RSA Conference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SPO1-R04

Board Room Rodeo:

How to Align the C-Suite and Make Better Security Decisions

Diana Kelley

Executive Security Advisor

IBM

@dianakelley14

#RSAC

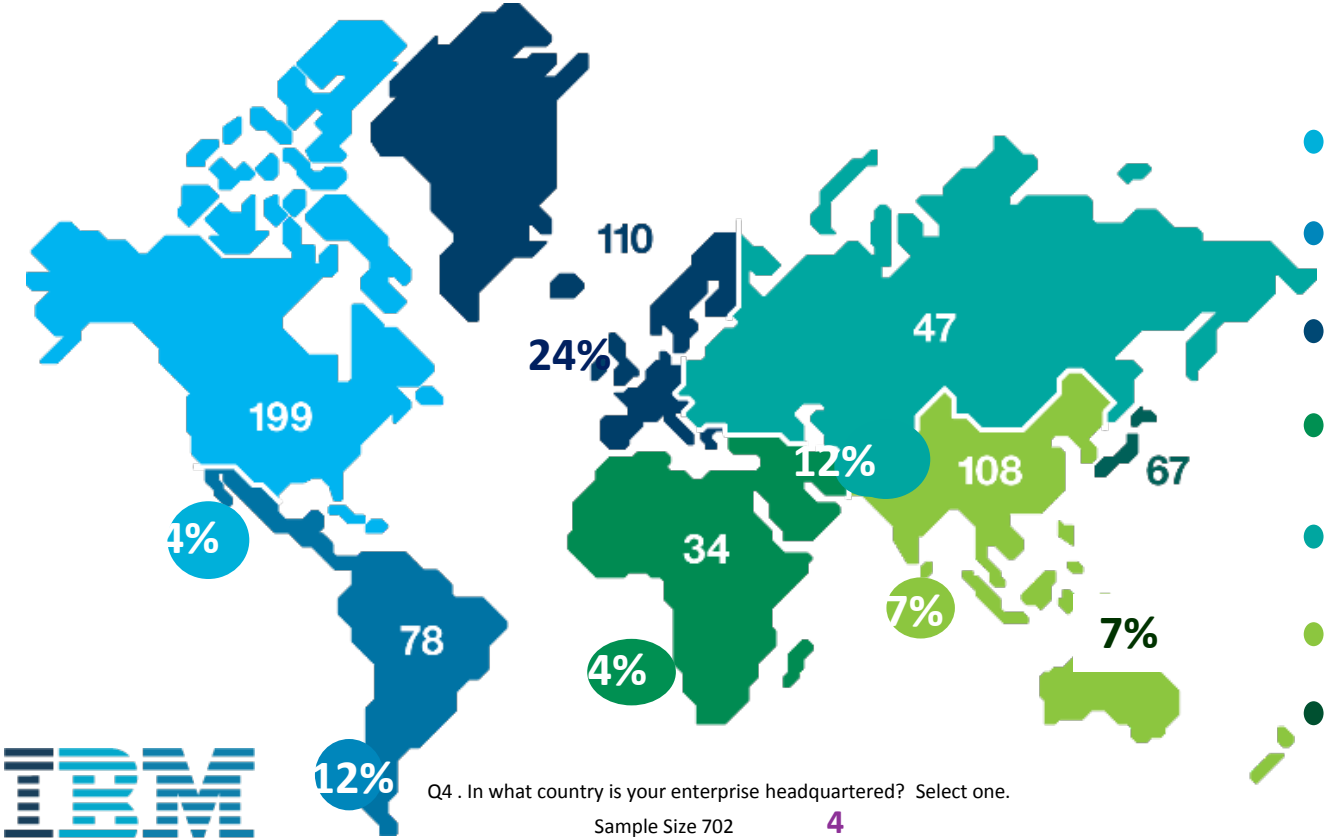
Why Survey the C-Suite about Cybersecurity?

Image Source: Cat Rodeo, Item #: 6079241
http://www.allposters.com/-sp/Cat-Rodeo-Posters_i6079241_.htm

Agenda

- **Approach and Demographics**
- C-Suite View
- Collaboration Factor
- Lessons Learned
- Recommendations

700 C-suite executives, 29 countries, 18 industries



Q4 . In what country is your enterprise headquartered? Select one.

Sample Size 702

20 questions for all, 3-5 specific to each role

Questions asked across C-suite roles

- 5 Demographic
- 5 Risk awareness
- 5 Capability and preparation
- 5 Governance

Role Specific Examples

CEO

- Cybersecurity importance relative to other strategic issues
- Willingness to share information (internally and externally)

CHRO

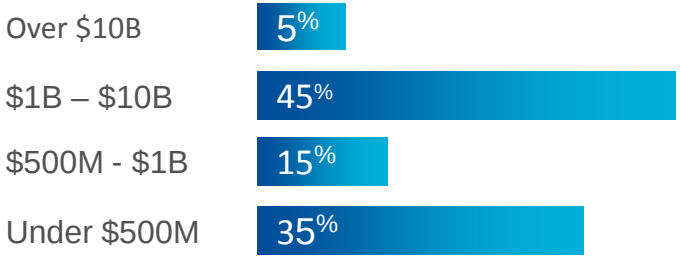
- Deployed employee education
- Protected critical employee personal sensitive data

CFO/CRO

- Degree security is incorporated into ERM plans
- Protected critical financial and risk data

Balanced across company size and role

Company size in $USD annualized revenue

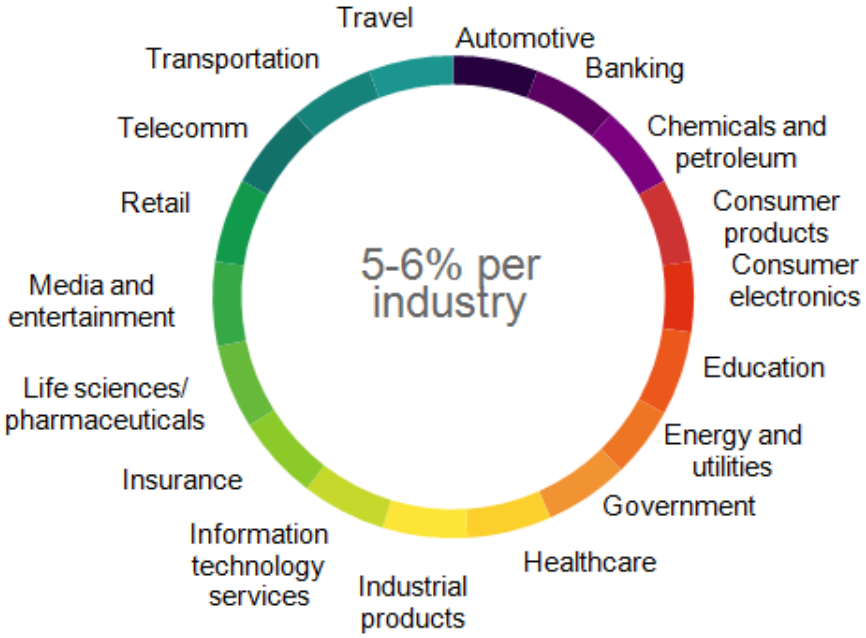


C-suite role

Chief Executive Officer	12%
Chief **Information** Officer	13%
Chief **Financial** Officer	13%
Chief **Marketing** Officer	13%
Chief **Human Resource** Officer	13%
Chief **Risk** Officer	12%
Chief **Legal/Compliance** Officer	12%
Chief **Operations** Officer	8%
Chief **Supply Chain** Officer	4%

Sample Size 702

Balanced across industry



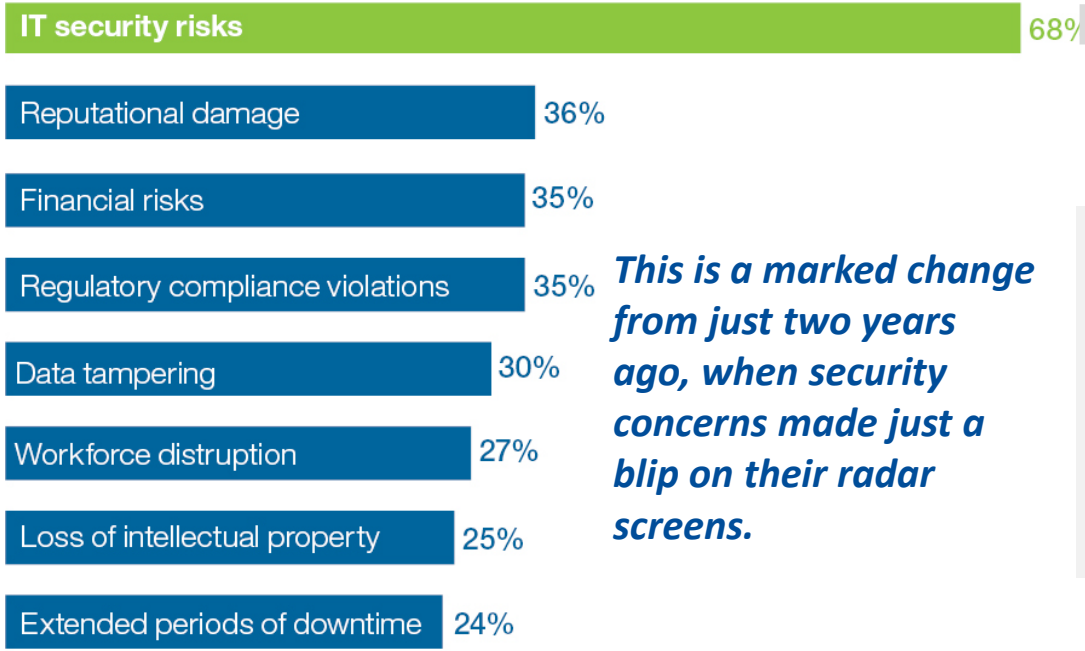
Sample Size 702

Agenda

- Approach and Demographics
- **C-Suite View**
- Collaboration Factor
- Lessons Learned
- Recommendations

IT Security Risks are Top of Mind

Greatest risks with emerging, disruptive technologies



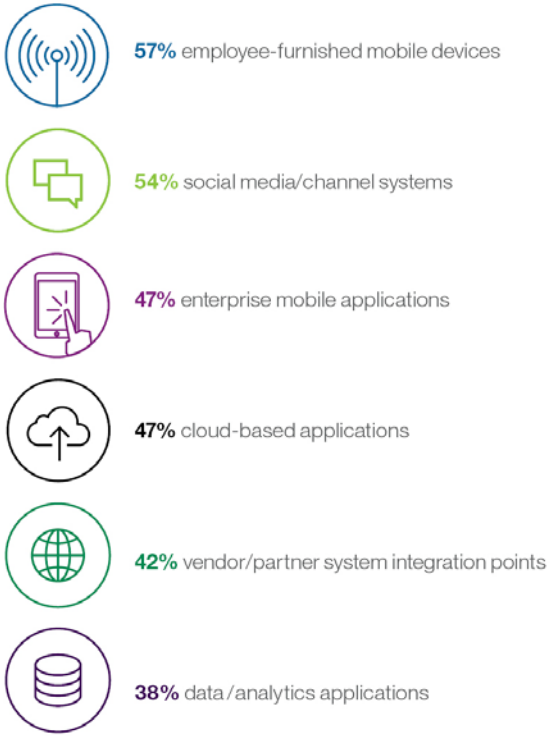
This is a marked change from just two years ago, when security concerns made just a blip on their radar screens.

Disruptive technologies where IT Security risk was selected as #1 Top Concern

- **Mobile solutions**
- **Cloud computing**
- **Smart, connected (IoT)**
- **Cognitive computing**
- **Advanced manufacturing technologies**
- **Man-machine hybrids**

IBM 2015 C-Suite Study: Source: Q1.4 Which of the following technologies will revolutionize your business in 3 to 5 years? [Rank up to 3] cut by Q2.3 Which of the following risks do you think may occur in 3 to 5 years as a result of the technology you ranked #1 in question 1.4? Rake-weighted n=5247

Fear of the new



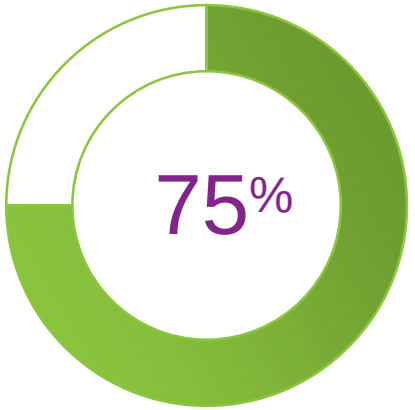
The latest "technologies du jour" such as mobile are capturing more Executive level attention, despite the fact that there are, currently, fewer known incidents through these channels than others (e.g. legacy applications, vendor/partner system integration points, network security).

Admittedly, legacy infrastructure vulnerabilities remain a top of concern for all. They are exacerbated by emerging technologies (e.g. API Security).

75% think a program is important

% of C-suite indicating cybersecurity plan components are important to extremely important

Weighted average response for whole cybersecurity plan is important to extremely important

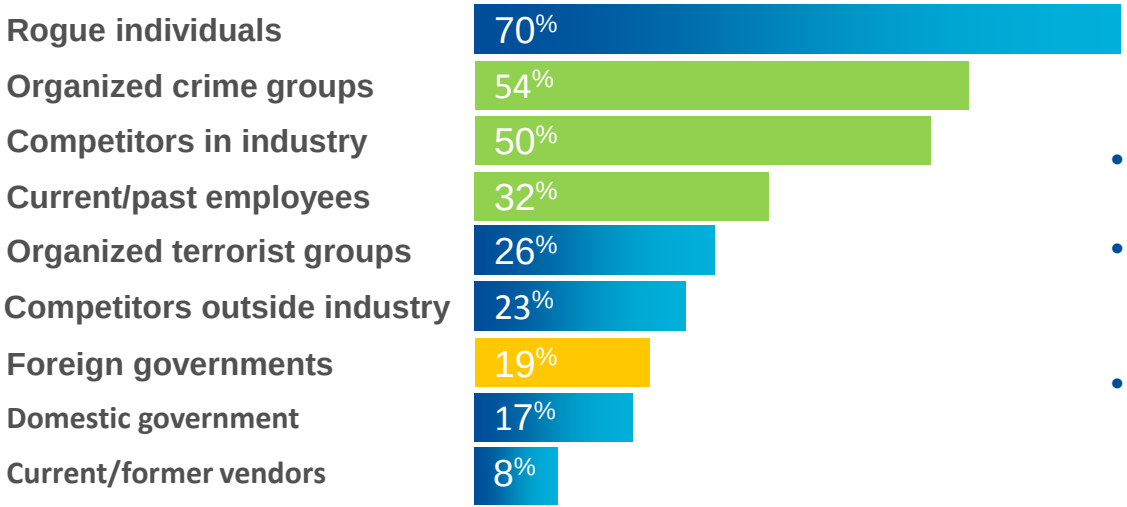


Sample Size = 691

Q12 . How important are the following elements of a cybersecurity plan in each of the areas described below? Please rate each item below on a scale of 1 to 5, with 1 being “Not at all important”, 5 being “extremely important”, or “Don’t know”.

Do they understand the biggest threats?

Riskiest threat actors selected by C-suite respondents



On average, they overstate the risk from Rogue actors and understate the risk from employees, foreign governments and industrial espionage

- ***80% of material threats arise from organized crime groups[1]***
- ***31.5% of data breaches are attributable to malicious insiders (employees, contractors, vendors)[2]***
- ***23.5% of data breaches are due to inadvertent actors, (insider errors, non-adherence to policy)[2]***

Sample Size = 702

Q7: Rank the top three entities that you believe represent the most significant threats to Cyber Security for your enterprise, with 1 being most significant.

1: UNODC Comprehensive Study on Cybercrime 2013

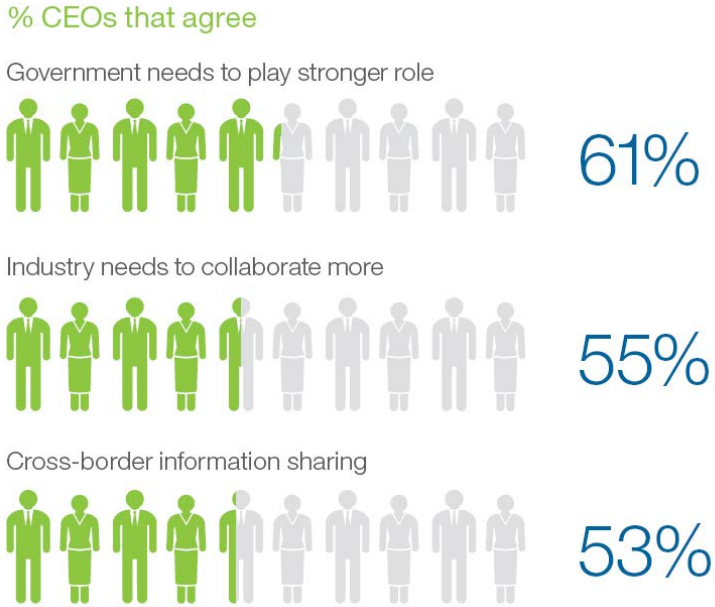
2: IBM 2015 Cyber Security Intelligence Index - https://securityintelligence.com/economic-espionage-the-global-workforce-and-the-insider-threat/

Agenda

- Approach and Demographics
- C-Suite View
- **Collaboration Factor**
- Lessons Learned
- Recommendations

Do as I say, not as I do?

CEO agreement with need for external collaboration with various groups



CEO reticence to participate in sharing incident information with them

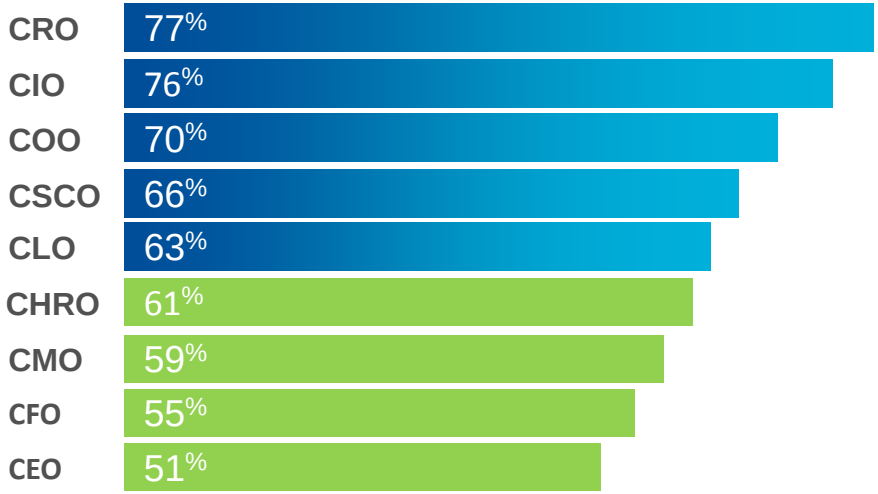
Sample Size = 87

Q2 – CEO: To what extent are you willing to disclose Cyber Security incidents with the following stakeholders on a scale of 1 to 5 with 1 being not at all and 5 being extensively. Externally = Vendors, Regulators, Industry Competitors, Third Party Security Experts

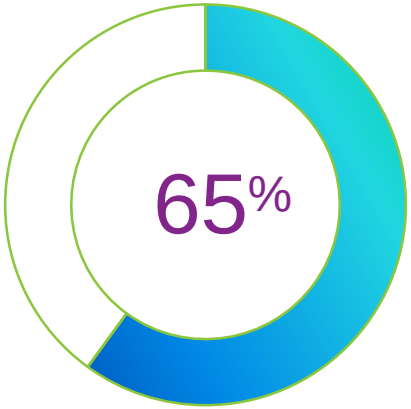
Q3-CEO: On the following Cyber Security related actions, please indicate if you agree or disagree with each statement

CEO: Least confident about the strategy

% C-suite respondents by role that report the cybersecurity strategy of their company is well established

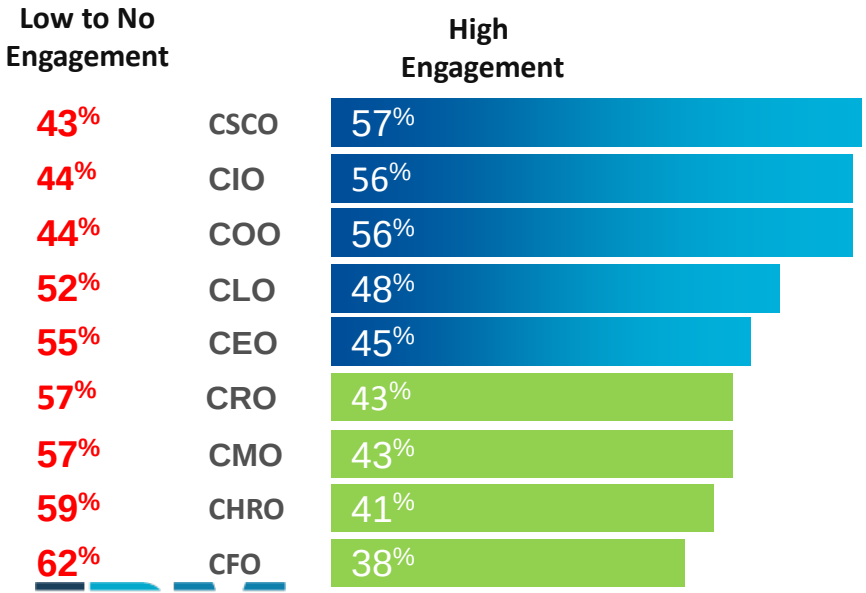


C-suite average response that the cybersecurity strategy of their company is well established

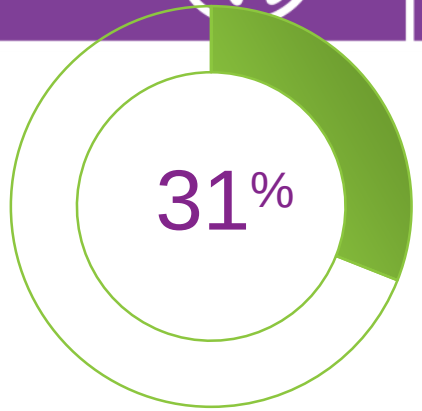


Key roles low on engagement

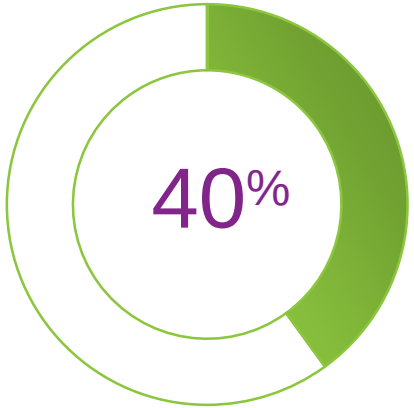
% C-suite respondents by role that report they are very engaged in security threat management discussions



% of C-suite agree cybersecurity plan incorporates C-suite collaboration



% of C-suite highly engaged in cybersecurity threat management



Agenda

- Approach and Demographics
- C-Suite View
- Collaboration Factor
- **Lessons Learned**
- Recommendations

Methodology to cluster effectiveness

3 Strategic components:

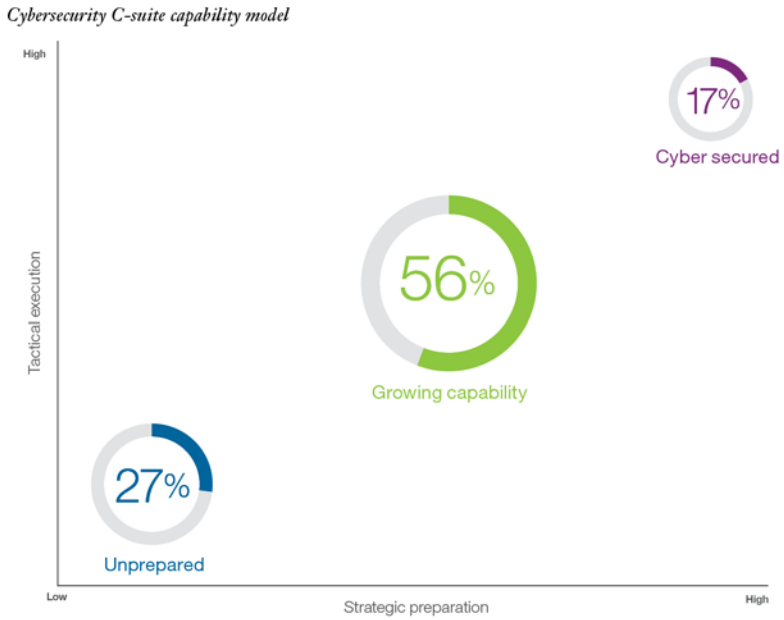
- Q10.1 Evaluating potential security issues across all initiatives (C-Suite collaboration)
- Q10.2 Indentifying critical enterprise data (the Crown Jewels)
- Q10.3 Developing an effective response plan in the event of a breach (internal & external)

4 Tactical components:

- Q13.1 Prevention: Having necessary prevention practices and tools in place
- Q 13.2 Detection: Deploying continuous monitoring & detection tools
- Q13.3 Response: Implementing a comprehensive response plan
- Q13.4 Remediation: Implementing remediation plans to strengthen security

We asked respondents how they have prepared strategically and tactically along these factors and used responses to these questions to see if clusters emerged, by capability.

Analysis clusters



Sample Size = 702

Q10. To what extent has your organization established and implemented Cyber Security plans and capabilities across your enterprise? Please rate each item below [Strategic Plan, Data Protected, Response Plan ready] , on a scale of 1 to 5, with 1 “Not at all”, 5 being “Extensively”

Q13 . Considering your entire enterprise, how effective are current Cyber Security plans in each of the areas described below [Prevention, Detection, Response, Remediation]? Please rate each item below on a scale of 1 to 5, with 1 “Not at all effective”, and 5 being “extremely effective”

Have a CISO

Have established an office of information security and appointed a Chief Information Security Officer (CISO)

79%
Cybersecured

32%
Growing capability

29%
Unprepared

Build collaboration in

C-suite collaboration built into cybersecurity plan (governance)

67%
Cybersecured

34%
Growing capability

10%
Unprepared

Promote transparency & communication

Cybersecurity is a regular topic on the board meeting agenda

56%
Cybersecured

27%
Growing capability

10%
Unprepared

Agenda

- Approach and Demographics
- C-Suite View
- Collaboration Factor
- Lessons Learned
- **Recommendations**

Recommendations

- Help CxOs understand the risks
- Collaborate, educate, empower
- Manage risk with vigilance and speed

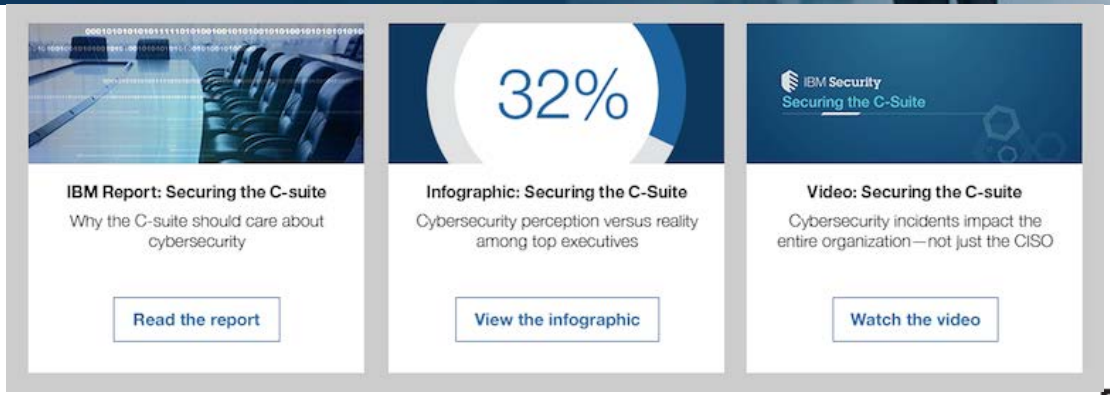
Only connect

E.M. Forster

Live in fragments no longer.

Learn more about the study: Securing the C-Suite

Visit ibm.com/security/ciso to download the report



Learn more about IBM Security

No. 1 enterprise security vendor in total revenue

25 industry analyst reports rank IBM Security as a **LEADER**

130+ countries where IBM delivers managed security services

12K+ clients protected *including…*

90% of the Fortune 100 companies

IBM Security

Intelligence. Integration. Expertise.

Watch our videos on YouTube
IBM Security Channel

Read new blog posts
SecurityIntelligence.com

Join IBM X-Force Exchange
xforce.ibmcloud.com

Follow us on Twitter
@ibmsecurity

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

THANK YOU

www.ibm.com/security

IBM Security

Intelligence. Integration. Expertise.