Deloitte.

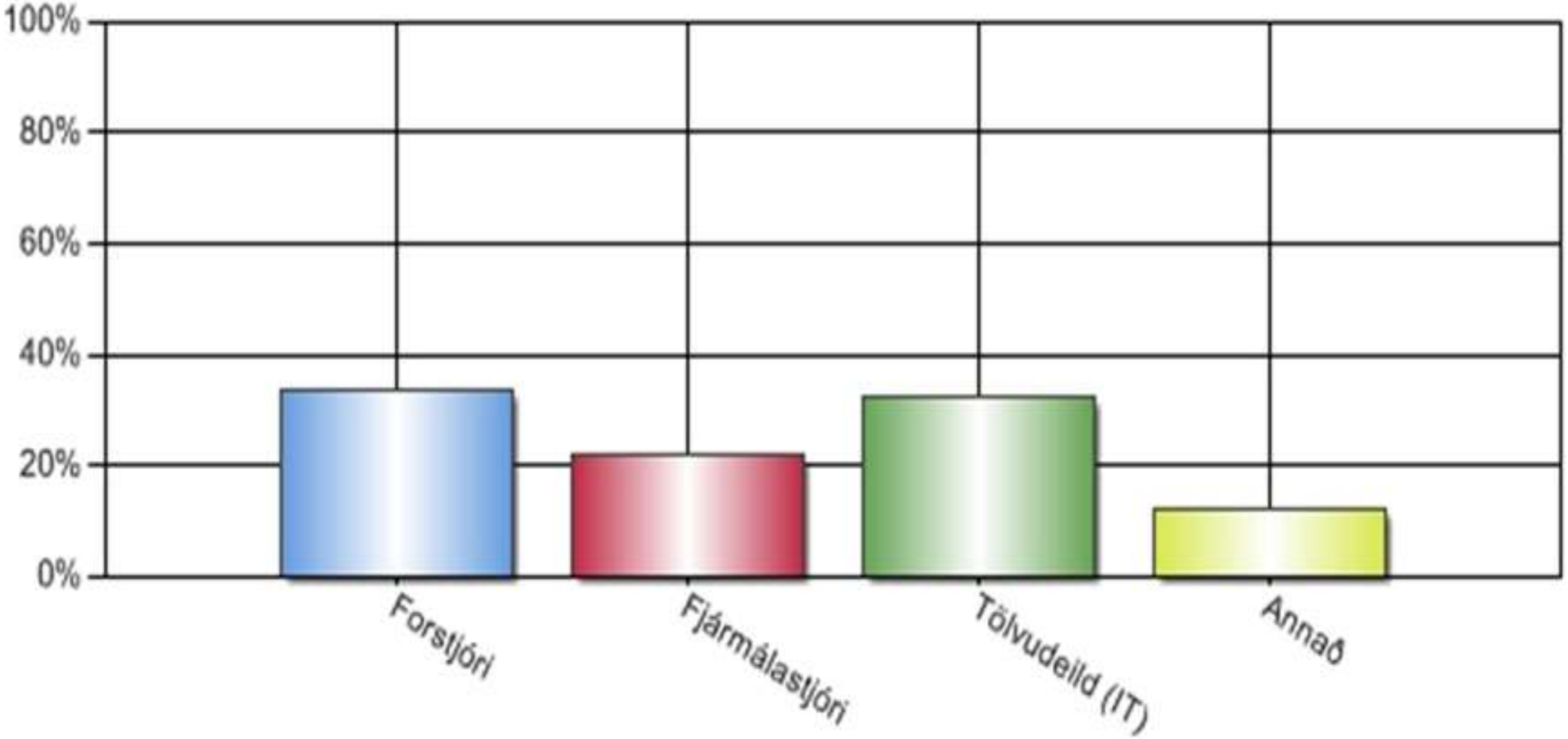
# IT Information Security in Iceland

## Survey Results and Best Practices

Akureyri
Egilsstaðir
Grundarfjörður
Neskaupsstaður
Snæfellsbær
Kópavogur/Reykjavík
Reykjanesbær
Vestmannaeyjar

**Dr. Rey Leclerc Sveinsson, CISSP, CIPP, CBCP**

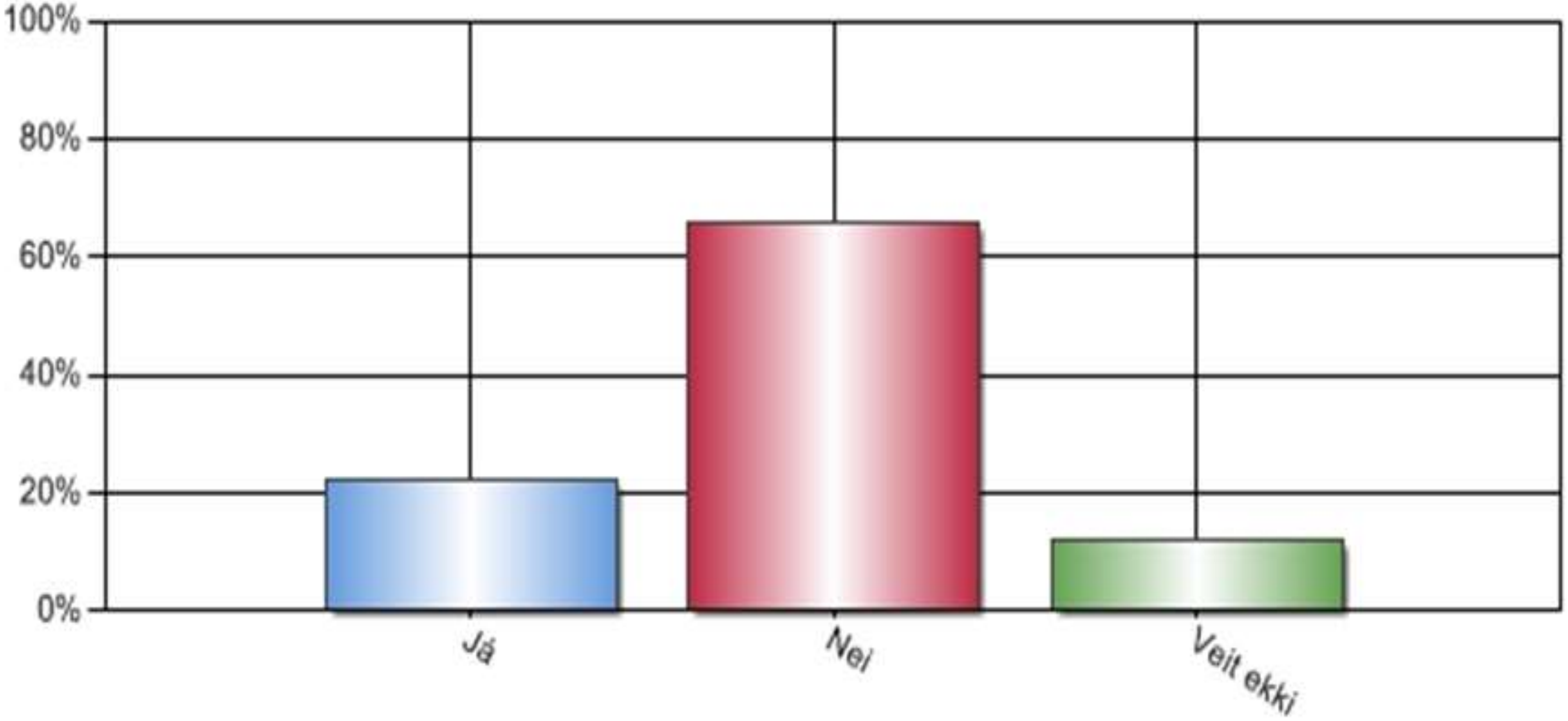
# Who answered?



| | |
|---|---|
| CEOs | 33,78% |
| COO /CFOs | 21,62% |
| IT Managers | 32,43% |
| Others | 12,16% |

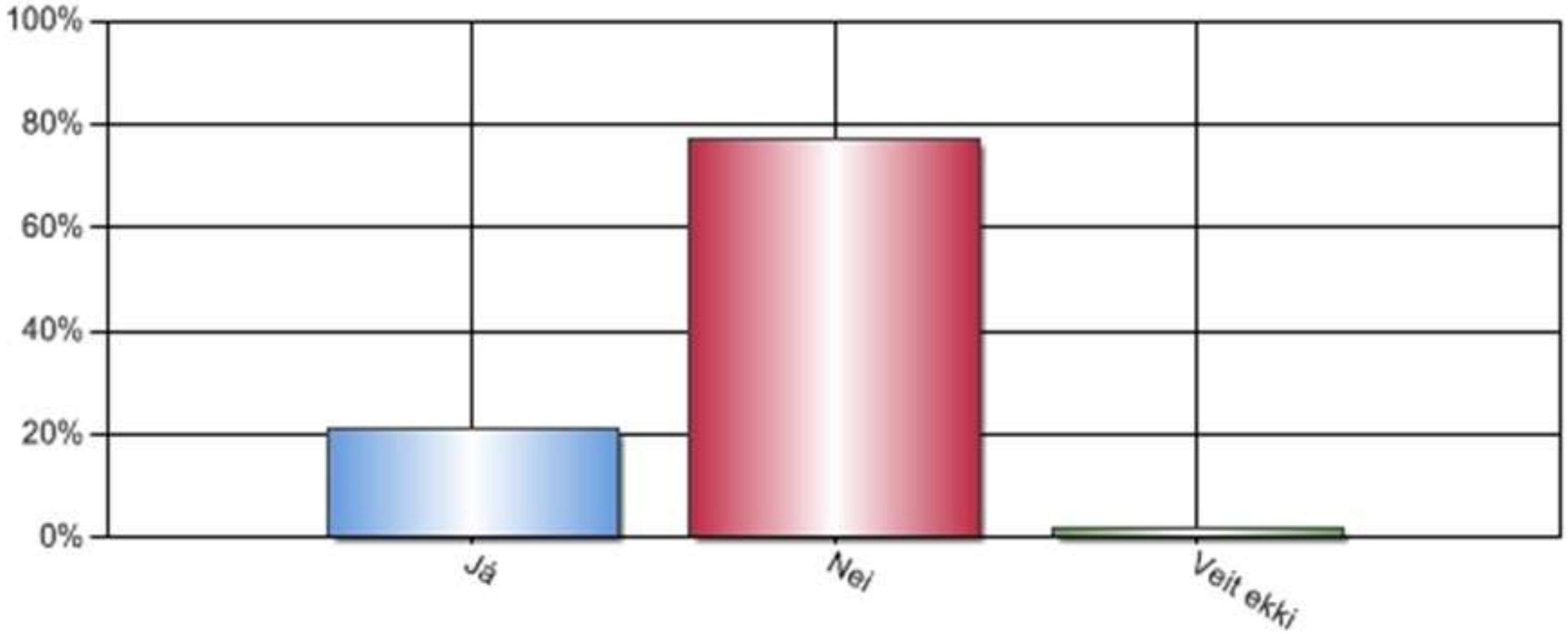
# Information Security and Risk Management

# Has your business suffered a computer attack of any kind in the last 12 months?



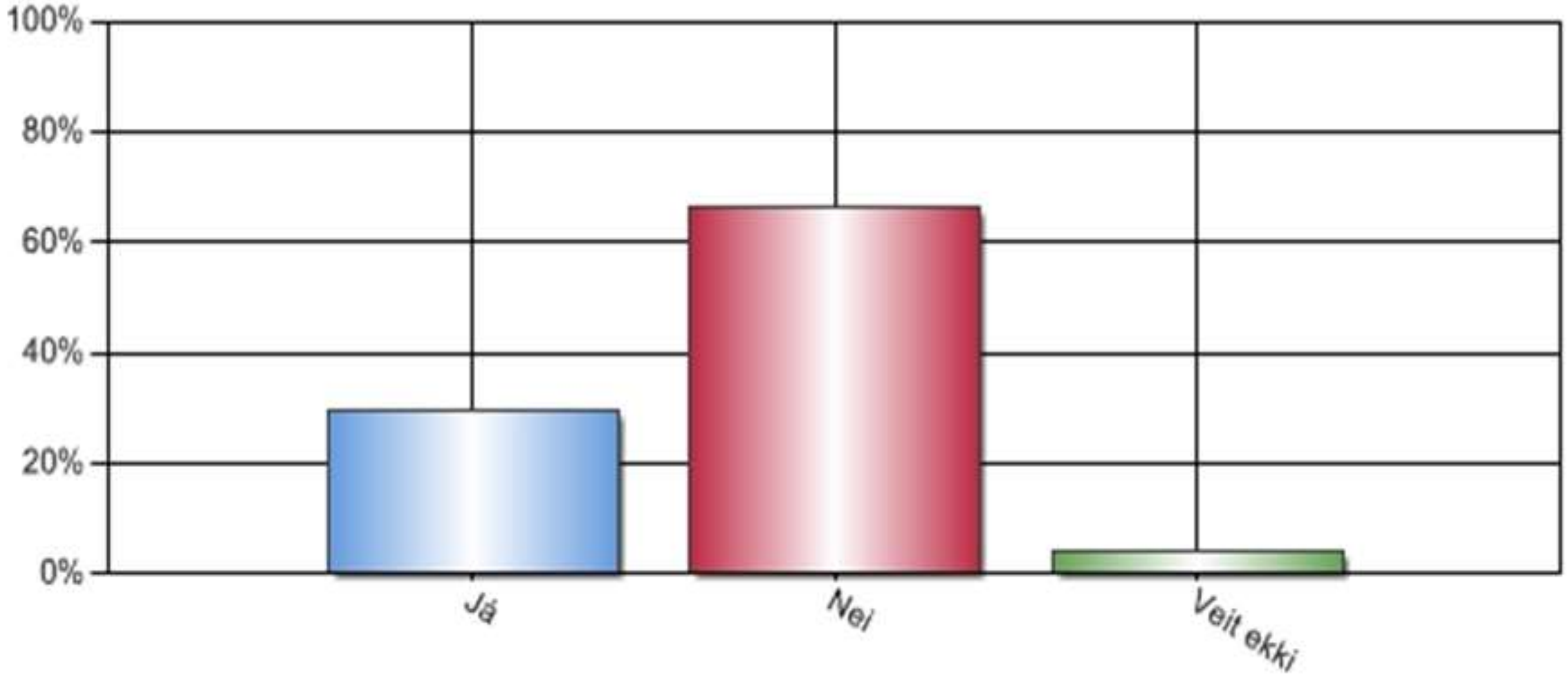
| | |
|---|---|
| Yes | 22,15% |
| No | 65,77% |
| Don´t Know | 12,08% |

# Has your business suffered financial losses due to computer attacks, malfunction of computer equipment or an error in the information systems over the last 12 months?



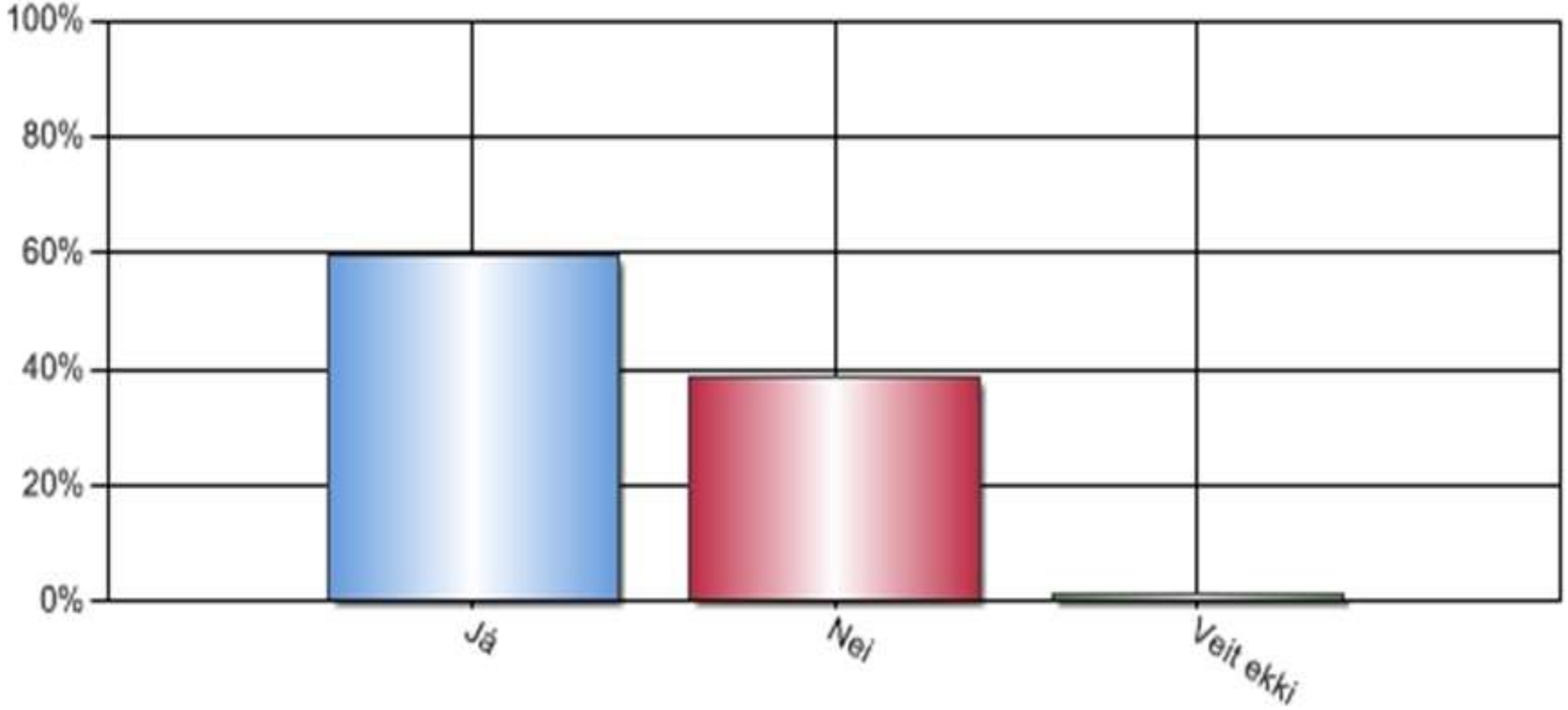
| | |
|---|---|
| Yes | 20,95% |
| No | 77,03% |
| Don´t Know | 2,03% |

# Is the company making a special budget for information security?



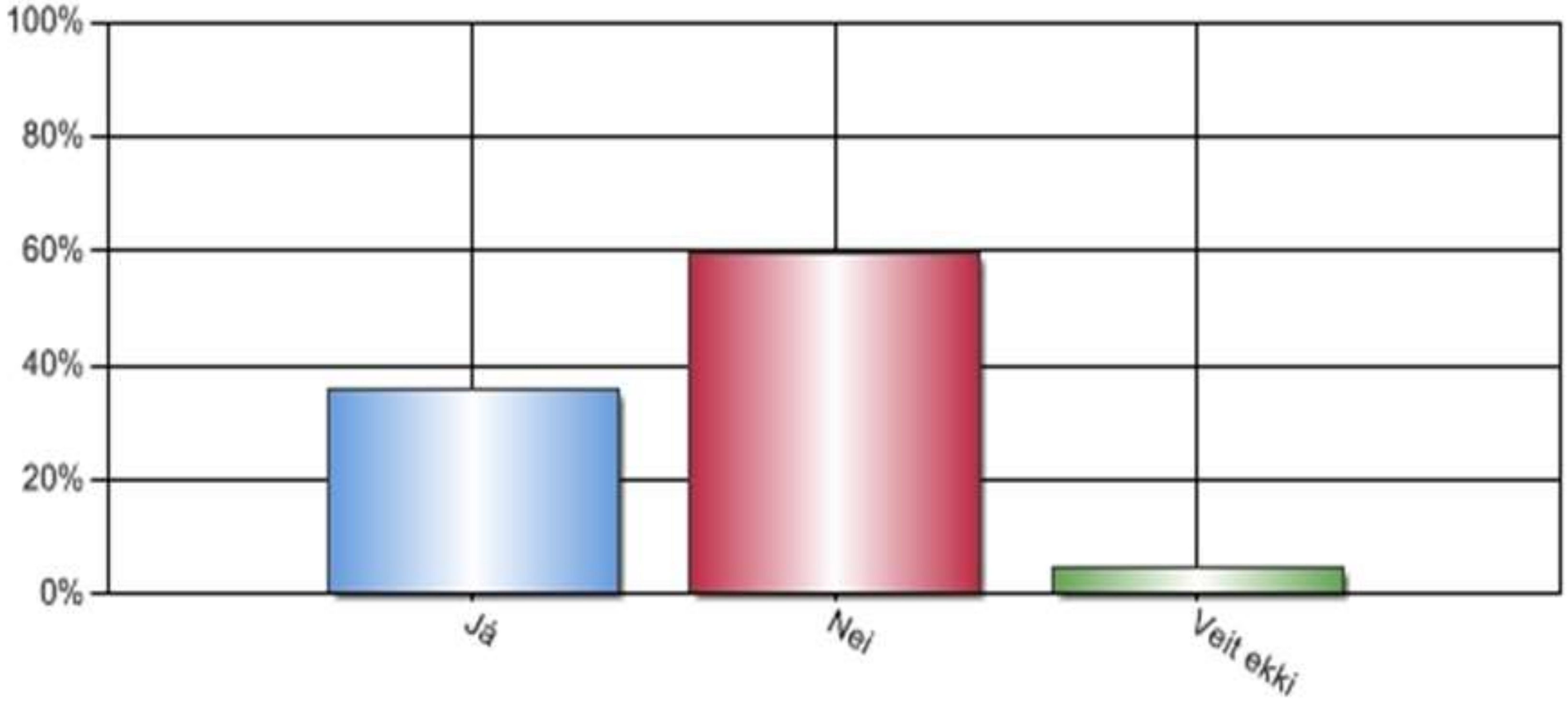
| | |
|---|---|
| Yes | 29,53% |
| No | 66,44% |
| Don´t Know | 4,03% |

# Does the Board take an active role in the formulation and decisions relating to information technology?



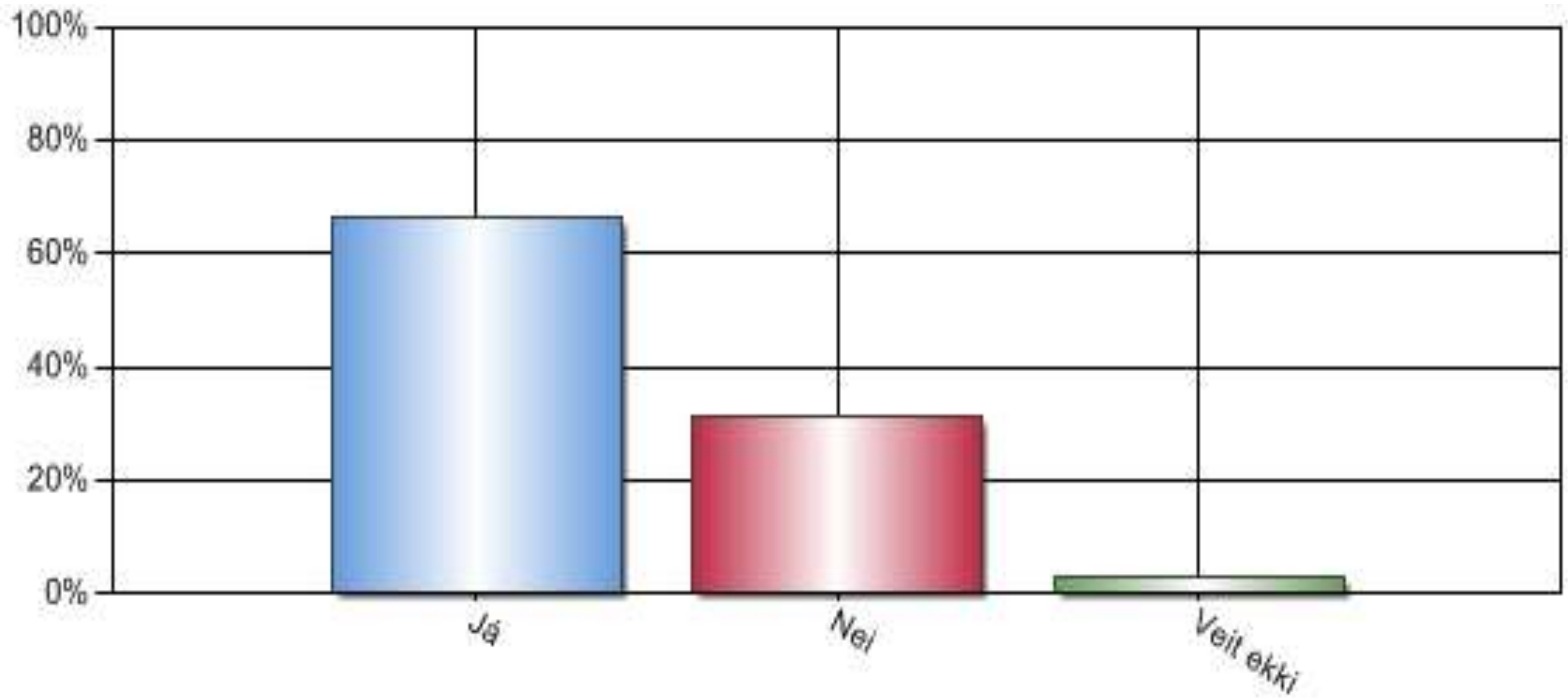
| | |
|---|---|
| Yes | 59.86% |
| No | 38,78% |
| Don´t Know | 1,36% |

# Do you have an IT risk management program in place?



| | |
|---|---|
| Yes | 35,81% |
| No | 59,46% |
| Don´t Know | 4,73% |

# Do you have information security policies?



|  |  |
|---|---|
| Yes | 66,22% |
| No | 31,08% |
| Don´t Know | 2,70% |

# What are the threats of most concern?

| Risk | Percentage |
|---|---|
| Leakage of Sensitive Information | 64,19% |
| Fire | 56,08% |
| External Fraud (non Employee) | 43,92% |
| Theft | 42,57% |
| Power Failure | 41,22% |
| External Vandalism | 36,49% |
| Employee Fraud | 34,46% |
| Natural Disasters | 30,41% |
| Organized Crime | 27,70% |
| Employee Theft | 23,65% |
| Infrastructure Damage | 22,97% |
| Spying | 12,84% |
| Others | 12,84% |
| Violations of property rights | 14,19% |

# Best Practices

- Organizations assign an Information Security or Data Protection Officer who is in charge of information security – maintaining confidentiality, integrity and availability of information
    - Upcoming EU Data Protection Regulation (2014/2015):
        - Companies should designate a data protection officer and have at least the following qualifications: extensive knowledge of data protection and mastery of technical requirements for privacy and data security.
- The Information Security/Data Protection Officer reports to senior management.
- Standardize procedures and controls for information security.
- Widely adopting and implementing procedures from ISO, CobiT, ITIL, PCI and other frameworks.
    - ISO 27001/2 recommended by Persónuvernd and FME
    - PCI required for all companies with credit card information

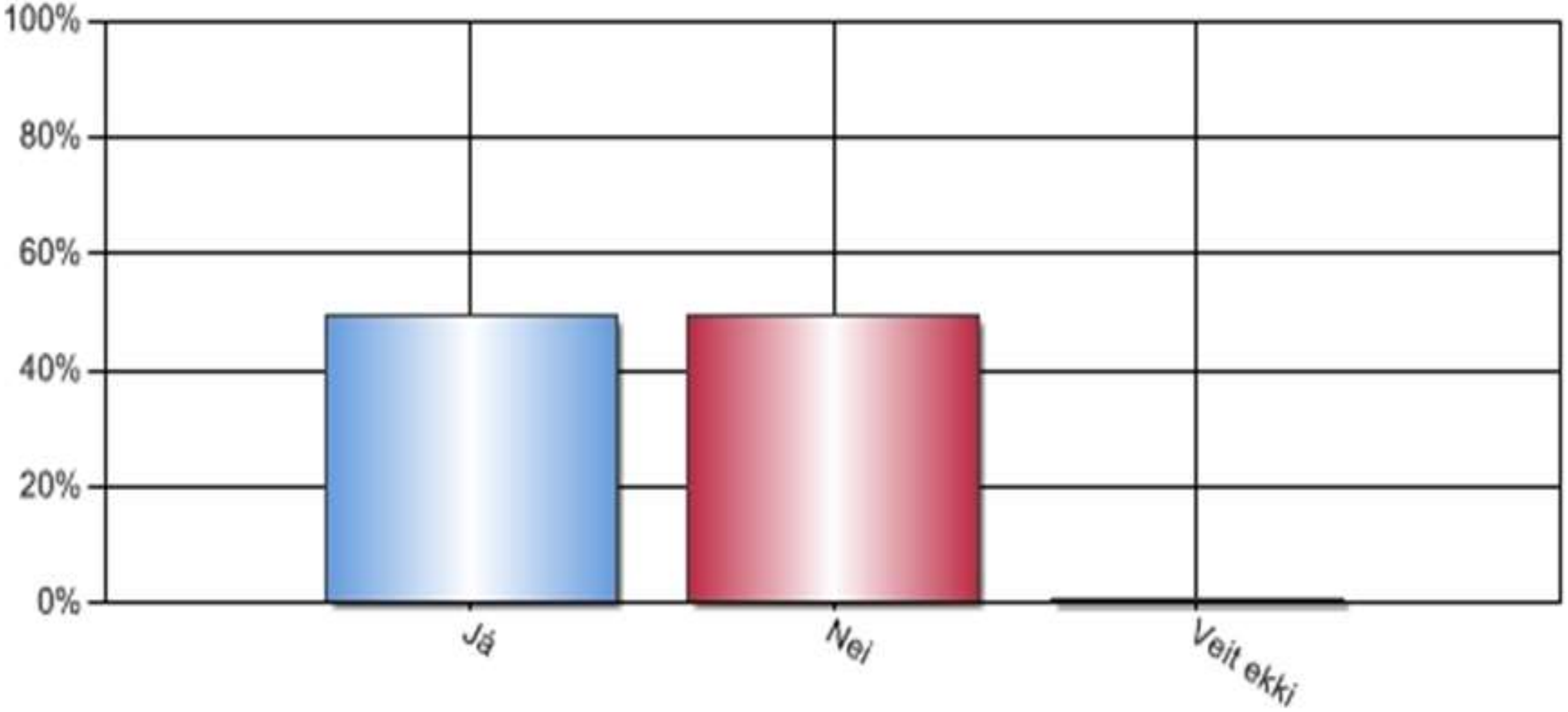
# Best Practices

- End User Acceptable Use Guidelines
- Risk assessment is reviewed at least once a year, or immediately, if the nature, the scope or the purposes of the data processing operations change significantly.
  - Required by new FME standards
  - Required by new EU Data Protection Regulation
- Measuring, assessing and reporting on risks on a regular basis.
- Establish a quality-improvement program for the information security and assurance program.
- Annual Updates and Reporting to senior management

# Secure Home and Mobile Working

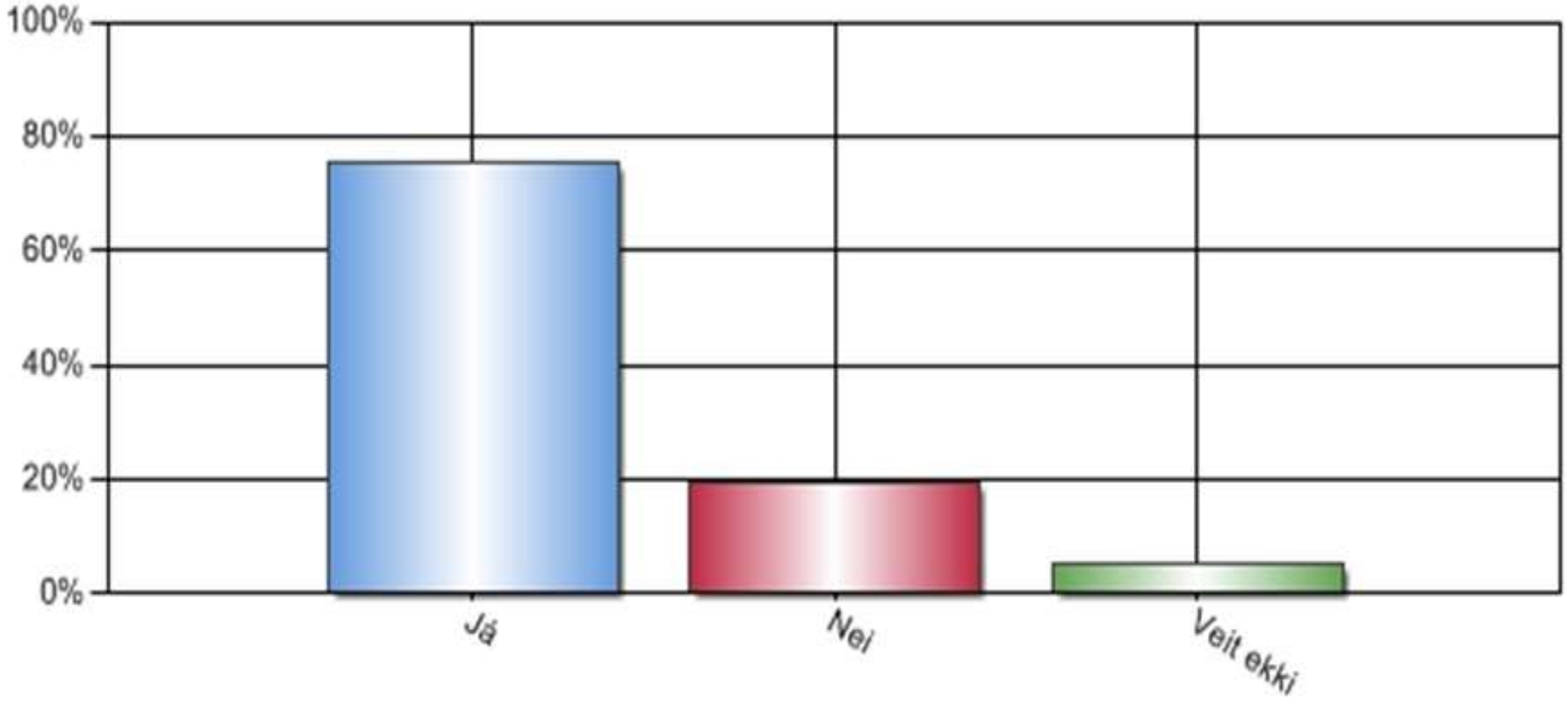
# Mobile Devices and Removable Media

# Do you have a mobile and home-working policies that staff have been trained to follow?



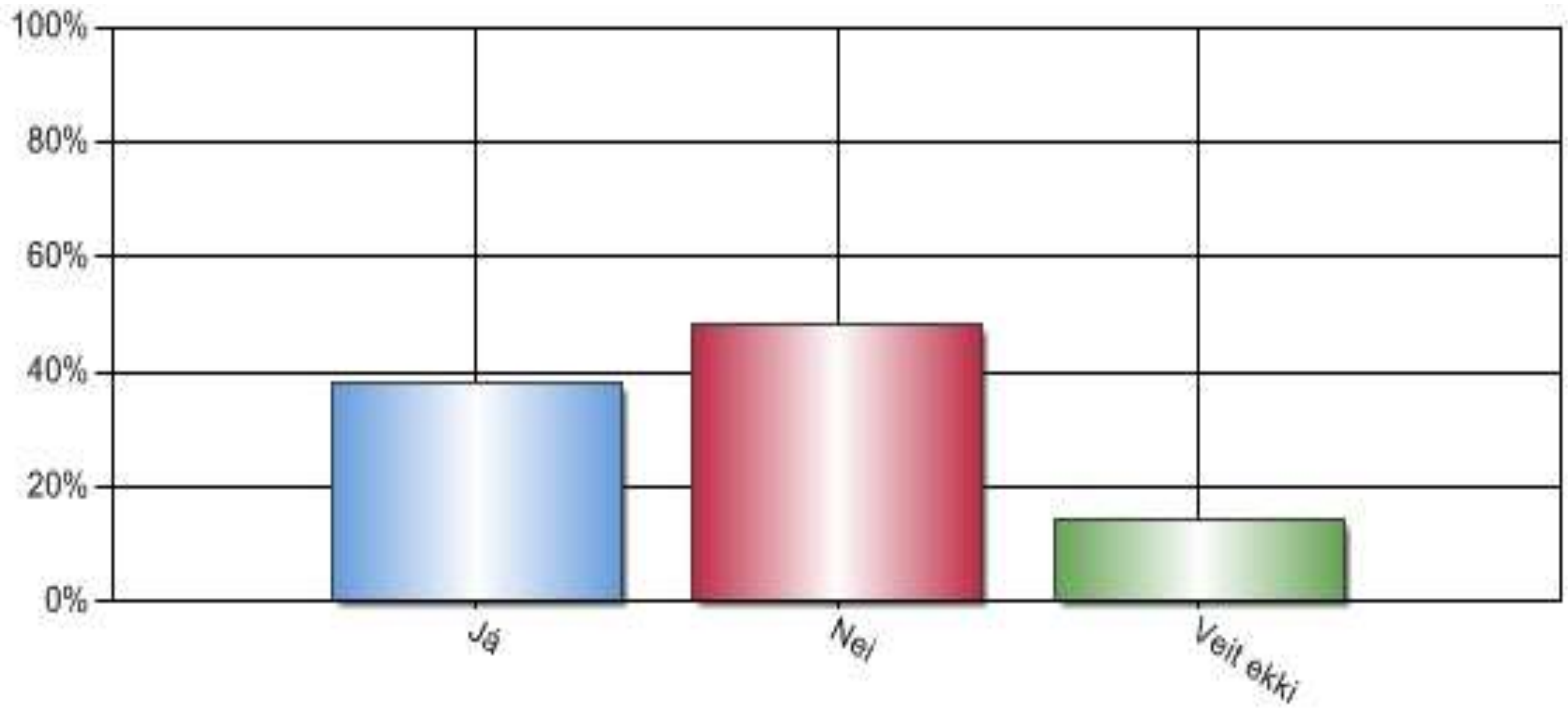
| | |
|---|---|
| Yes | 49,66% |
| No | 49,66% |
| Don´t Know | 0,67% |

# Do you have a secure baseline device build in place for mobile devices?



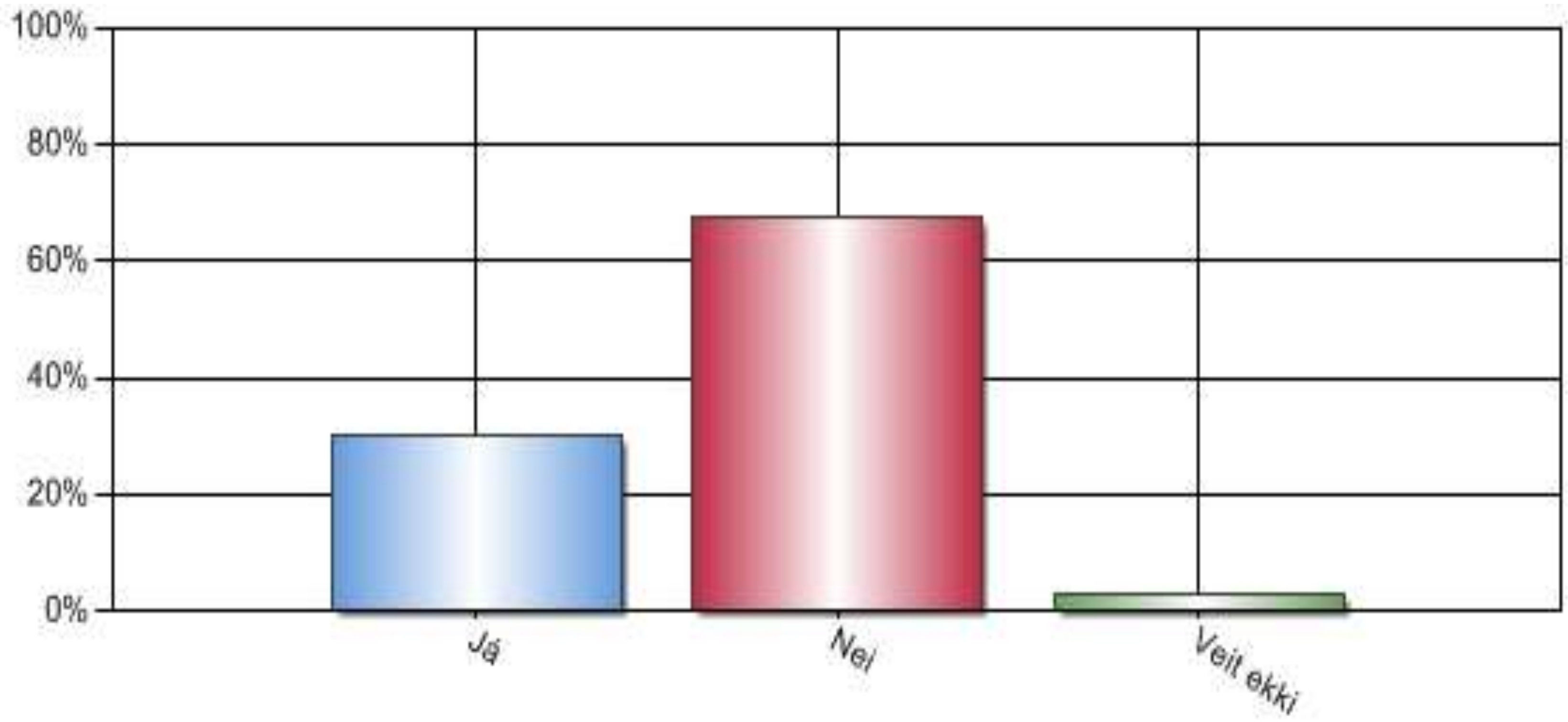
| | |
|---|---|
| Yes | 75,33% |
| No | 19,33% |
| Don´t Know | 5,33% |

# Are you protecting data both in transit and at rest?



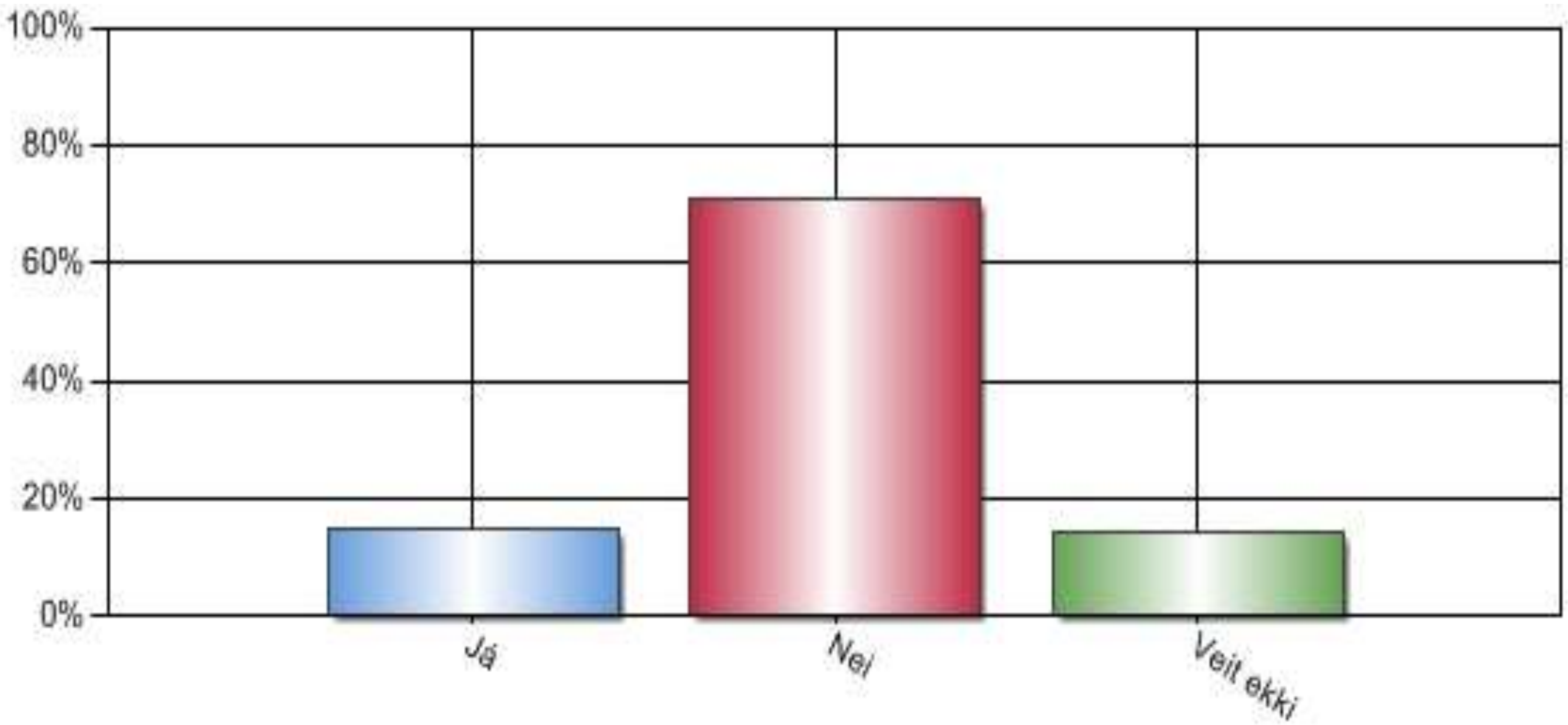
| | |
|---|---|
| Yes | 38,00% |
| No | 48,00% |
| Don´t Know | 14,00% |

# Do you have a policy controlling mobile and removable computer media?



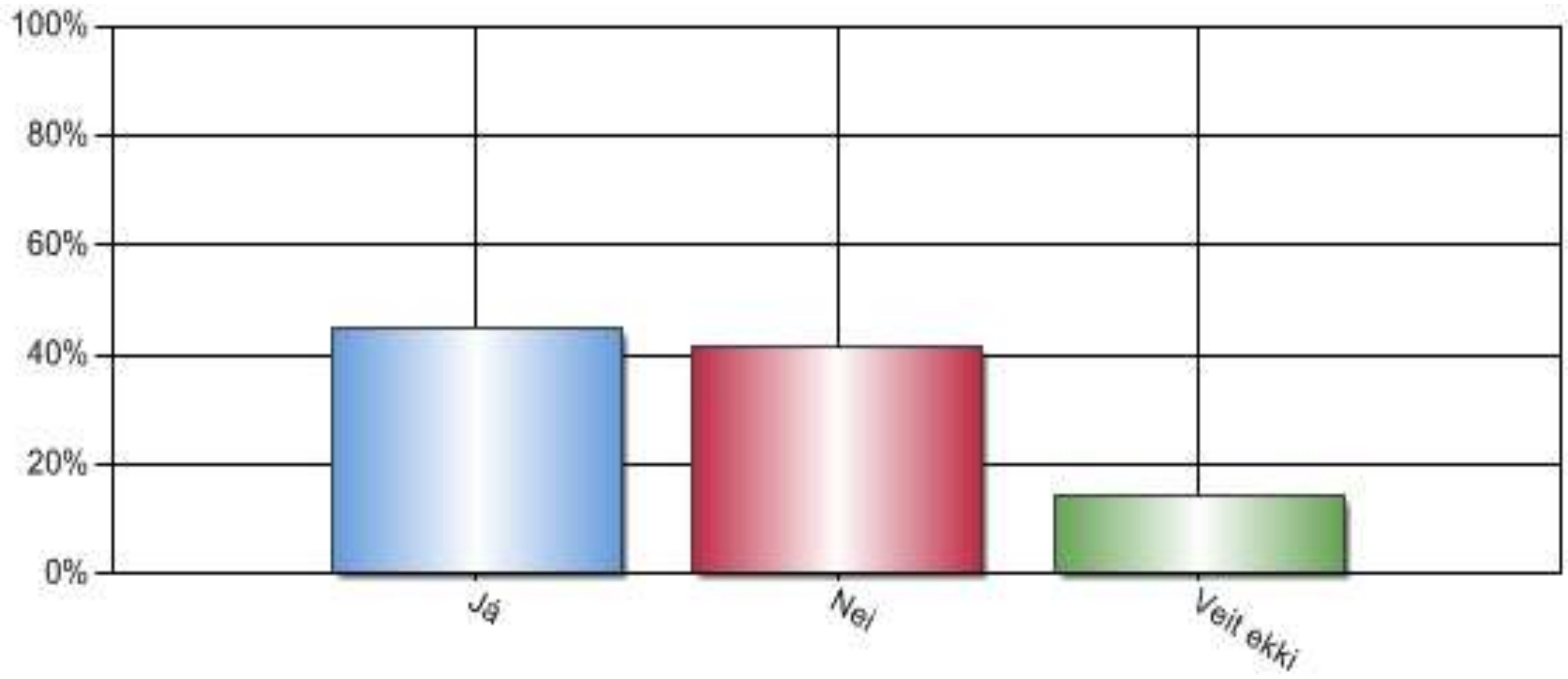
| | |
|---|---|
| Yes | 29,93% |
| No | 67,35% |
| Don´t Know | 2,72% |

# Are all sensitive devices appropriately encrypted?



|  |  |
|---|---|
| Yes | 14,77% |
| No | 71,14% |
| Don´t Know | 14,09% |

# Do you scan for malware before allowing connections to your systems?



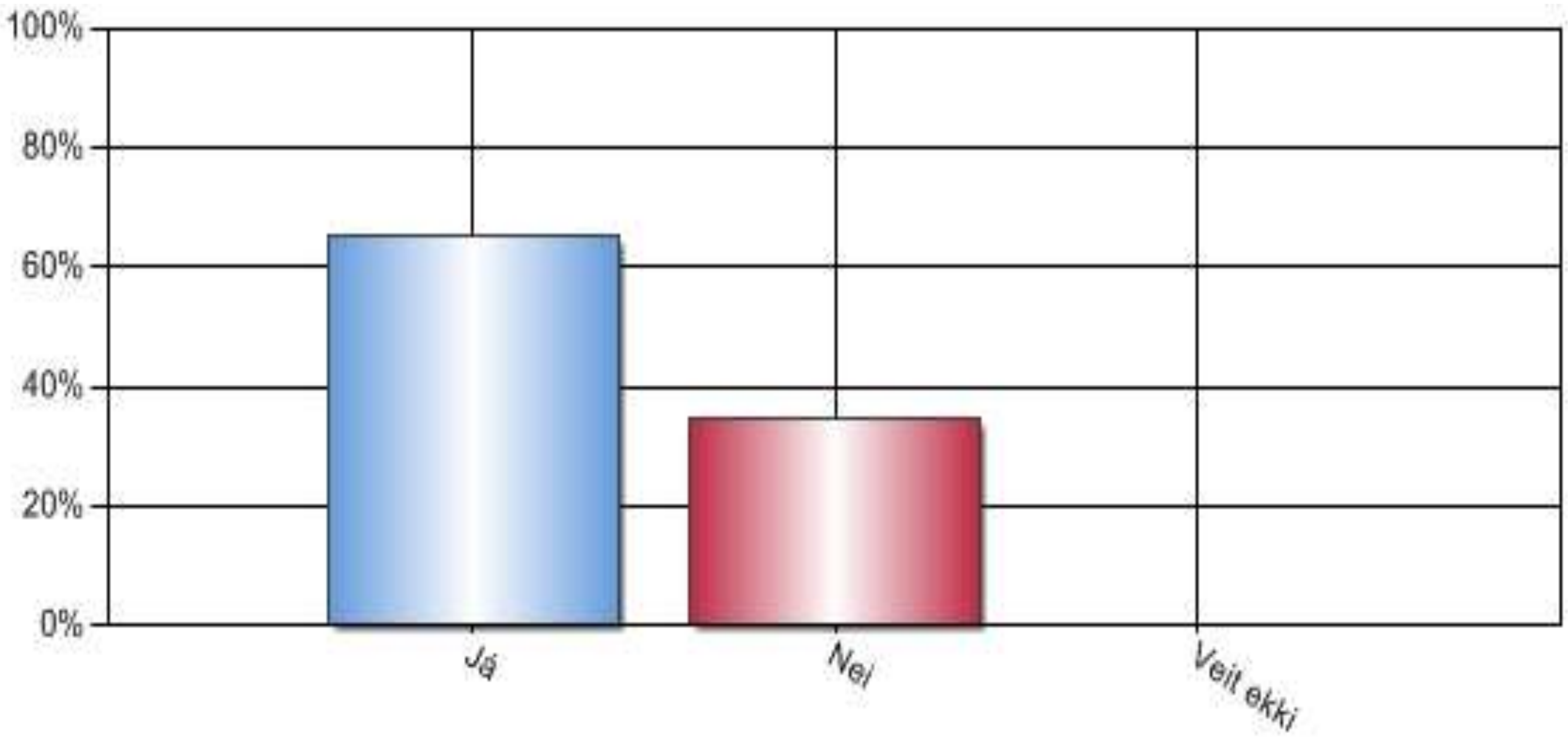
| | |
|---|---|
| Yes | 44,67% |
| No | 41,33% |
| Don´t Know | 14,00% |

# Best Practices

- Provide a firewall capability and install a comprehensive security suite, e.g. McAfee, Symantec
- Limit the use of Administrator accounts
- Keep patches up to date
- Secure mobile devices
  - Physical Security
  - Hard to guess password
  - Consider usage of privacy screens
- Use caution when accessing public hotspot
- In ideal scenario, do not exchange home and work content
- Be wary of storing personal information on the Internet and take precautions on social networking sites
- Unable the use of encryption
  - Consider laptops and USB encryption
  - Encrypted transmission – required for PCI

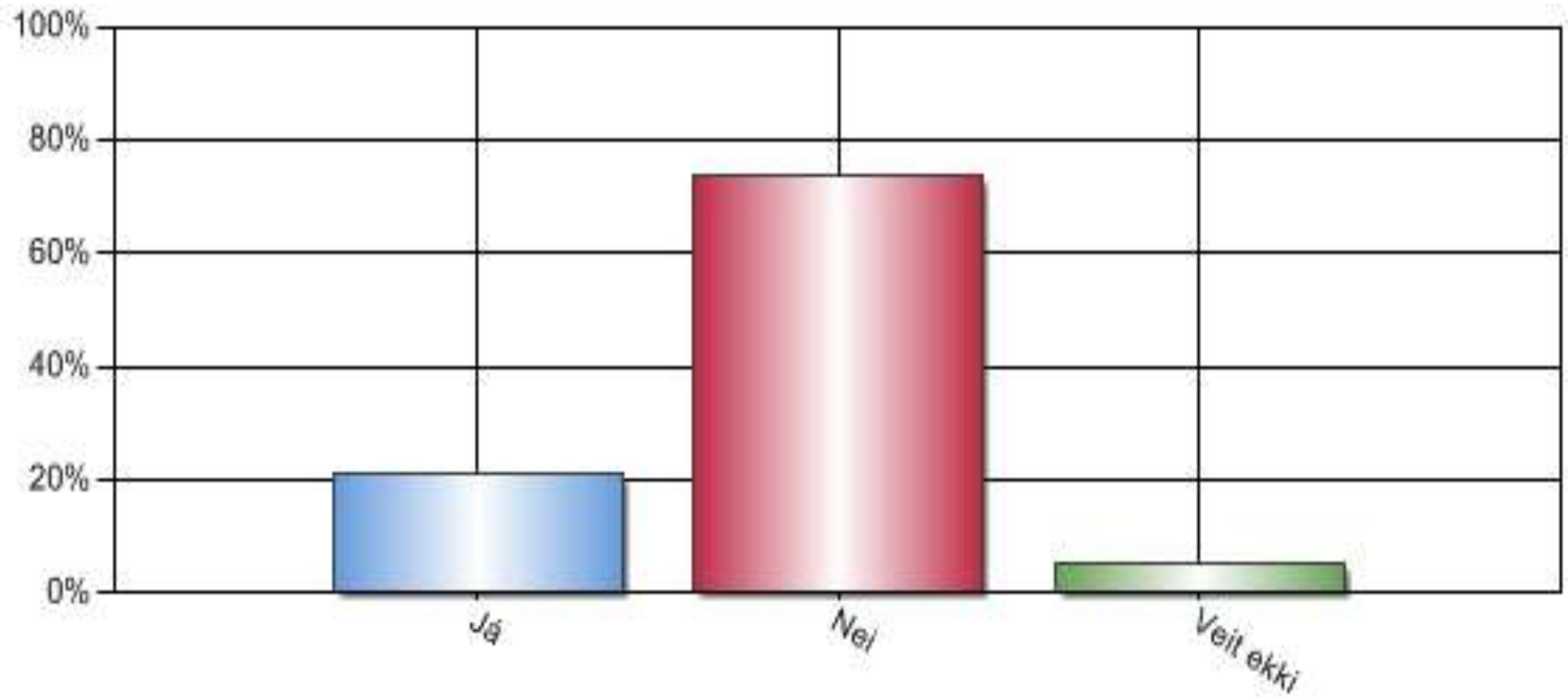
# User Education and Awareness

# Do you have acceptable use policies covering staff use of system and equipment?



| | |
|---|---|
| Yes | 65,10% |
| No | 34,90% |
| Don´t Know | 0,00% |

# Do you have a relevant staff training program?



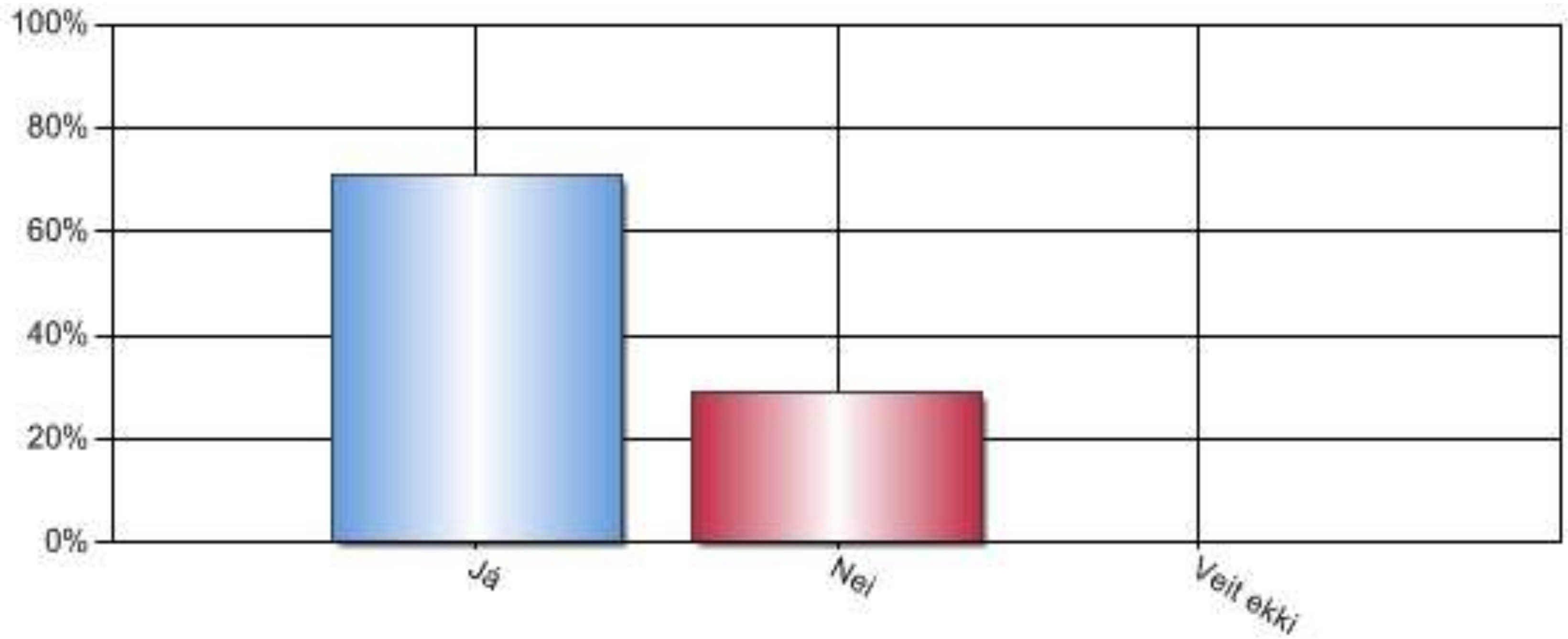
|  |  |
|---|---|
| Yes | 20,81% |
| No | 73,83% |
| Don´t Know | 5,37% |

# Best Practices

- Senior Management support
- Partnering with key departments
- Creativity is a must
- Quarterly plans – Keep it fresh!
    - Security Tip of the Week / Month
- Multimedia awareness materials
    - Desktop Checklist – Deloitte Mousepads example
    - Online Training
    - Videos
    - E-mails

# Access Controls and Privilege Management

# Do you have clear user access management, with a strong password policy and a limited number of privileged accounts?



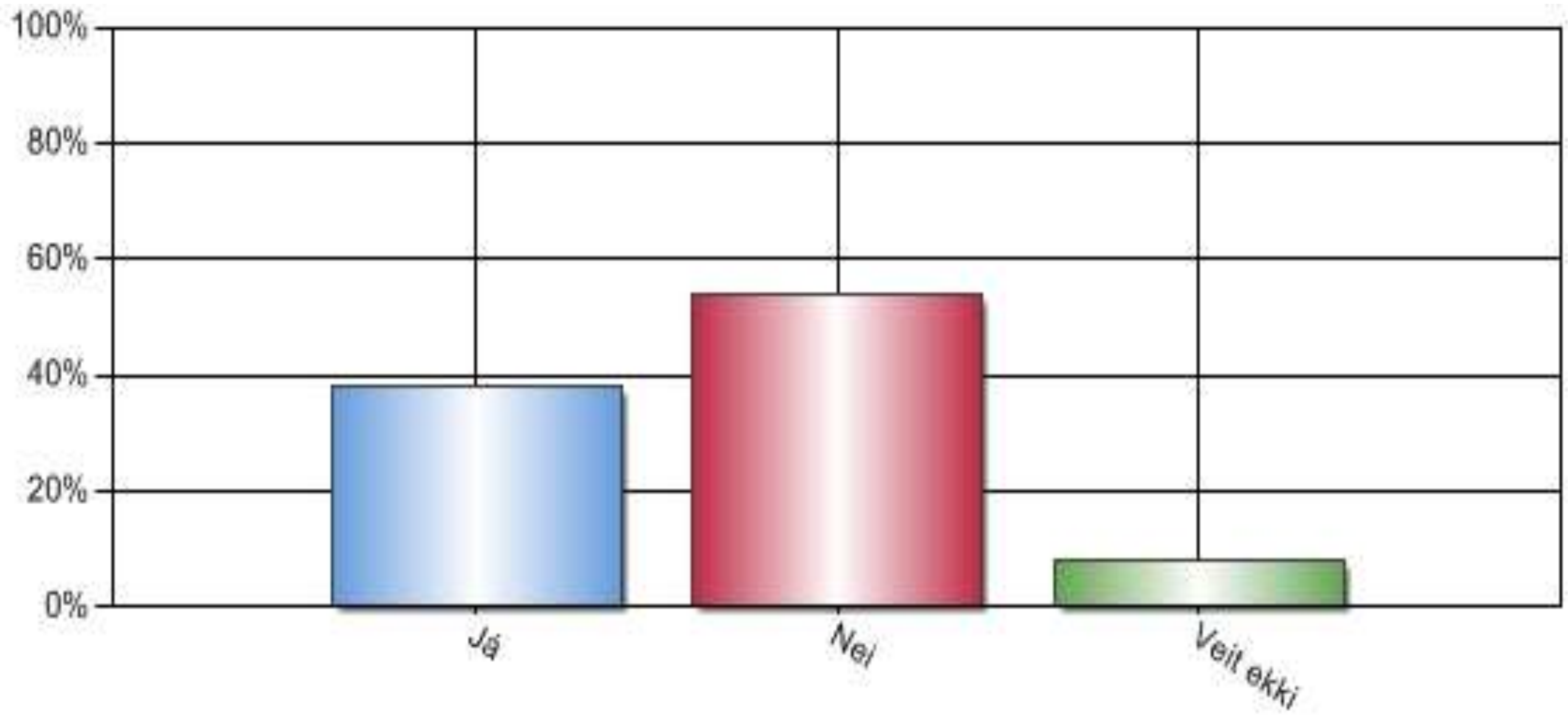
| | |
|---|---|
| Yes | 71,14% |
| No | 28,86% |
| Don´t Know | 0,00% |

# Best Practices

- Limit access to sensitive information
- Access should be granted on a need to know basis
- Password protect sensitive files
- Limit the use of Administrator accounts

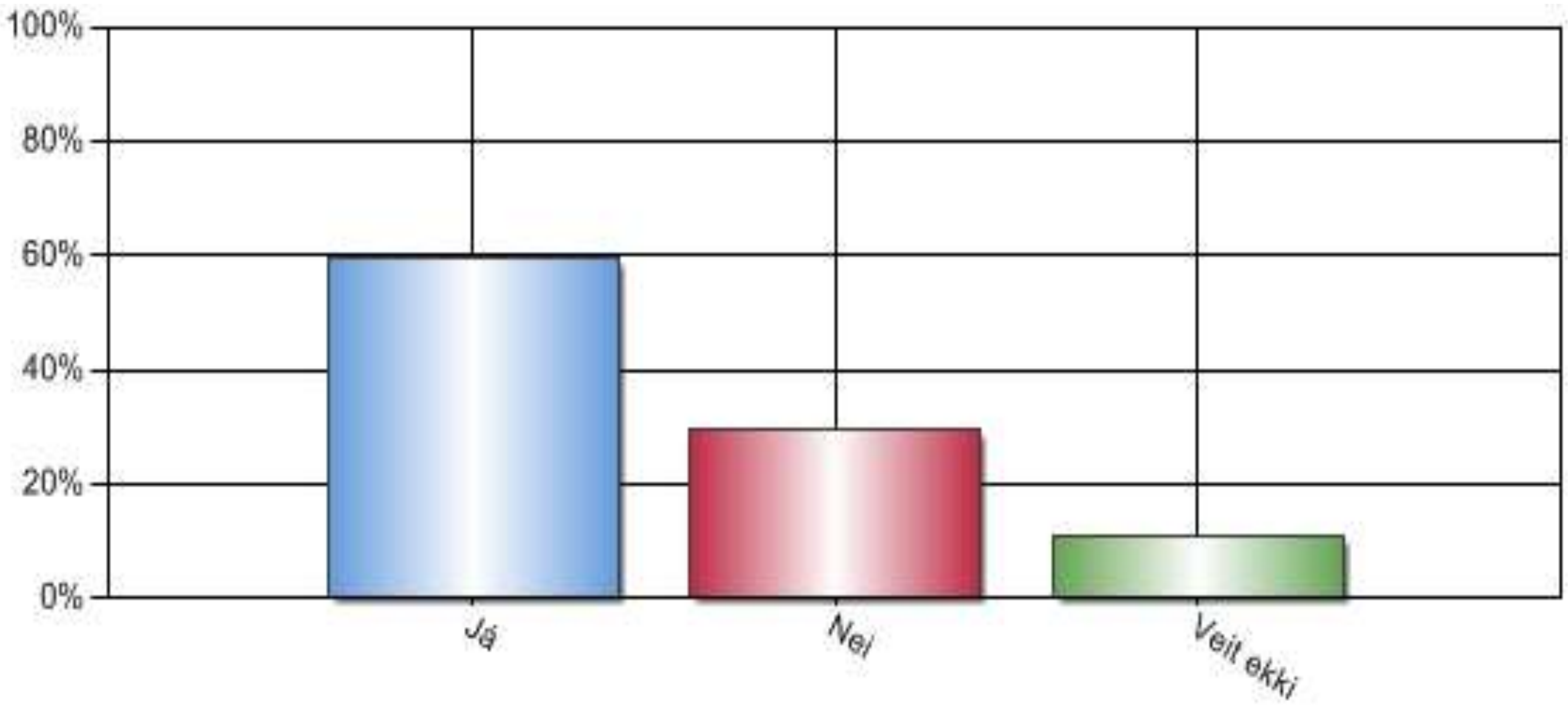
# Activity Monitoring

# Do you monitor user activity?



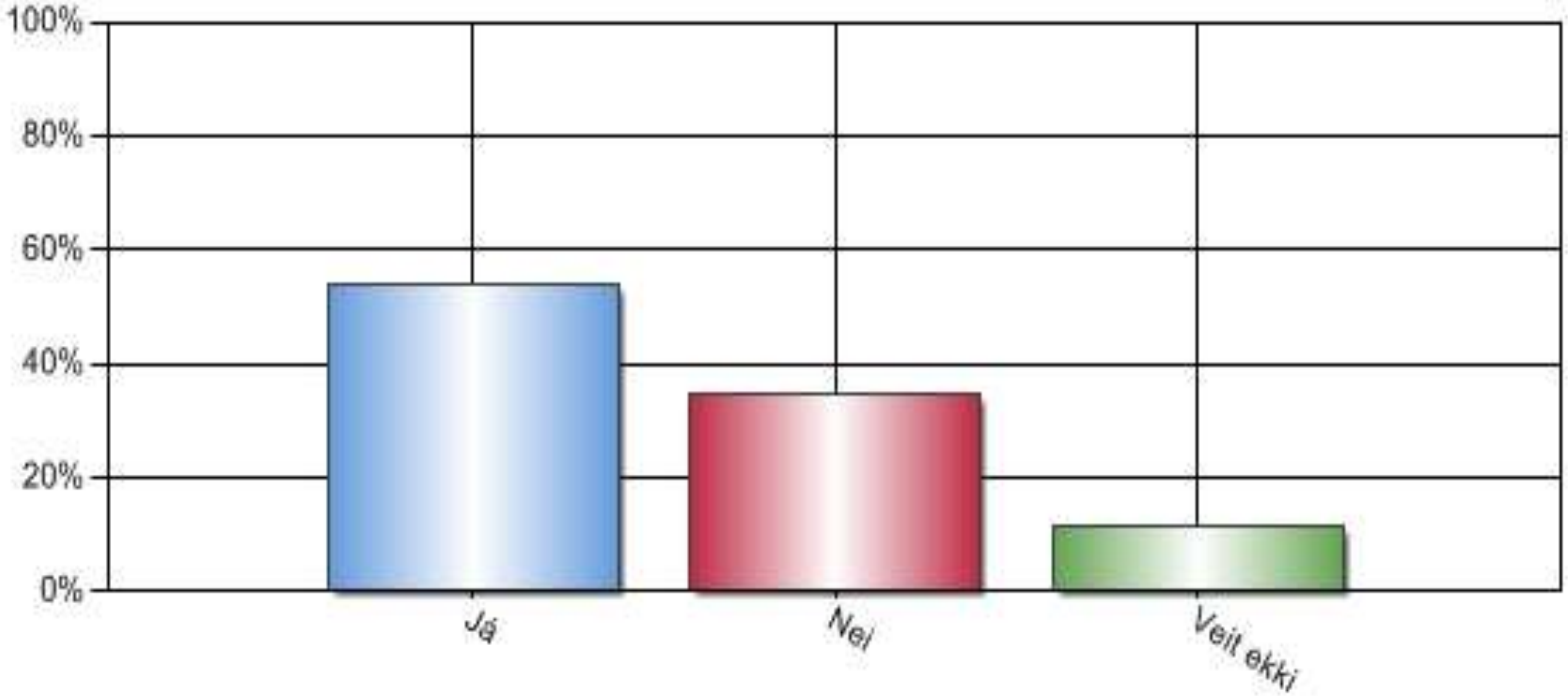
| | |
|---|---|
| Yes | 38,00% |
| No | 54,00% |
| Don´t Know | 8,00% |

# Do you have and review activity and audit logs?



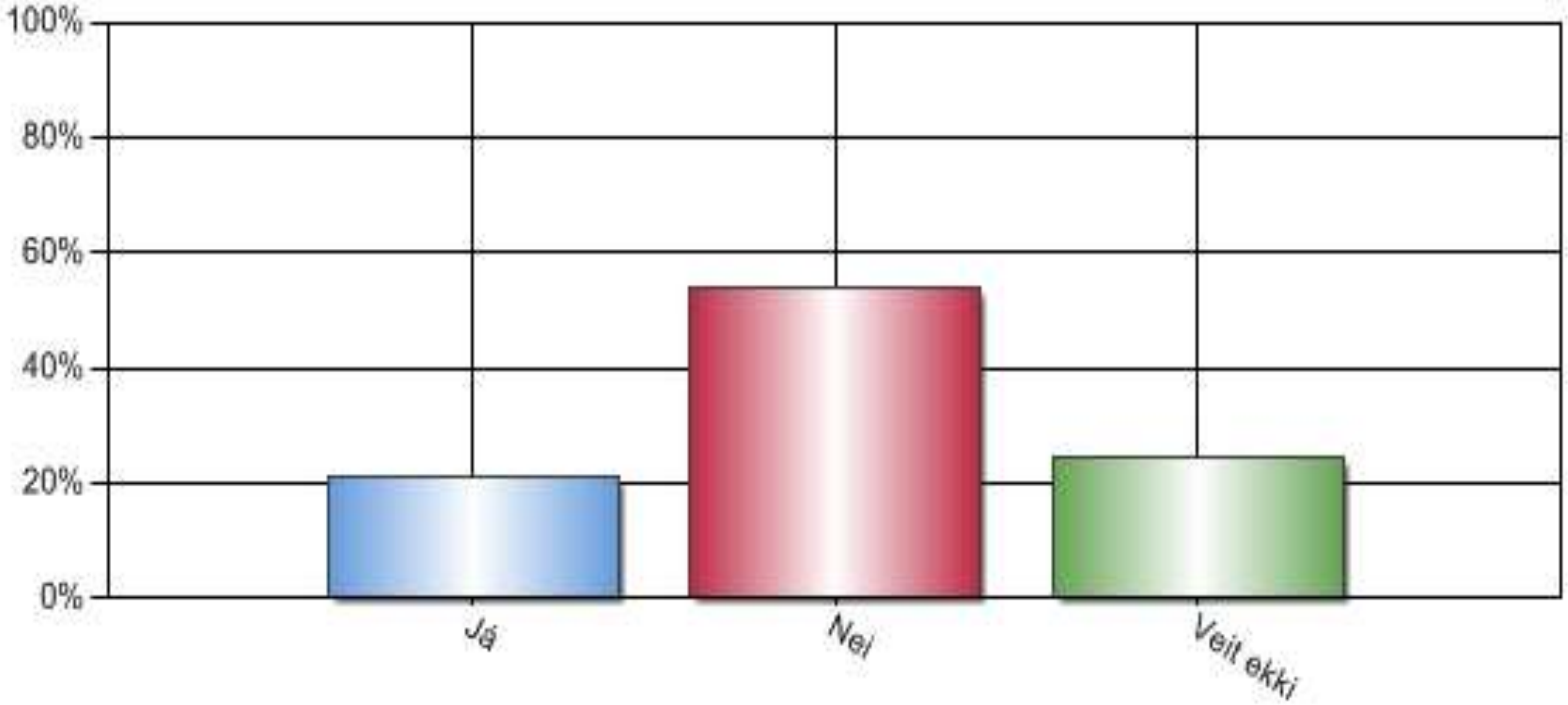
| | |
|---|---|
| Yes | 59,73% |
| No | 29,53% |
| Don´t Know | 10,74% |

# Do you continuously monitor activity on IT systems and networks, including for rogue wireless access points?



|  |  |
|---|---|
| Yes | 53,74% |
| No | 34,69% |
| Don´t Know | 11,56% |

# Do you analyze network logs in real time, looking for evidence of mounting attacks?



|  |  |
|---|---|
| Yes | 21,33% |
| No | 54,00% |
| Don´t Know | 24,67% |

# Best Practices

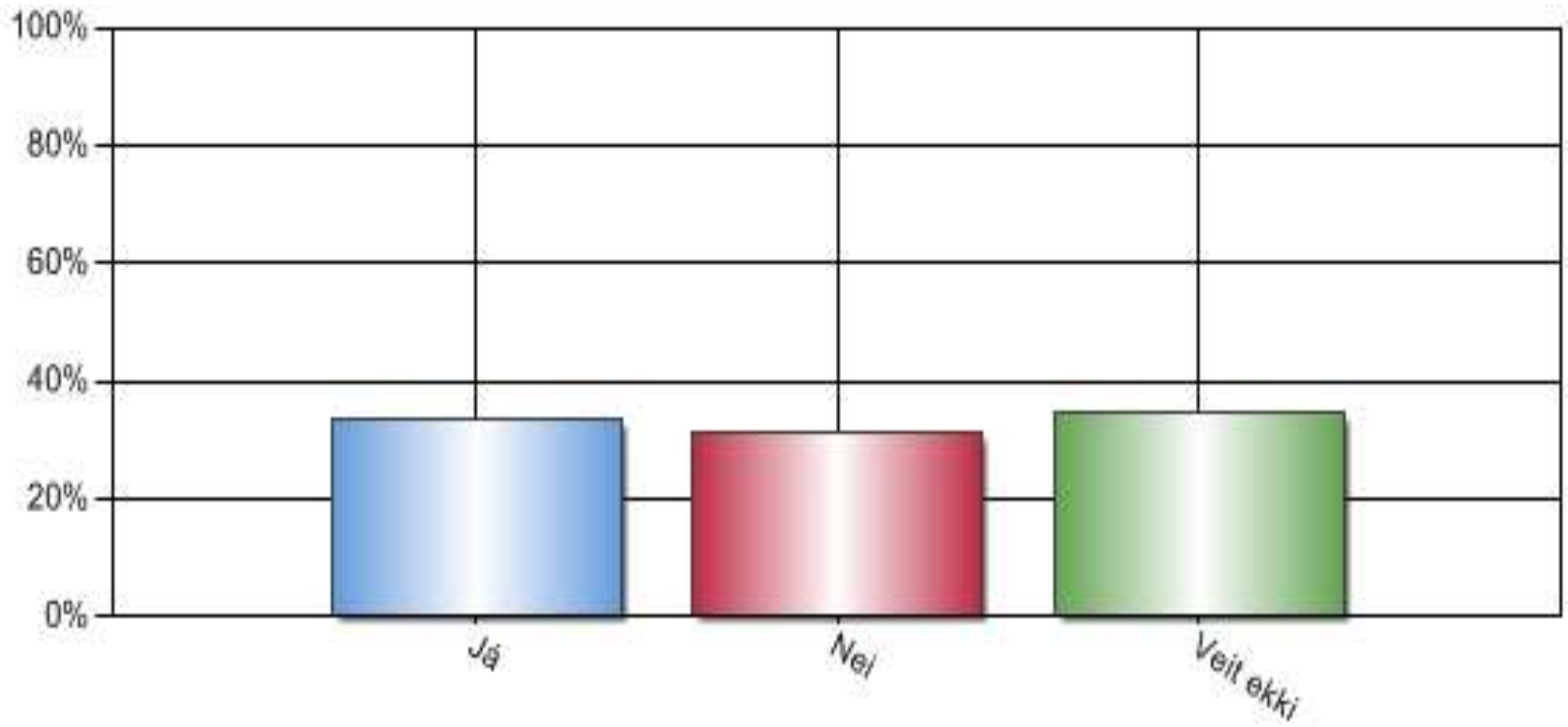
- Audit logs should be reviewed periodically

- Monitor usage and block content
  - Inform employees you're tracking their Internet usage. It will deter them from going to inappropriate sites, improve productivity and let them know exactly where the company stands.
  - Decide if you need to track sites visited or go a step further and block access to certain URLs.

- In addition to making users more productive and keeping them off inappropriate sites, web monitoring is also useful for blocking sites that produce malware.

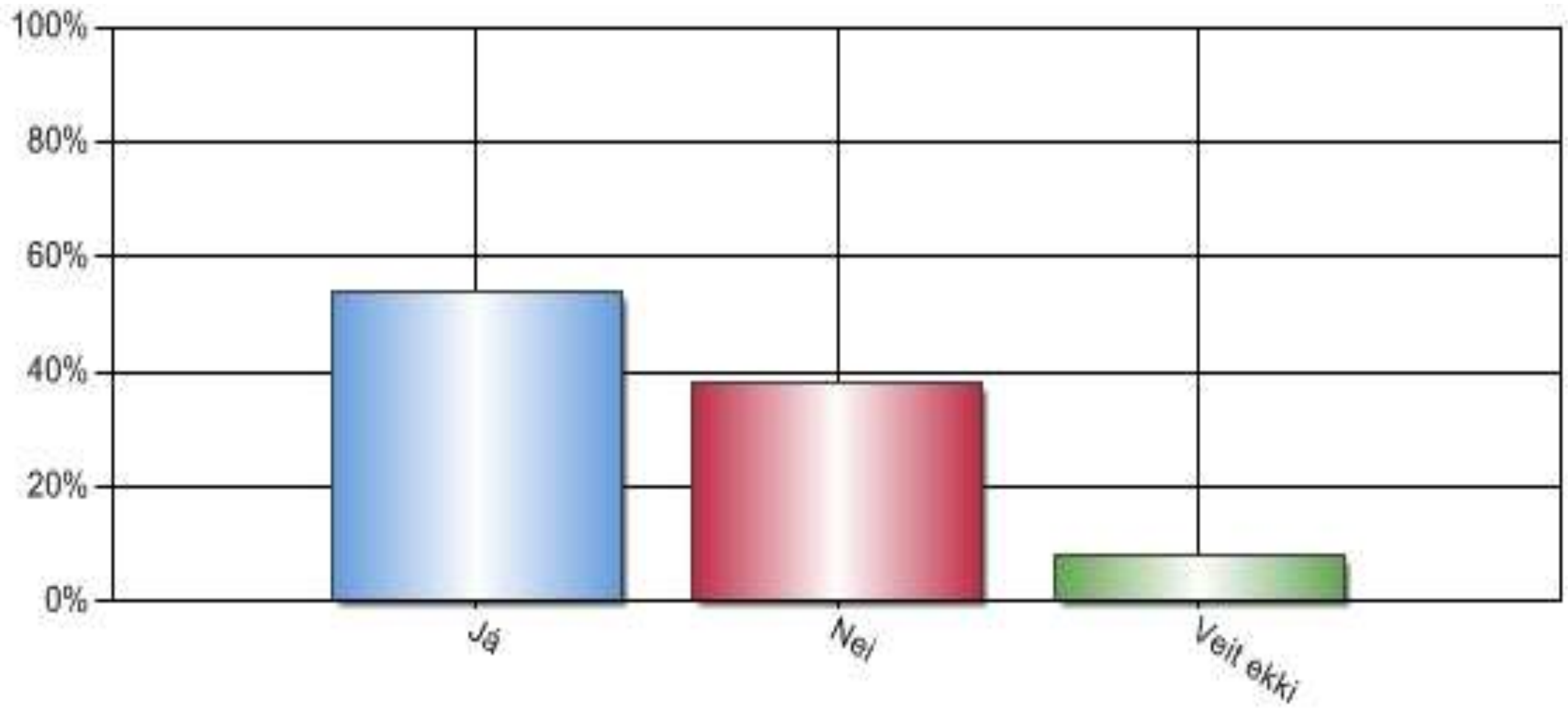
# Secure Configurations

# Are your IT devices configured for maximum security?



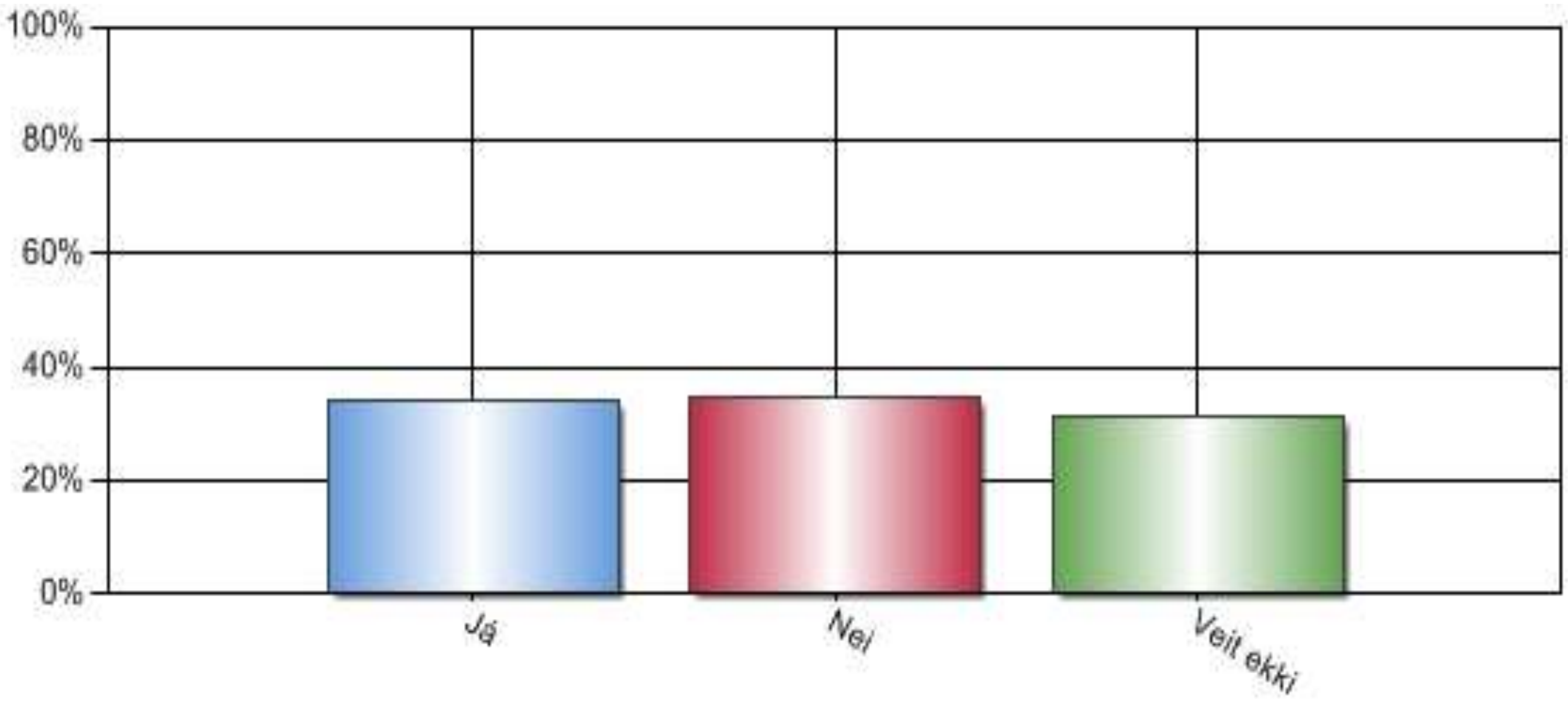
| | |
|---|---|
| Yes | 33,56% |
| No | 31,54% |
| Don´t Know | 34,90% |

# Do you have an asset inventory of authorized devices?



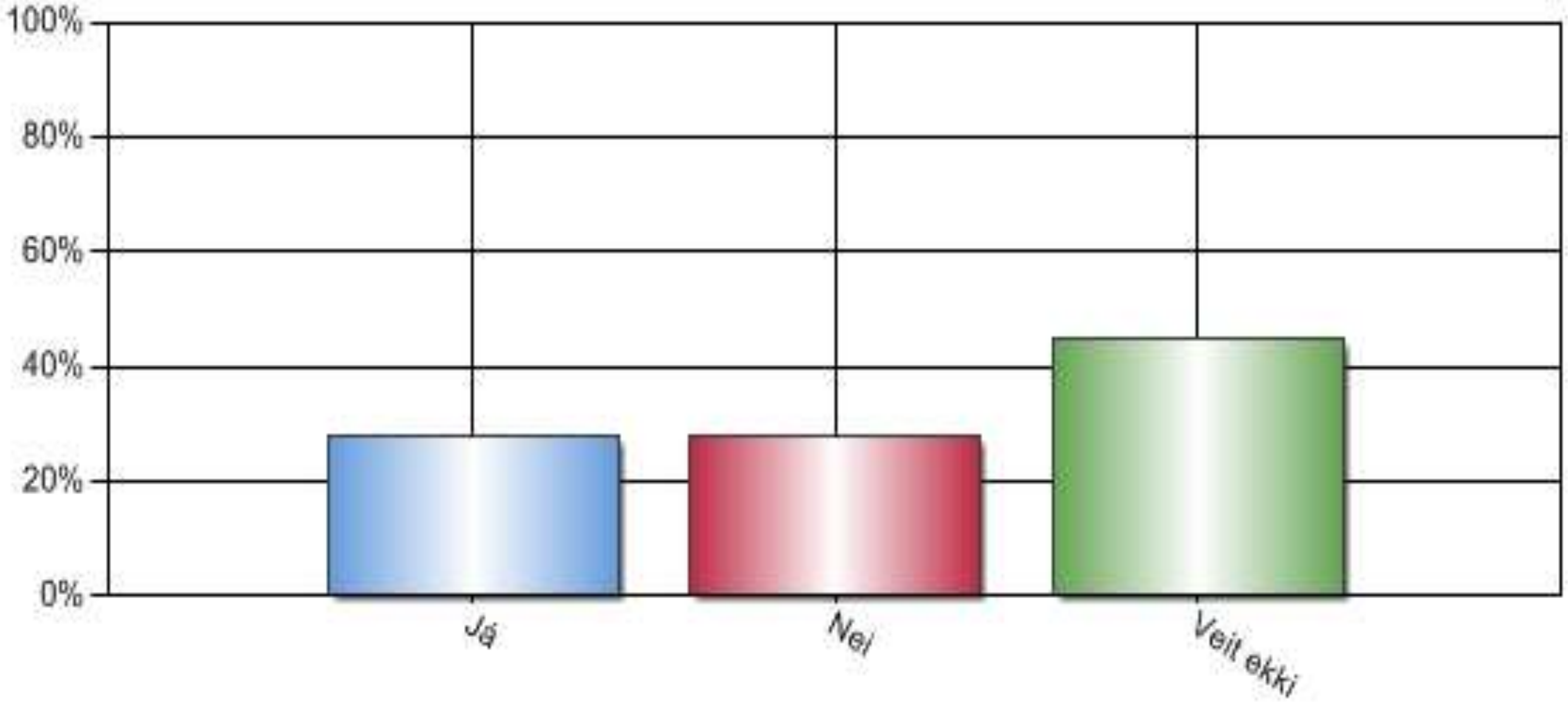
| | |
|---|---|
| Yes | 53,69% |
| No | 38,26% |
| Don´t Know | 8,05% |

# Do you have a standard build for all approved equipment?



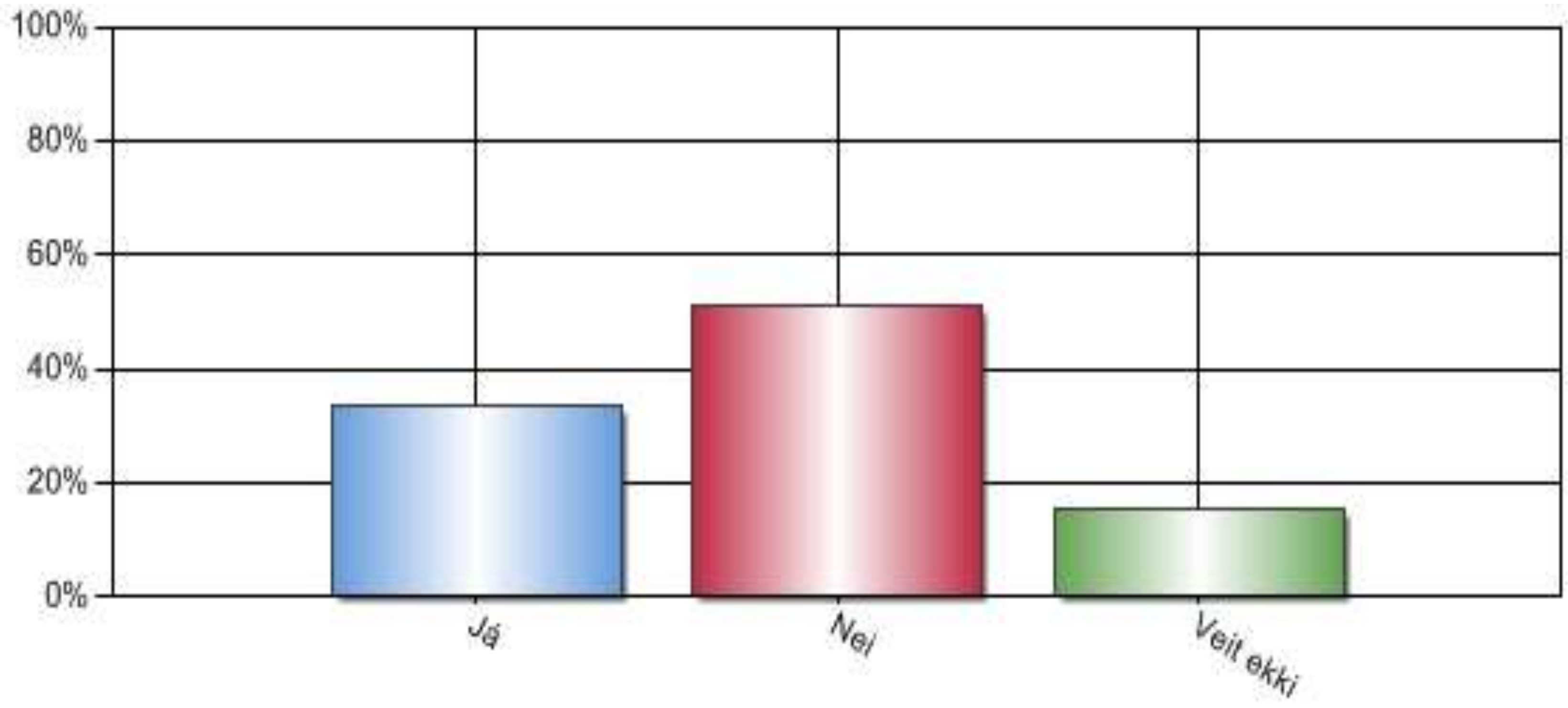
| | |
|---|---|
| Yes | 34,01% |
| No | 34,69% |
| Don´t Know | 31,29% |

# Do you have a technical vulnerability patching program in place and is it up-to-date?



| | |
|---|---|
| Yes | 27,70% |
| No | 27,70% |
| Don´t Know | 44,59% |

# Do you continuously scan for new technical vulnerabilities?



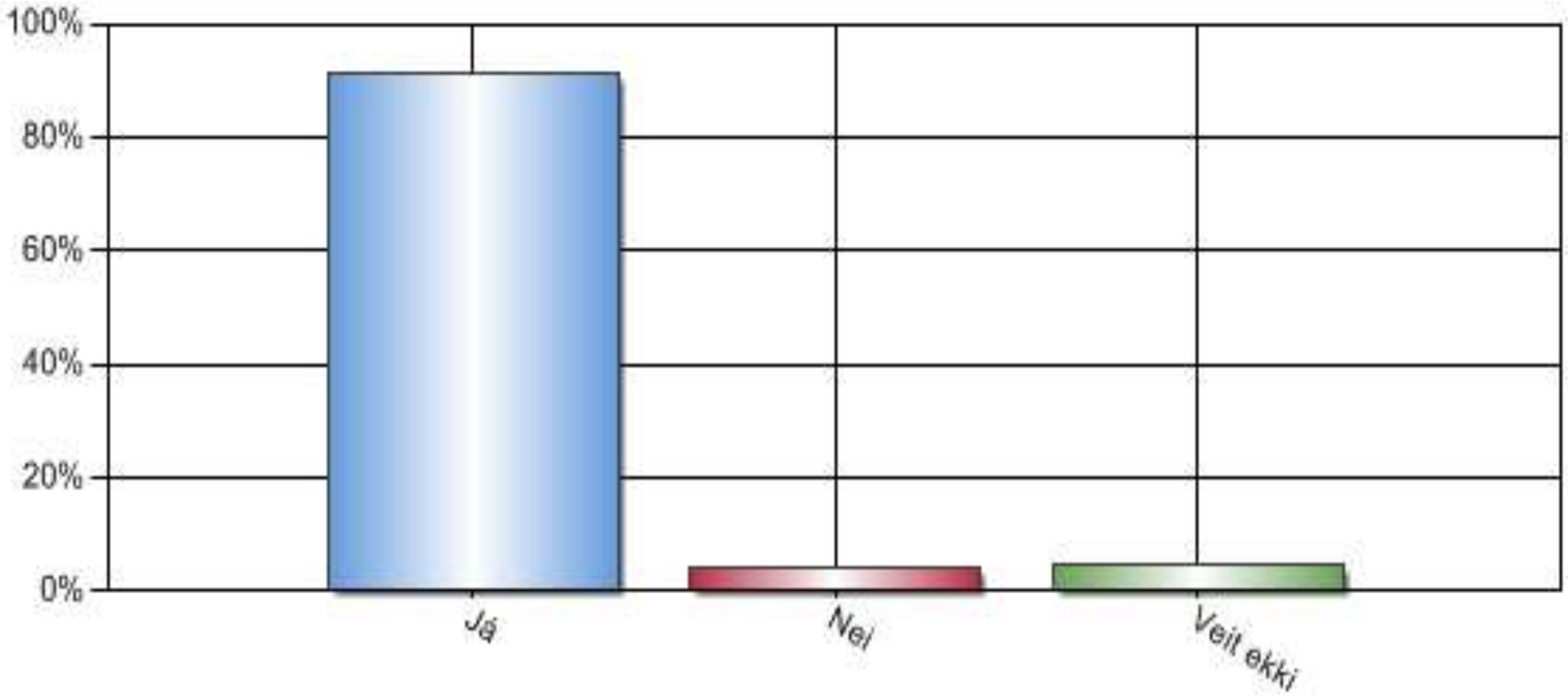
| | |
|---|---|
| Yes | 33,33% |
| No | 51,02% |
| Don´t Know | 15,65% |

# Best Practices

- Maintain an asset inventory
- Consider using security benchmarks for standard builds
  - Good source: benchmarks.cisecurity.org
- Apply the latest patch(es) on a regular basis and keep up date
  - Make sure patches are tested before implementing
- Run patch management software at least once a month to check for unpatched computers
- Scan for technical vulnerabilities on a regular basis, e.g. Nessus, Qualys

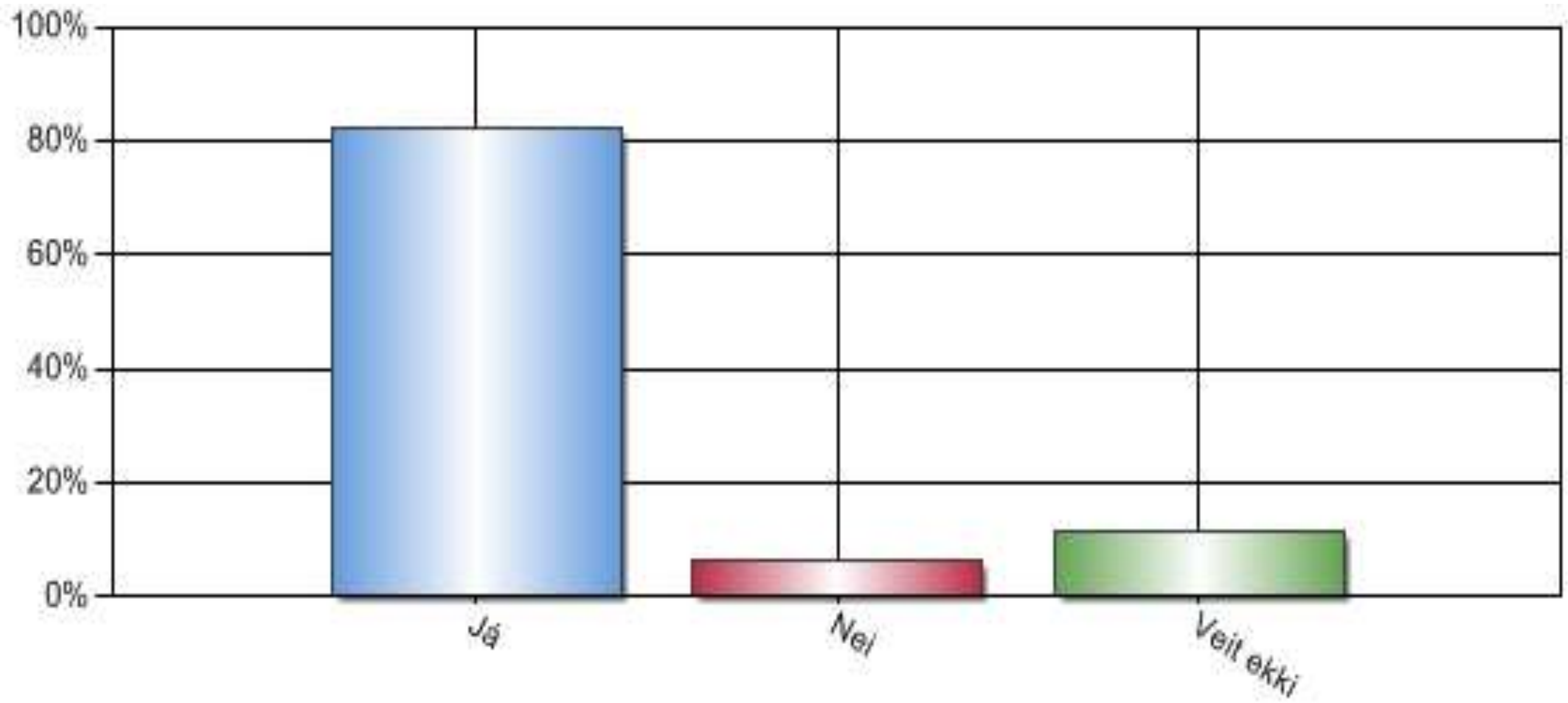
# Virus and other Malware Protection

# Do you have an anti-malware policy and practices that are effective against likely threats?



| | |
|---|---|
| Yes | 91,10% |
| No | 4,11% |
| Don´t Know | 4,79% |

# Do you continuously scan the network and attachments for malware?



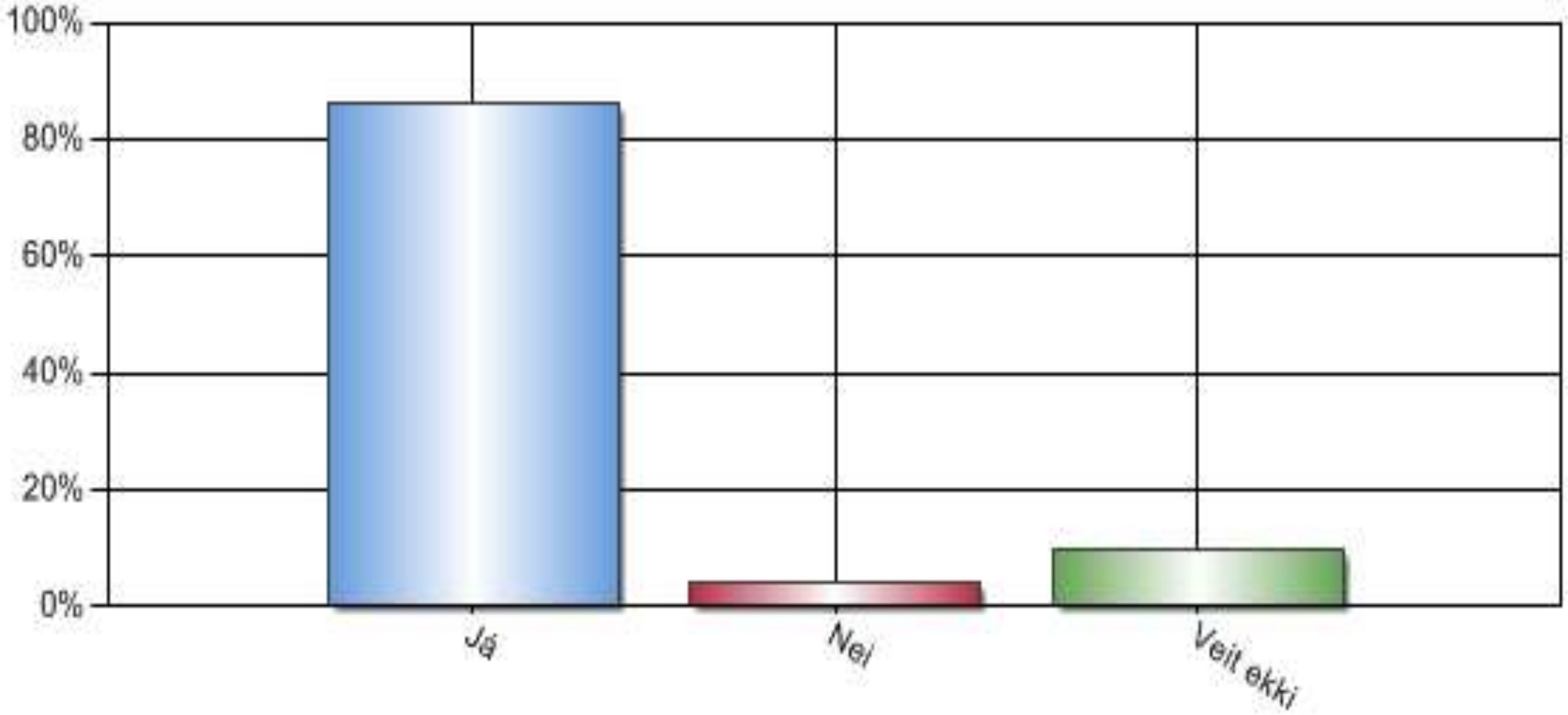
| | |
|---|---|
| Yes | 82,43% |
| No | 6,08% |
| Don´t Know | 11,49% |

## Best Practices

- Install an antivirus application and/or a comprehensive security suite, e.g. McAfee, Symantec
- Use anti-spyware application
- Educate users not to click on links they do not trust
- Do not open suspicious links or files especially from instant messengers, emails from unidentified users and from pop-up windows
- Educate users for possible phishing attacks

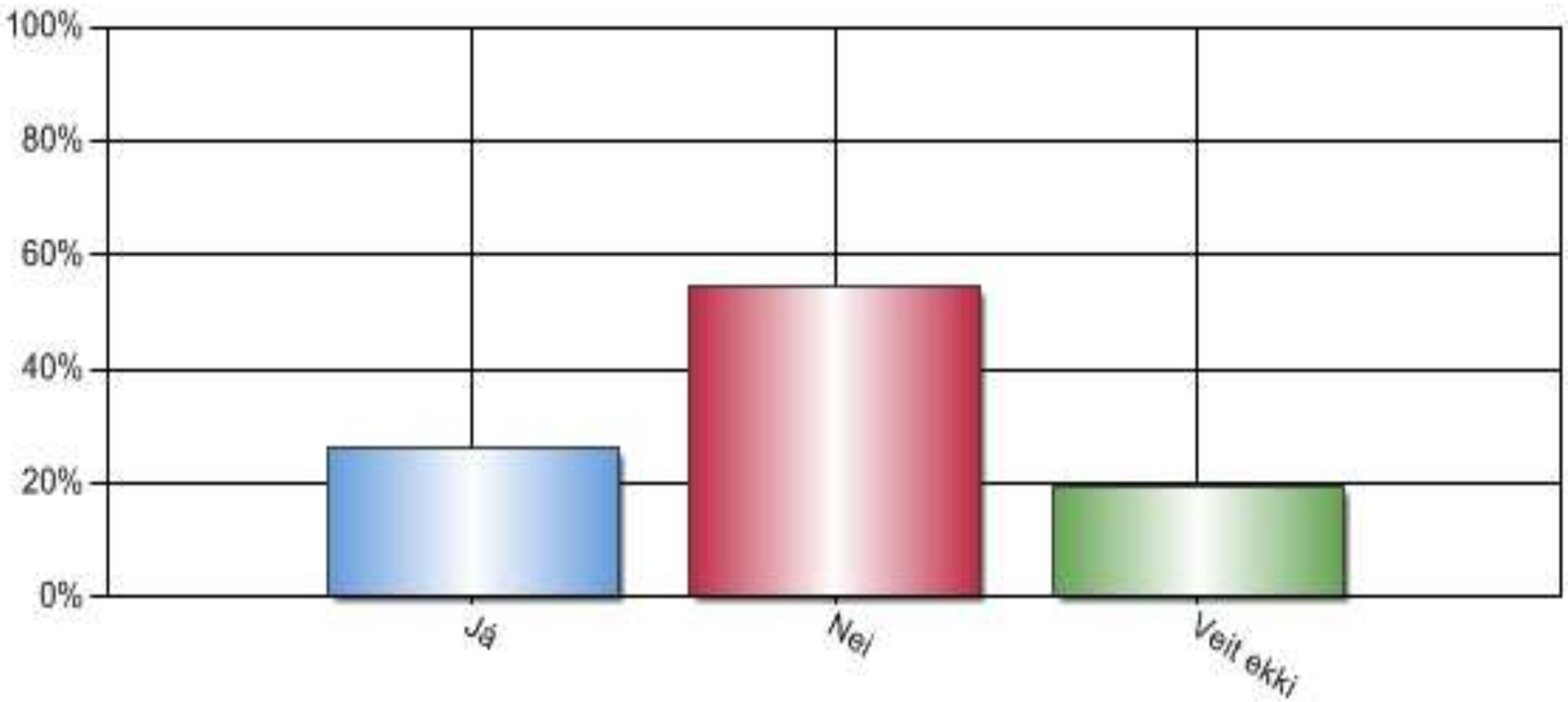
# Network Security

# Do you protect your networks against internal and external attacks with routers and firewalls?



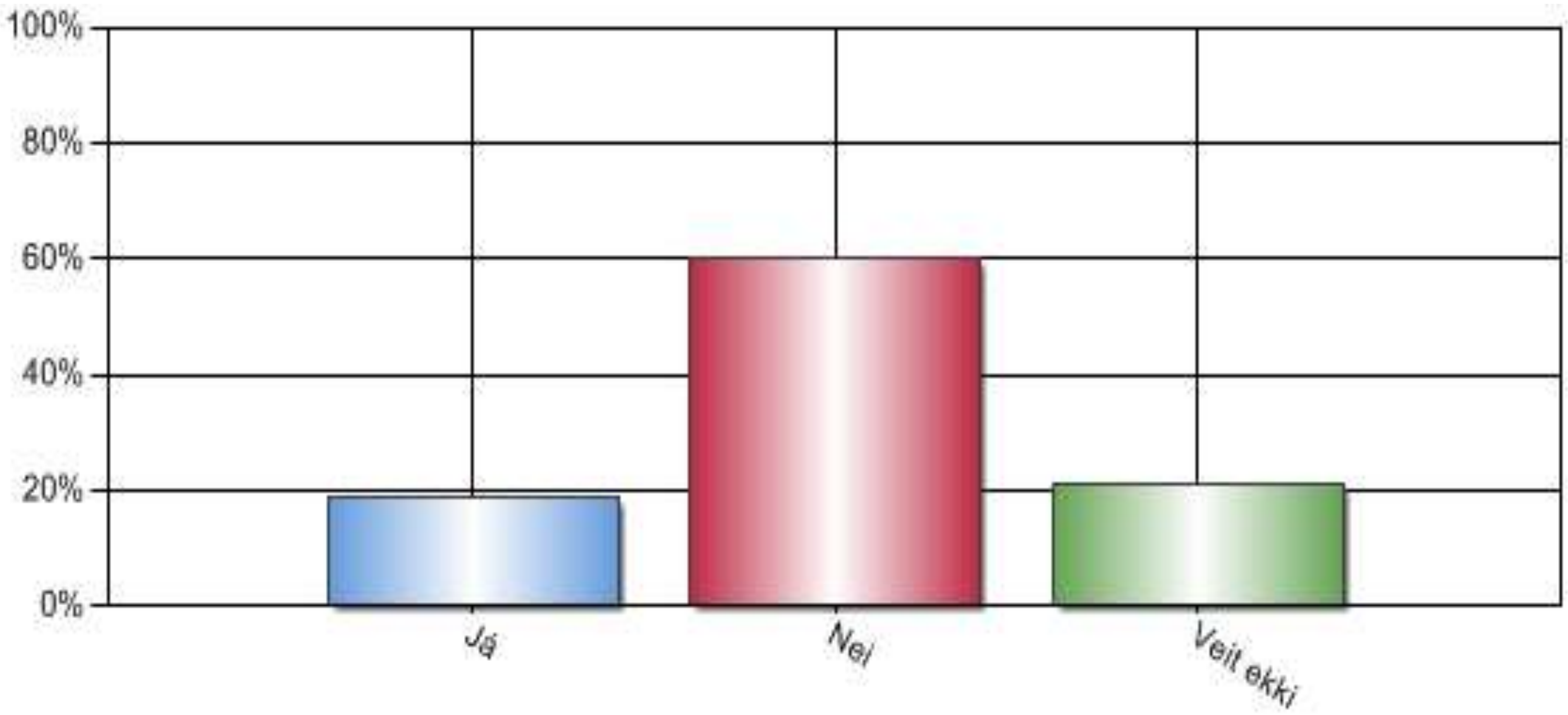
| | |
|---|---|
| Yes | 86,30% |
| No | 4,11% |
| Don´t Know | 9,59% |

# Have you conducted a vulnerability testing?



| | |
|---|---|
| Yes | 26,17% |
| No | 54,36% |
| Don´t Know | 19,46% |

# Have you conducted a penetration testing?



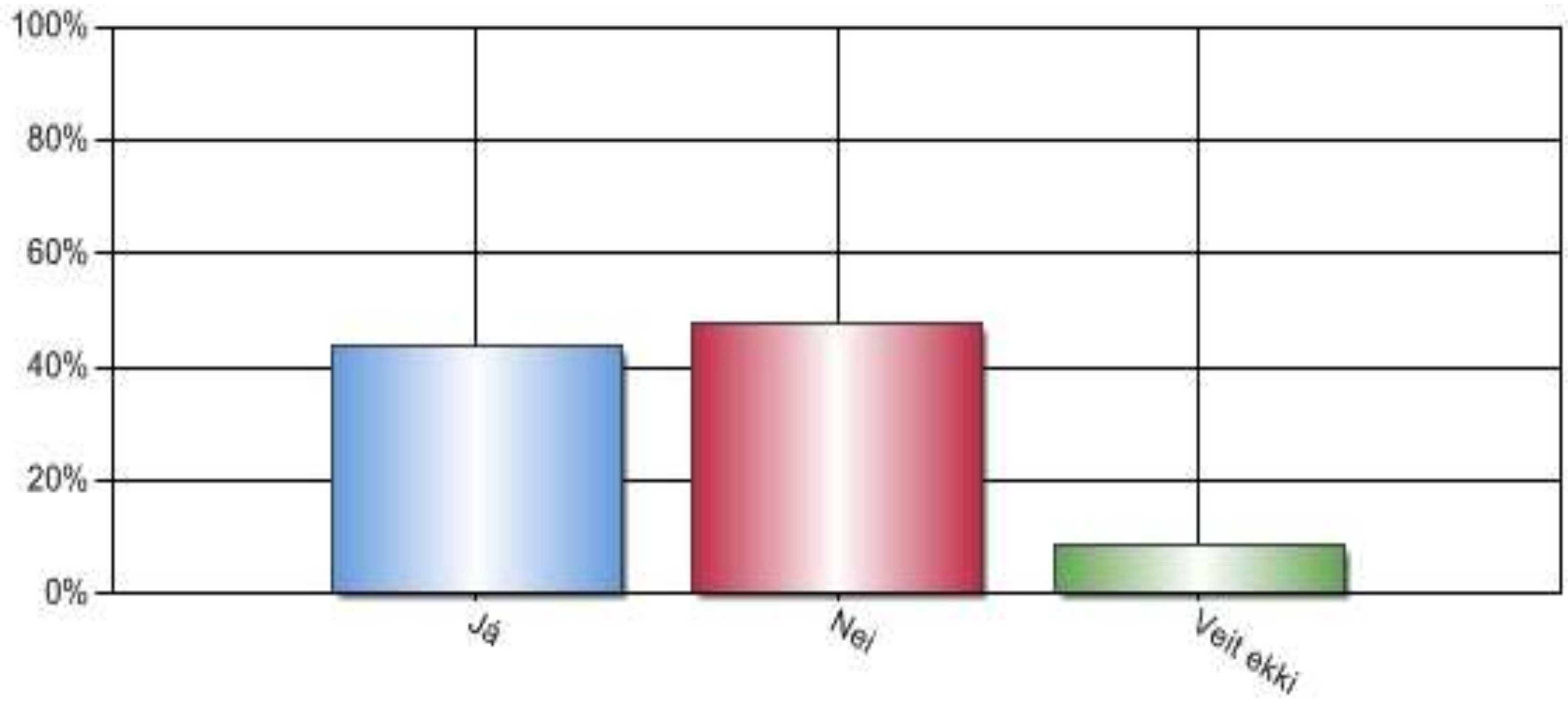
| | |
|---|---|
| Yes | 18,92% |
| No | 60,14% |
| Don´t Know | 20,95% |

# Best Practices

- Use routers and firewalls
- Review and audit routers and firewall configuration and access controls on a regular basis
- Conduct a vulnerability assessment on a periodic basis
  - PCI requires quarterly
- Conduct a penetration testing on a periodic basis
  - PCI requires annually

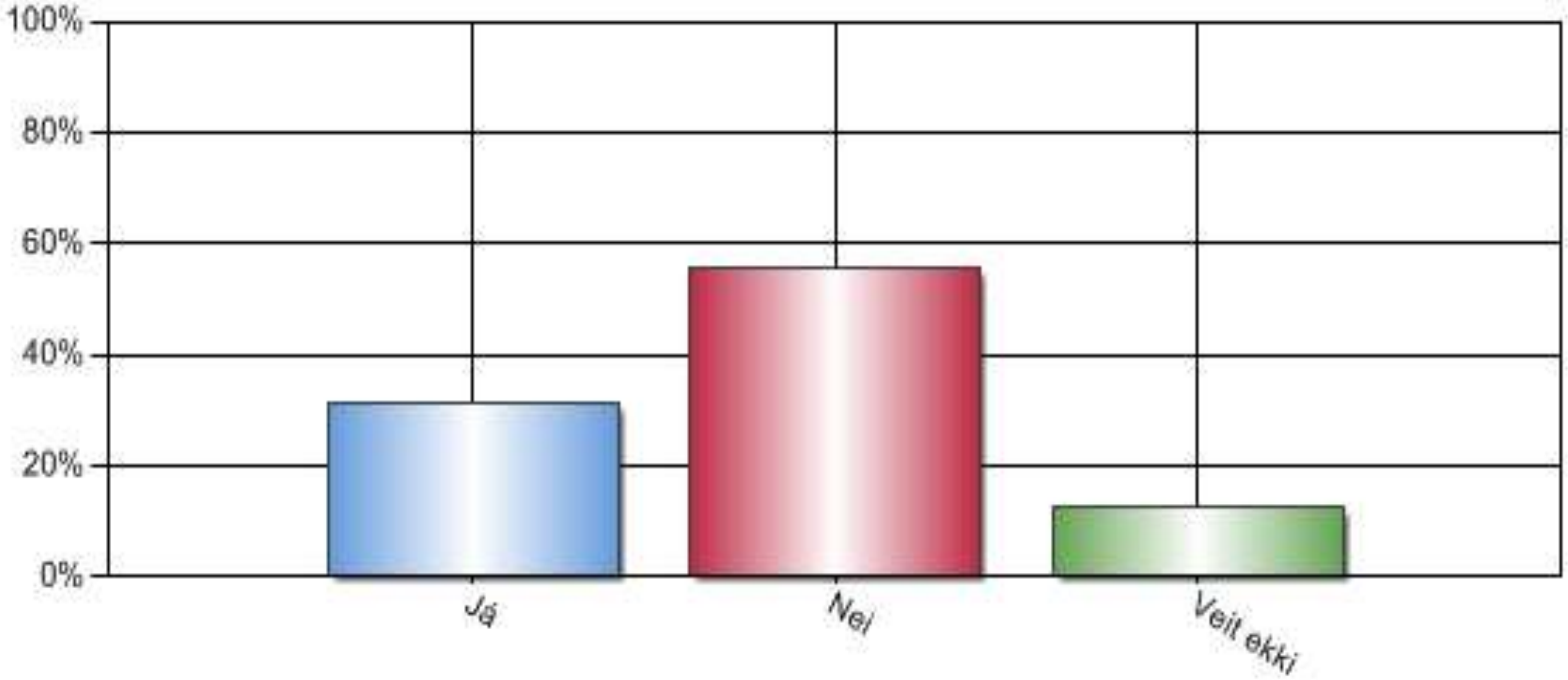
# Business Continuity and Incident Management

# Do you have an incident response and disaster recovery plan?



| | |
|---|---|
| Yes | 43,62% |
| No | 47,65% |
| Don´t Know | 8,72% |

# Is the Disaster Recovery Plan tested and/or audited for readily identifiable compromise scenarios?



| | |
|---|---|
| Yes | 31,54% |
| No | 55,70% |
| Don´t Know | 12,75% |

# Best Practices

- Define a team structure
- Establish a plan
- Test for incident handling, business continuity and disaster recovery
- Create a crisis communications strategy
- Educate people on safety procedures

**Worth Noting:**

- All critical infrastructure will be required to report a breach to Póst- og fjarskiptastofnun (PFS).
- In EU Data Protection Regulation, when personal data breach, companies shall without undue delay notify the personal data breach to Persónuvernd.
- Persónuvernd shall keep a public register of the types of breaches notified

# Penalties with Upcoming EU Data Protection Regulation

- To anyone who does not comply with the obligations laid down in the EU Data Protection Regulation, Persónuvernd shall impose at least one of the following sanctions:
  - a warning in writing in cases of first and non-intentional non-compliance;
  - regular periodic data protection audits;
  - a fine up to 100,000,000 EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater.

# Questions ?

Deloitte.

“Deloitte” is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, and tax services to selected clients. These firms are members of Deloitte Touche Tohmatsu Limited (DTTL), a UK private company limited by guarantee. Each member firm provides services in a particular geographic area and is subject to the laws and professional regulations of the particular country or countries in which it operates. DTTL does not itself provide services to clients. DTTL and each DTTL member firm are separate and distinct legal entities, which cannot obligate each other. DTTL and each DTTL member firm are liable only for their own acts or omissions and not those of each other. Each DTTL member firm is structured differently in accordance with national laws, regulations, customary practice, and other factors, and may secure the provision of professional services in its territory through subsidiaries, affiliates, and/or other entities.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 200,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entitites (collectively, the “Deloitte Network”) is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.