RSACONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

# Why Cyber Incident Response Teams Get No Respect

SESSION ID: CISO-WO2

**Moderator:** Dr. Larry Ponemon
Chairman & Founder, Ponemon Institute

**Panelists:**

Dr. Chris Pierson
Chief Security & Compliance Officer, EVP
Viewpost

Tom Cross
Director of Security Research
Lancope

Jill Phillips
Chief Privacy Officer
General Motors

Mark Weatherford
Principal
Chertoff Group

# What is a CSIRT?

- A team of security experts within an organization whose main focus is to respond to computer security incidents, provide the necessary services to handle them and support the organization to quickly recover from security breaches.
- Ideally CSIRTs should be a regular and prominent part of doing business; not just a siloed effort relegated to the IT team.

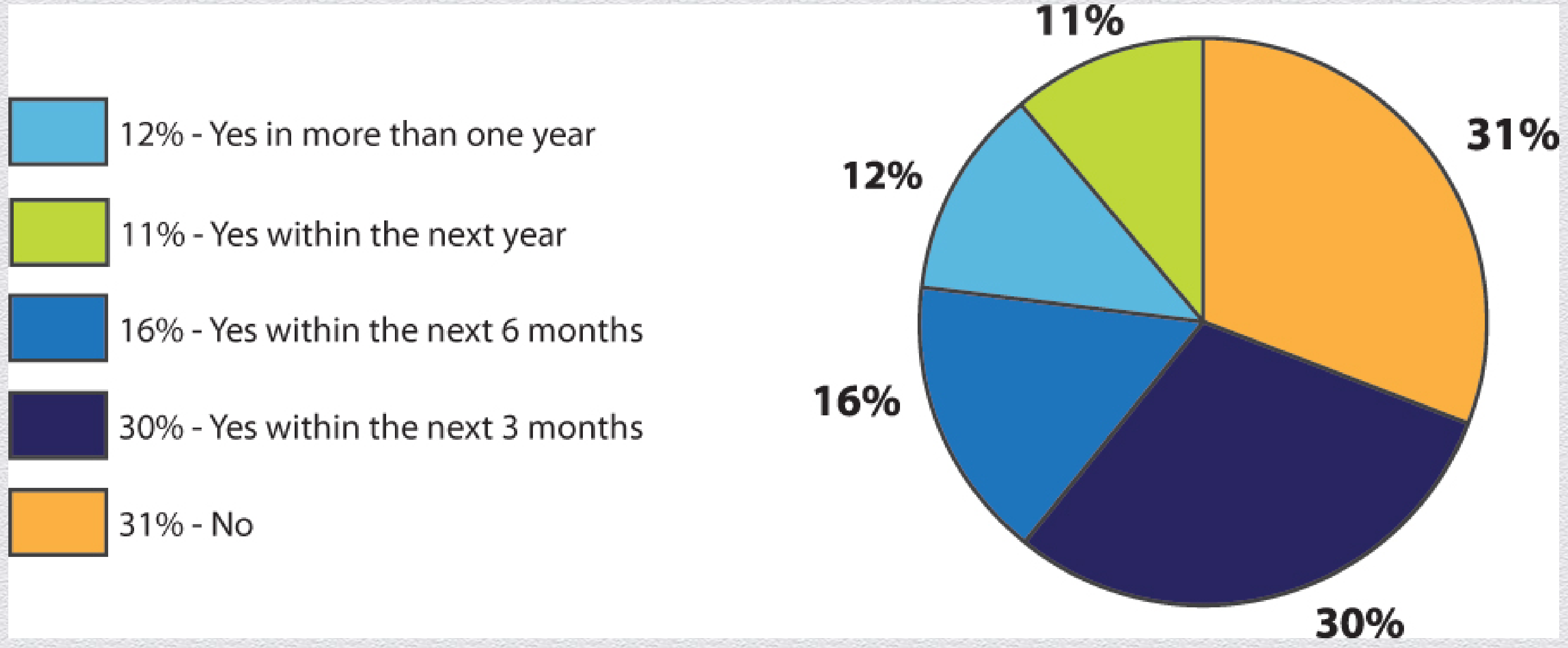
# Ponemon Study: Key Findings

CYBER SECURITY INCIDENT RESPONSE:
Are we as prepared as we think?

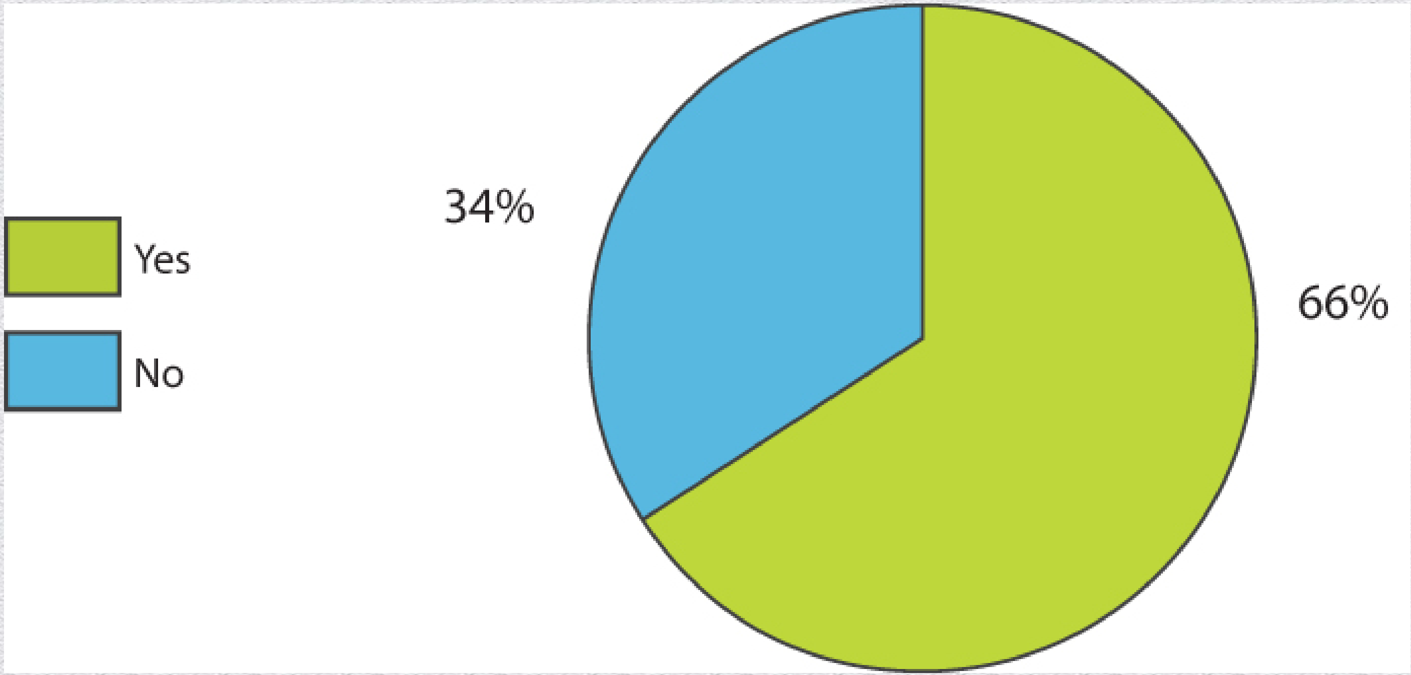
Sponsored by Lancope
Independently conducted by Ponemon Institute LLC
Publication Date: January 2014

- CSIRTs are ill-prepared to respond to cyber threats.
- Investment is critical for effective cyber incident response programs.
- Management is largely unaware of cyber security threats.

# Do you anticipate a material security breach in the future?

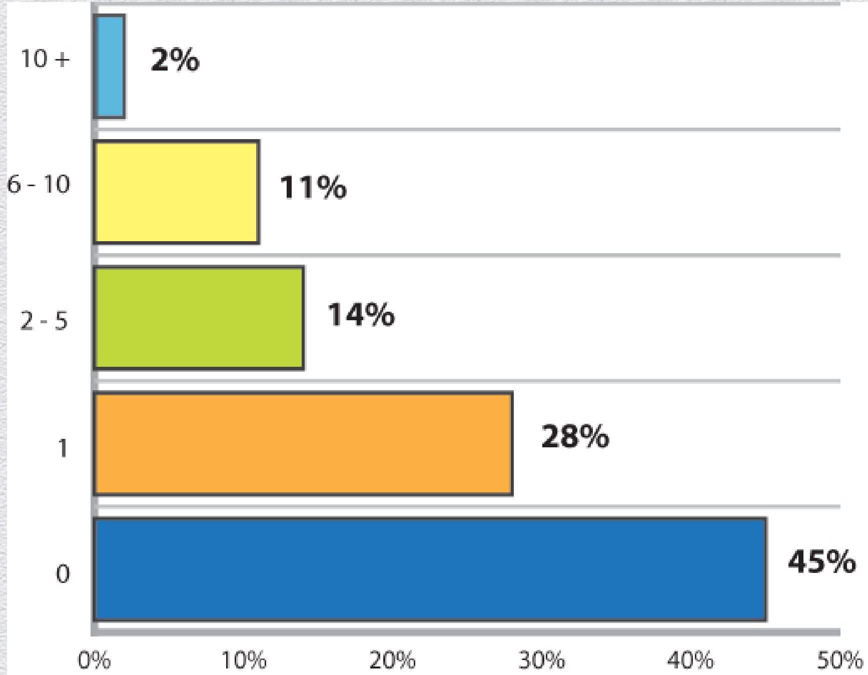


# Do you have a fully functional CSIRT?

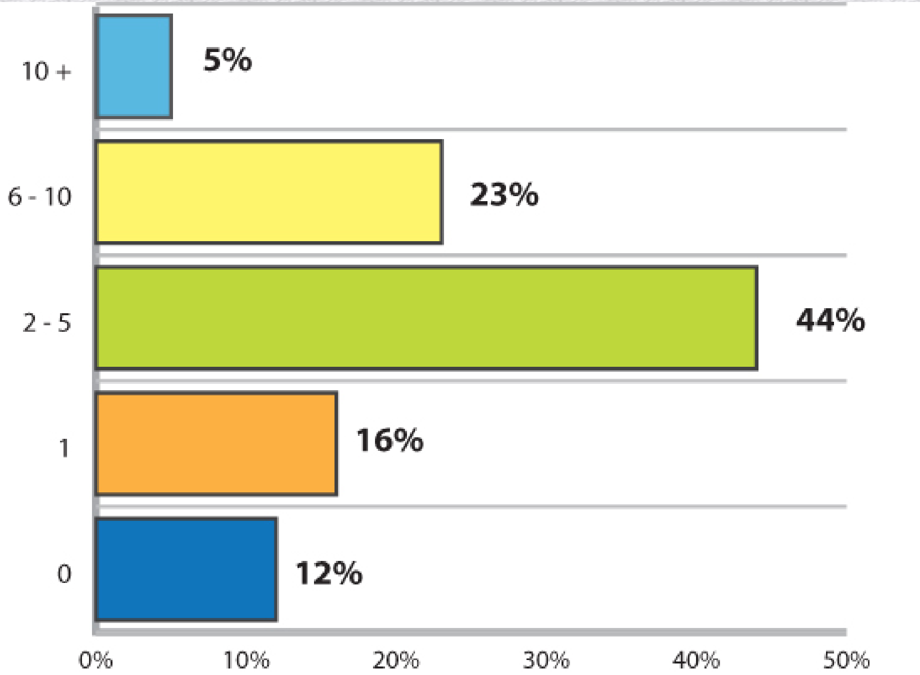


# How many employees are dedicated to incident response?

## Full Time



## Part Time

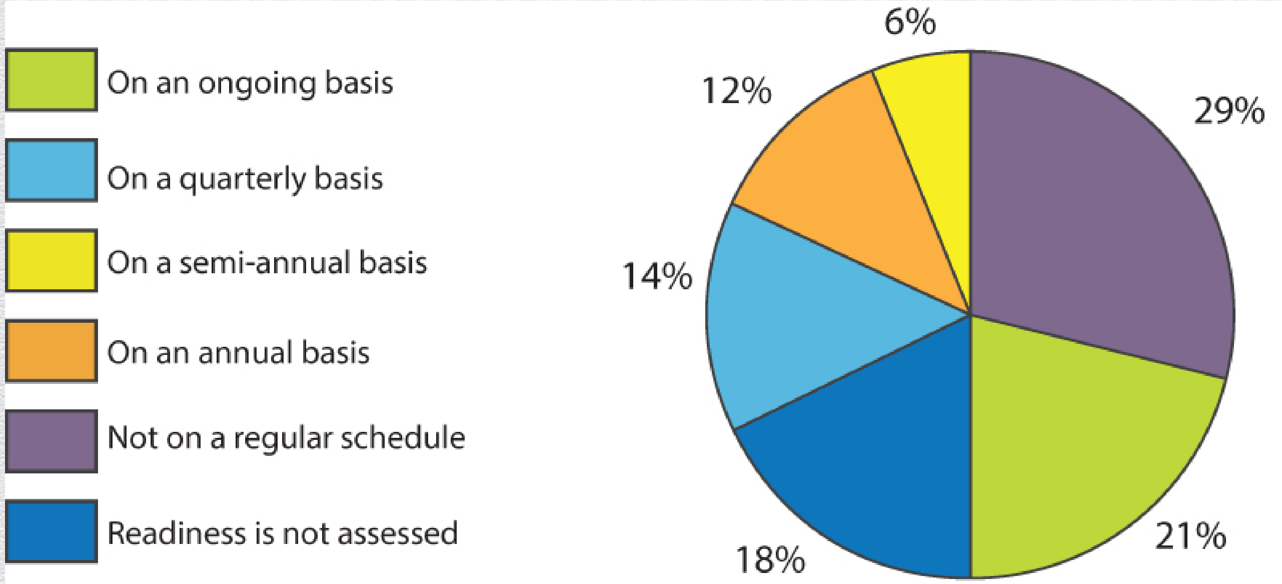


Ponemon INSTITUTE

#RSAC

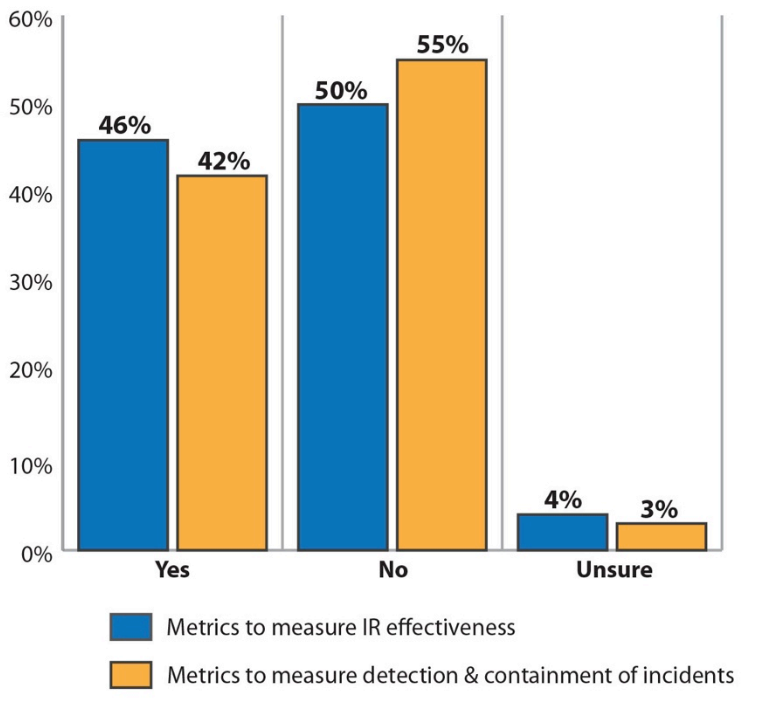
RSACONFERENCE2014

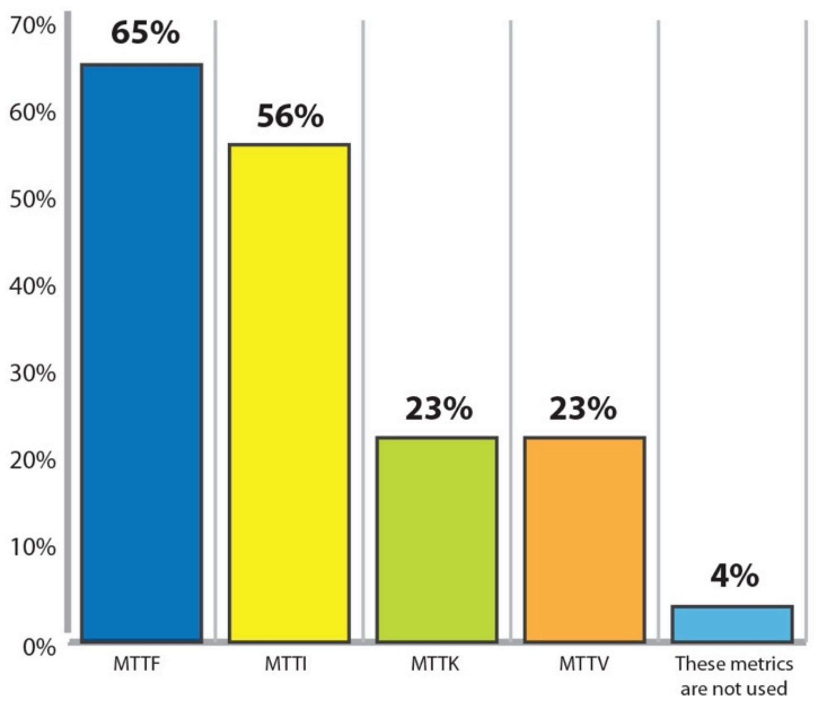
# How frequently do you assess the readiness of your Incident Response team?



Ponemon INSTITUTE

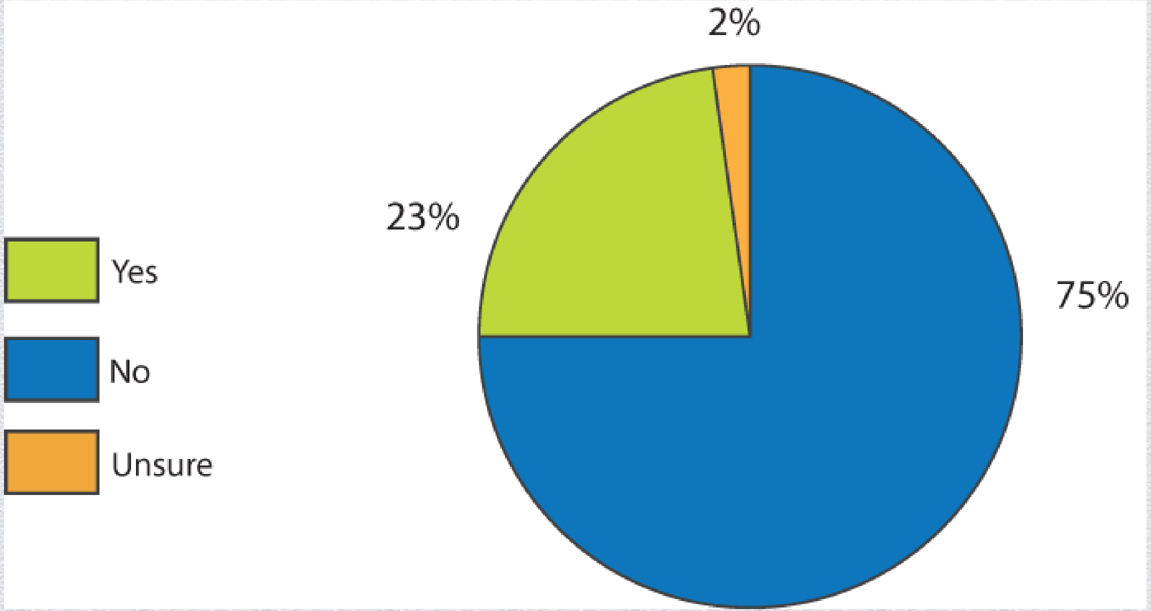
# Does your organization use metrics to measure incident response effectiveness?



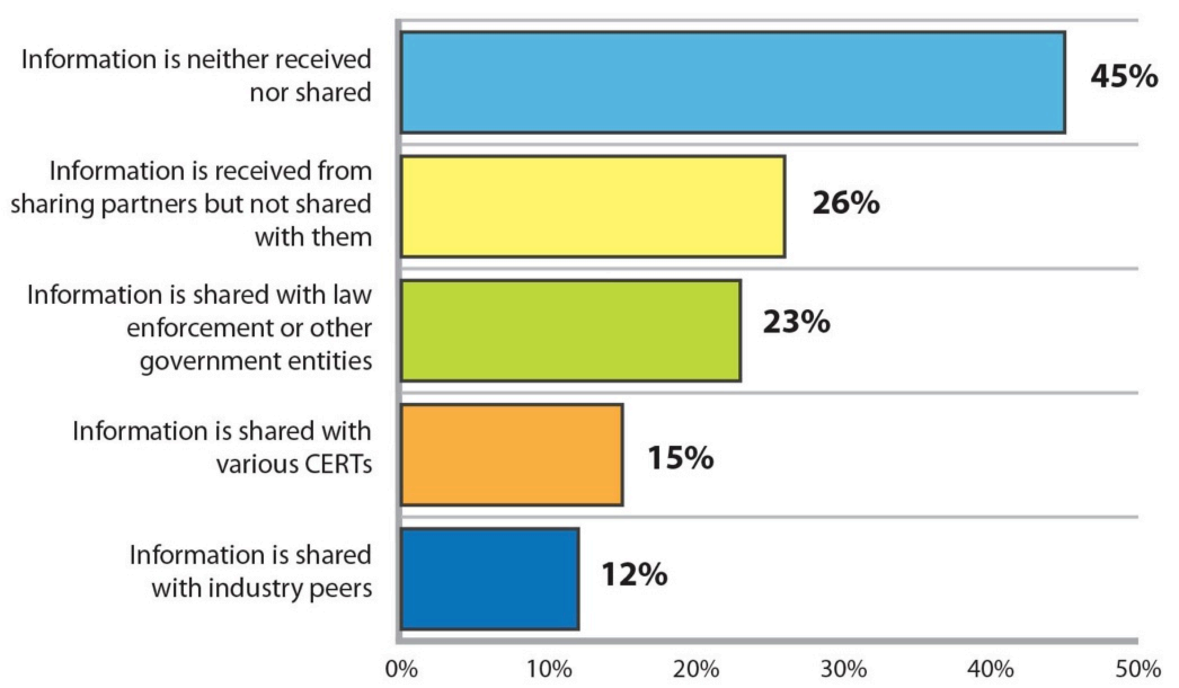


Ponemon INSTITUTE

# Do you have a PR and Analyst Relations plan in place in the event of a breach?

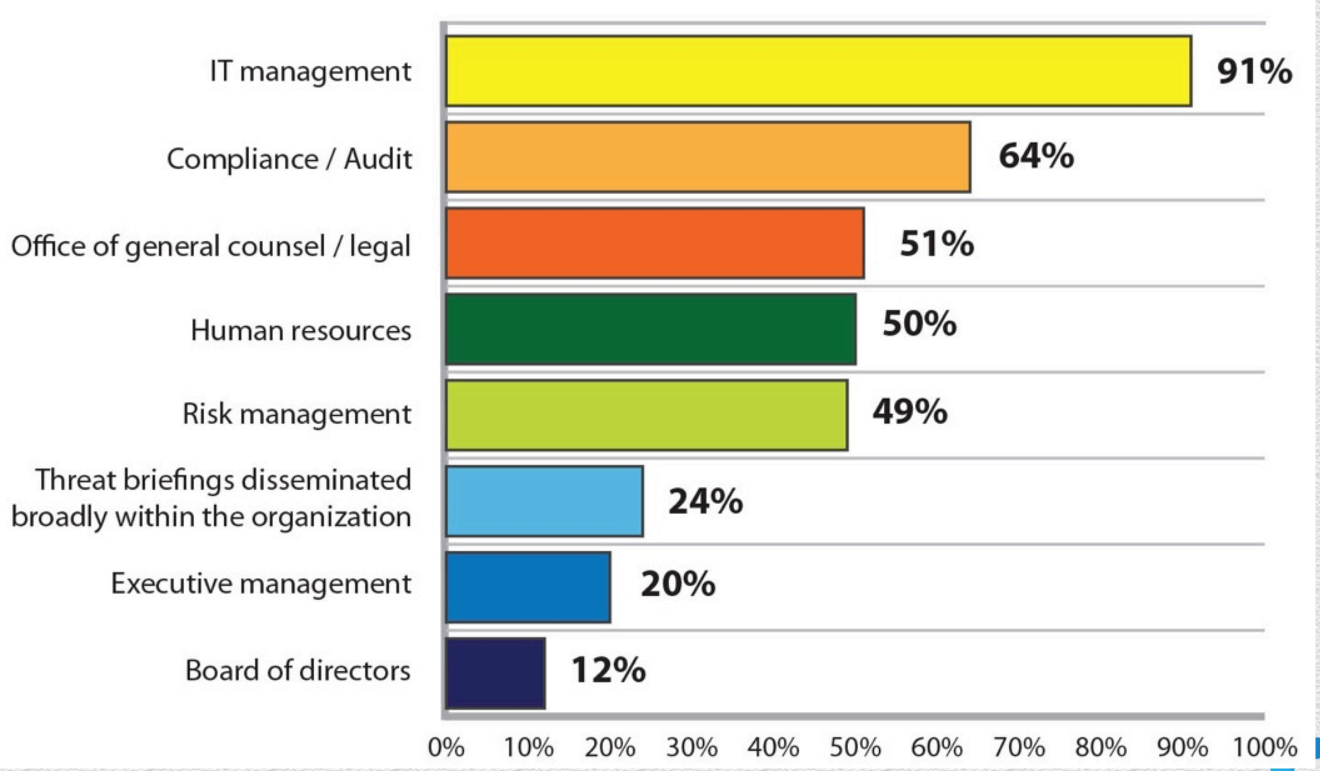


# Are you sharing threat intelligence?



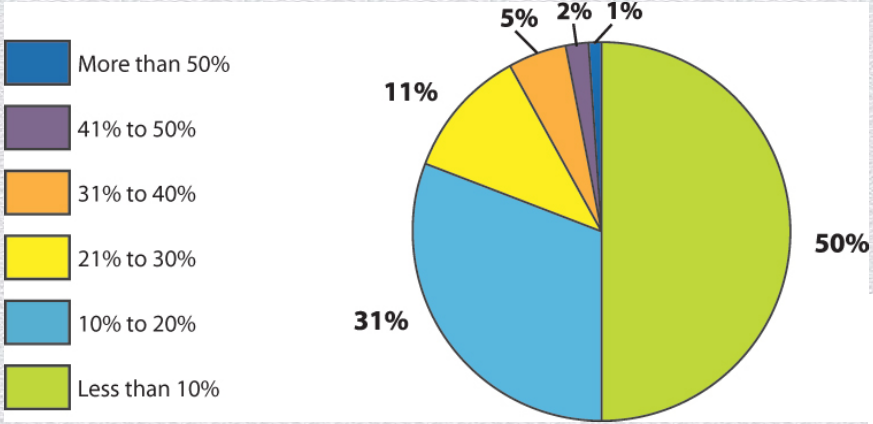
Ponemon INSTITUTE

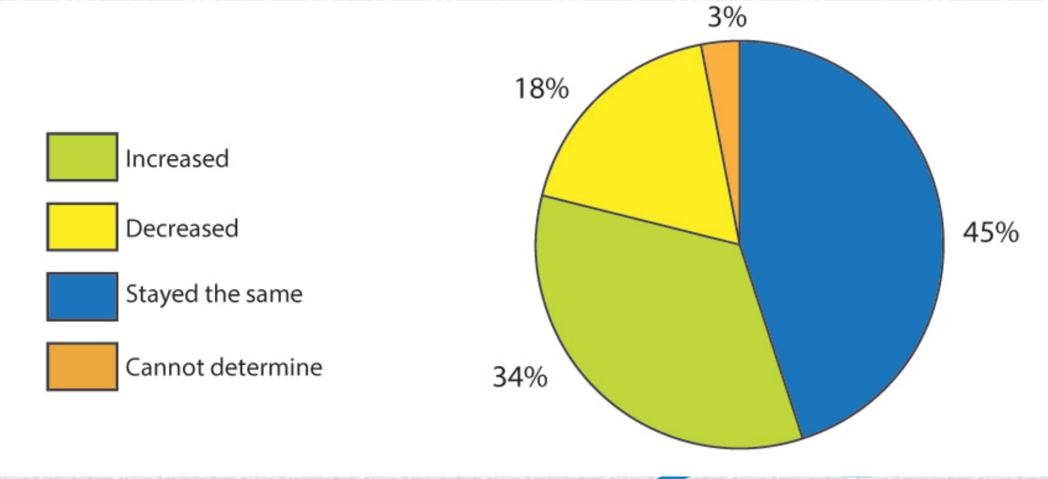
# Frequency of Cyber Threat Briefings?



Ponemon INSTITUTE

# What percentage of your security budget is spent on incident response preparedness?





Ponemon INSTITUTE

# How to get respect

- Make it a priority to build an incident response team consisting of experienced, full-time members
- Assess the readiness of incident response team members on an ongoing basis.
  - Table top exercises are a must; Include your service providers
- Create clearly defined rules of engagement for the incident response team.
- Have meaningful operational metrics to gauge the overall effectiveness of incident response.
- Get the support and endorsement of a senior executive

# More respect

- Translate the results of these measures into user-friendly business communications.
- Involve multi-disciplinary areas of the organization in the incident response process.
- Share results from the news surrounding other breaches/responses.
- Invest in technologies that support the collection of information to identify potential threats.
- Consider sharing threat indicators with third-party organizations to foster collaboration.

CYBER SECURITY INCIDENT RESPONSE:

Are we as prepared as we think?

Sponsored by Lancope

Independently conducted by Ponemon Institute LLC

Publication Date: January 2014

Ponemon Institute

To obtain a copy of our report:

Cyber Security Incident Response: Are we as prepared as we think?

please visit:

http://www.Lancope.com/Ponemon-incident-response

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

# Why Cyber Incident Response Teams Get No Respect