NSDL
Technology, Trust & Reach
Celebrating 20 Years

Technical Task Force

Presentation on Cyber Resilience Survey

May 2018

Cyber Resilience Survey

Objectives

A survey was conducted covering some key dimensions of Cyber Security.

Governance

Technology

Security Awareness

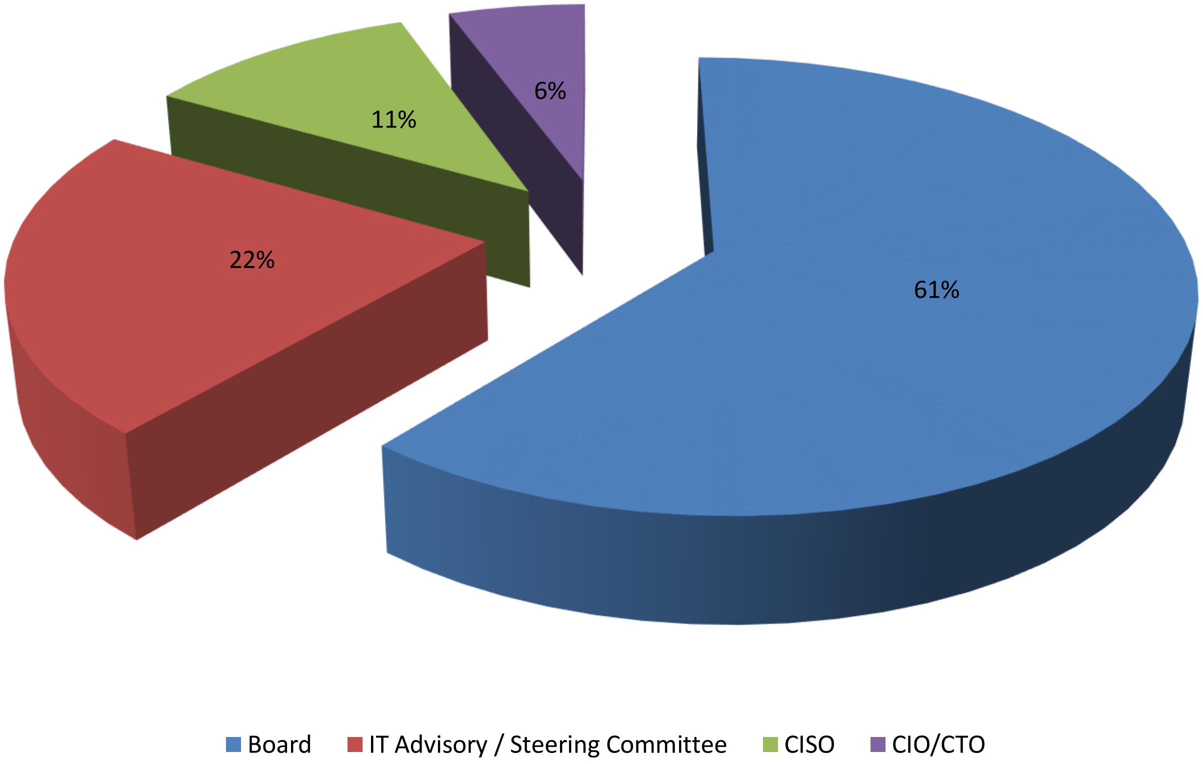
Incident Management

The responses were collated and analysed. They are being summarized in the following slides.

Cyber Resilience Survey

Governance

- **Tone from the top- Security is a topic of Boardroom Discussion**

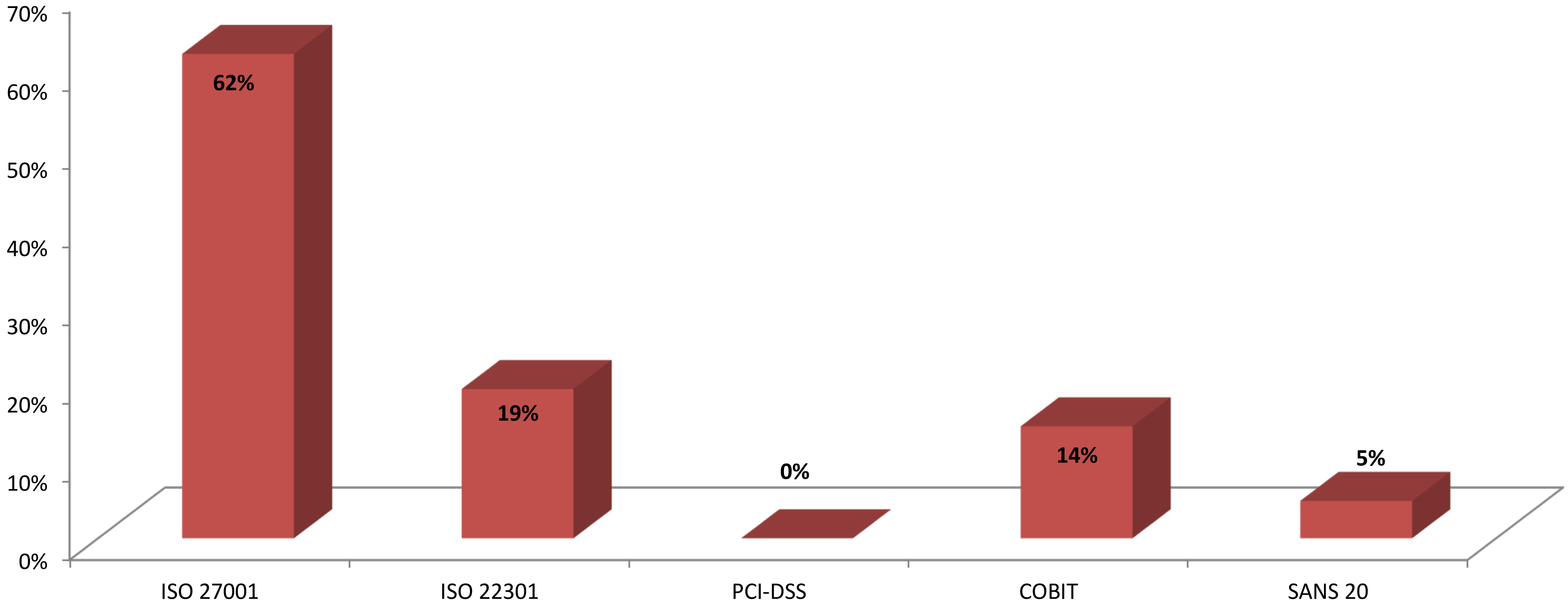


Maximum respondents have agreed to have multiple levels of approving authority. 59% of respondents have mentioned “Board” as the approving authority.

Cyber Resilience Survey

Governance

- **Security de-facto standard**

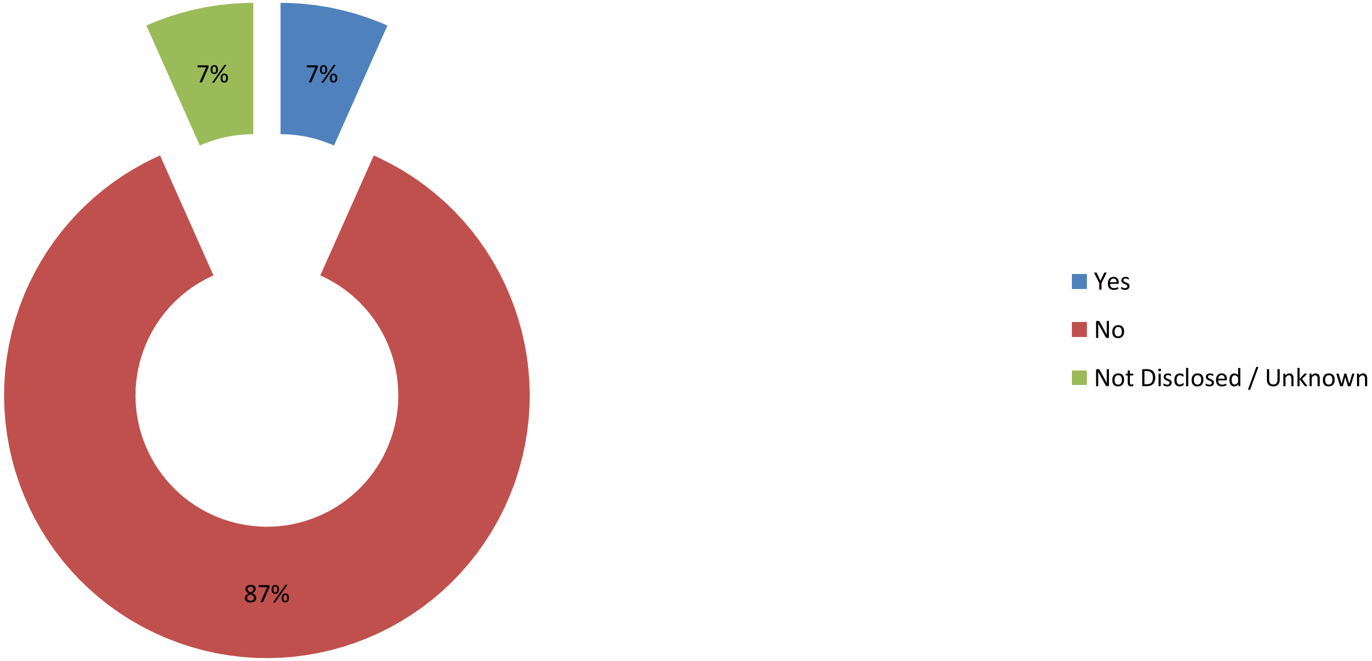


Most of us use ISO 27001 as the guiding standard for Security

Cyber Resilience Survey

Governance

- **Security Technologies adoption - Deception**

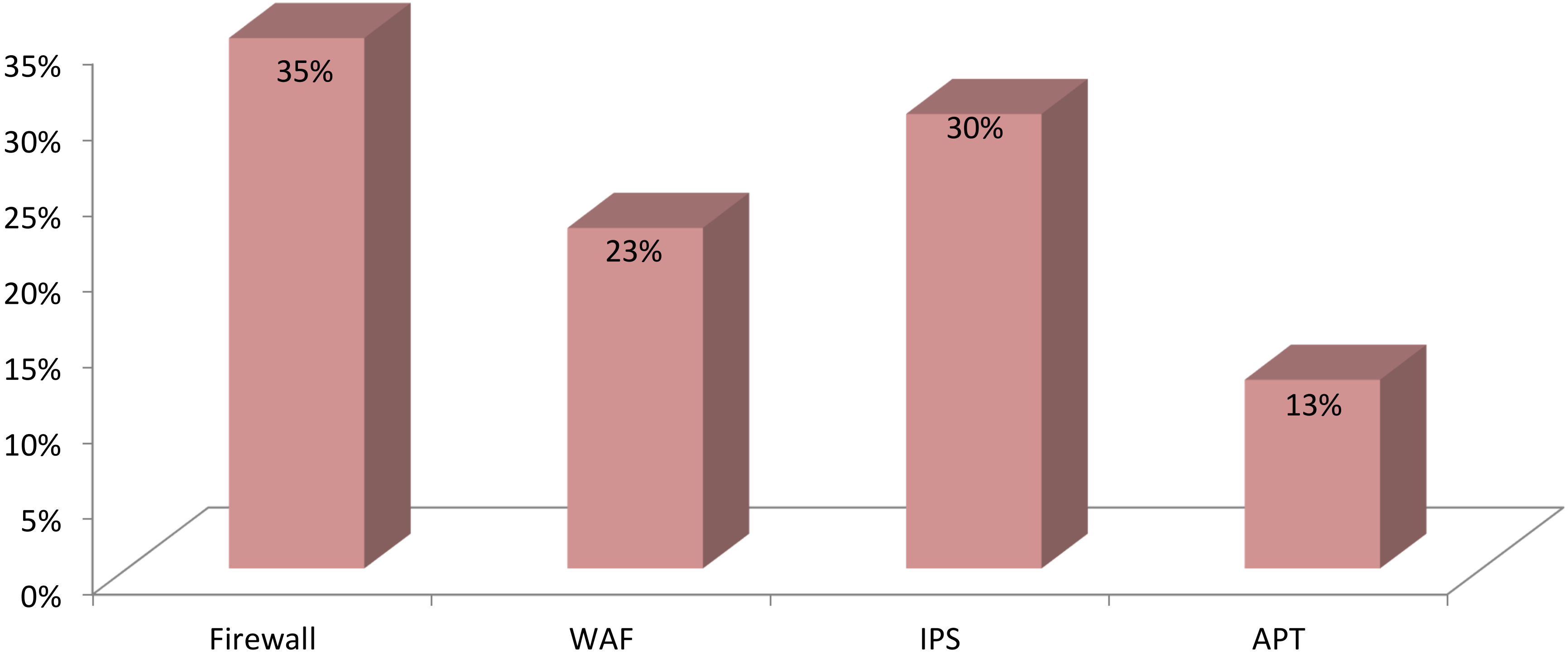


Deception and Decoy in the security arena is yet to gather momentum

Cyber Resilience Survey

Technology

- **Security Infrastructure**

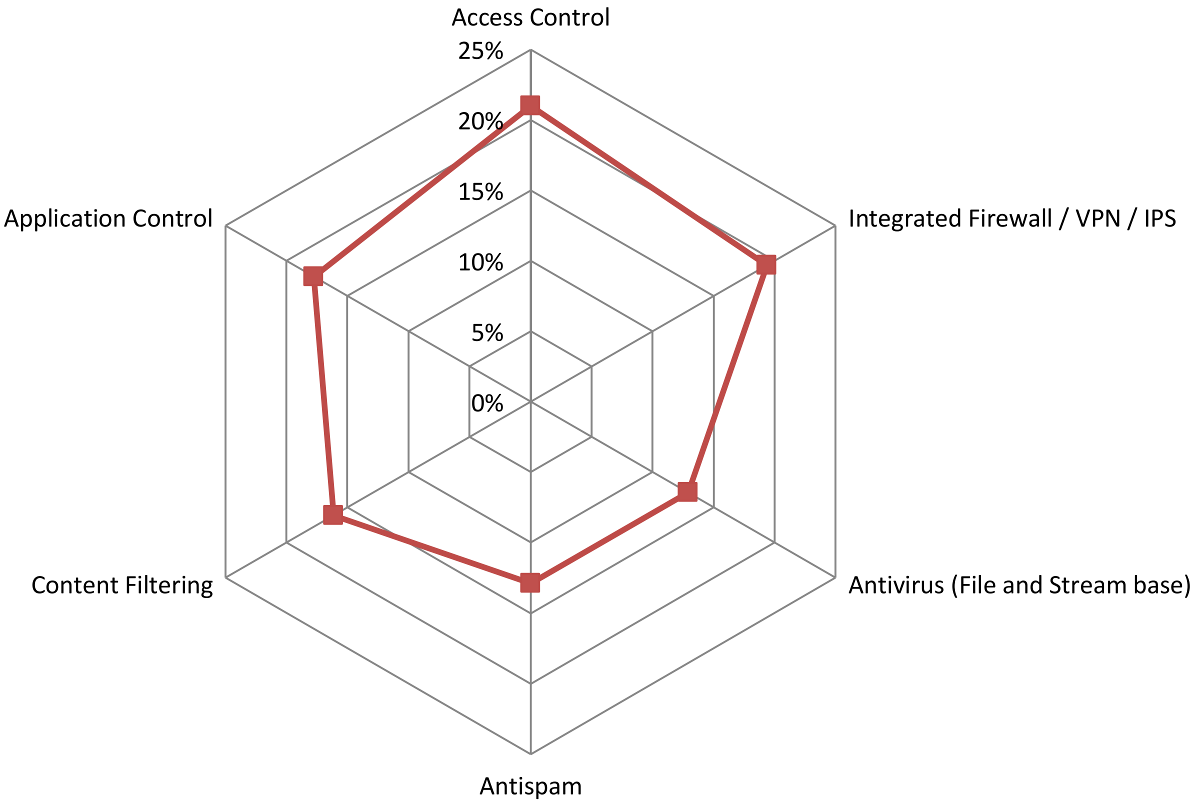


Most of us use Firewall and IPS at the perimeter. Use of WAF and advanced technologies for threat detection is picking up.

Cyber Resilience Survey

Technology

- Features desired in an enterprise-grade firewall

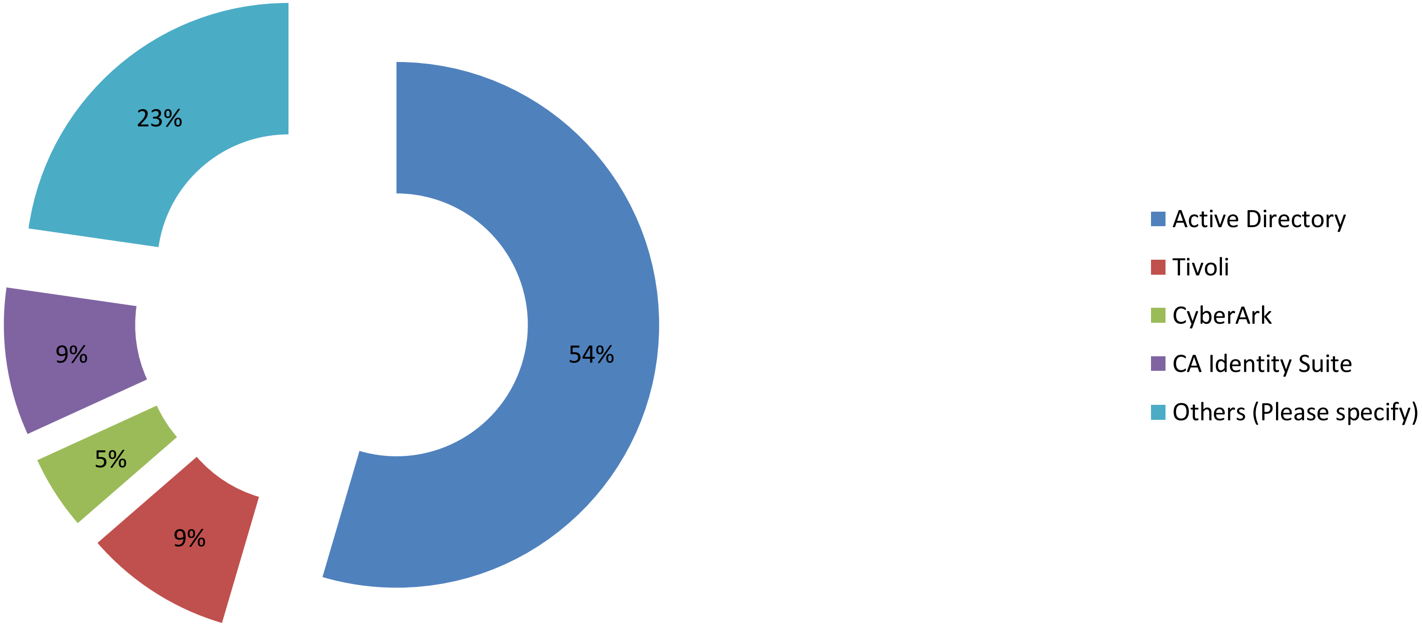


Access Control, Content Filtering and Integrated firewall/VPN/IPS are the features at least every 5th depository desires

Cyber Resilience Survey

Technology

- Identity Management Suite used by CSD

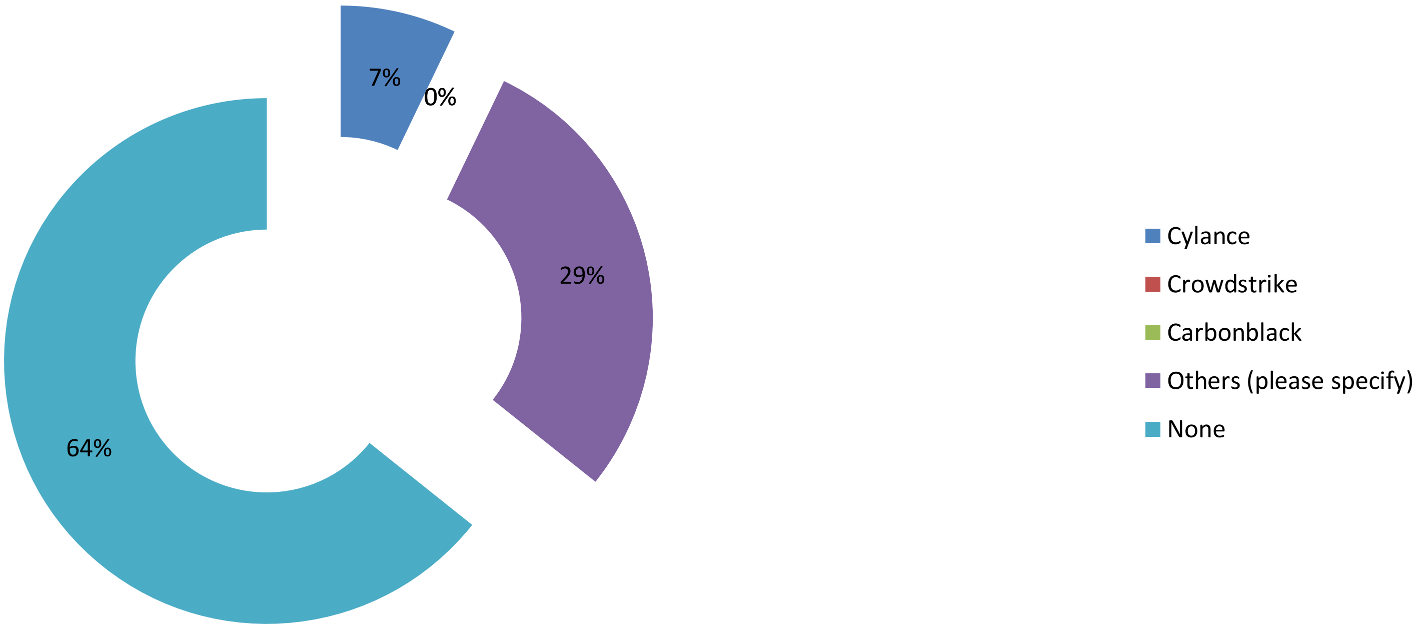


58% of CSD respondents have acknowledged use of Active Directory (AD) for identity management

Cyber Resilience Survey

Technology

- End-point APT solution deployed at CSD

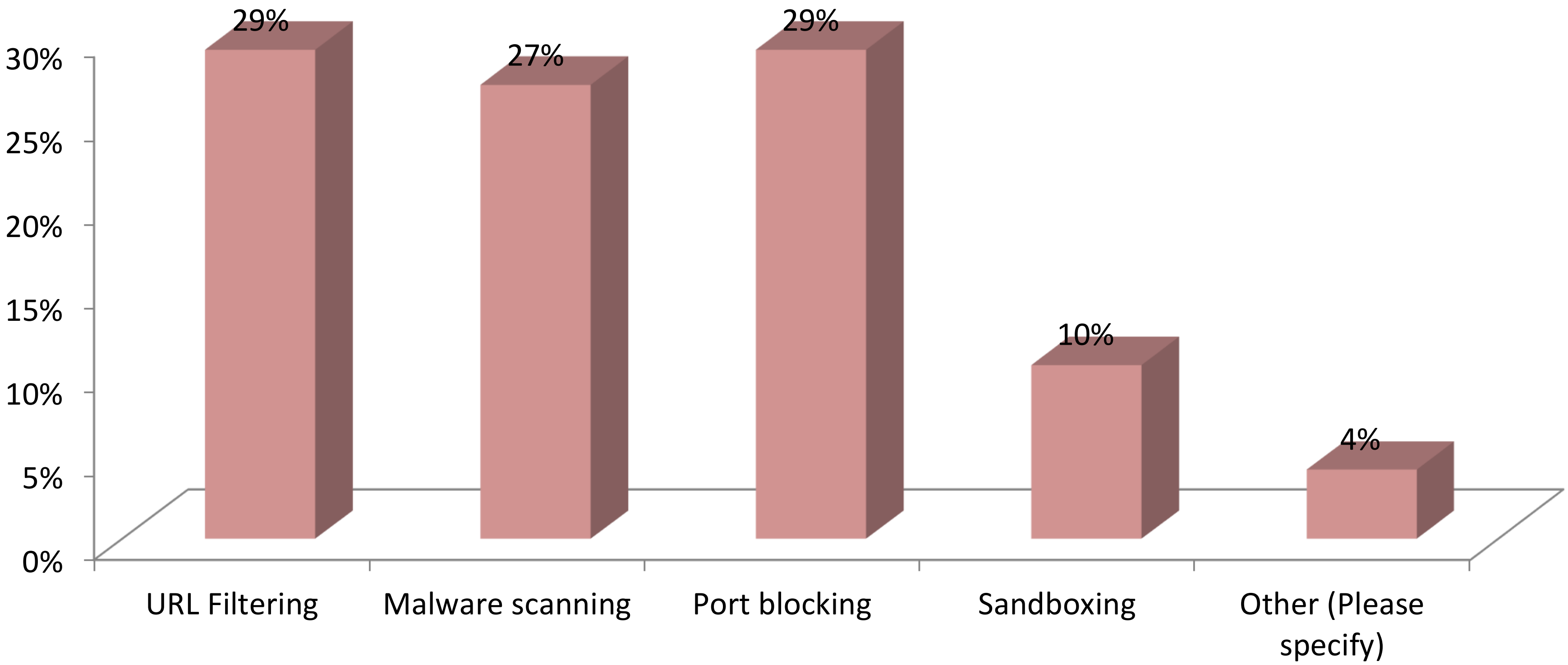


9 out of 13 respondents have confirmed to NOT have any end-point APT solution (such as, Symantec, XecProbe, Ahnlab APT, etc.).

Cyber Resilience Survey

Technology

- Methods to secure internet access



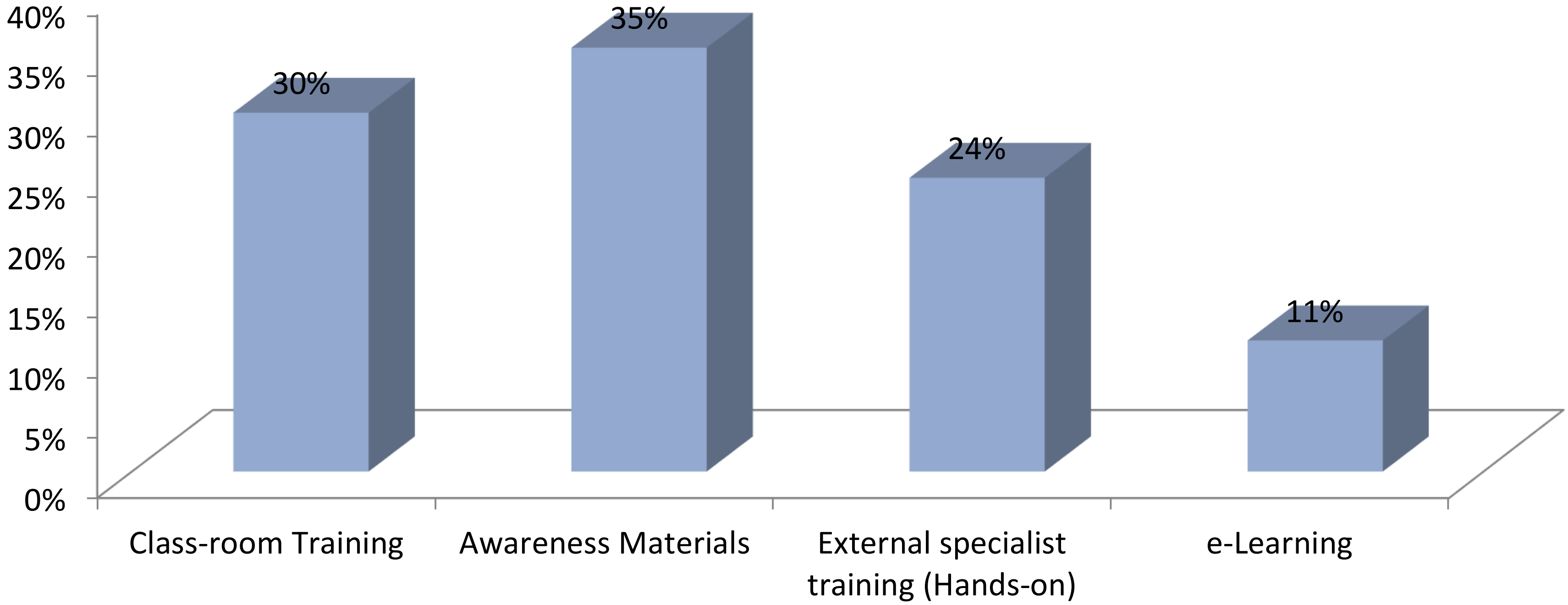
Most preferred methods by CSDs to secure internet access are URL filtering and port blocking.

Malware scanning is also next best method to secure internet access.

Cyber Resilience Survey

Security Awareness

- Preferred media to educate workforce

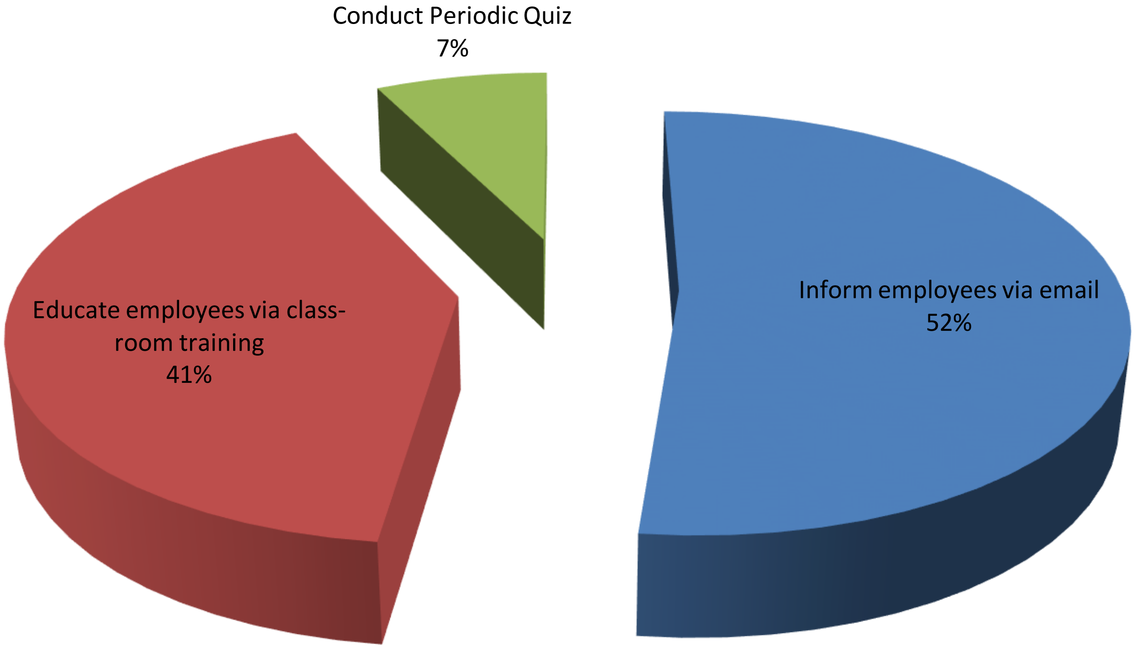


Most preferred method by CSDs to educate workforce is through Awareness materials.

Cyber Resilience Survey

Security Awareness

- Ways to inform employees about new cyber-attacks and threats

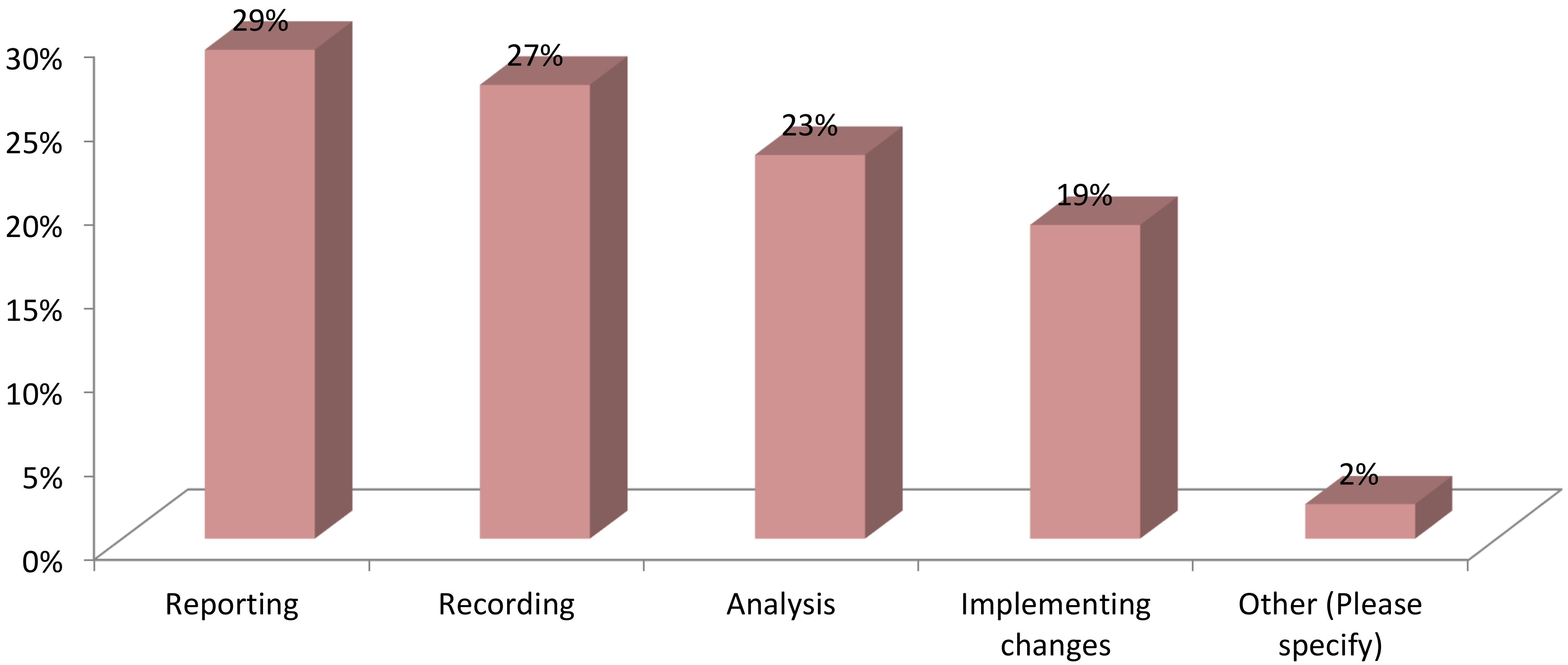


54% of CSD respondents prefer email communication to inform employees about new cyber-attacks and threats

Cyber Resilience Survey

Incident Management

- Features in CSD's security incident management system

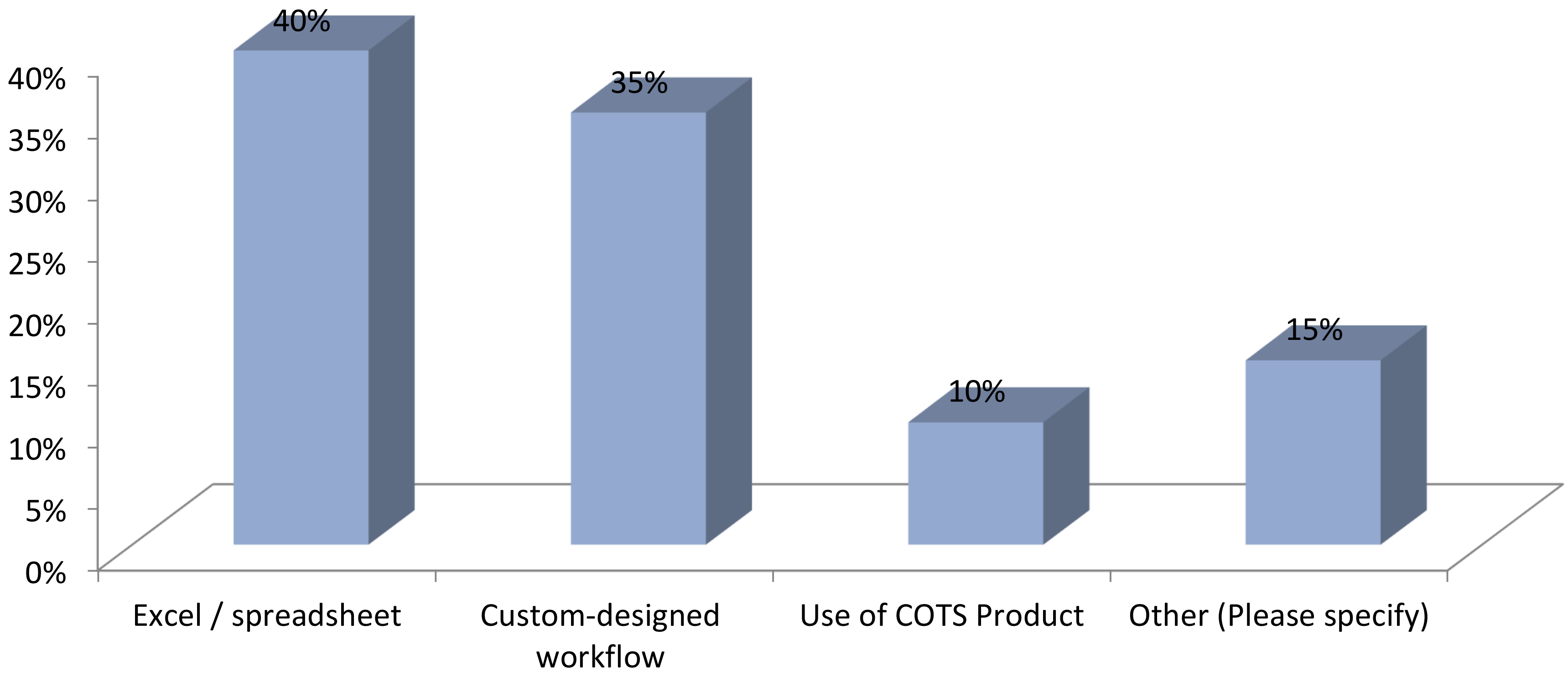


Reporting and Recording are the features mostly available in respondents' security incident management system.

Cyber Resilience Survey

Incident Management

- Tools to support security incident management system



Excel/spreadsheet is the highest voted tool to support security incident management system.

Cyber Resilience Survey

Key Takeaways

- Security is being discussed and decisions are being taken at the highest level, usually the Board
- ISO27001 has become the de-facto standard for security; adoption of any other standard is yet to pick-up
- Adoption of advanced security technologies is slowly gathering momentum.
- We tend the stick to time tested basic identity management solution like the AD for most cases
- Many ways are adopted to make employees aware of the growing cyber threats
- We still are equally dependent on Excel sheets and custom workflows for managing incident lifecycle

Thank you