research

CONTROL ENGINEERING

Cyber Security

June 2015

CFE Media

Table of contents

Introduction and methodology

Objective
This study was conducted by *Control Engineering* to evaluate cyber security implementation, resources, and training. Specifically, the study examines:

- Control system cyber security threats and threat levels
- Vulnerability assessment and internal assessment teams
- Cyber-related incidents and reporting
- Emergency response teams and training
- Government and industry regulations or compliance
- Mobile device security
- Resources for monitoring cyber security events.

The current survey replicates a study conducted in 2014. The questionnaire and survey methodologies are virtually the same with a few exceptions. Where appropriate, 2015 results are compared to the findings from 2014.

Sample
The sample was selected from recipients of *Control Engineering* for whom e-mail addresses were available.

Method
Subscribers were sent an e-mail asking them to participate in this study. The e-mail included a URL linked to the questionnaire. Qualifying questions limited survey respondents to those who are directly involved in aspects of control system cyber security within their organization.

- **Data collected:** Jan. 30 through Mar. 20, 2015
- **Number of qualified respondents:** 284
  - *Margin of error: +/-5.8% at a 95% confidence level*
- **Incentive:** Survey participants were offered the opportunity to enter a drawing for a $50 gift card.

Key findings

Respondents to the *Control Engineering* 2015 Cyber Security Study identified seven high-level findings impacting control systems today:

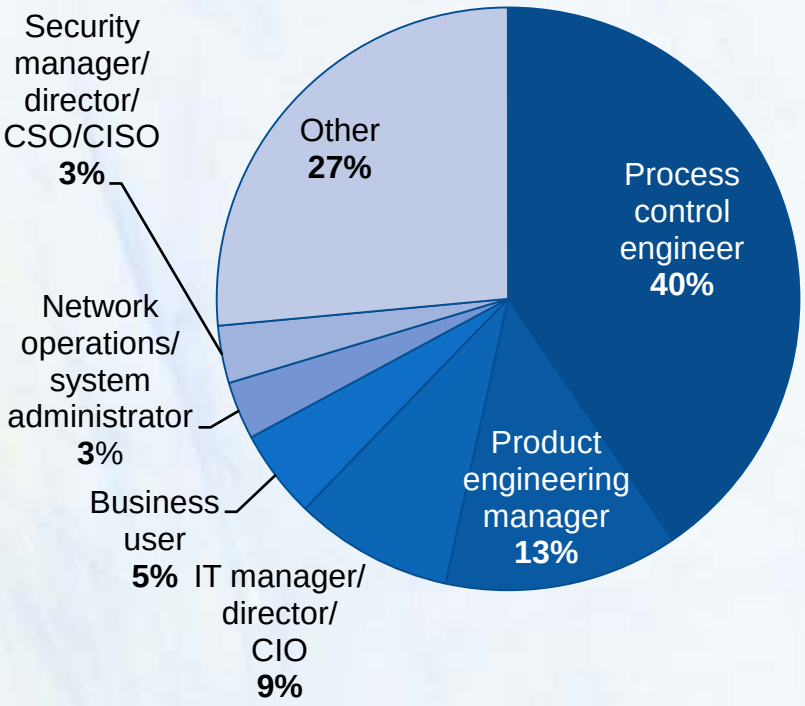
1. **Threat levels:** Forty-seven percent of respondents perceive their control systems to be moderately threatened by cyber attacks, while 25% say theirs are highly threatened and 8% are at a severe threat level.
2. **Most concerning threat:** Malware from a random source is the most concerning control system threat for 35% of respondents. Another 18% are worried about theft of intellectual property, and 8% fear attacks from “hacktivists” with a political or environmental agenda.
3. **Vulnerable system components:** The top most vulnerable system components within respondents’ organizations are connections to other internal systems (70%), computer assets (70%), network devices (67%), and wireless communication devices and protocols used in automation systems (60%).
4. **Vulnerability assessments:** One in four respondents reported that their organizations have performed some type of vulnerability assessment within the past three months. The average facility has checked their vulnerabilities within the past seven months.
5. **Cyber-related incidents:** Nearly half of respondents have experienced a malicious cyber incident into their control system networks and/or control system cyber assets—that they are aware of—within the past 24 months. Forty-three percent of these attacks were accidental infections, 8% were targeted in nature, and 38% were both accidental and targeted.
6. **Mobile devices:** Thirty percent of organizations do not allow mobile devices—such as smart phones and tablets—to connect to networks or enter work areas, while 21% allow network access, and 15% allow them in the work areas only.
7. **Training:** Half of respondents said their organizations train employees on identifying things that may indicate a cyber incident or attack, and another 34% train them on identifying social engineering attacks.

Respondent profile

Job title, industry experience

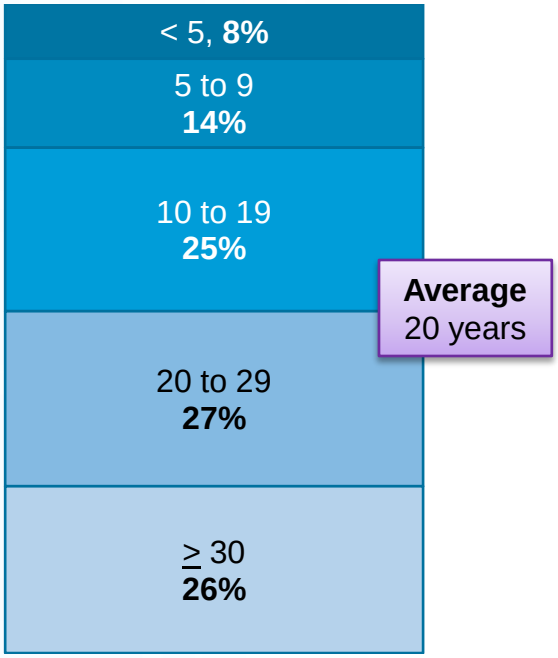
Forty percent of respondents are process control engineers, and the average respondent has worked in their current industry for 20 years.

Job title



Industry experience

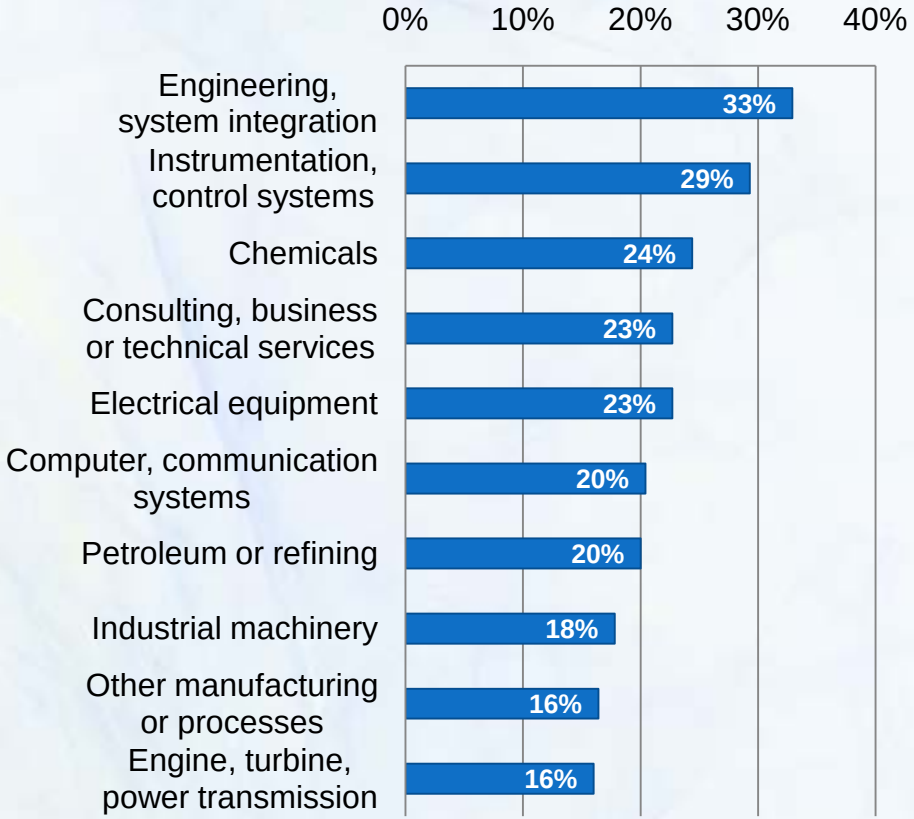
Years

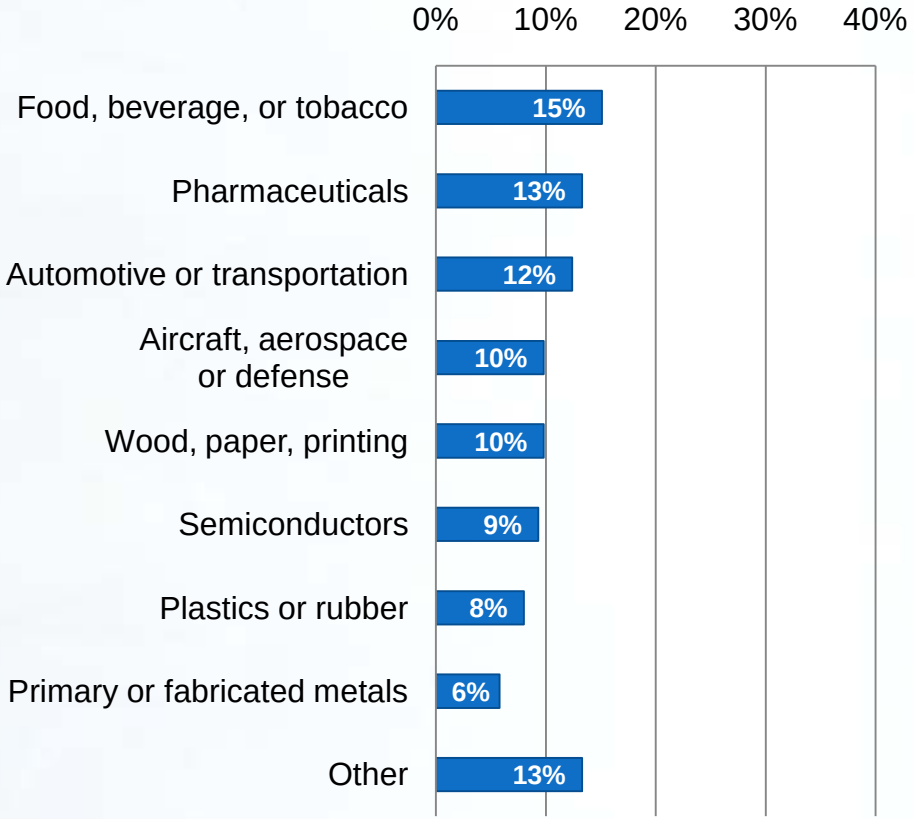


Q: Which of the following best represents your job title? (n=284); Q: For approximately how many years have you worked in your current industry? (n=226)

Industry involvement

The top industries served by respondents are engineering or system integration (33%), instrumentation or control systems (29%), and chemicals (24%).



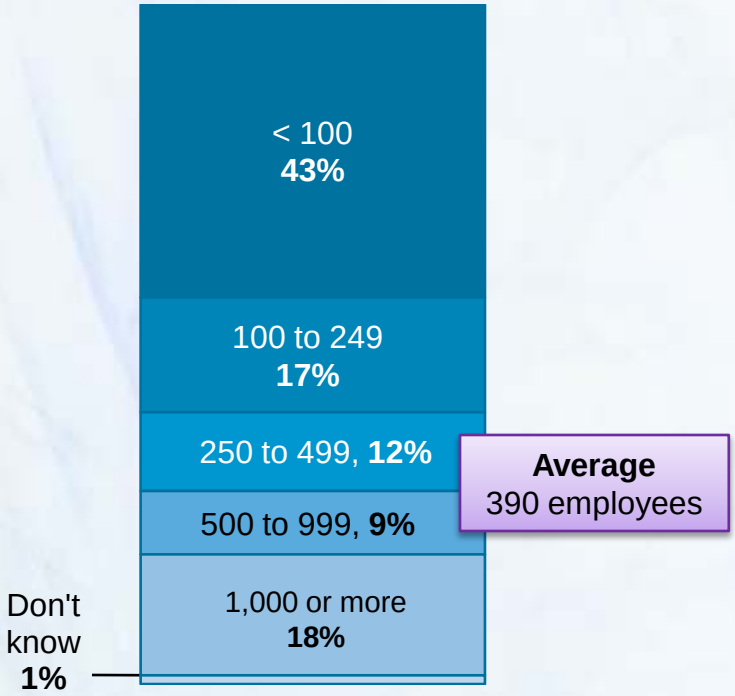


Q: In which of the following industries is your company involved? (n=225)

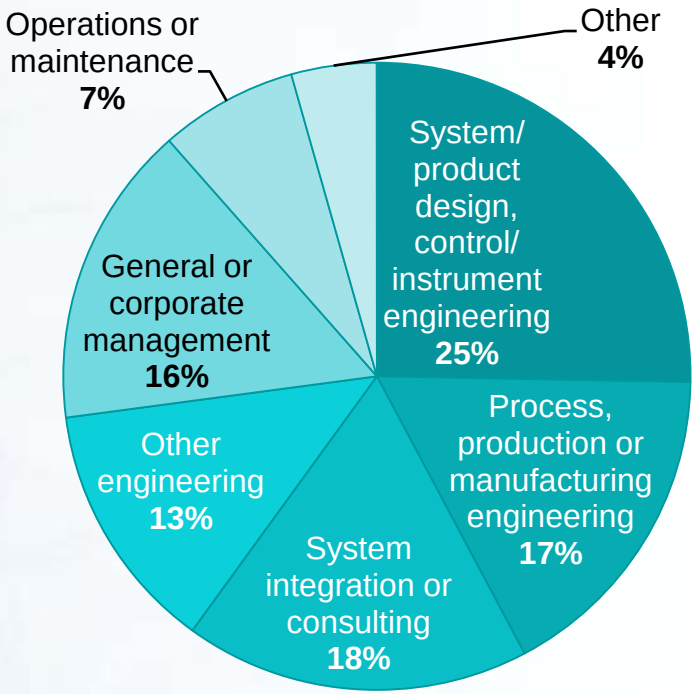
Company size, primary job function

The average facility respondents work at employs 390 people. One in four respondents' primary job functions include system or product design and/or control or instrument engineering.

No. of employees



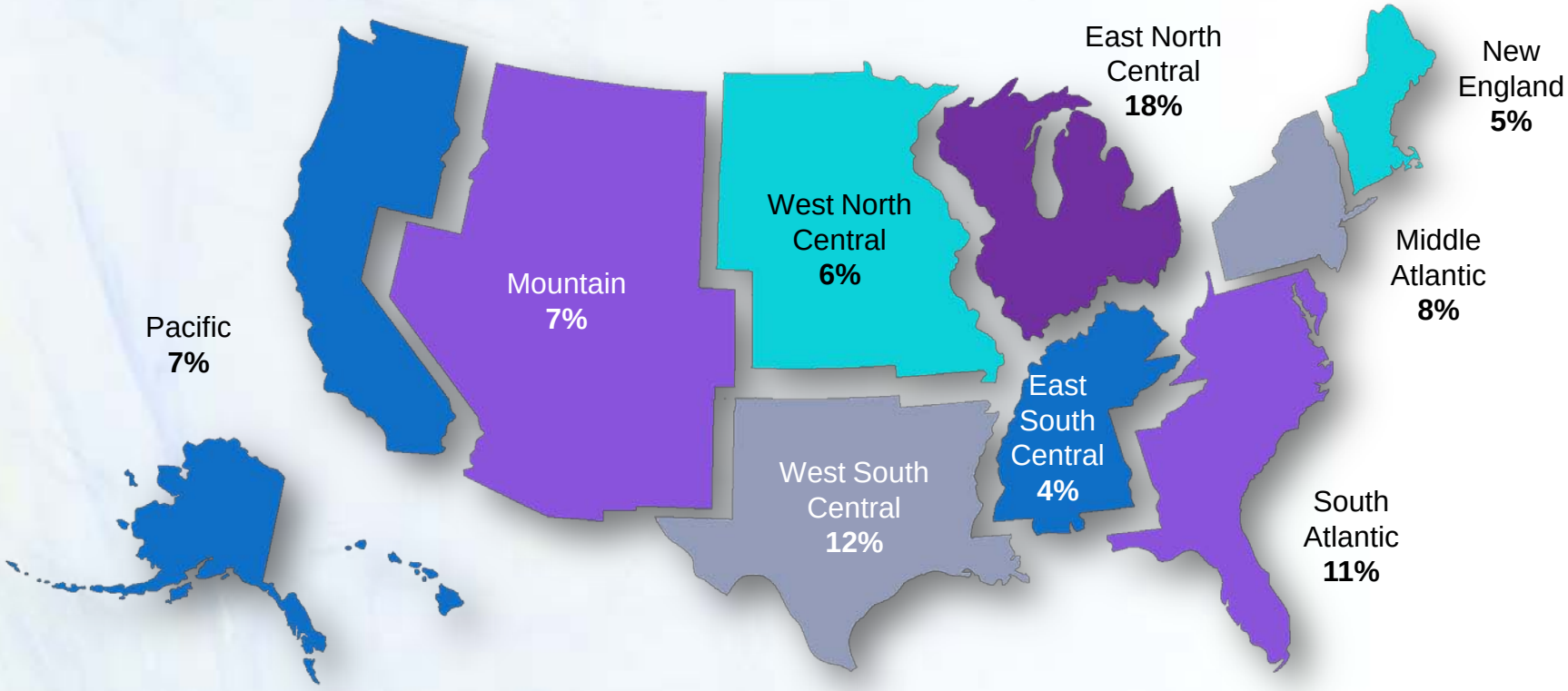
Primary job function



Q: Approximately how many people work at your location? (n=225); Q: Please indicate your primary job function. (n=225)

Location

Twenty-four percent of respondents are based in the North Central regions of the United States, and another 22% are based beyond the U.S. border.



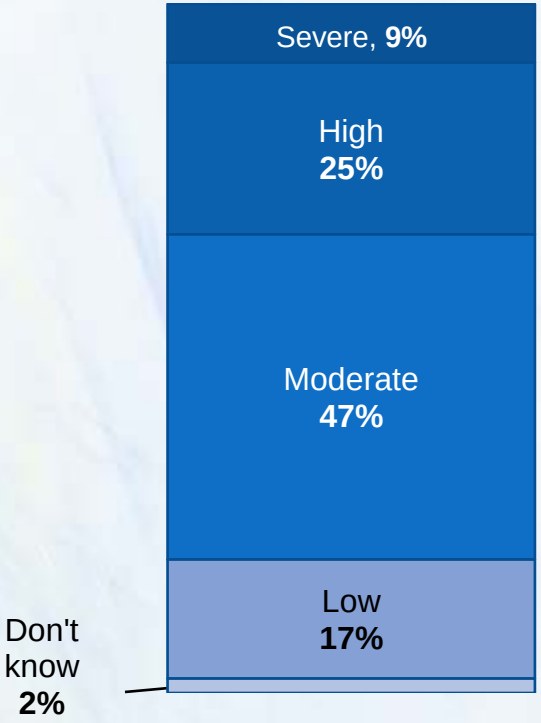
Q: In which region of the country are you based? (n=225)

Cyber security practices

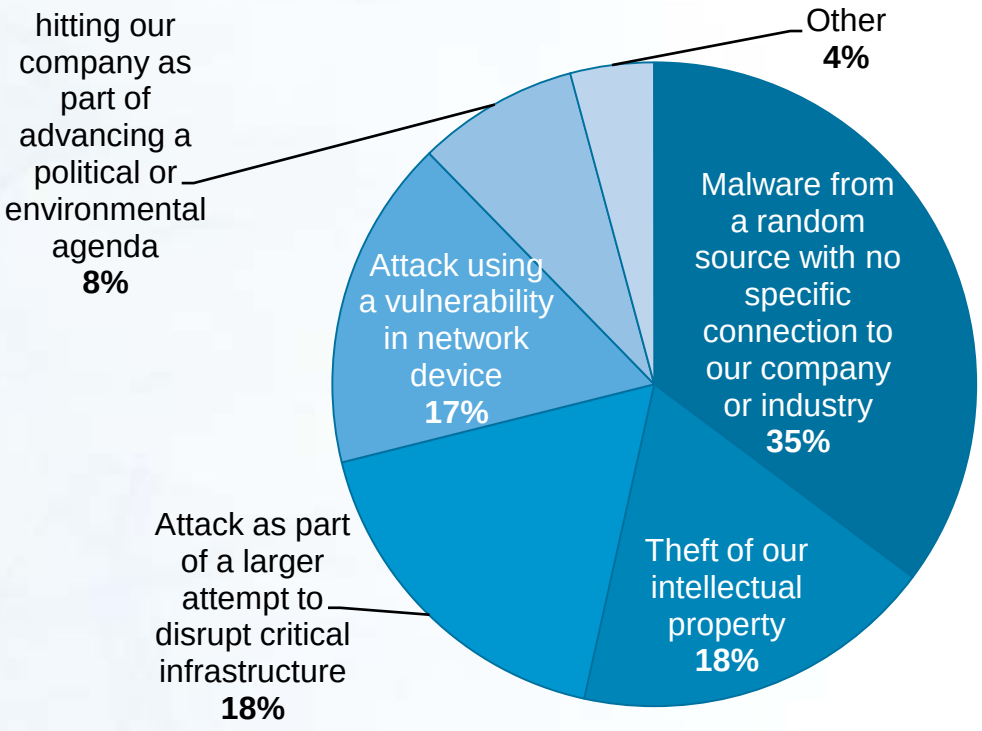
Cyber security threats

Sixty-four percent of respondents indicated that their control system cyber security threat level is low to moderate, and 35% are most concerned about malware threats coming from a random source.

Threat levels



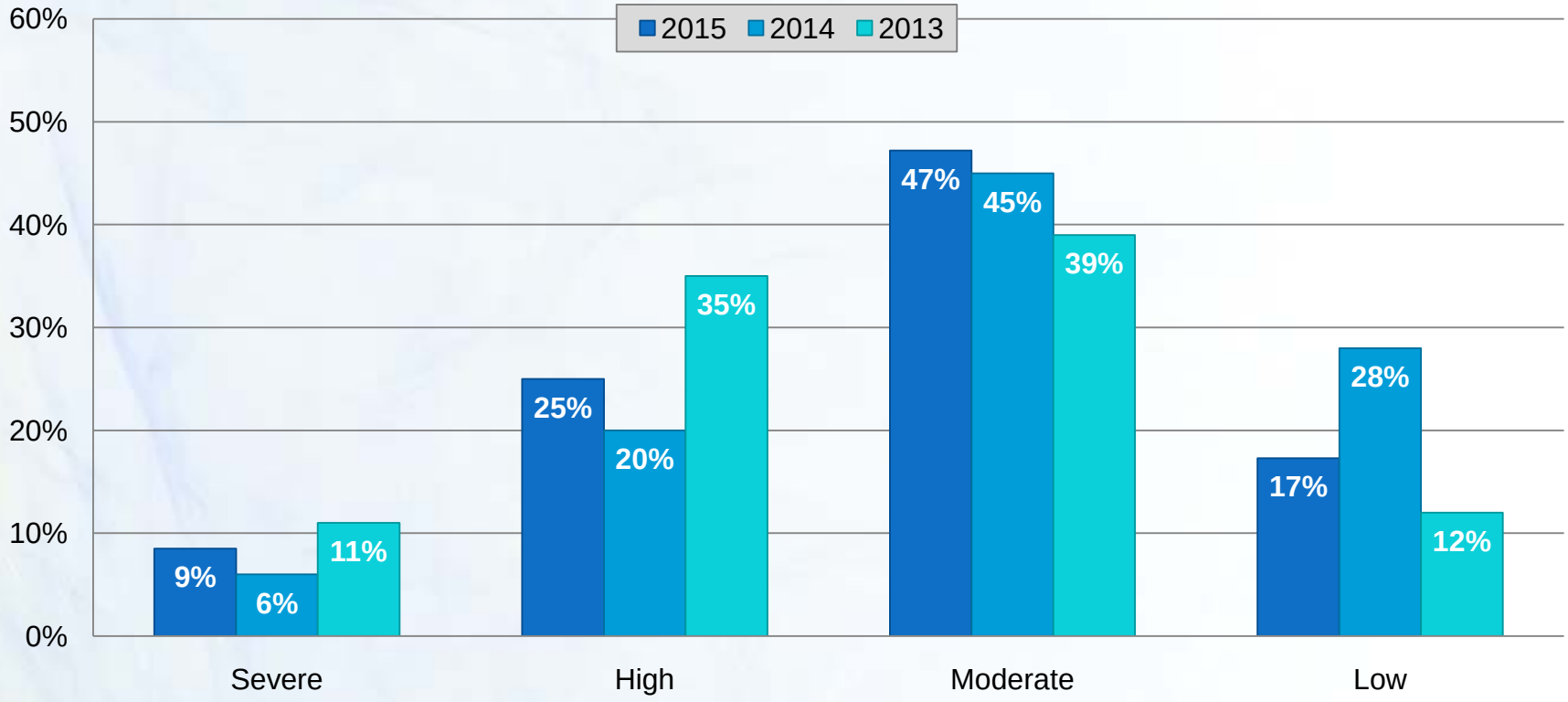
Most concerning threats



Q: What level do you perceive the control system cyber security threat within your organization to be? (n=284); Q: What type of threat to your control system concerns you the most? (n=284)

Threat levels: Year-over-year

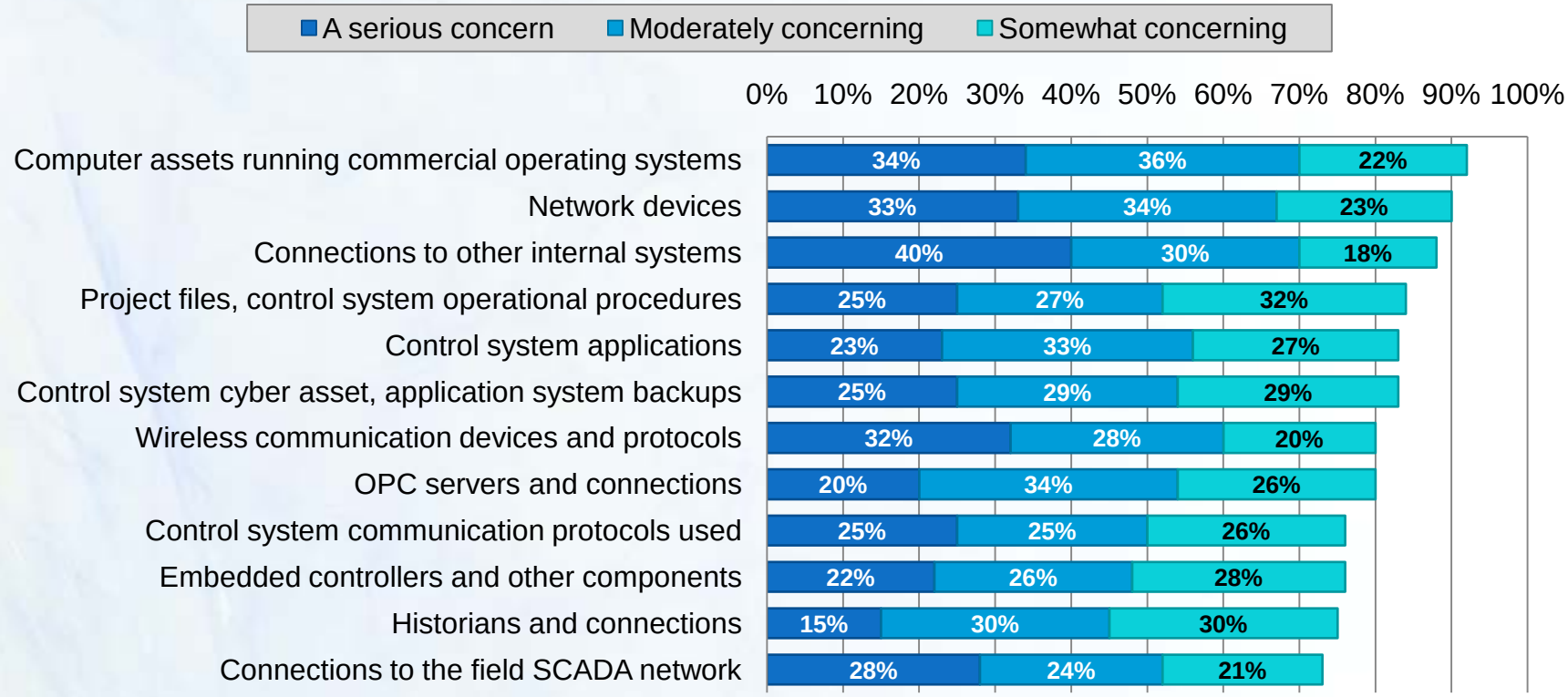
Comparing 2015 results to 2014, threat levels have generally increased, with high threat levels increasing five percentage points.



Q: What level do you perceive the control system cyber security threat within your organization to be? (n=278;186;317)

System component vulnerability

Regarding cyber security, the system components that are most concerning or vulnerable to attacks are computer assets running commercial operating systems, network devices, and connections to other internal systems.

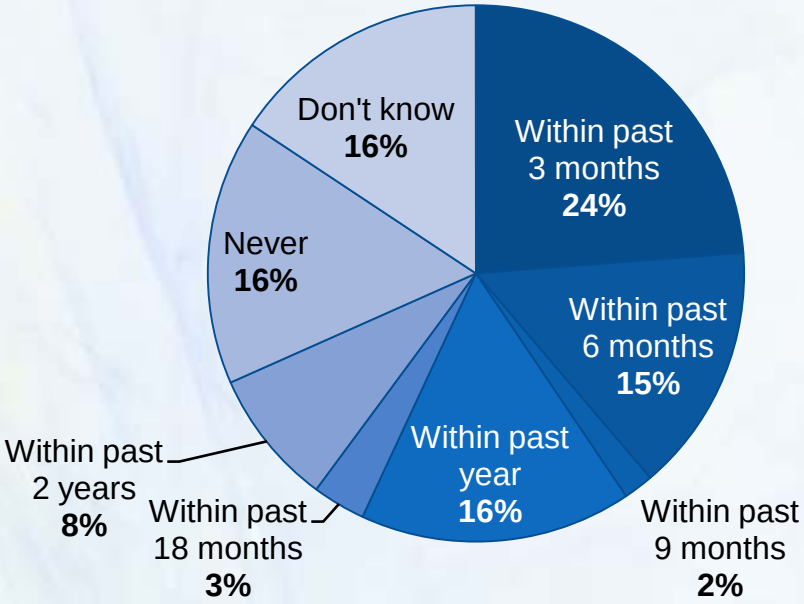


Q: Regarding the cyber security, how concerned are you about the following system components within your organization? (n=283;280;281;280;280;280;280;280;280;280;280;280)

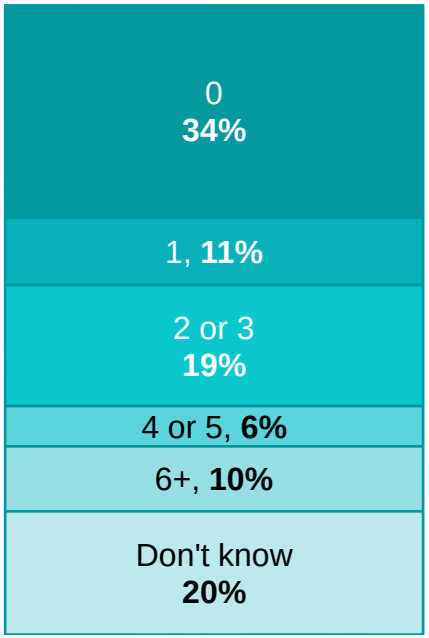
Vulnerability assessments

Thirty-nine percent of respondents claim their last vulnerability assessment was performed within the past six months, while 16% have never executed one. One-third said their assets haven't been breached within the past 2 years.

Recent vulnerability assessment



No. of cyber incidents within past 24 mos.

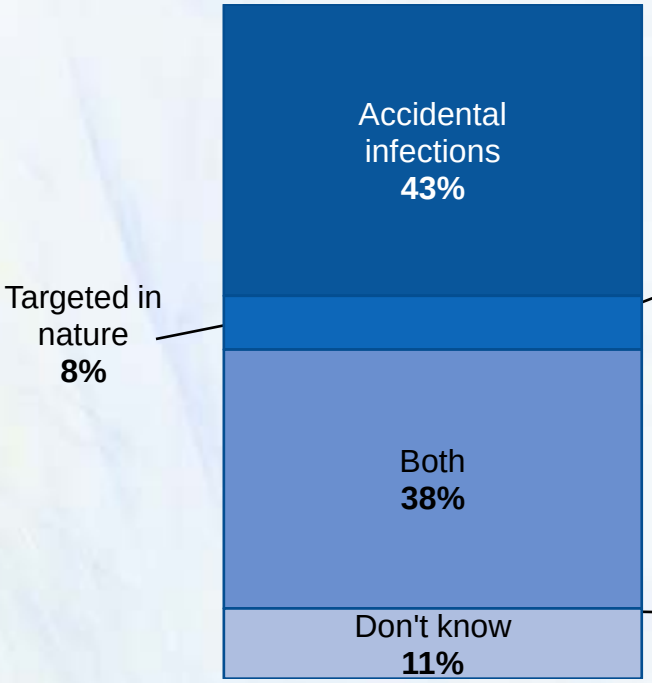


Q: When is the last time your organization performed any type of a vulnerability assessment? (n=281);
Q: How many malicious cyber incidents (infections, intrusions, etc.) into control system networks and/or control system cyber assets have you been aware of in the past 24 months? (n=281)

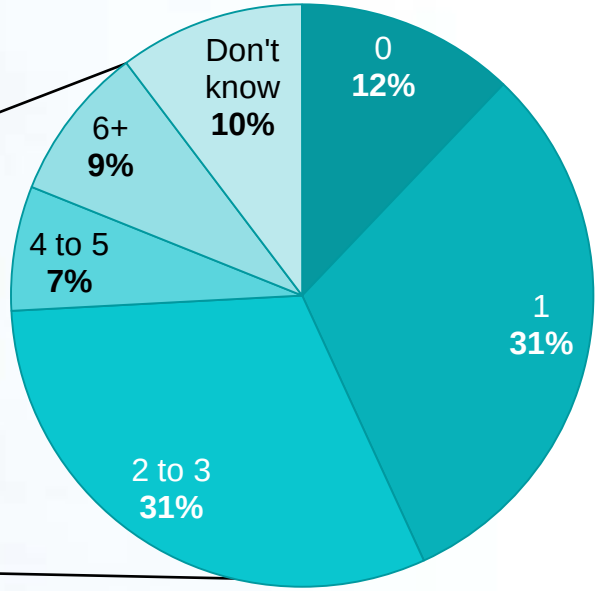
Cyber-related incidents

Of the respondents who said they have seen one or more cyber incidents in the past 2 years, 46% said these incidents were either targeted in nature or both accidental and targeted.

Nature of incidents



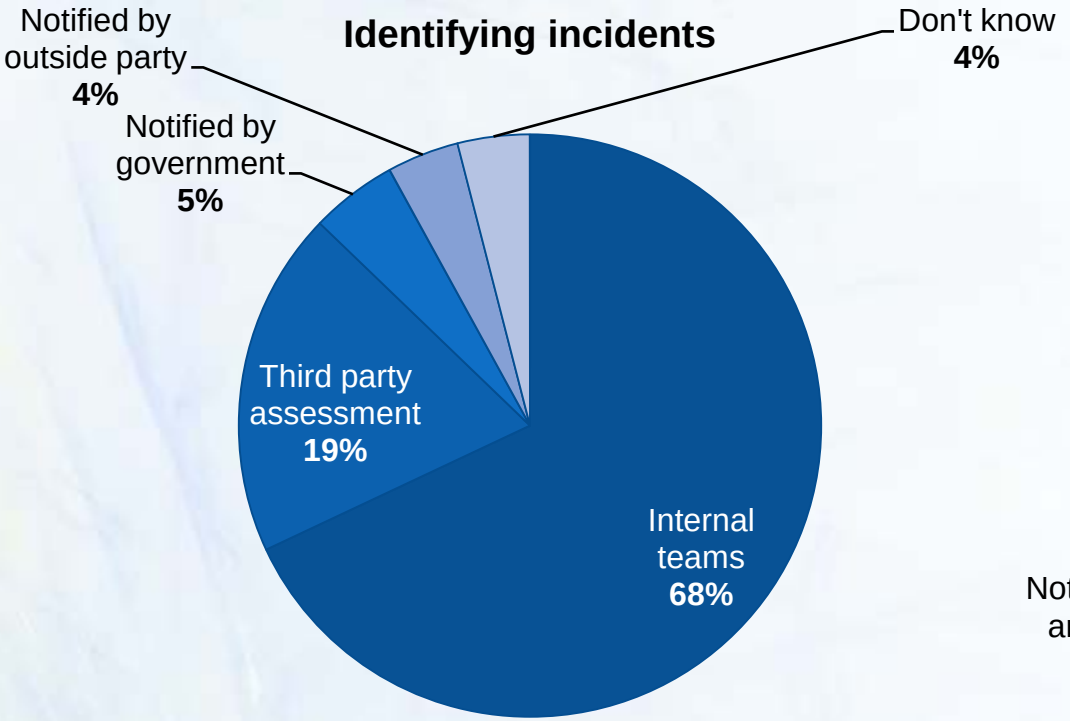
No. of advanced targeted intrusions

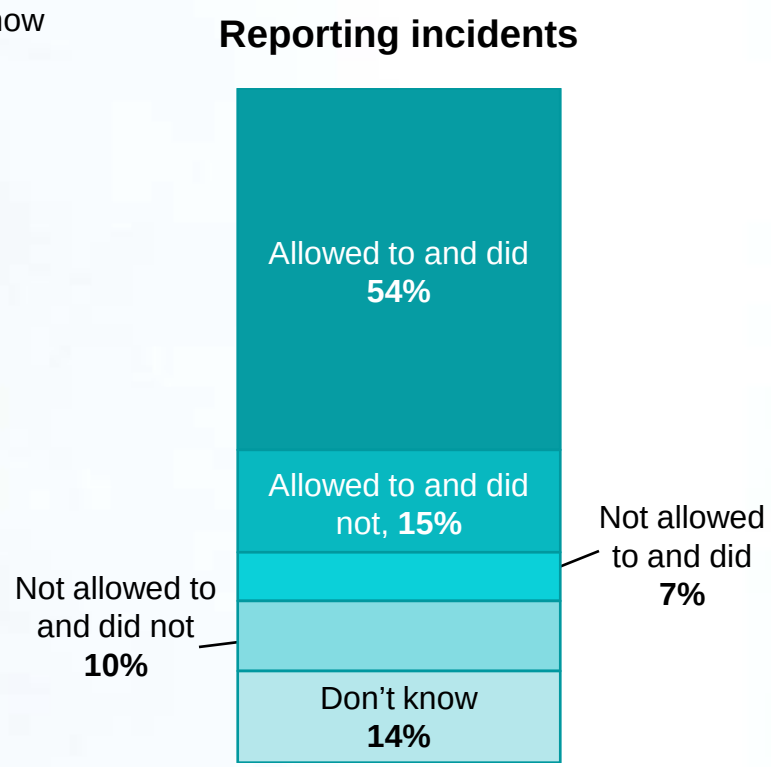


Q: Of the cyber-related incidents you've seen, they were: (n=125); Q: Of the targeted intrusions, how many would you label as advanced? (n=58)

Identifying and reporting incidents

Most cyber-related incidents are identified by internal teams, according to respondents. More than half said their management team was allowed to report these incidents and did.



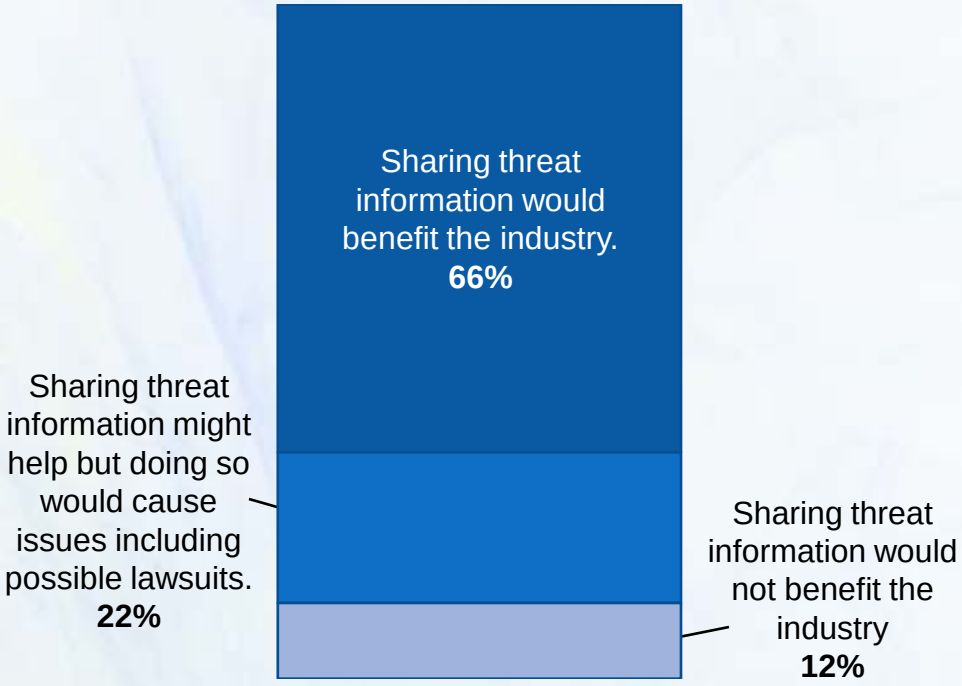


Q: Of the cyber incidents you are aware of how were they identified? (n=125); Q: Of the cyber-related incidents, did you feel you or your management team was allowed to report the incident? (n=125)

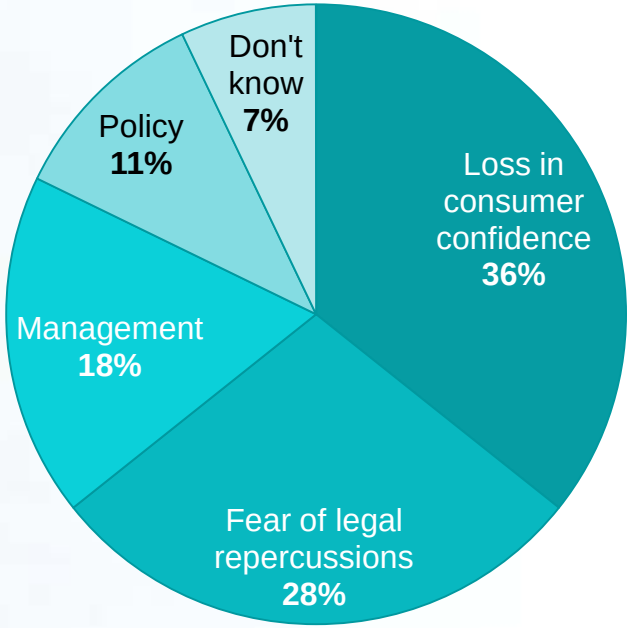
Publicly reporting incidents

Two-thirds of respondents say publicly reporting information on cyber-related incidents would benefit the industry, and 36% agree that the biggest problem with reporting is the fear of losing consumer confidence.

Opinion on sharing incident reports



Issues with reporting incidents

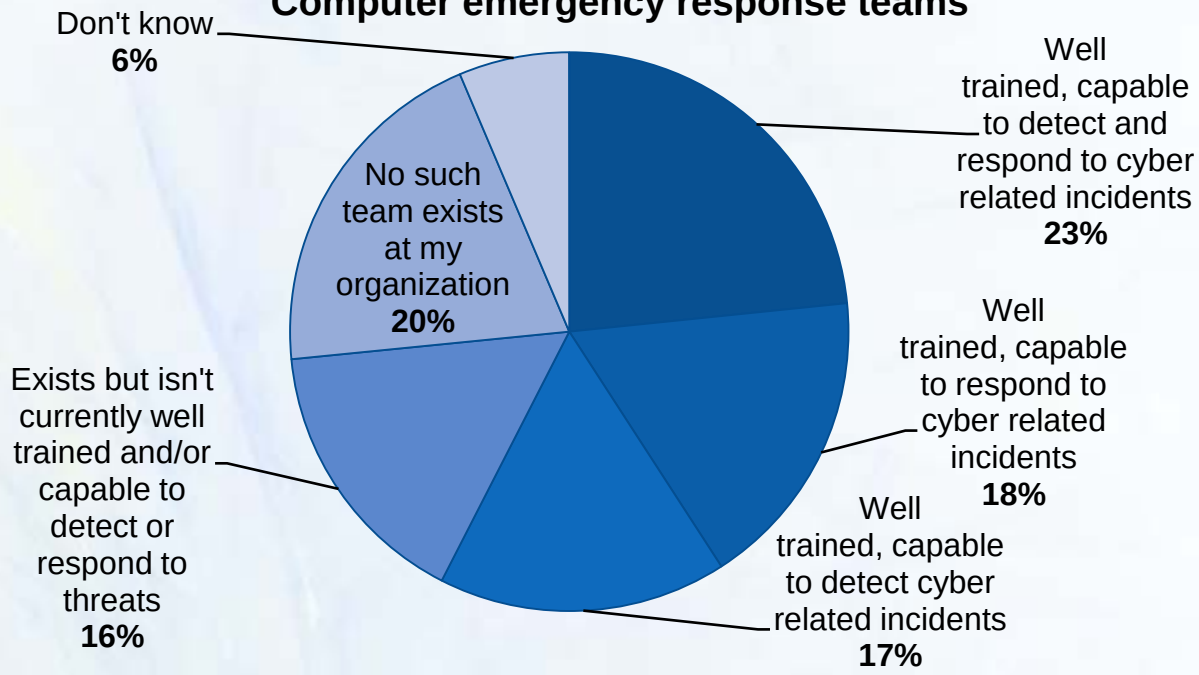


Q: If you were able to publicly report on cyber incidents, which of the following best represents your opinion? (n=125); Q: What do you feel is the biggest problem in reporting cyber related incidents? (n=28)

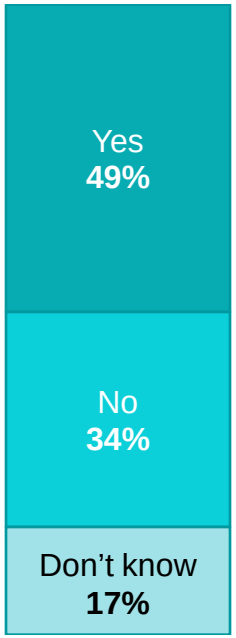
Emergency response teams

Twenty-three percent of respondents say their computer emergency response teams appear well training and capable of detecting and responding to cyber-related incidents, while 49% report having an operating operational incident response team within their organization.

Computer emergency response teams



Operating incident response team

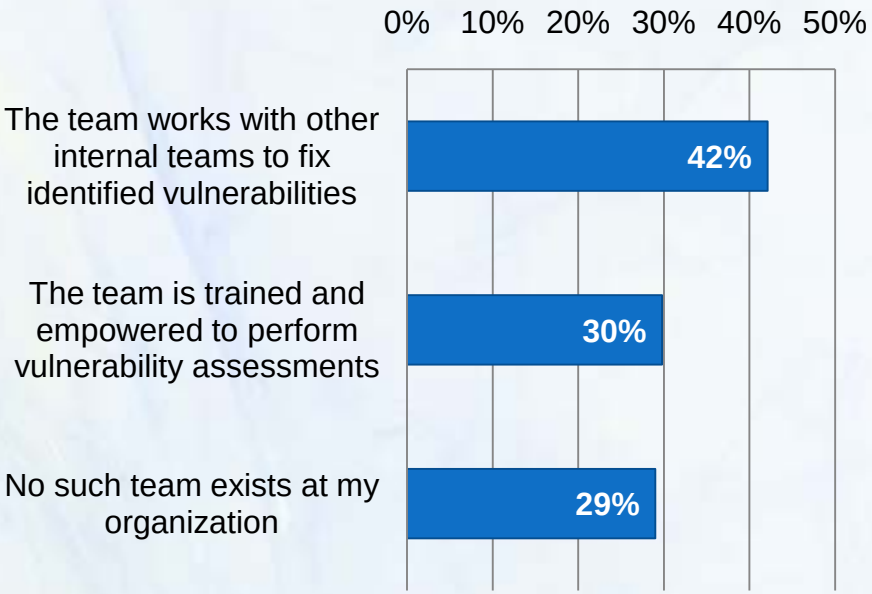


Q: Please choose one of the following regarding your computer emergency response team: (n=252);
Q: Does your organization have an operating operational incident response team to respond to any type of a security breach/incident? (n=252)

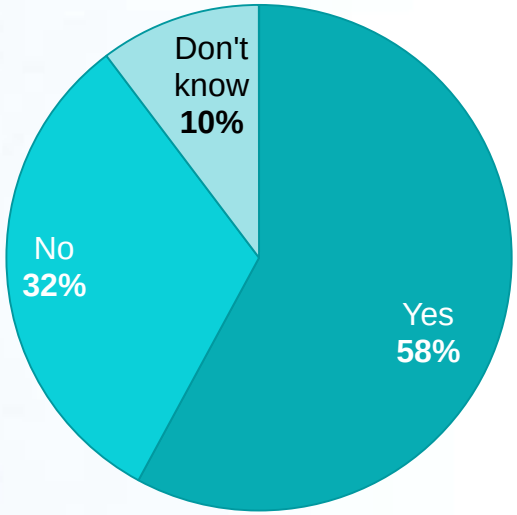
Internal vulnerability assessments, processes

Forty-two percent of respondents say their internal vulnerability assessment team works with other internal teams to fix identified vulnerabilities, and 58% said their organization has implemented a change control process for cyber assets that is able to prevent unauthorized and potentially vulnerable changes from taking place.

Internal vulnerability assessment team



Change control process for cyber assets

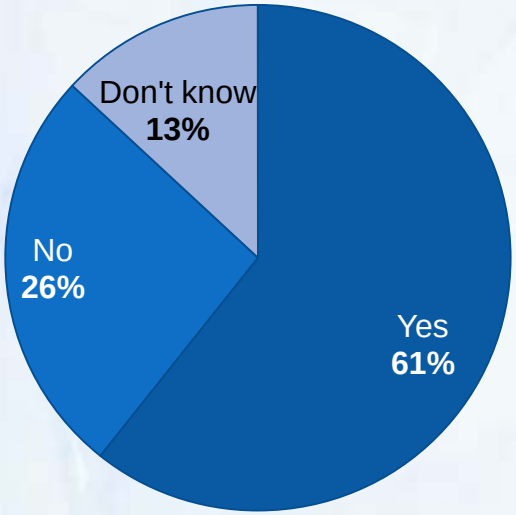


Q: Which of the follow statements describe the team at your organization that performs internal vulnerability assessments? (n=225); Q: Has your organization implemented a change control process for cyber assets that is able to prevent unauthorized and potentially vulnerable changes from taking place on your control system? (n=252)

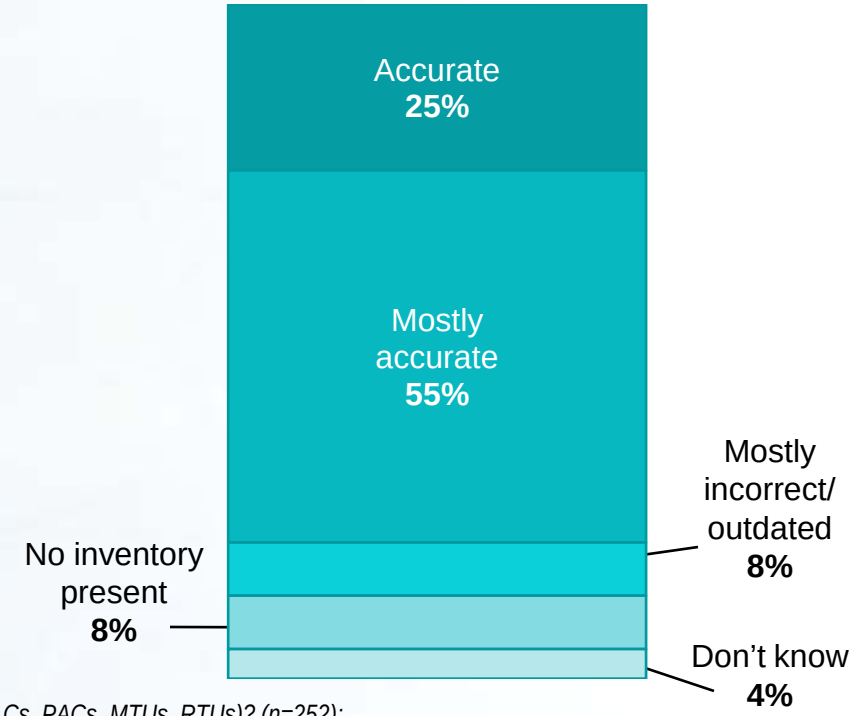
Logical configurations, systems inventory

Six in 10 of respondents' organizations protect the logical configurations of all control system devices, and only 25% have a complete inventory of information systems that reside and operate on control networks.

Protecting device logical configurations



Inventory of information systems

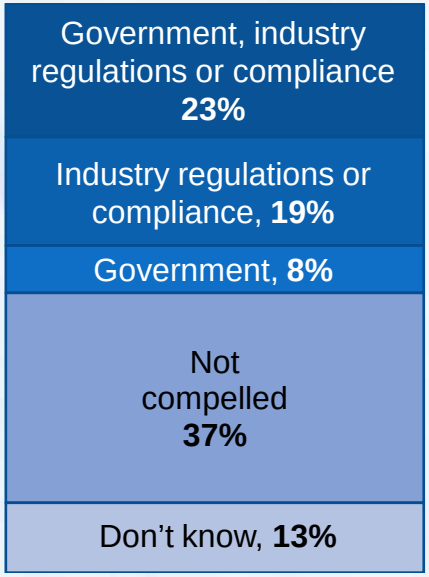


Q: Does your organization protect the logical configurations of all control system devices (e.g. PLCs, PACs, MTUs, RTUs)? (n=252);
Q: How would you describe your organization's inventory of information systems that reside and operate on the control network? (n=252)

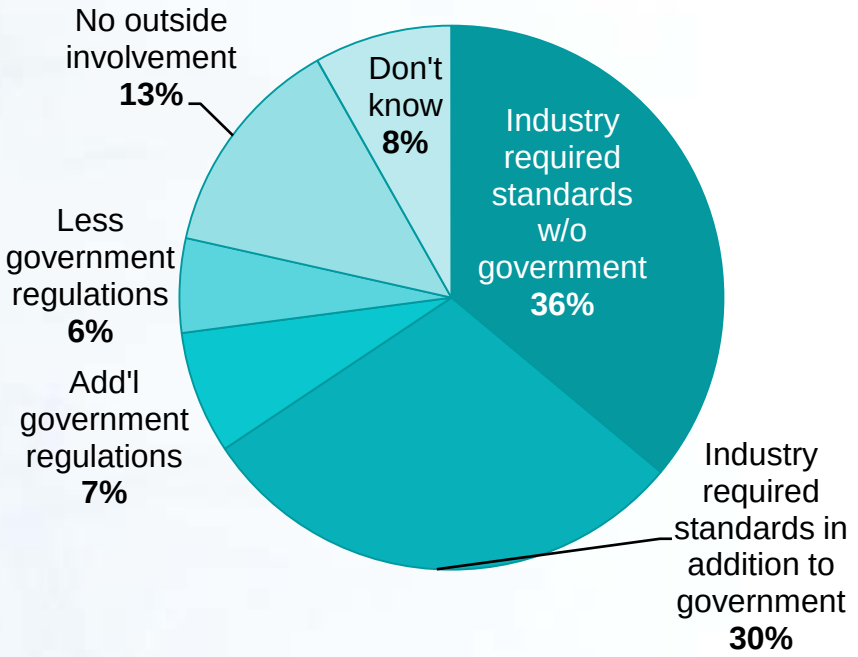
Government and outside involvement

Twenty-three percent of respondents say they are compelled by the government and industry regulations or compliance to enact information control systems protections for cyber assets, and 36% say that only required industry standards would improve their efforts towards a proper security system.

Information control system protections



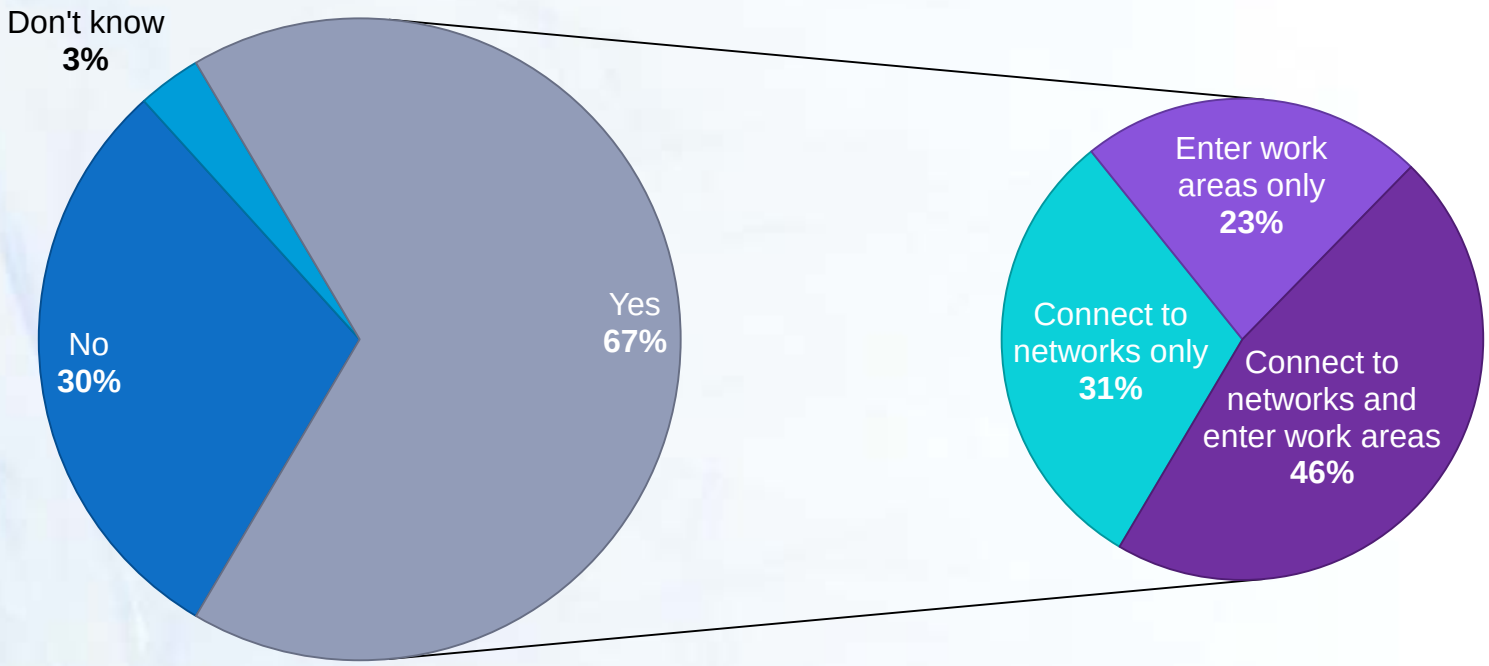
Improving system security controls



Q: Please choose one of the following with regards to your organization being compelled to enact information control system protections for control system cyber assets: (n=252);
Q: What do you feel would improve or enable your efforts to implement proper control system cyber security controls? (n=233)

Mobile device security

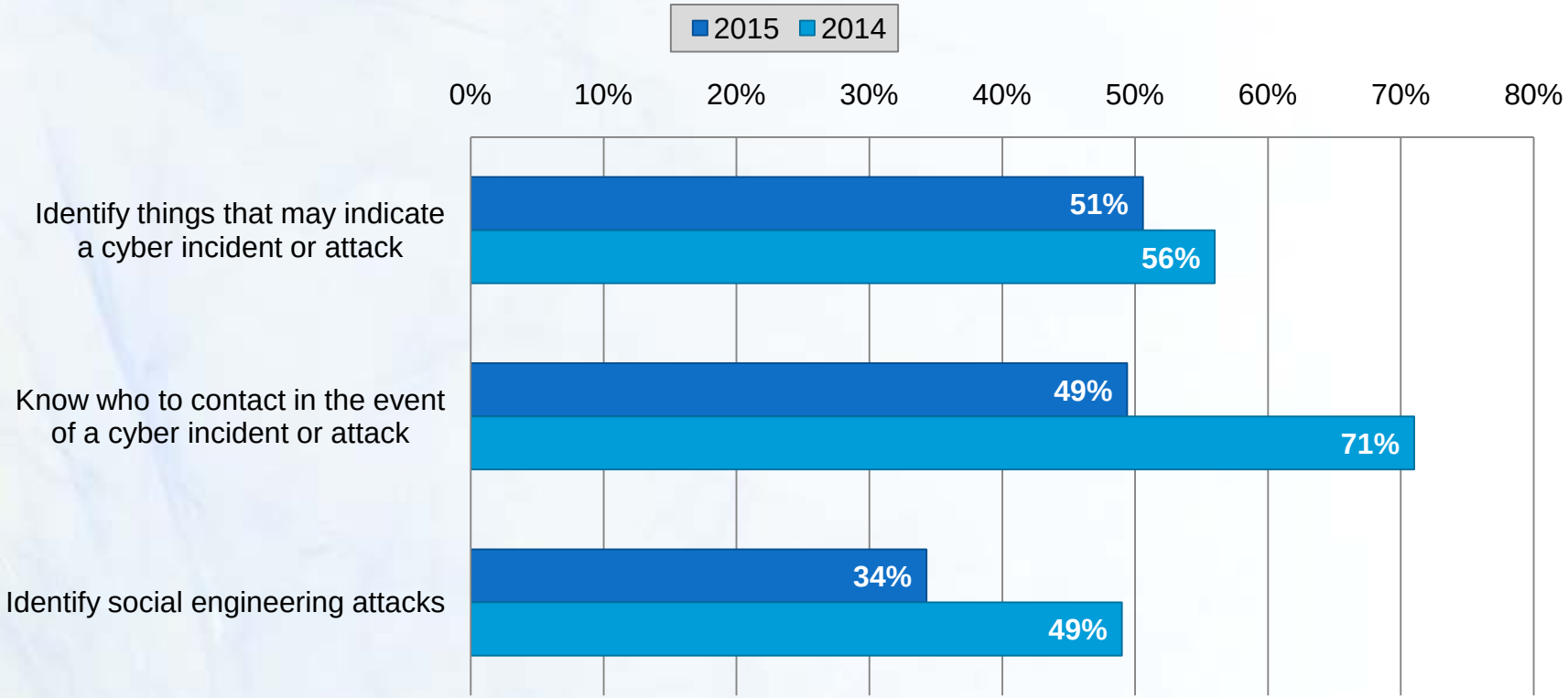
Of the organizations that allow mobile device usage, 46% allow them to connect to networks and enter work areas, while 23% only allow them to enter the work areas and 31% only allow them to connect to networks.



Q: Does your organization allow mobile devices—such as smartphones and tablets—to connect to networks or enter work areas? (n=252)

Employee training

Forty-nine percent of organizations inform their employees about who to contact in the event of a cyber incident or attack, compared to 71% in 2014.

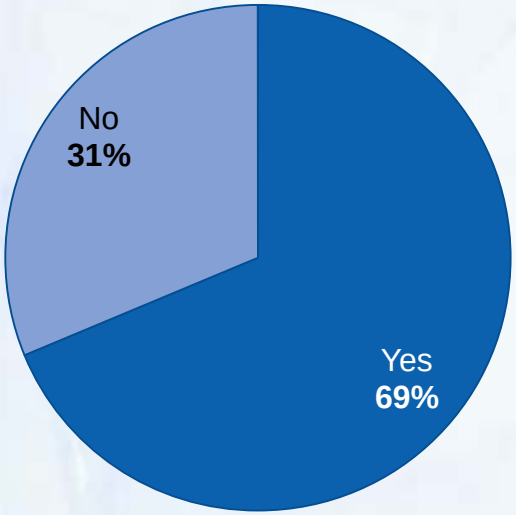


Q: Please select the training that employees at your organization receive: (n=172;189)

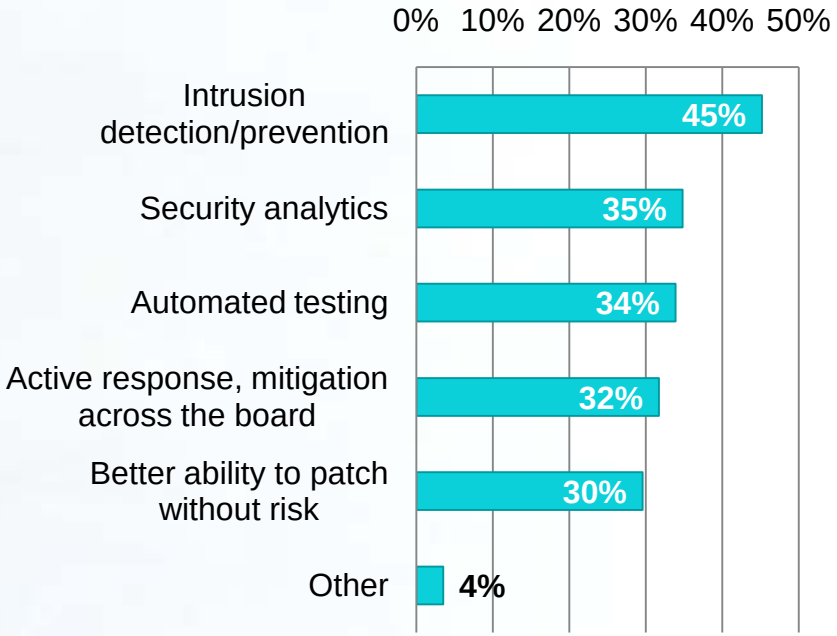
Network connections, desired capabilities

Seven in 10 respondents have an accurate depiction of all control system cyber assets and their network conditions. When asked which capabilities they wished they were able to perform, top answers included intrusion detection/prevention (45%), security analytics (35%), and automated testing (34%).

Have an accurate depiction of assets, connections



Desired security capabilities

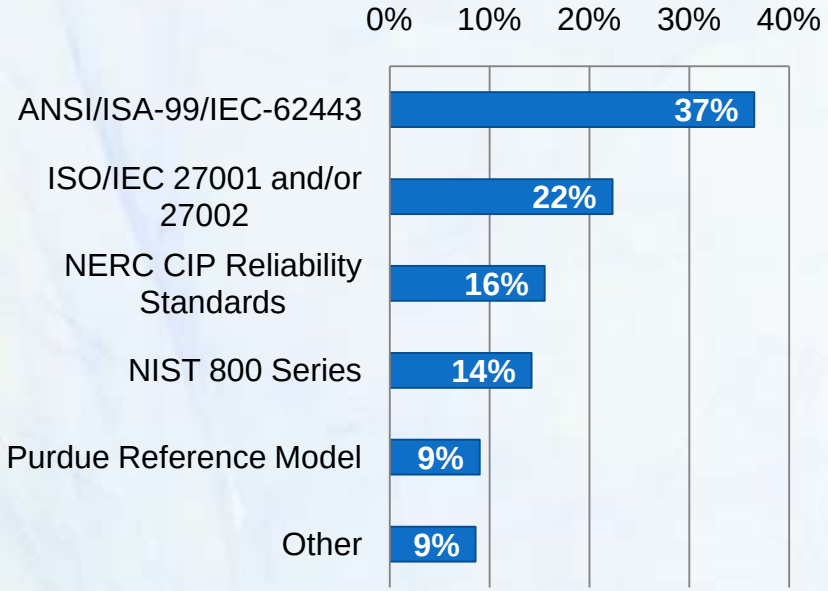


Q: Do you have an accurate depiction of all control system cyber assets and their network connections? (n=233); Q: What cyber security capability do you wish you had the ability to perform? (n=210)

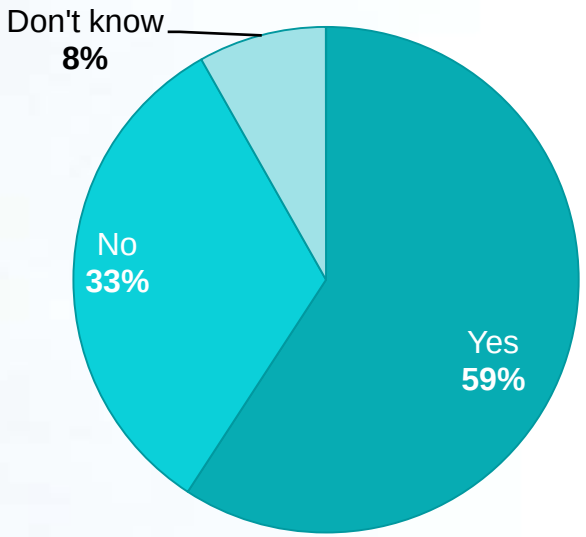
Guidelines followed, corporate/control connections

Thirty-seven percent of respondents say they follow ISA/IEC-62443 to protect their control systems. Three out of five respondents say their engineers, technicians, and/or subcontractors use computer systems that move from corporate to control network connectivity.

Requirements, standards, guidelines used



Use computer systems from corporate to control networks

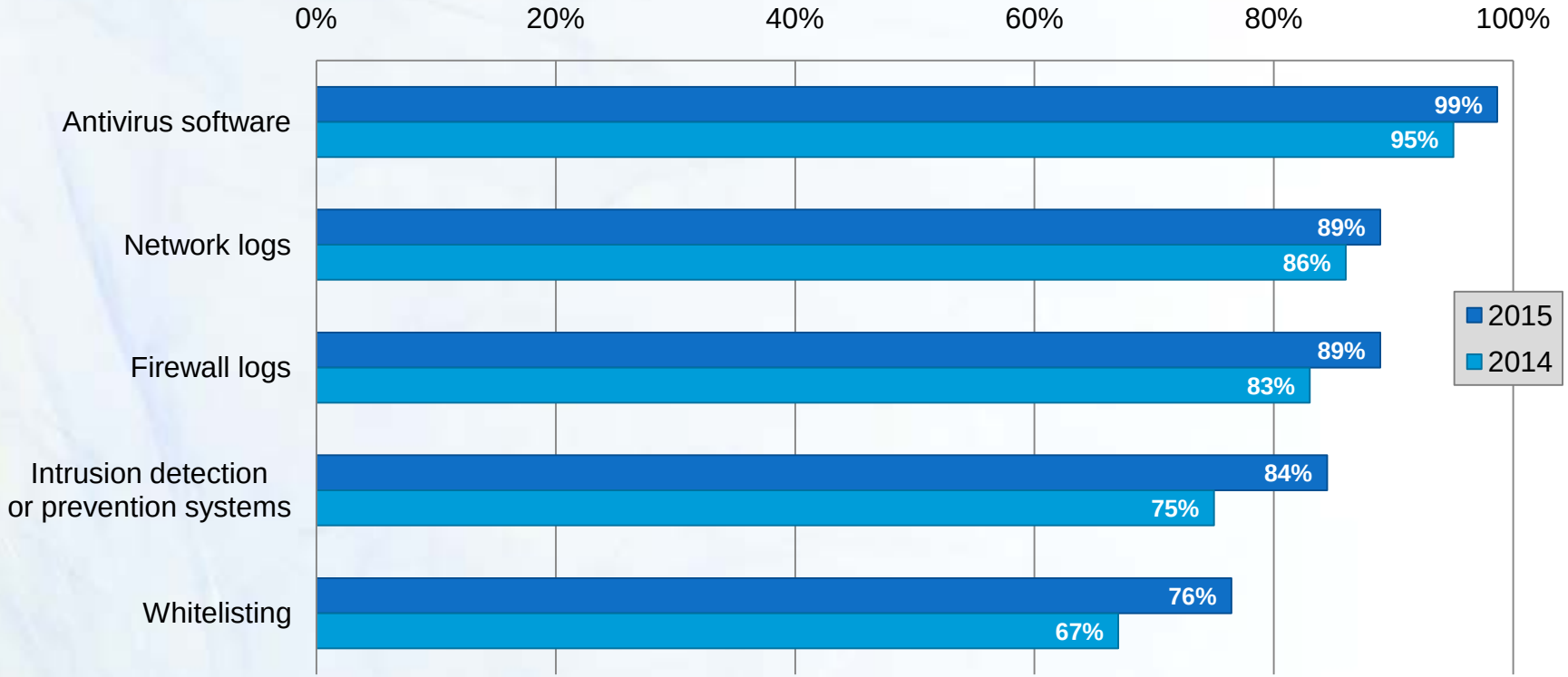


Q: What requirements, standards, or guidelines do you use to protect your control system? (n=152);
Q: Do your engineers, technicians, and/or subcontractors use computer systems that move from corporate network connectivity to control network connectivity? (n=233)

Resources for monitoring cyber security events

Resources used

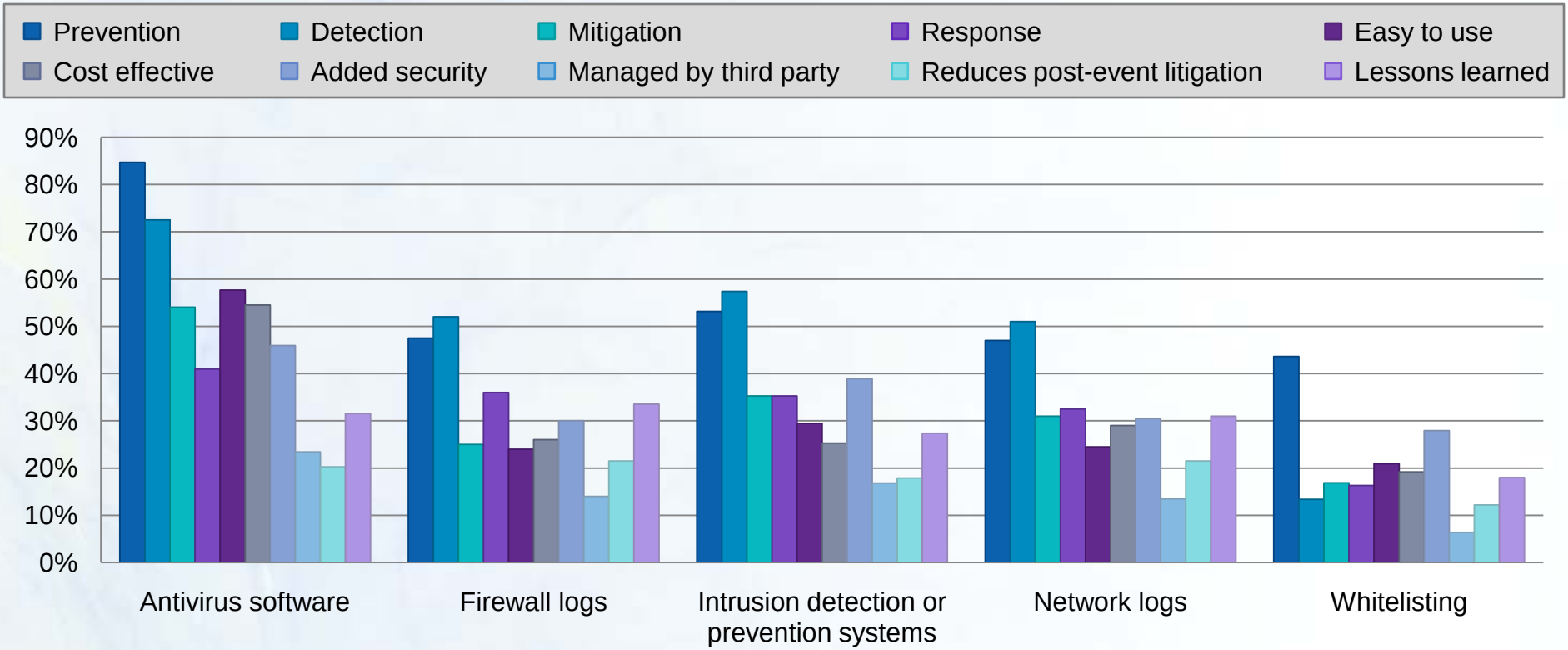
The top three resources used by respondents to monitor control system cyber security events are antivirus software (99%), network logs (89%), and firewall logs (89%).



Q: What resources do you use to monitor control system cyber security events? (n=225;189)

Resource advantages

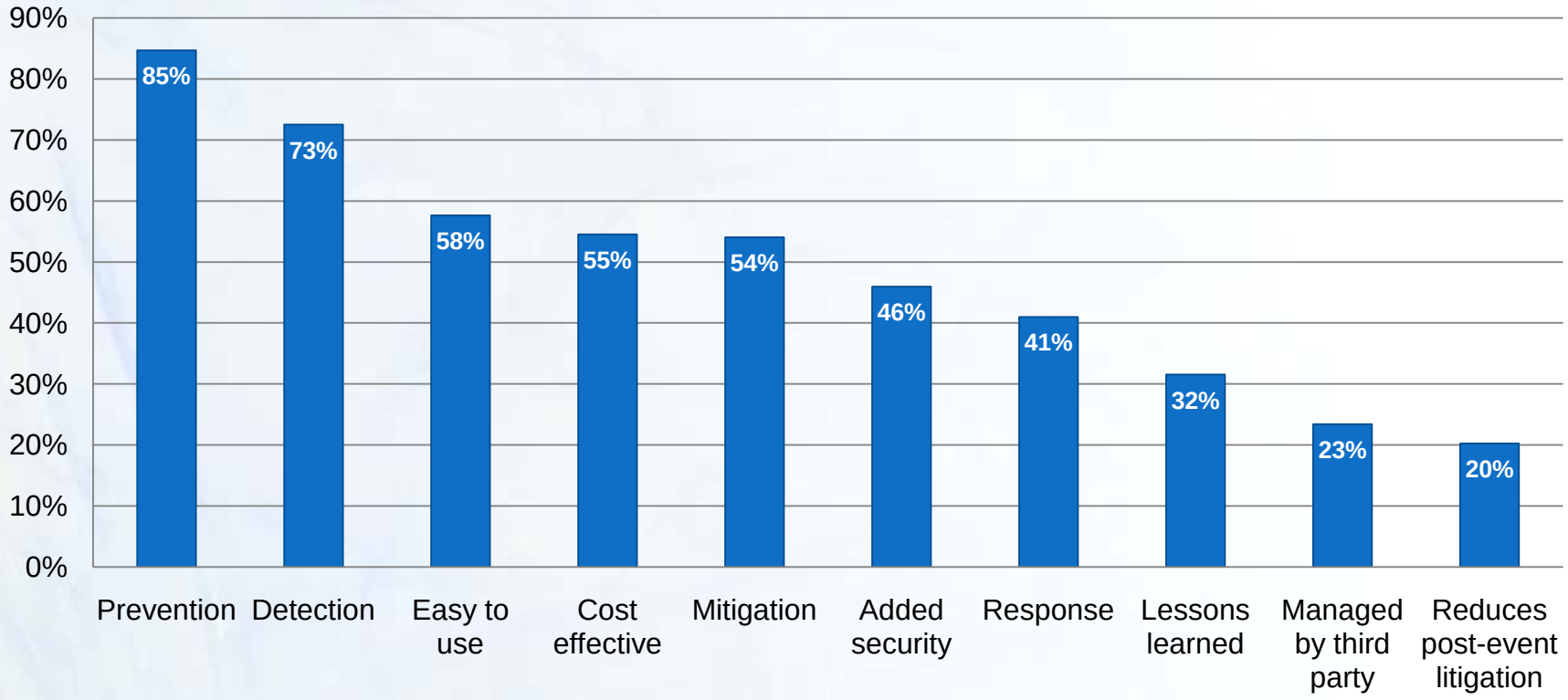
Prevention, detection, and added security are among the top factors respondents value when choosing monitoring resources for control system cyber security events.



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=216;209;179;162;169;164;162;102;104;132;101)

Antivirus software

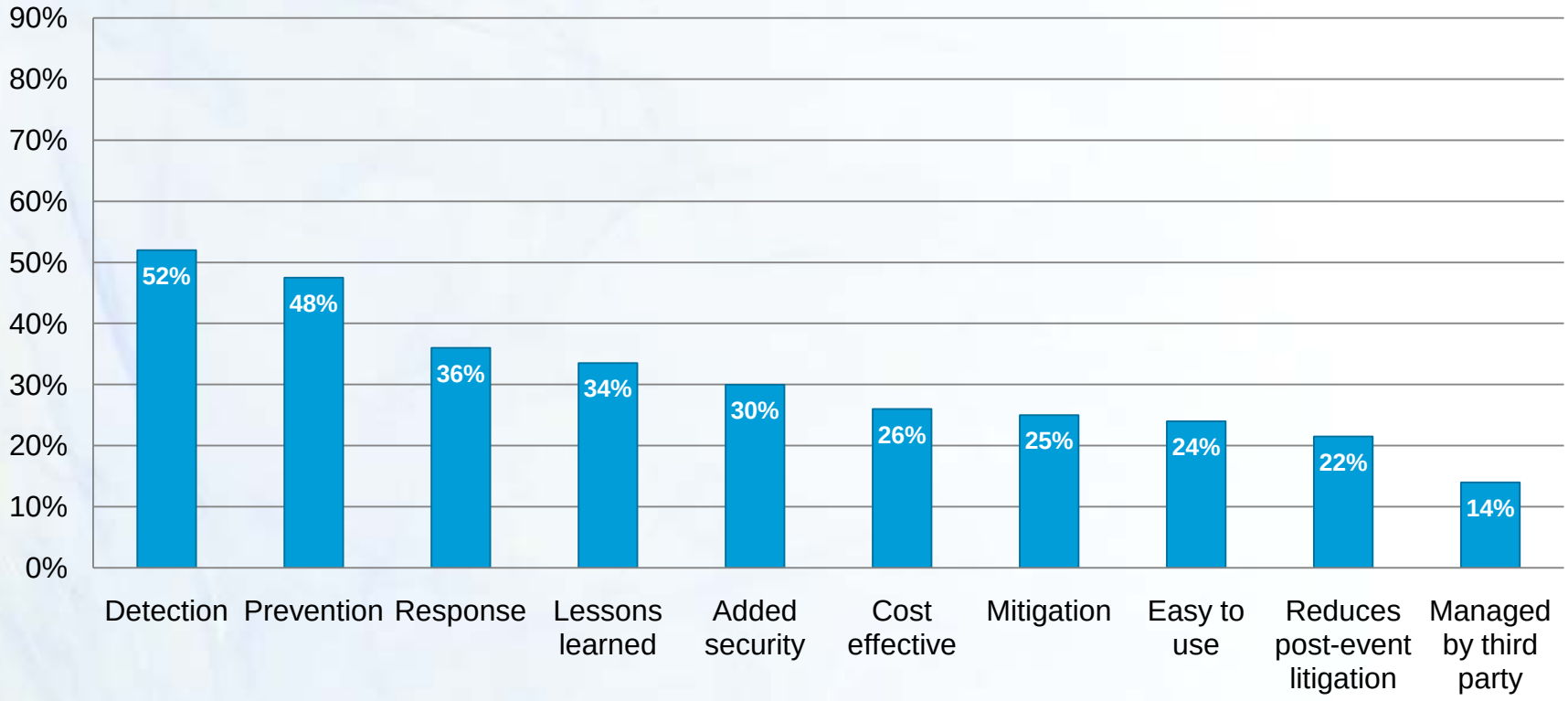
Respondents who use antivirus software to monitor control system cyber security do so for the prevention (85%), detection (73%), and easy-of-use benefits (58%).



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=222)

Firewall logs

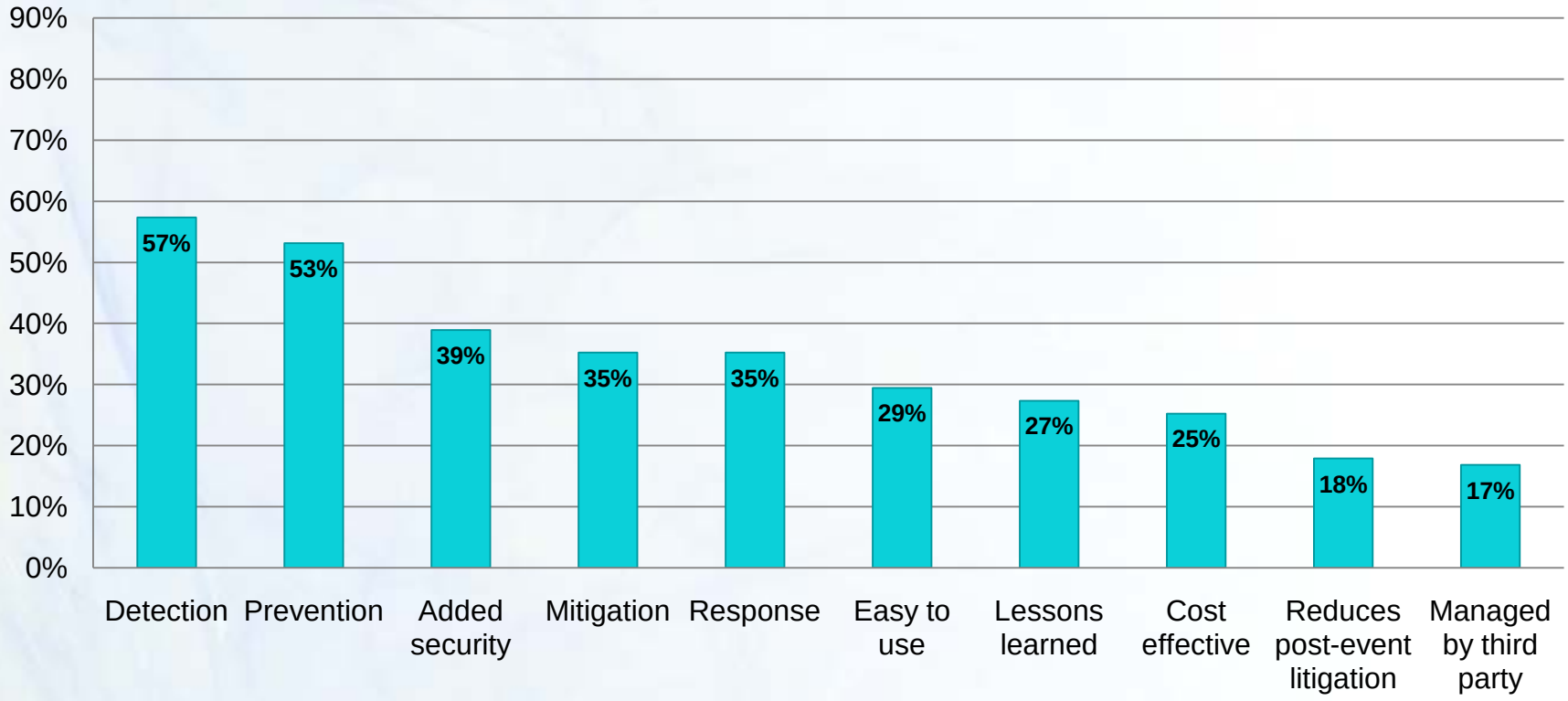
Fifty-two percent of respondents use firewall logs to monitor control system cyber security events for their detection benefits, while prevention (48%) and response time (36%) are other key advantages.



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=172)

Intrusion detection or protection systems

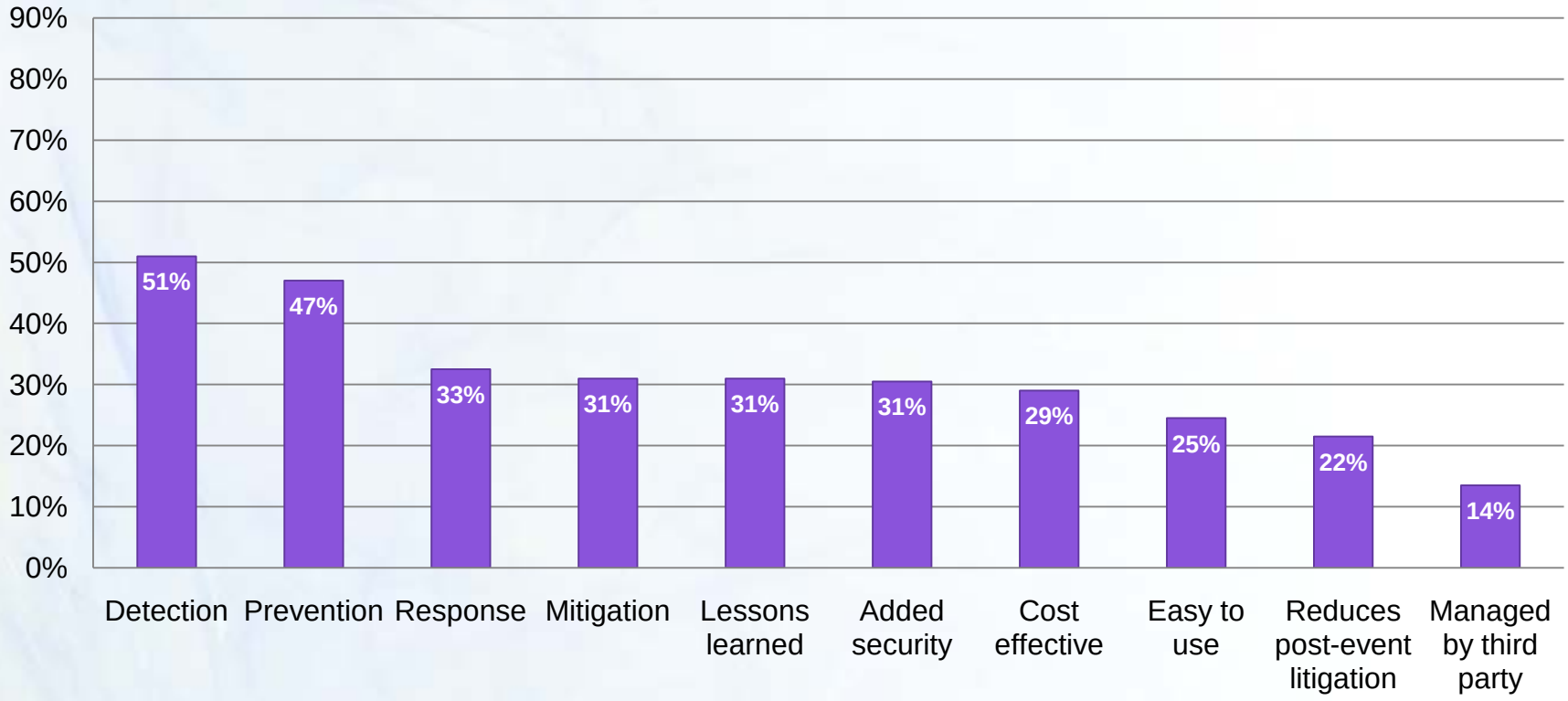
The top advantages to using intrusion detection or protection systems to monitor control system cyber security events, according to respondents, are detection (57%), prevention (53%), and added security (39%).



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=190)

Network logs

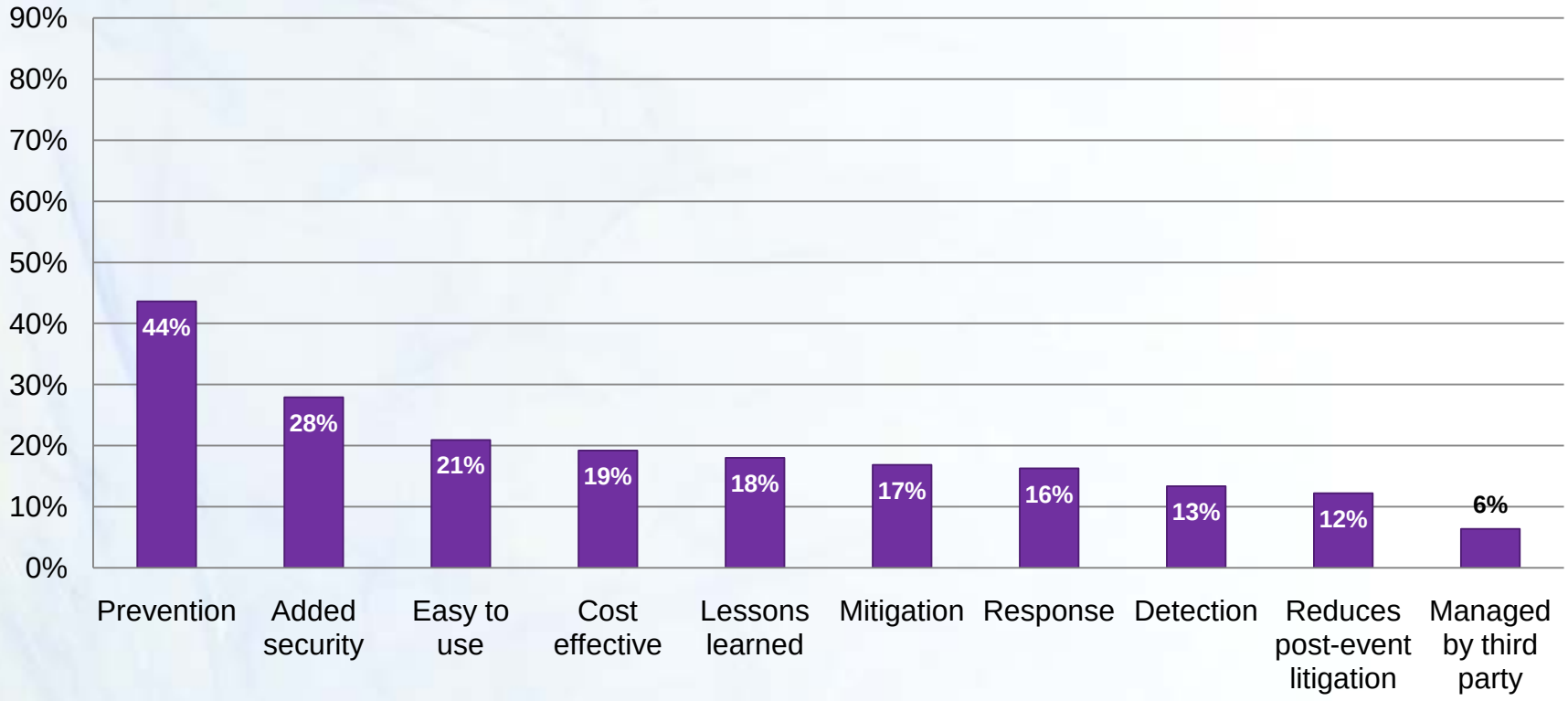
The top advantages of using network logs to monitor control system cyber security events are detection (51%), prevention (47%), and response time (33%).



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=200)

Whitelisting

Forty-four percent of respondents who use whitelisting to monitor control system cyber security events do so for its prevention benefits—down from 65% in 2014—but only 13% use it for detection.



Q: What are the advantages to the resources you use to monitor control system cyber security events? (n=200)

Additional resources

Thank you for downloading the *Control Engineering* 2015 Cyber Security Study. Use the links below to access additional information on related news, products, and research.

Articles and news

- Virtualization, cloud
- Cyber security
- Ethernet
- Wireless
- Other networks
- I/O systems, modules

Programs and resources

- Apps for Engineers
- Global System Integrator Database
- Online Training Center
- Videos
- Webcasts
- Products
- Case studies
- eGuides
- Safety & Security eNewsletter

Editorial research studies

- 2014 Mobility, Ethernet & Wireless
- 2014 Information Integration
- 2014 System Integration
- 2014 Cyber Security
- 2013 Salary & Career Survey

Contact information

Amanda Pelliccione
Director of Research
apelliccione@cfemedia.com
631-320-0655

Mark Hoske
Content Manager
mhoske@cfemedia.com
847-830-3215