World Institute for Nuclear Security

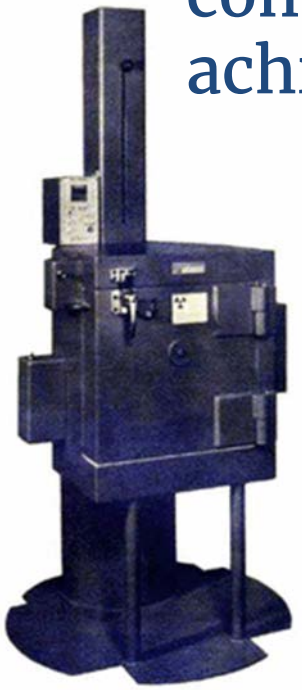
Round Table on Cybersecurity Best Practices for Users of Radioactive Sources.

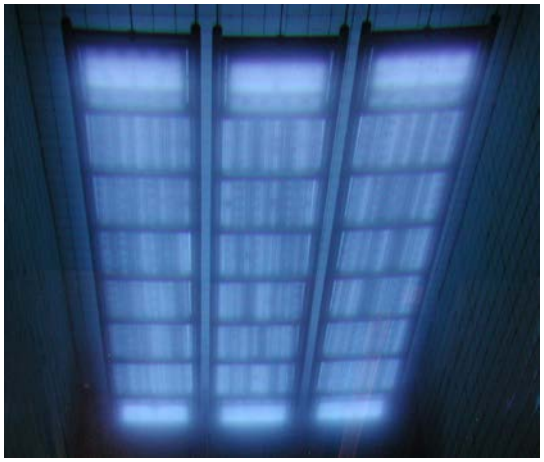
10 and 11 September 2019. Vienna, Austria

Pierre Legoux, WINS Head of Programmes

The WINS Vision

All nuclear and other radiological materials and facilities are effectively secured by demonstrably competent professionals applying best practice to achieve operational excellence.





WINS Activities Supporting the Strengthening of Radiological Security Worldwide

Sharing Operational Experience

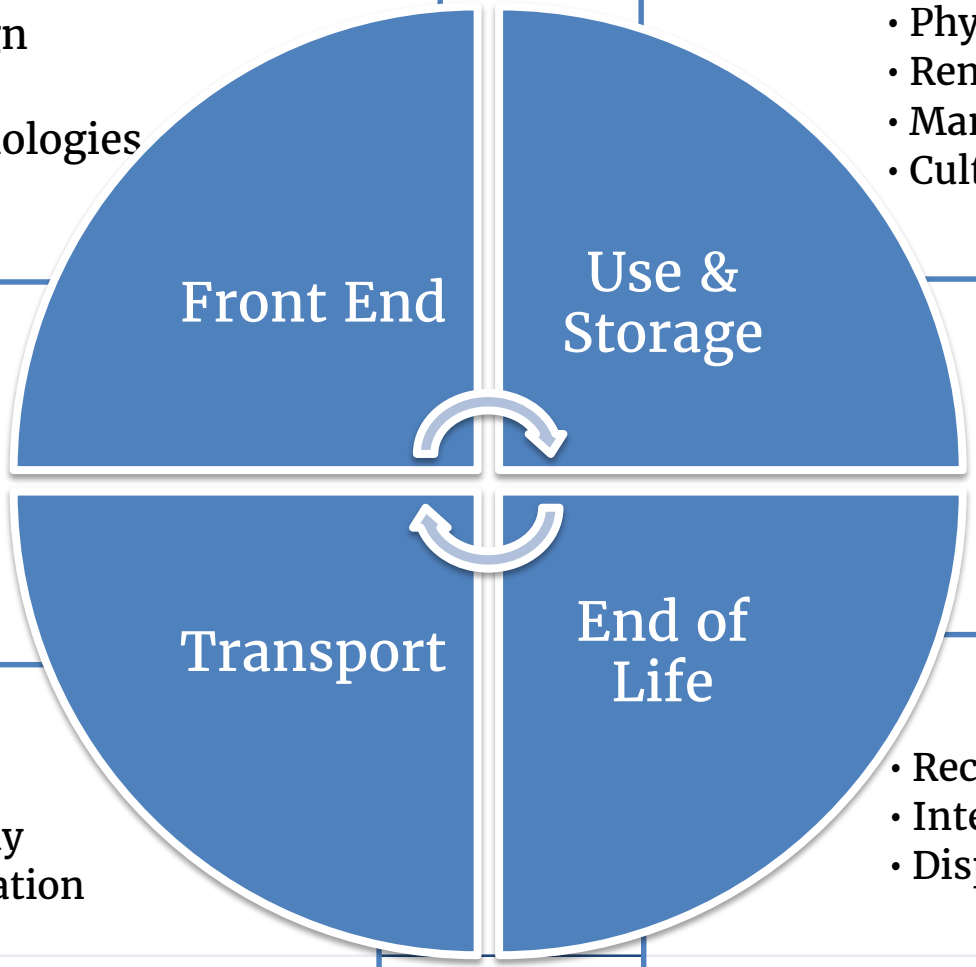
Knowledge Centre

Training & Certification

Evaluation

WINS Knowledge Centre: International Best Practice Guides

A comprehensive approach to the security of sources



- Security by Design
- In-device delay
- Alternative technologies

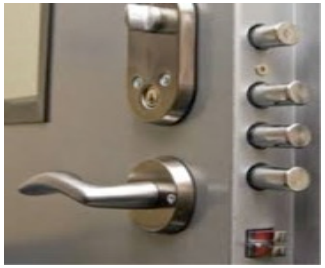
- Inventory
- Physical Security
- Remote Monitoring
- Management
- Culture & Sustainability

- Tracking
- Access Delay
- Communication
- Response

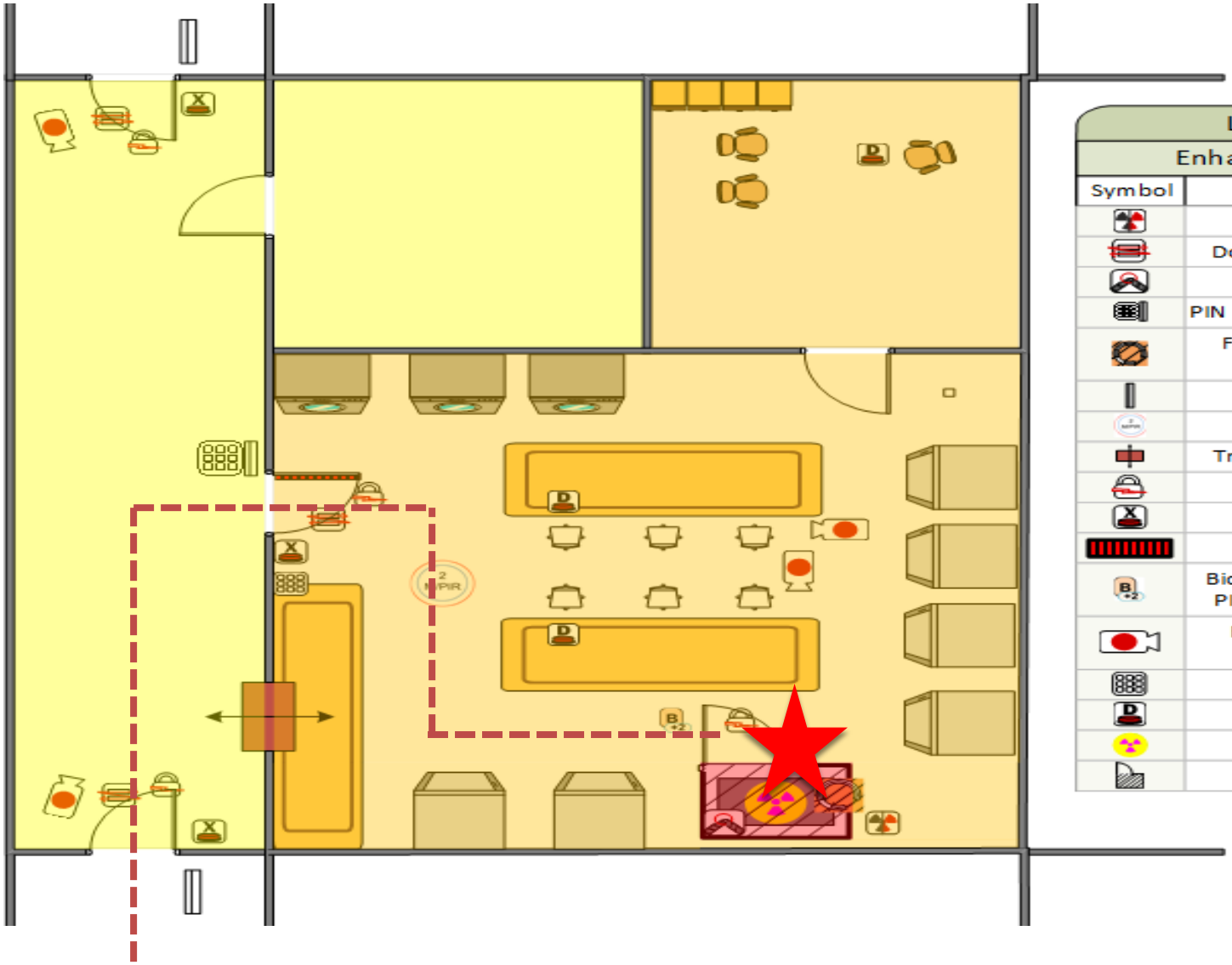
- Recycling & Reuse
- Interim Storage
- Disposal

WINS World Institute for Nuclear Security

Detection, Delay and Response



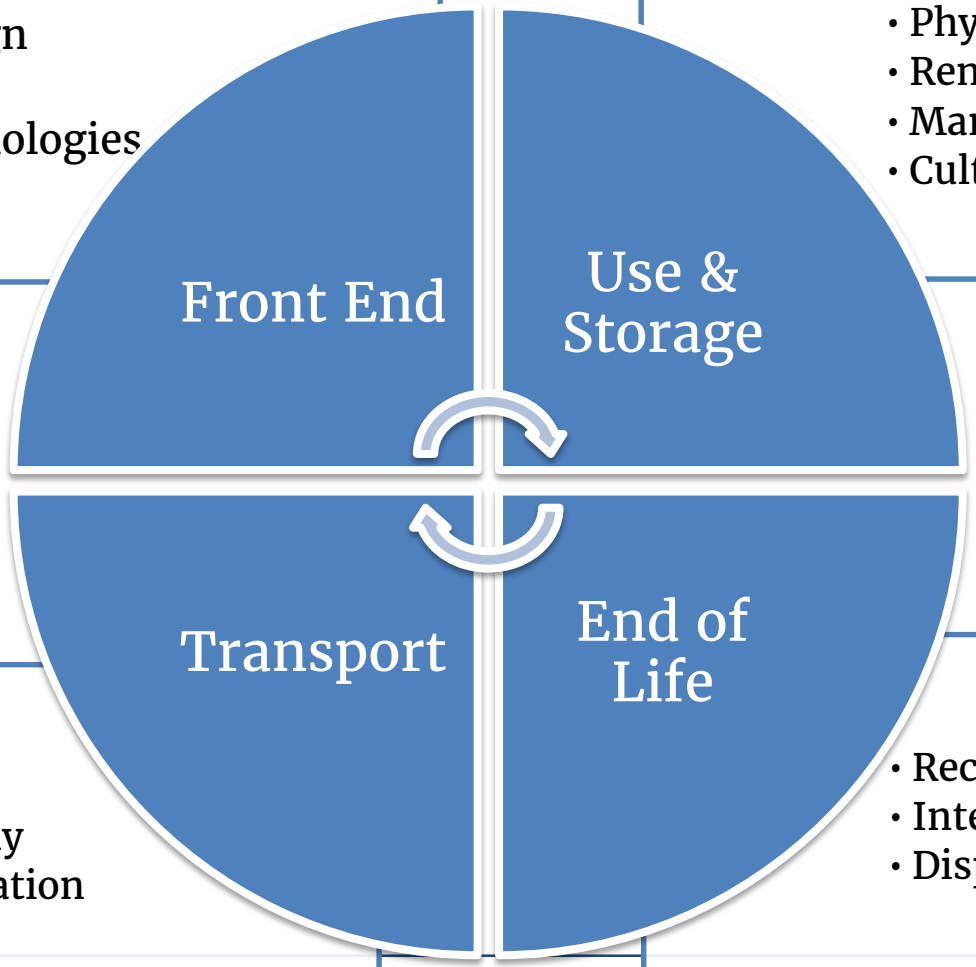
Security Layout



Legend	
Enhancements	
Symbol	Description
	Radiation Sensor
	Door Position Sensor
	Device tie down
	PIN Pad and Card Reader
	Fiber Optic Tamper Indicating Device
	Card Reader
	Motion Sensor
	Transaction Window
	Electric Lock
	Request to Exit
	Hardened Door
	Biometric Reader with PIN and Card Reader
	Fixed Infrared (IR) Camera
	Alarm Key Pad
	Duress switch
	Irradiator
	Sensored Cage


CYBER ATTACK

A comprehensive approach to the security of sources



- Security by Design
- In-device delay
- Alternative technologies

- Inventory
- Physical Security
- Remote Monitoring
- Management
- Culture & Sustainability

- Tracking
- Access Delay
- Communication
- Response

- Recycling & Reuse
- Interim Storage
- Disposal

WINS World Institute for Nuclear Security

Round Table Objectives

- ✓ Identify the magnitude of the cyber risk as it relates to the management of sources
- ✓ Specifically discuss potential impact of cyberattacks on physical protection systems, information security and the operation of devices containing sources
- ✓ Review the key elements of an effective cybersecurity programme
- ✓ Review the status of regulatory requirements an of the international recommendations on the topic
- ✓ Discuss mechanisms to increase awareness and collaboration amongst stakeholders
- ✓ **Develop a way forward to strengthen cybersecurity of radioactive sources**

Agenda

DAY 1 – TUESDAY 10 SEPTEMBER 2019

Opening: Developing a Common Understanding

Session 1: Understanding Cyber Threats and Associated Risks for Rad. Sources

Session 2: Protecting Physical Security Systems Against Cyber Attacks

Session 3: Cyber Security for Radiation Devices

DAY 2 – WEDNESDAY 11 SEPTEMBER 2019

Session 4: Developing a Comprehensive Approach to Cybersecurity

Session 5: Raising Cybersecurity Awareness Amongst Key Stakeholders

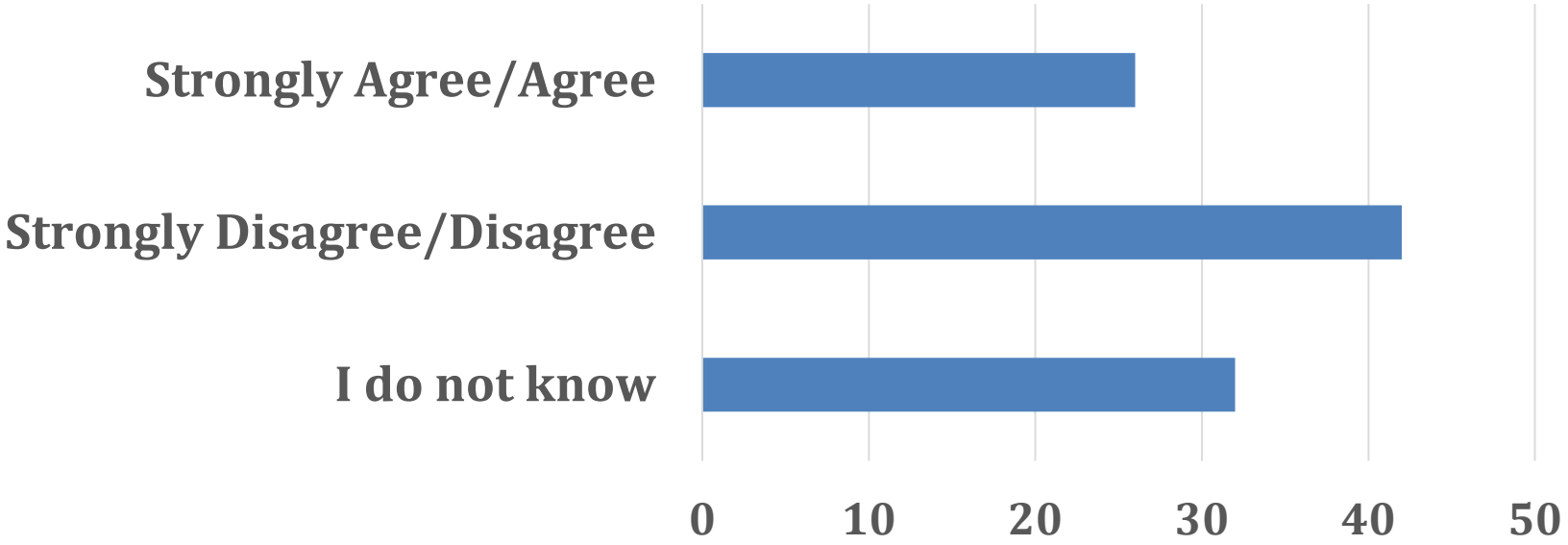
Closing: Key Findings and Next Steps

Round Table Process

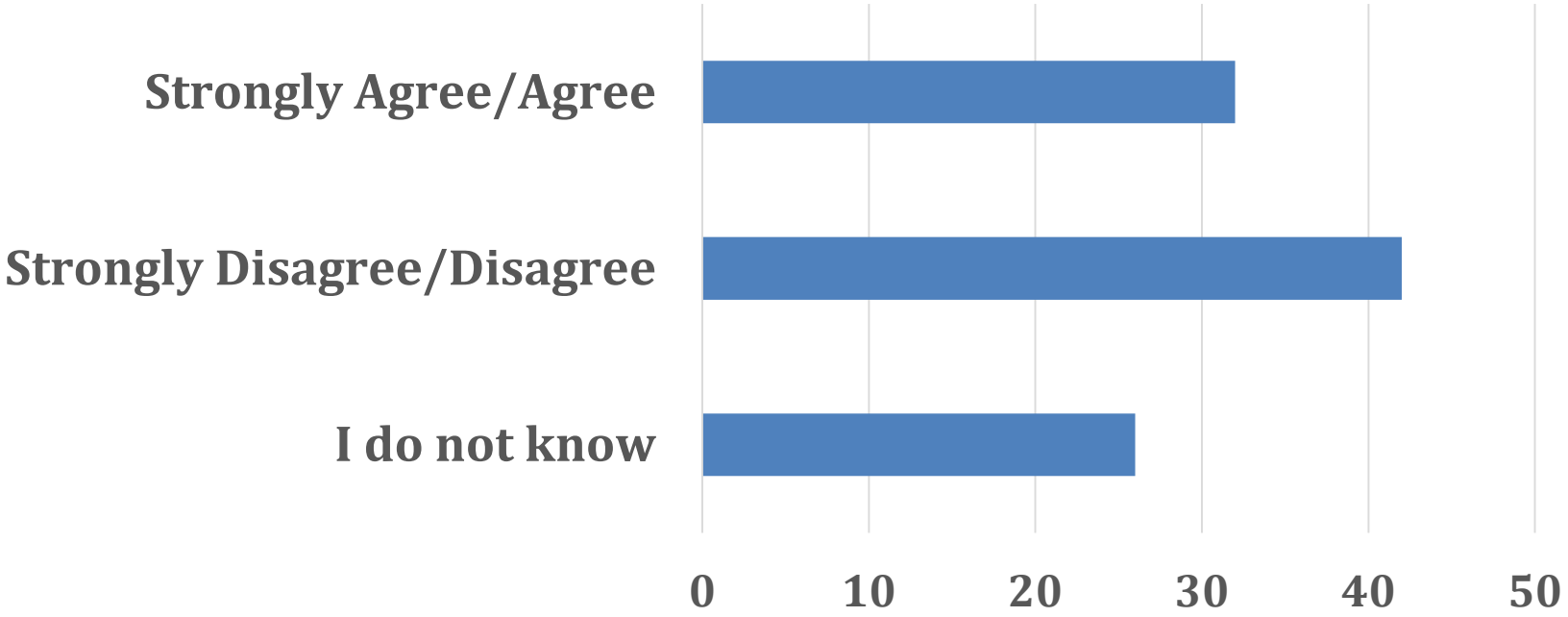
- ❑ PRESENTATIONS
- ❑ PLENARY DISCUSSIONS
- ❑ GROUP DISCUSSIONS
- ❑ E-VOTING

Survey Results

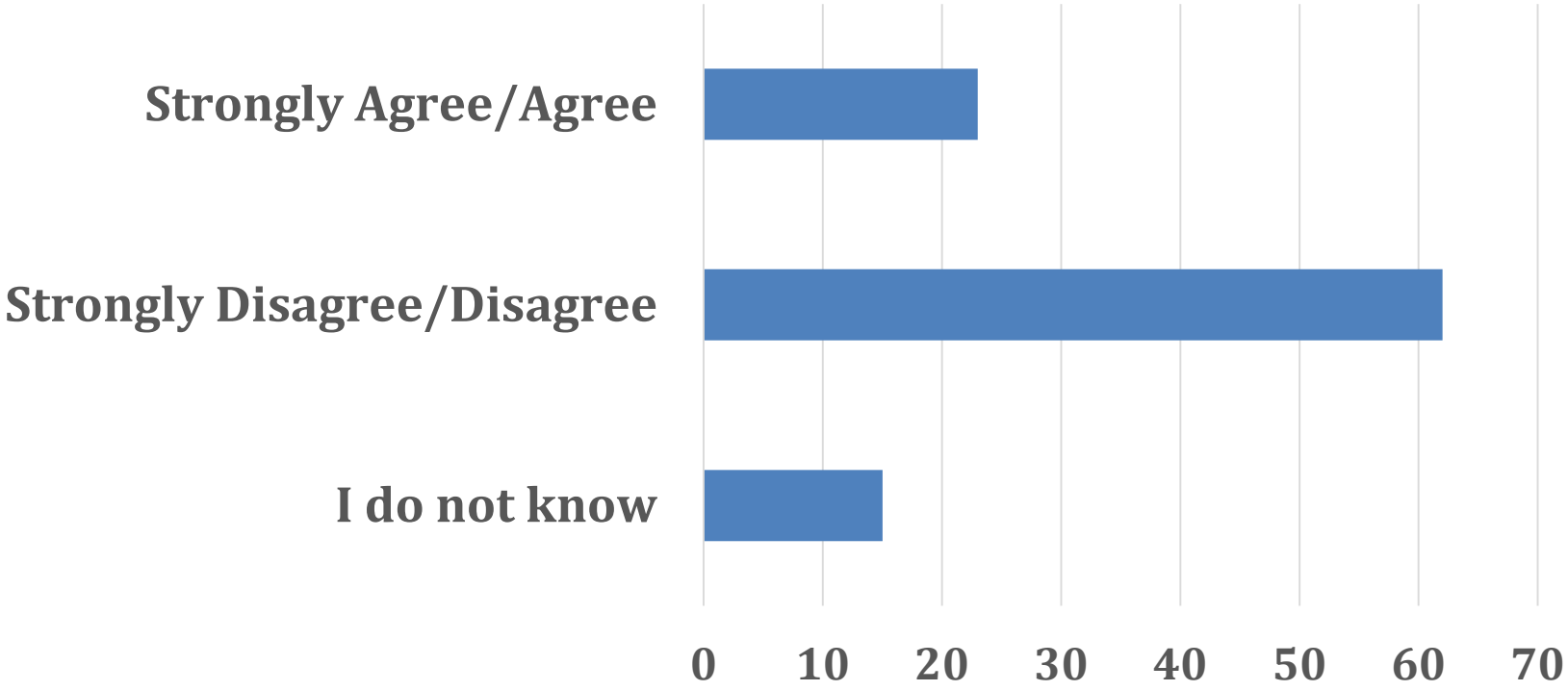
Radioactive source practitioners (stakeholders) clearly understand the cyber risks faced by radioactive sources and associated devices.



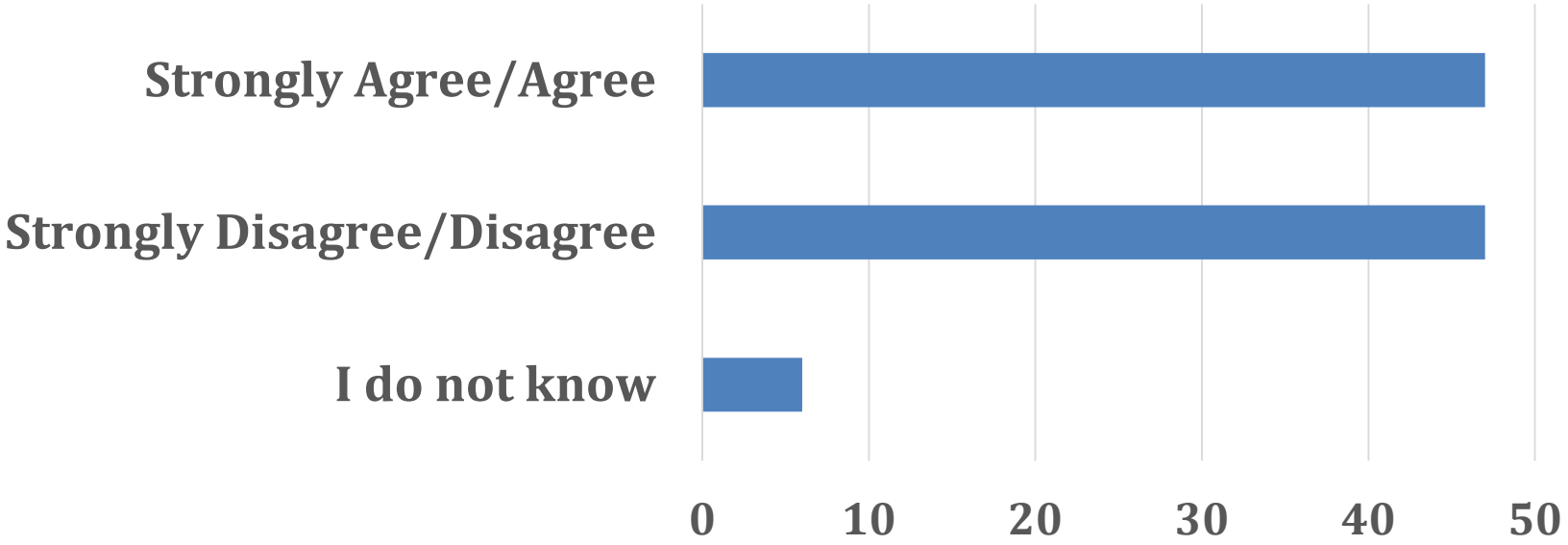
The cybersecurity measures that end users and device manufacturers implement are commensurate with this risk.



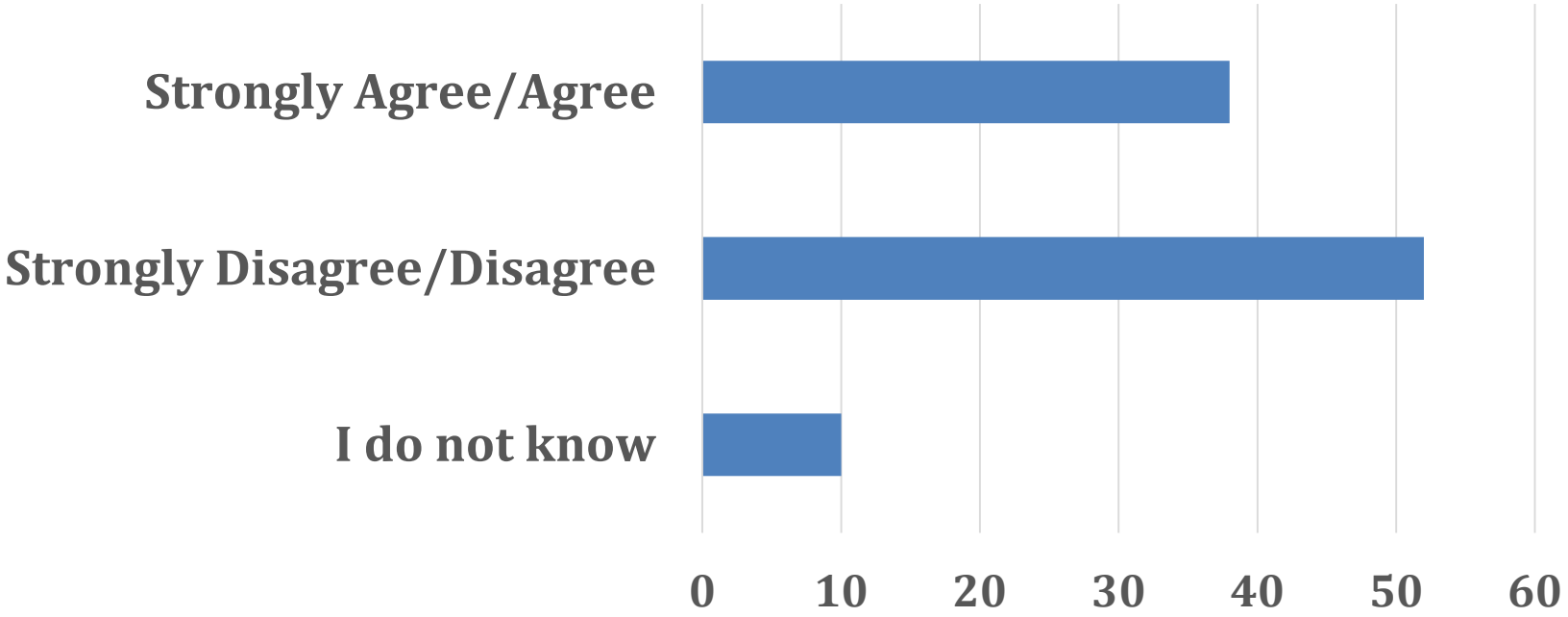
Information about the threat is effectively disseminated to people who need to know.



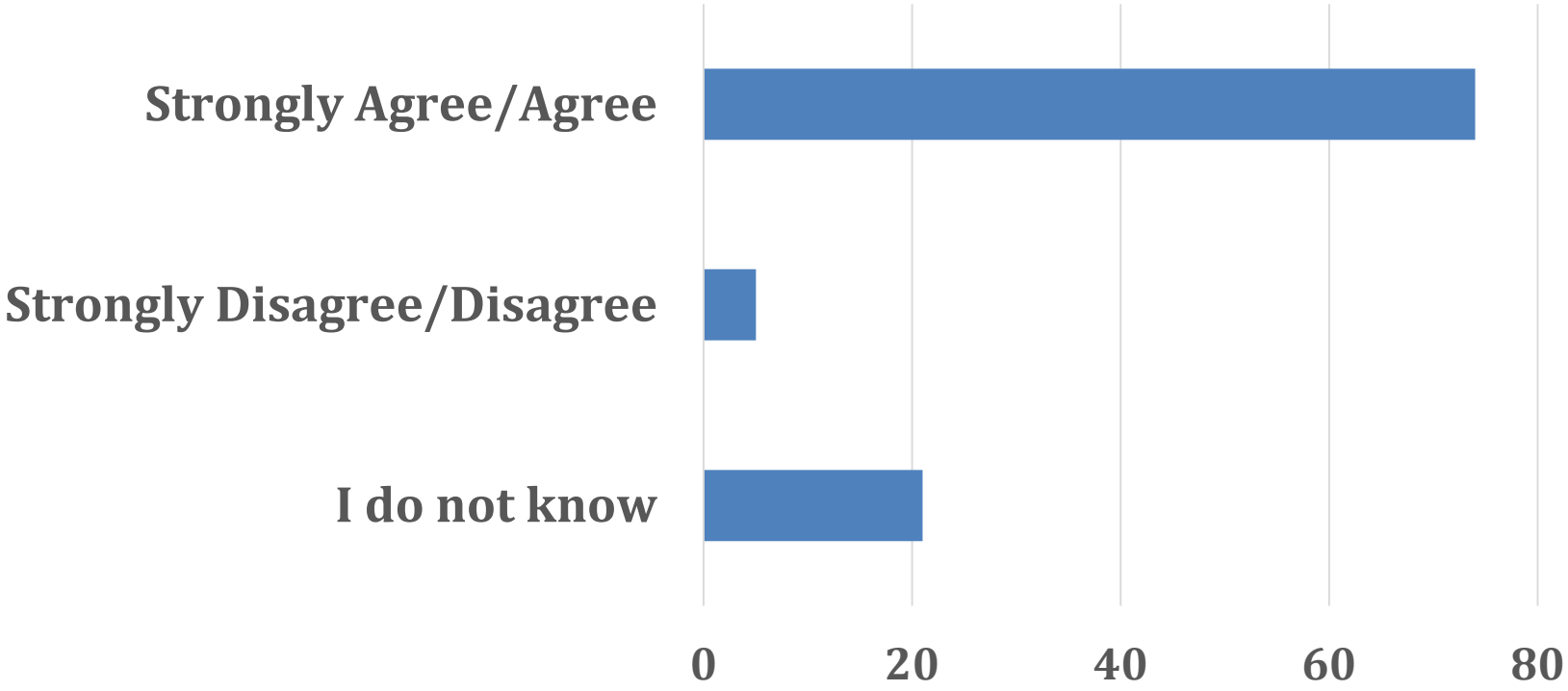
The physical and cybersecurity measures that end users implement to protect radioactive sources support each other and work effectively together.



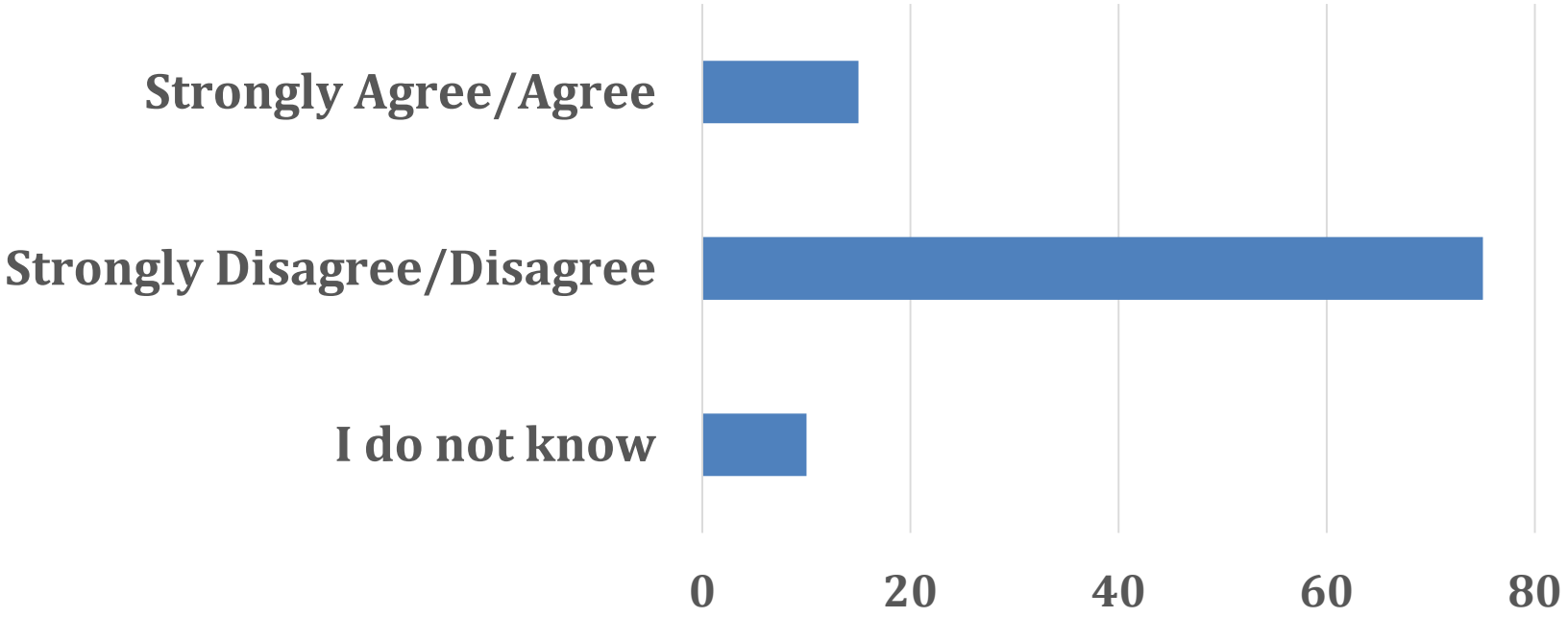
Senior management allocates the resources that are necessary to mitigate cyber security risks.



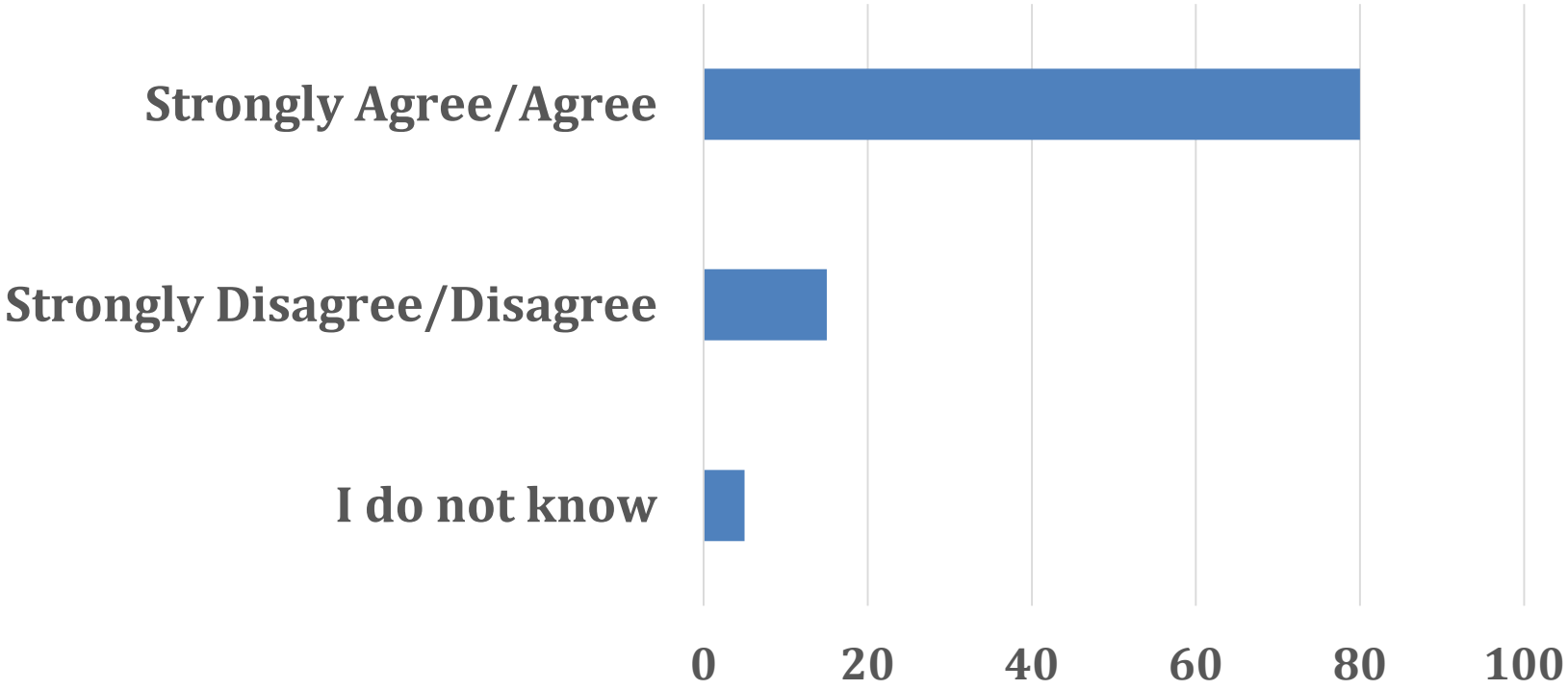
The staff members who are in charge of cybersecurity matters are competent.



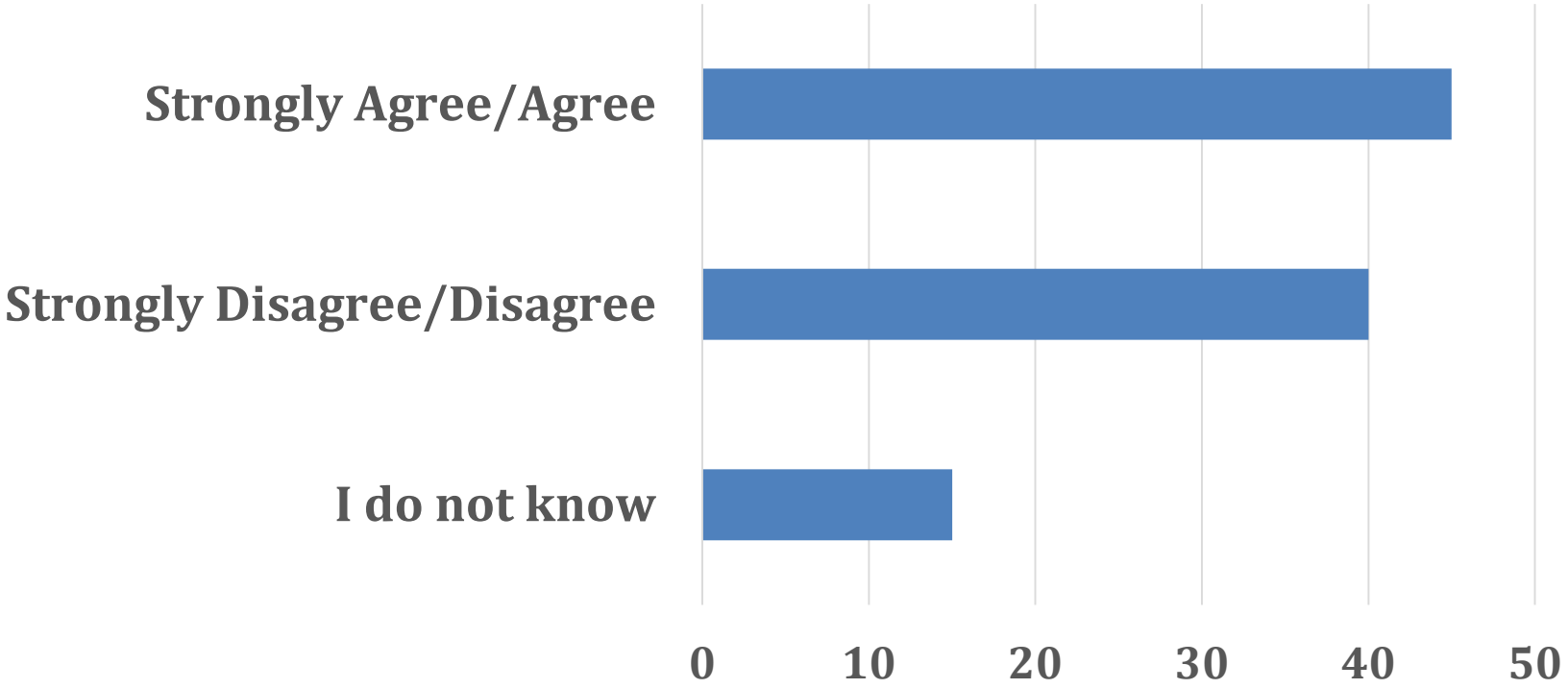
End user staff are aware of cyber threats and contribute effectively to mitigation measures.



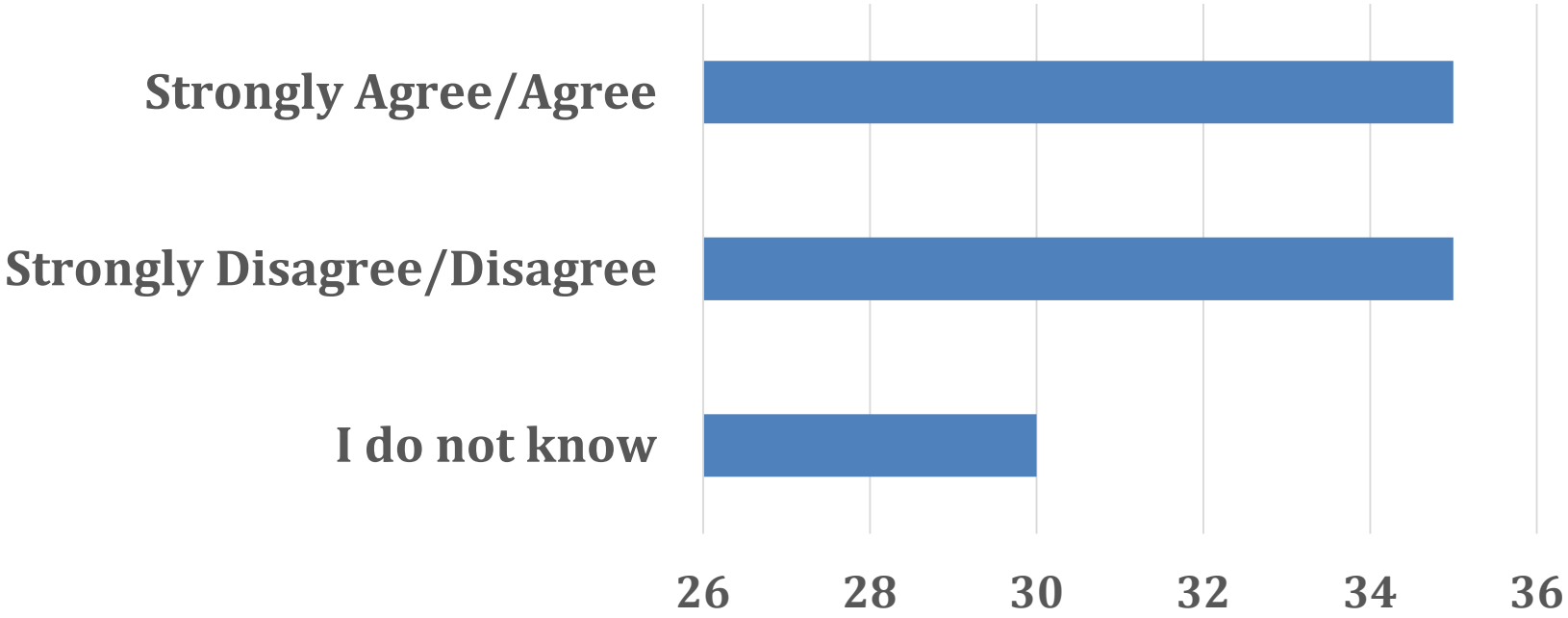
Numerous opportunities already exist for professional development in cybersecurity.



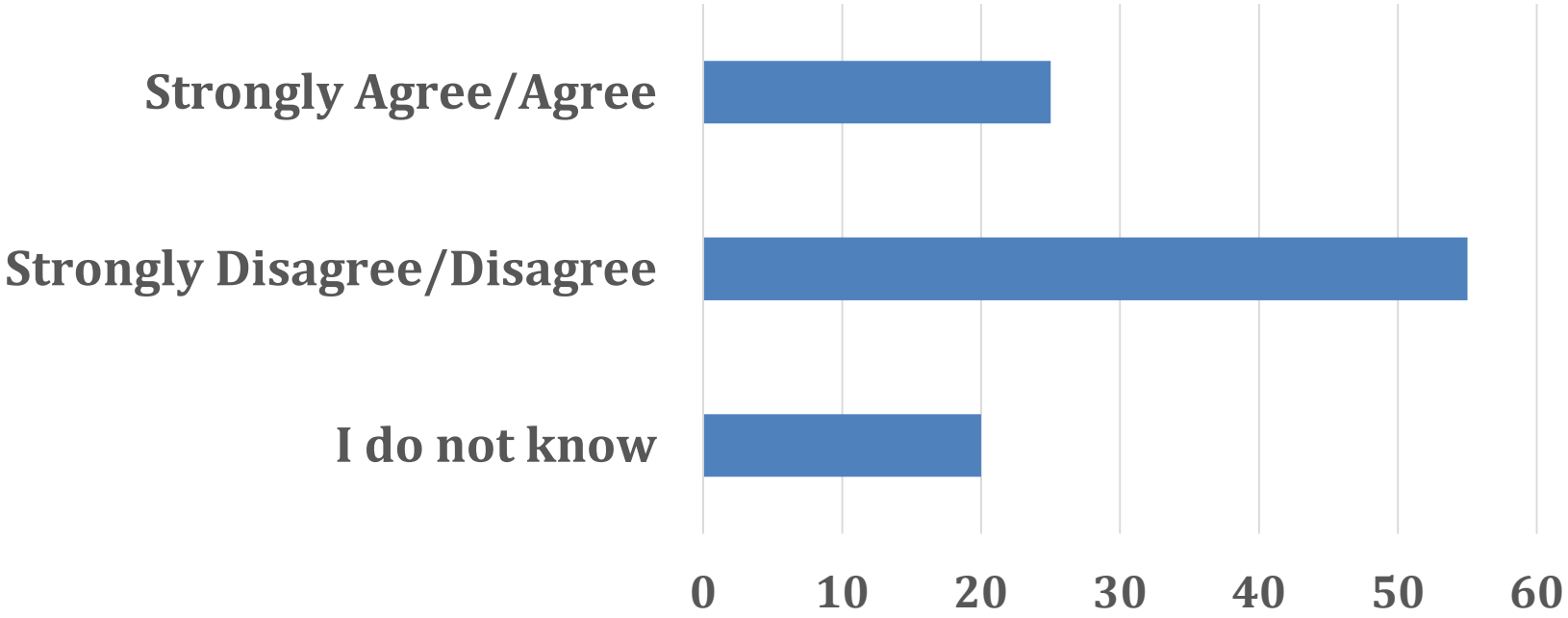
It is easy to find relevant cybersecurity standards and guidelines.



Radioactive source stakeholders (industry, end users, regulators, etc.) work effectively together to mitigate the cybersecurity risk.



Enough opportunities already exist in which to discuss cybersecurity matters related to radioactive sources.



Some Expectations

- Increase my knowledge and get better at my job
- Receive information about the latest developments regarding cyber security of radioactive sources and feedback it to my colleagues
- Express my needs and challenges. Explore possible solutions, not just admire the problem
- Understand how others perceive the risk and learn more about best practices
- Share experiences; understand the general issues and what actions are needed
- Understand applicable requirements and learn about possible guidance
- Better understand options to raise cybersecurity awareness of the community

The most serious cyber threat/risk to radioactive sources

- Lack of awareness of the threat and of understanding of the risks
- Lack of basic cyber security requirements such as system patching and updates.
- The human factor
- Misuse act to harm member of the public
- Blended cyber/physical attacks, where cyber vulnerabilities are exploited to decrease the efficiency of the physical security arrangements
- Unauthorized access to the computer systems the protect sensitive information and physical protections.
- Unwitting insider (unknowingly spreading a virus or trojan inside the network/organization)

Some of the most urgent actions to take

- Develop a proper understanding of the risks across all stakeholders.
- Communicate the risk elements (threats, consequences & likelihood) to the community of users
- Understand vulnerabilities. Hire creative, competent, trustworthy red teams to explore the risks. Bring independent cybersecurity expertise to the field.
- Identify four major cybersecurity challenges and 10 critical actions that the federal government and other entities need to take to address them.
- Raise awareness, improve skills and competencies
- Remove the targets (sources)
- Establish a proper defensive computer security architecture
- Establishing regulatory requirements

Examples of questions to be discussed

- What actual examples of cybersecurity incidents do we have? How can we better share them? How can we use them to raise awareness?
- Do we foresee any significant evolution in the threat in the near future?
- What can we expect from regulators in the short to long term future?
- What type of computer (cyber) security controls are in place to protect radioactive information and sources? What others are doing?
- What are the required capabilities and competencies (in cyber security) for people responsible for securing radiological material?
- Has any member of the community (e.g., manufacturer, owner/operator, research institution) engaged with a competent cyber/physical red team to evaluate the cybersecurity posture of devices that use radiological sources?
- What are five tangible elements of a path forward that, if pursued by all users/sites, would enhance the security of the industry?

Success Criteria

- LEARN, SHARE, CONTRIBUTE
- MEET & NETWORK
- ENJOY YOUR TIME
- **AGREE ON FOLLOW UP ACTIO**

World Institute for Nuclear Security

Round Table on Cybersecurity Best Practices for Users of Radioactive Sources.

10 and 11 September 2019. Vienna, Austria

Pierre Legoux, WINS Head of Programmes