RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: AST1-R02

State of Cybersecurity: 2016 Findings and Implications

Jennifer Lawinski
Editor-in-Chief
RSA Conference
Jennifer.lawinski@rsa.com

Ron Hale Ph.D., CISM
Chief Knowledge Officer
ISACA
rhale@isaca.org

Topics Professionals Want to Know About

RSA Conference submissions tell the story:

Top 10 Topics

1. Internet of Things
2. Industrial Control Systems and the Industrial Internet of Things
3. Encryption
4. Artificial Intelligence and Machine Learning.
5. Crowdsourcing
6. The Role of the Researcher
7. Healthcare and Automotive
8. Security Meets the Board of Directors
9. Privacy and Legislative Volatility
10. INAMOIBW

The Internet of Things is a Big Deal

For the second year in a row submissions around IoT surged, showing that it's a topic on the minds of security professionals.

The survey this year asked questions about IoT and respondents agree it's a major issue that they'll be facing in years to come.

AI and Machine Learning Have You Worried

More sessions focused on artificial intelligence and machine learning like “Rise of the Hacking Machines," and the survey results showed that security pros are concerned.

Security Meets the Board of Directors

Companies are looking to bridge the gap between threat intelligence and risk management, but many of the respondents to our survey don't feel they have the security personnel and processes in place to handle serious security threats.

Survey Results Review

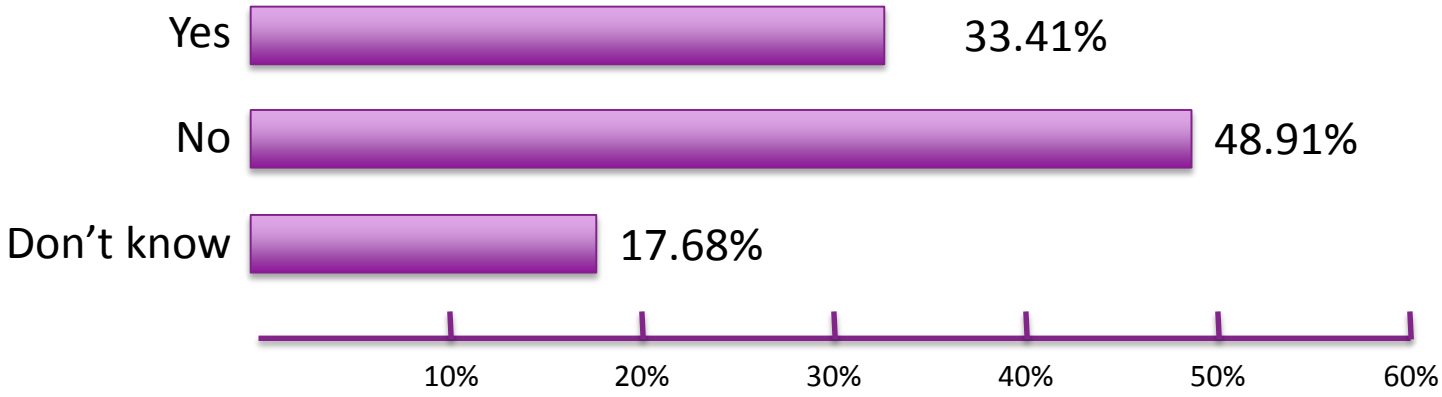
The State of Cybersecurity 2016

Summary Findings

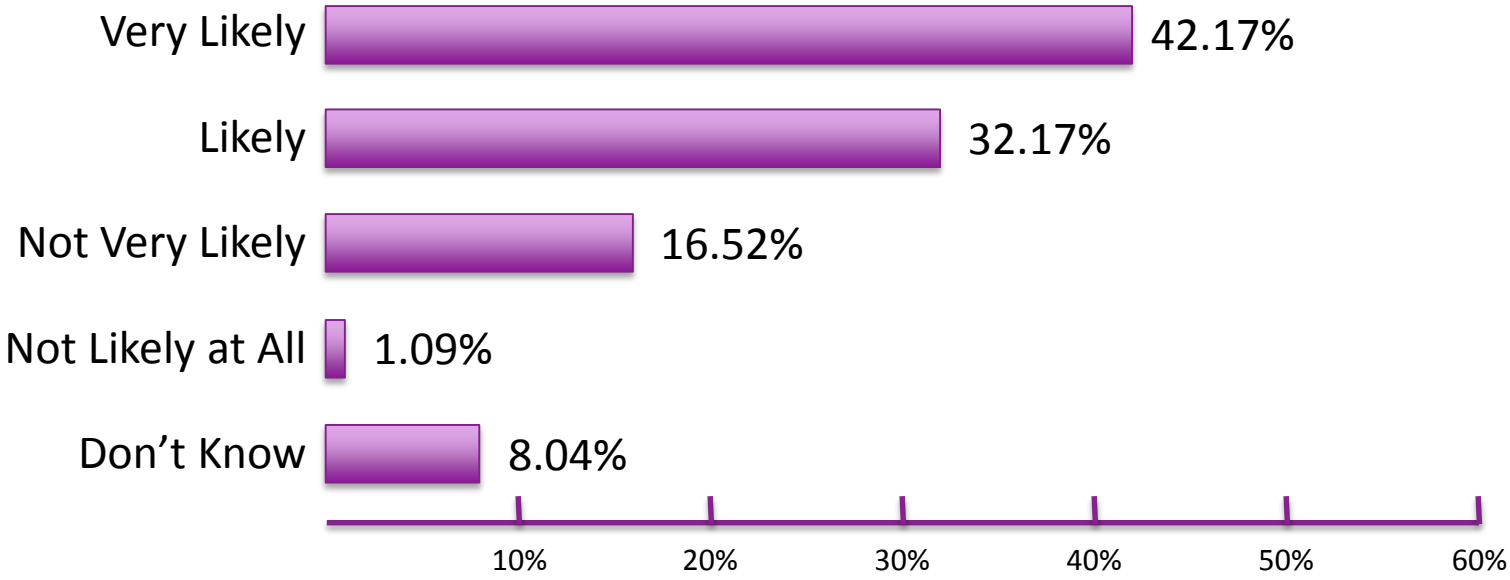
Four Prominent Questions

1. What are enterprises experiencing in terms of cyber-incidents?
2. How concerned are enterprise decision makers?
3. Are security organizations capable of addressing cyber-incidents?
4. What does the future hold given new technology directions?

Were You a Victim in 2015?



Likelihood of Being a Victim in 2016?



Frequency of Attack

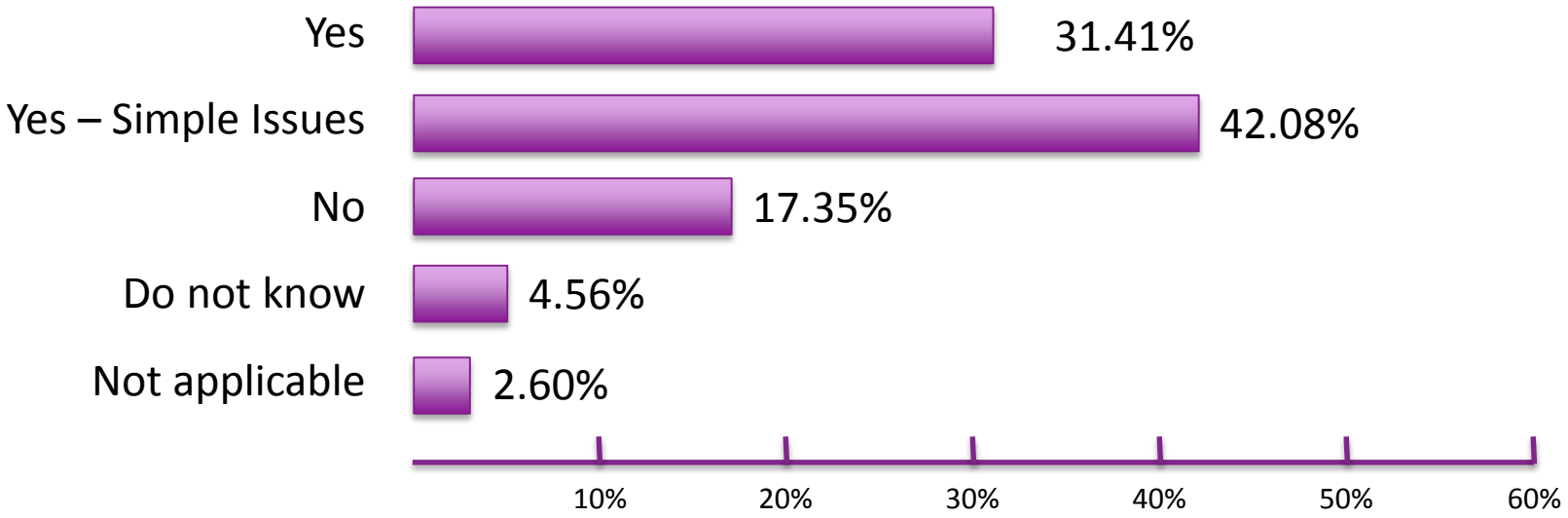
	Daily	Weekly	Monthly	Quarterly
Online Identity Theft	4.08%	4.56%	5.52%	20.62%
4 Hacking	11.06%	7.29%	9.18%	25.18%
2 Malicious Code	16.36%	12.38%	12.85%	26.40%
Loss of Intellectual Property	1.44%	2.40%	4.08%	19.90%
Intentional Damage to Computer Systems	0.95%	1.43%	5.01%	18.38%
3 Physical Loss	1.42%	6.38%	9.69%	37.12%
1 Phishing	29.67%	16.82%	15.19%	18.69%
Denial of Service	4.05%	5.48%	9.76%	27.38%
Insider Damage	2.91%	1.69%	9.69%	21.79%
Don't Know	13.13%	2.32%	3.86%	6.18%
	8.4%	6.3%	8.7%	22.8%

CSX CYBERSECURITY NEXUS

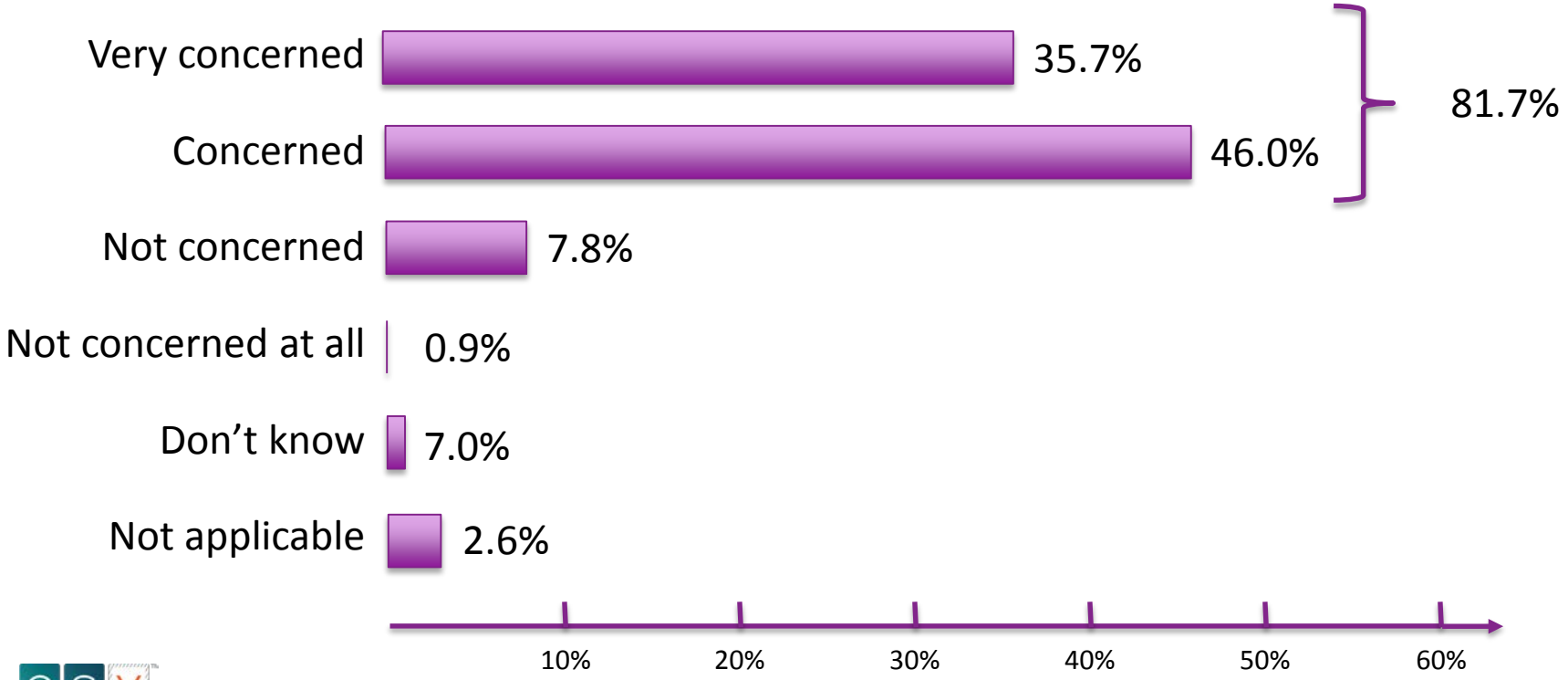
Frequency of Attack – Known and Unknown

	Known	Unknown
Online Identity Theft	34.77%	65.23%
Hacking	52.71%	47.29%
Malicious Code	67.99%	32.01%
Loss of Intellectual Property	27.82%	72.18%
Intentional Damage to Computer Systems	25.78%	74.22%
Physical Loss	54.61%	45.39%
Phishing	80.73%	19.63%
Denial of Service	46.67%	53.33%
Insider Damage	36.08%	63.92%
Don't Know	25.48%	74.52%
	46.2%	53.8%

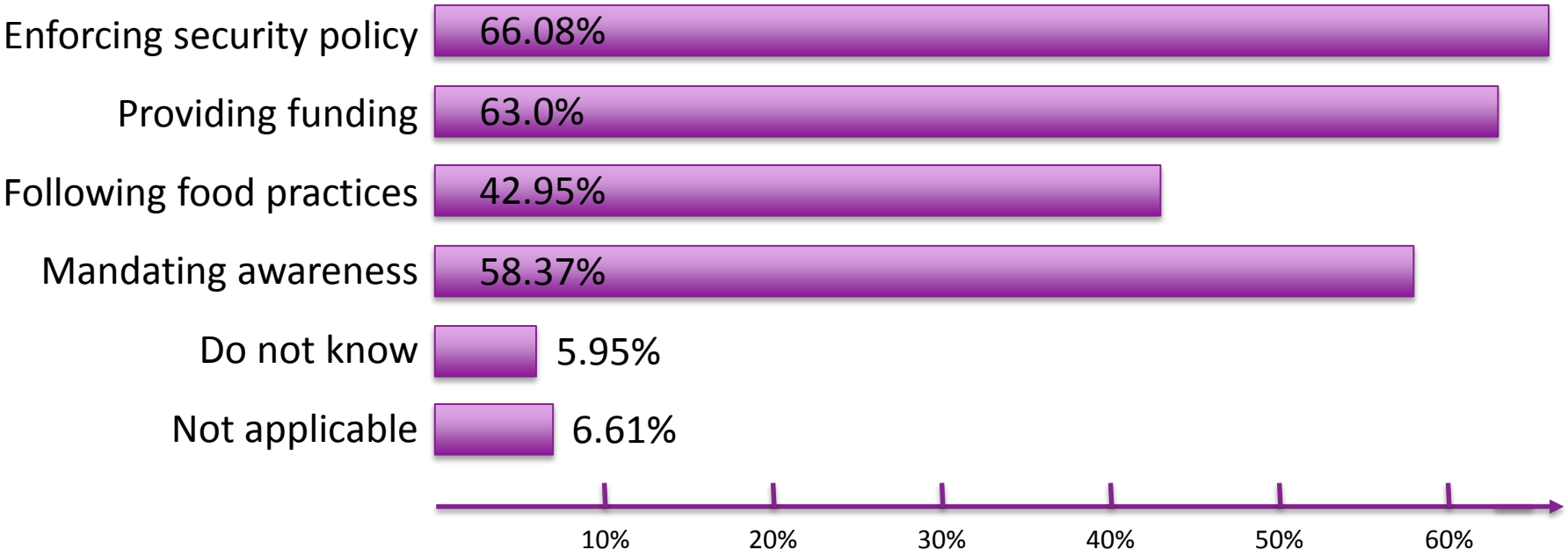
Ability to Detect and Respond



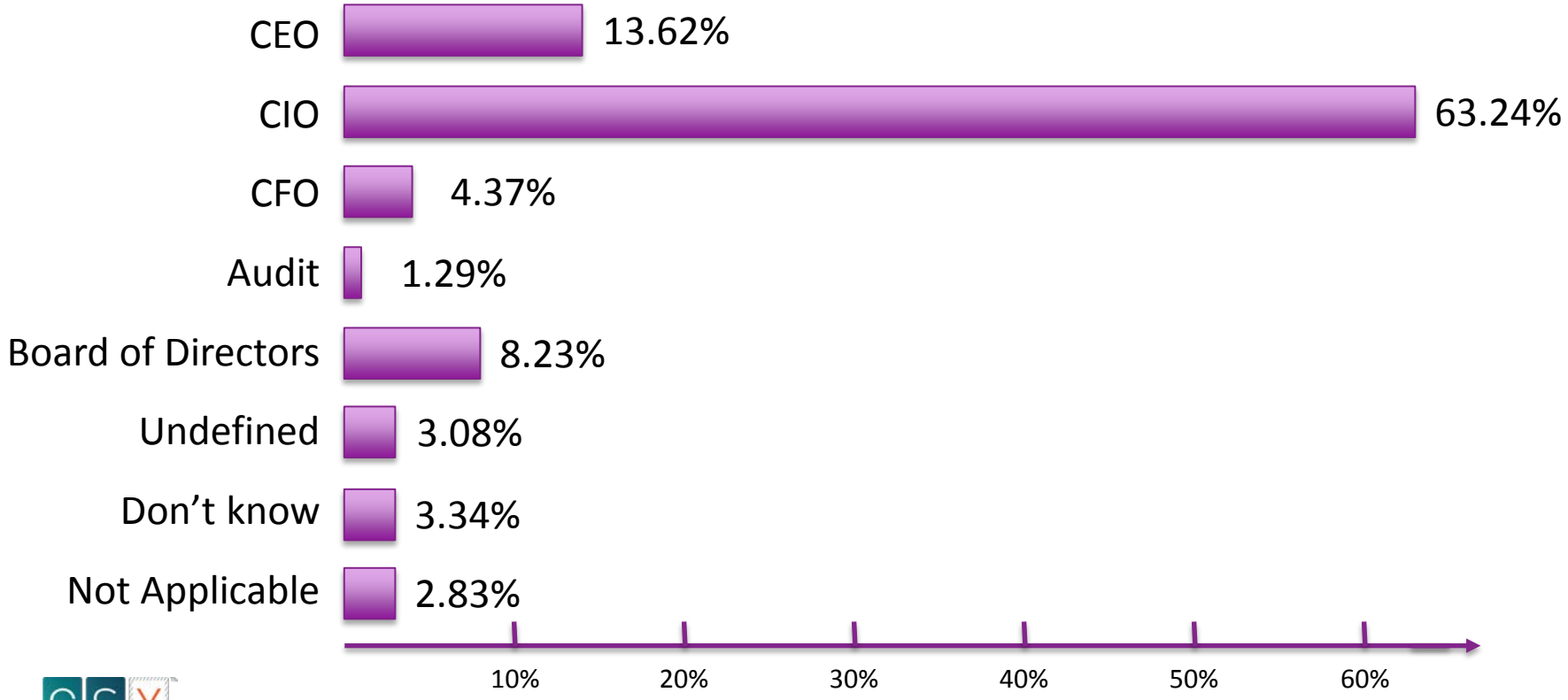
Level of Board Concern



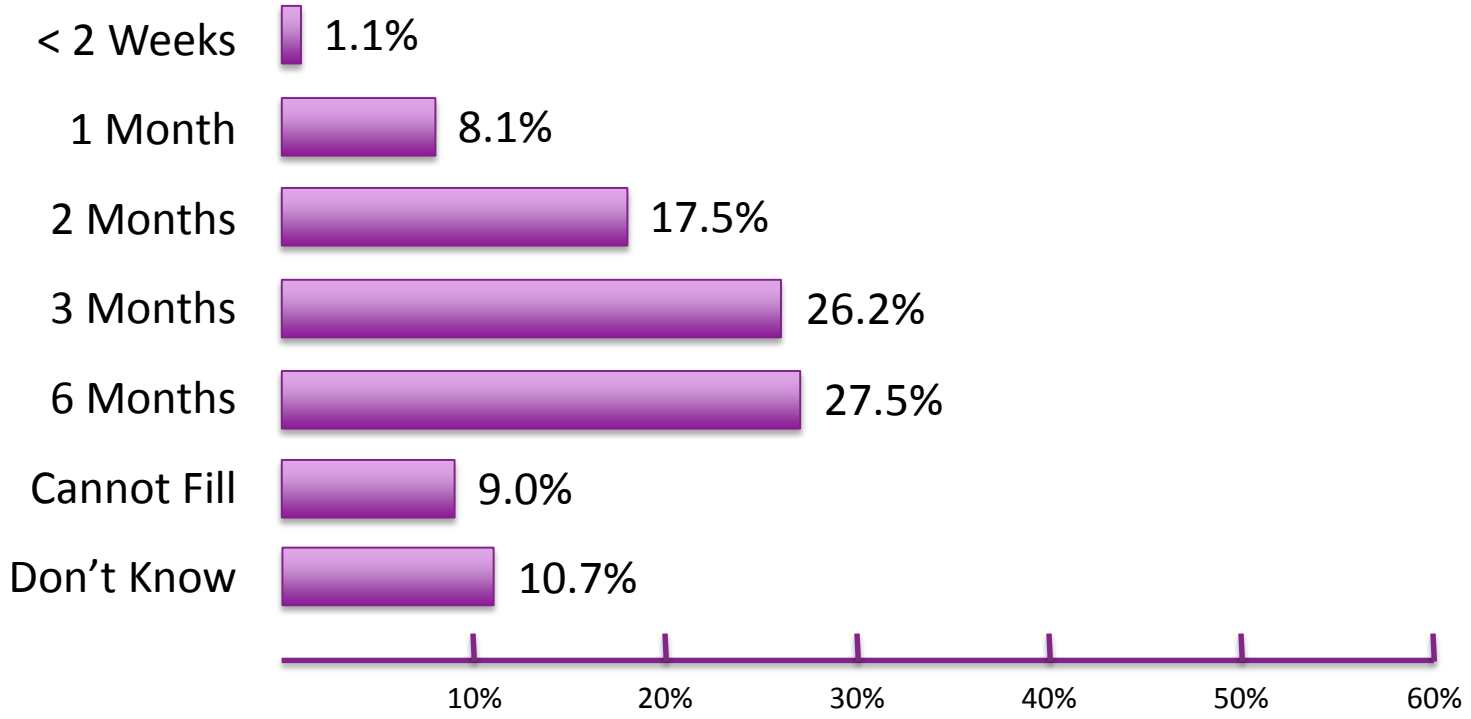
Executive Team Support for Risk Mitigation



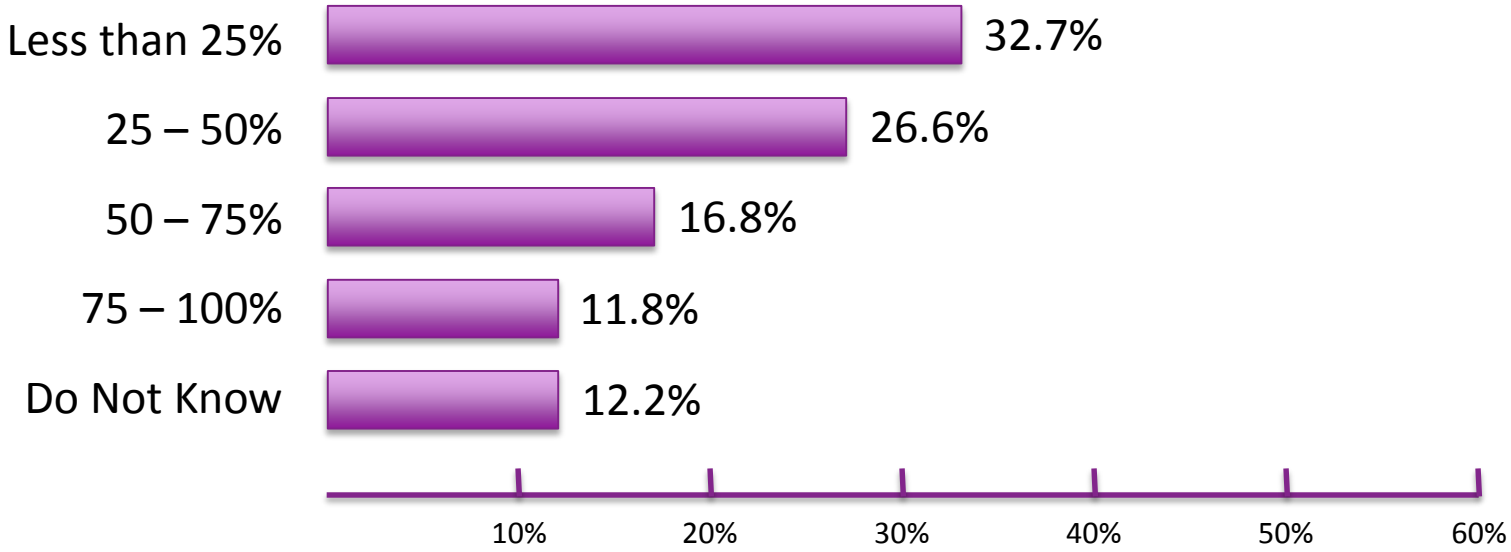
Security Reporting Structure



Time to Fill Open Cyber Positions



Applicants Qualified on Hire

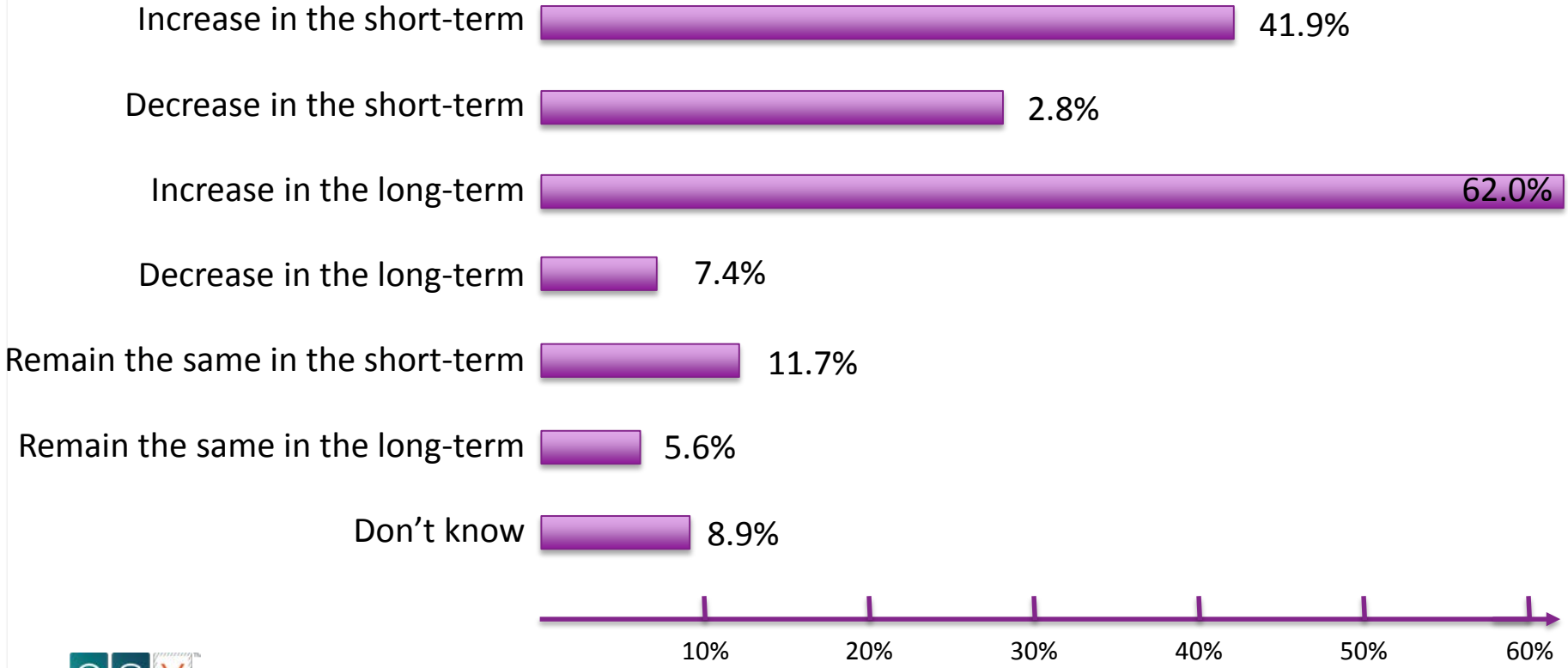


Most Significant Skill Gap

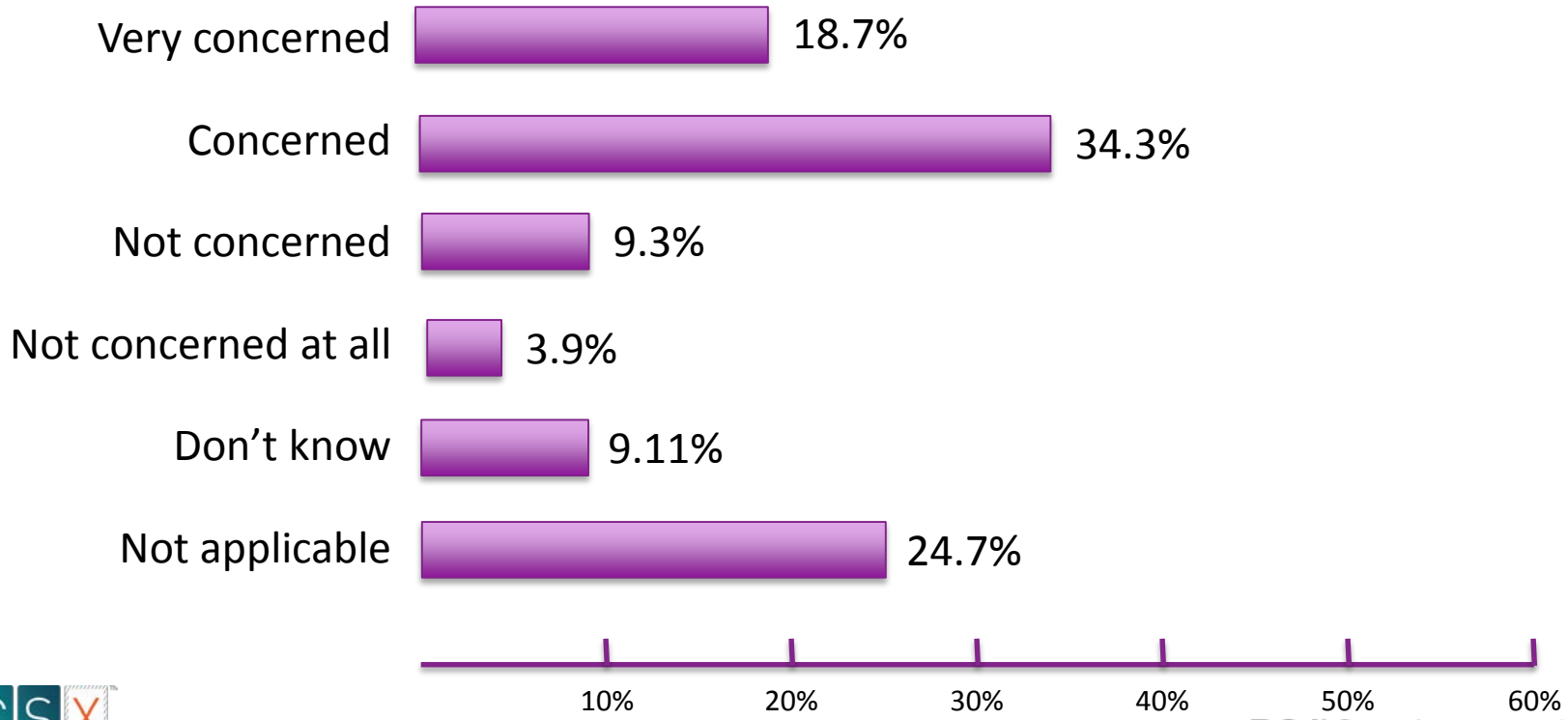
How Are Skills Developed

On the job training	85.8%	#1
Skilled based training / Performance based testing	38.1%	
Vendor specific tool training	51.9%	#4
Other training & certifications	63.2%	#2
Formal education	16.0%	
Technical training center or 3rd party trainers	26.7%	
Cyber competitions	5.3%	
Online training / webinars	47.9%	
Self-instruction	58.0%	#3
Not developing skills	7.0%	
Does not need to develop skills	0.9%	
Other	4.8%	

Artificial Intelligence and Cyber Risk



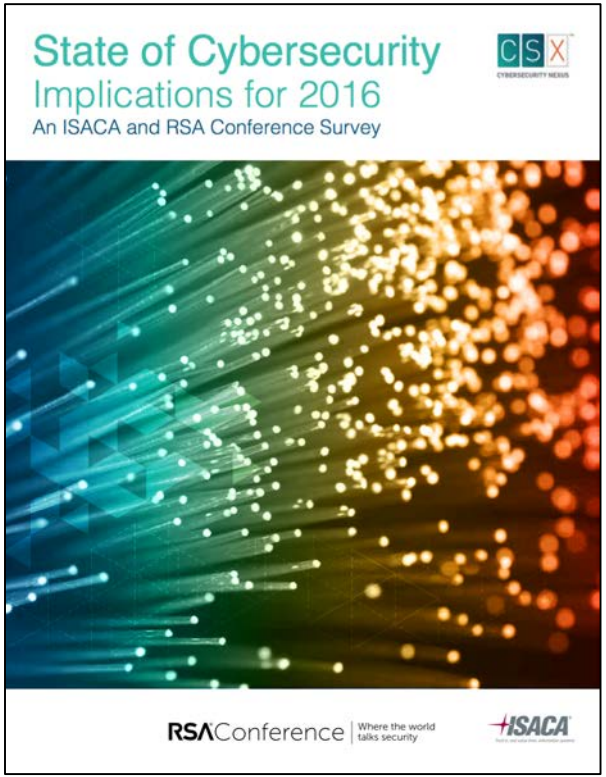
Concern for Internet of Thing Risk



Action Items

- Assess your capabilities to detect and respond to incidents
- Have an honest discussion with decision makers
- Identify skill needs and develop a strategy

For a Copy of the Report



www.isaca.org/state-of-cybersecurity-2016