements tested?



Q. Does your firm maintain a dedicated cyber-security insurance policy?



% of firms with a cyber-security insurance policy who have coverage for the following liabilities

Environment

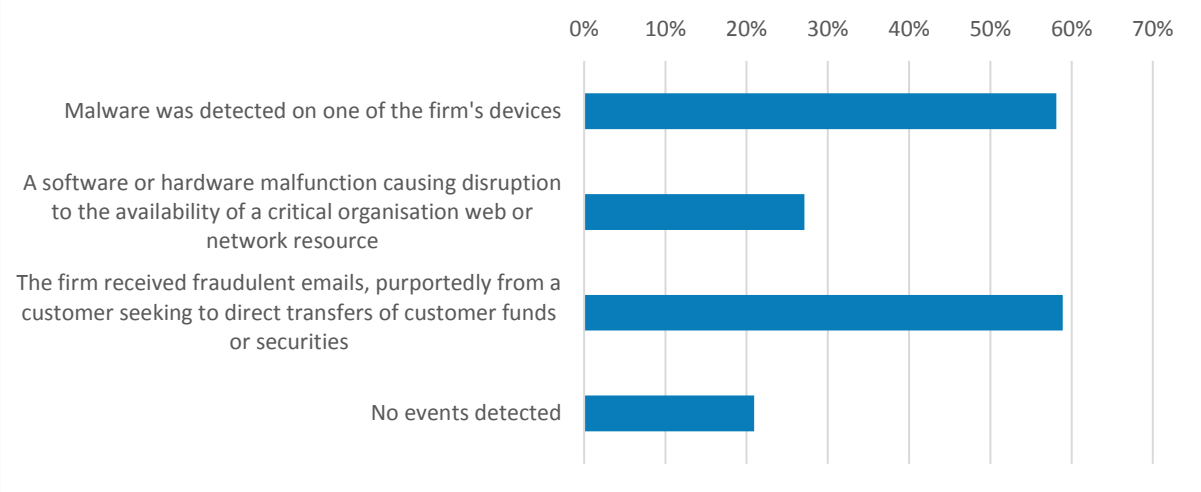
Cyber-Security Threats

Q. Please select what you consider to be the top five threats to your firm's cyber-security in 2017?

% of firms ranking the top five threats 1st, 2nd, 3rd, 4th and 5th[2]	1st	2nd	3rd	4th	5th
Unintentional information leakage/sharing	14%	16%	17%	3%	3%
Fraud	36%	2%	2%	5%	2%
Deliberate information leakage	9%	18%	5%	0%	3%
Malicious Code/software/activity	4%	3%	7%	5%	8%
Social engineering	5%	3%	7%	5%	8%

Cyber-Security Events

Q. Have any of the following types of events been experienced by your firm since 1 January 2016?

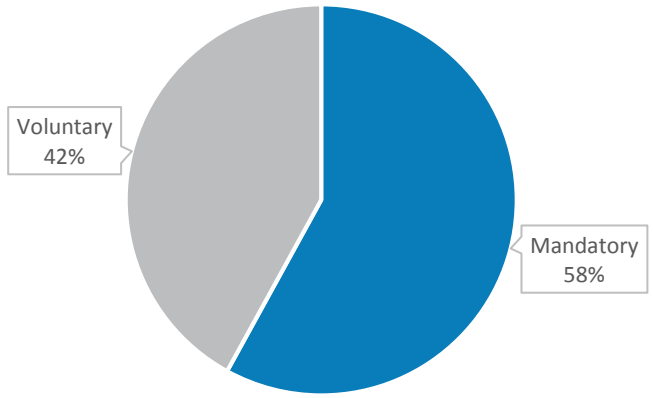


A denial of service attack blocking access to a firm website or network resource **6% /** Breach of your firm's network by an unauthorised user resulting in misappropriation of assets, confidential customer or organisation information, or damage to the firm's network or data **3% /** A compromised computer belonging to a customer or vendor being used to remotely access the firm's network resulting in fraudulent activity, such as efforts, to fraudulently transfer funds from a customer or the submission of a fraudulent payment request purportedly on behalf of a vendor **2% /** An extortion attempt by an individual or group threatening to impair access to or damage the firm's data, devices, network or web services **9% /** An employee or other authorised user of the firm's network engaged in misconduct resulting in misappropriation of assets, confidential customer or organisation information, or damage to the firm's network or data **6%**

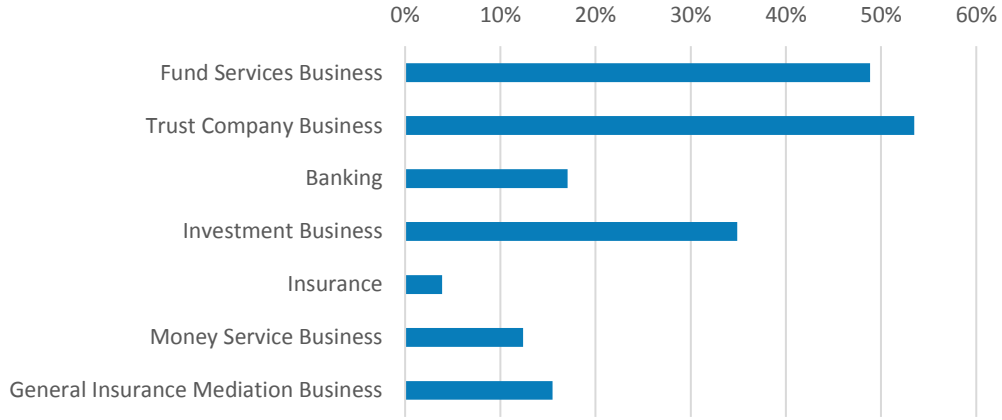
[2] For the purposes of consistency respondents were provided with the list of threats from the ENISA Threat Taxonomy v 2016 https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/at_download/file

Breakdown of Survey Respondents

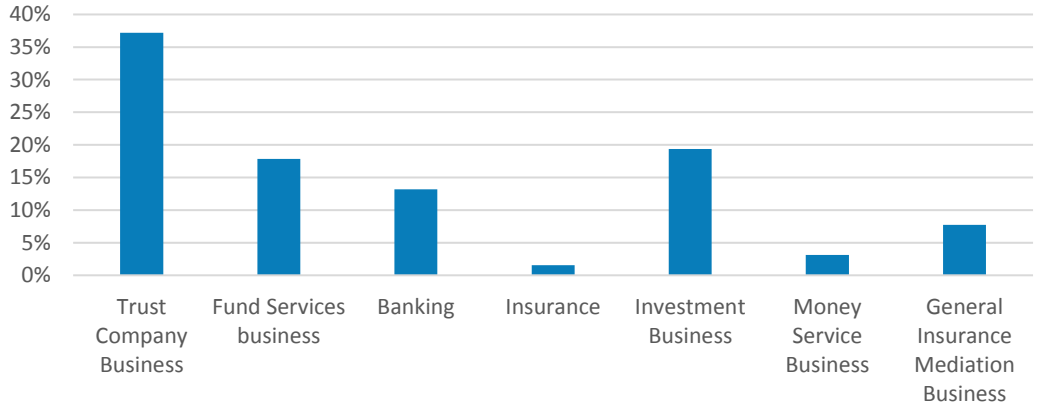
Volunatry /Mandatory



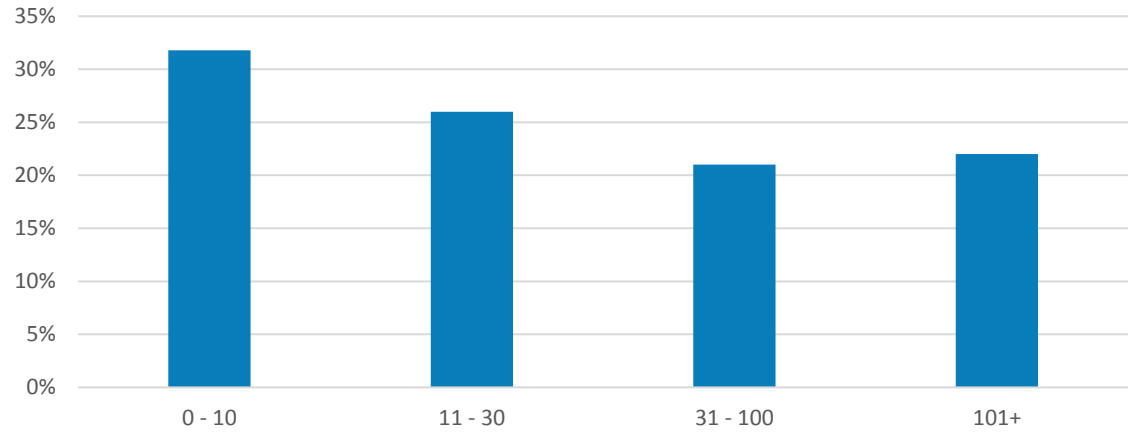
Licences held



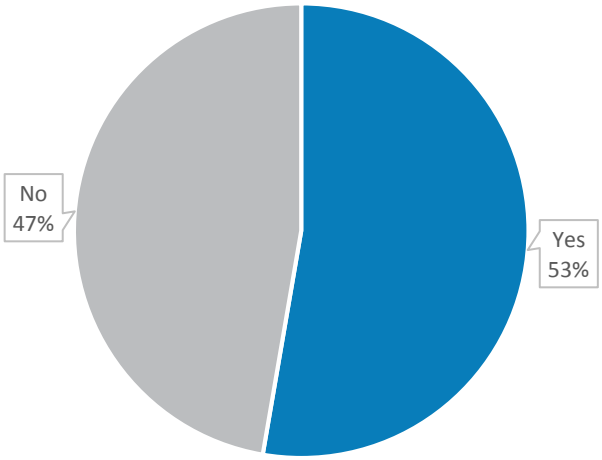
Main area of regulated activity



Number of employees



Provide services to clients through the internet (e.g. internet banking, customer portals etc.)



Limitations

- The survey sample was made up of firms who were required to respond and those who responded voluntarily. The mandatory sample was selected in order to include a range of firms across the various regulated sectors. However, statistical inferences, margins of error and confidence intervals cannot be applied to this data given our sample was not statistically selected.
- 42% of firms completing the survey did so on a voluntary and anonymous basis and it is therefore possible that those firms that chose not to respond may be substantially different from those that chose to respond.
- All data is based upon the responses provided by firms and no attempt has been made to validate or seek evidence for the responses given.
- The JFSC cannot accept any liability for reliance by any person on this report or any of the information, opinions or conclusions herein.

Appendices