

RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

SESSION ID: SOP-R04

Cybersecurity Awareness for Executives

Rob Sloan

Head of Cyber Content and Data
Dow Jones
 @_rob_sloan



CHANGE
Challenge today's security thinking

Session Overview

- ◆ Aim:
 - ◆ Provide a high level overview of an effective cybersecurity awareness program for executives in any size of enterprise
- ◆ Objectives:
 - ◆ Discuss necessity, scope and pre-requisites
 - ◆ Consider challenges of delivery
 - ◆ Focus on individual elements of program
- ◆ Application:
 - ◆ Putting a program into practice and content suggestions

Dow Jones and Cyber Risk



 GitHub Status
@githubstatus



The ongoing DDoS attack has changed tactics. We are experiencing intermittent service outages and working to mitigate.



RETWEETS 76 FAVORITES 24 

1:18 AM - 29 Mar 2015



Hackers in China Attacked The Times

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

AP The Associated Press 

Breaking: Two Explosions in the White House and Barack Obama is injured



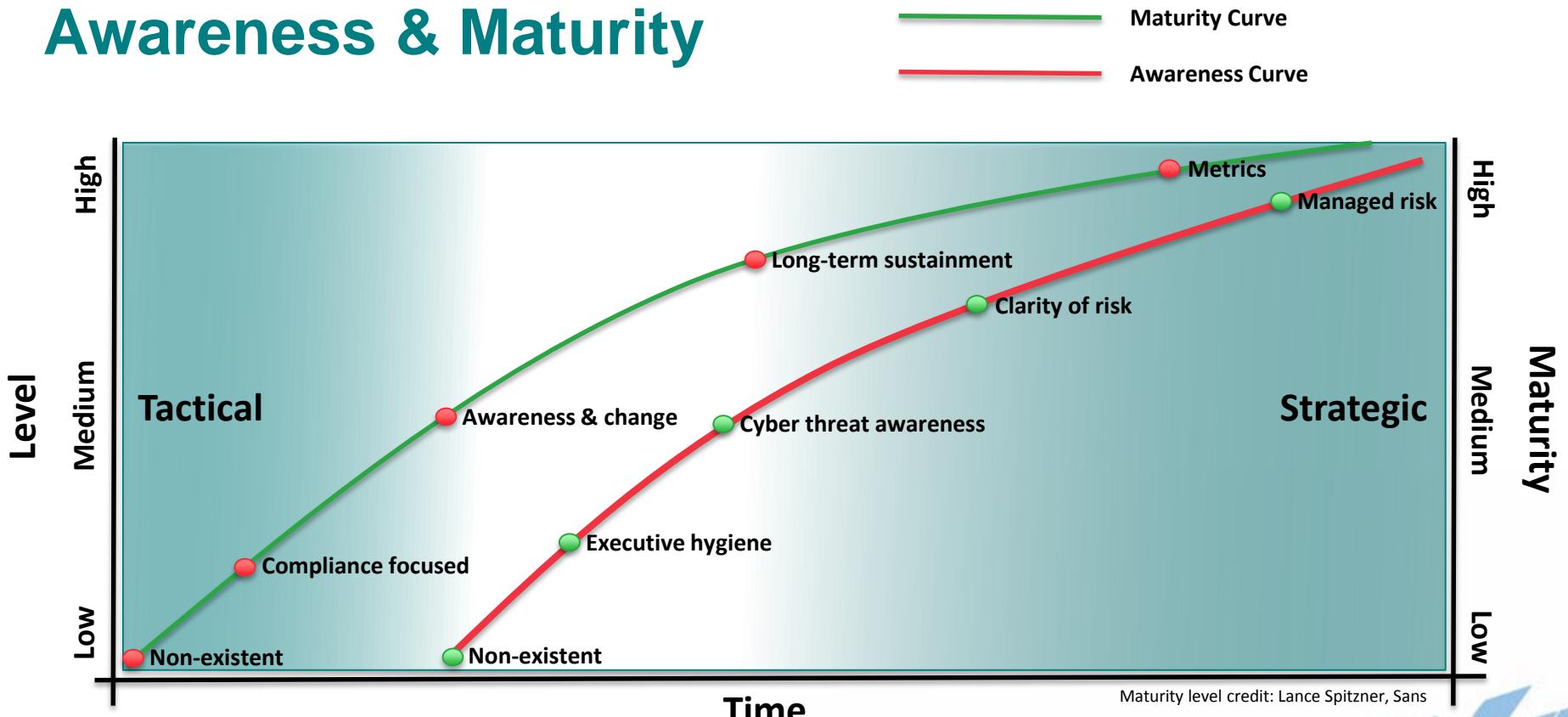
3,256 RETWEETS 154 FAVORITES 

10:07 AM - 23 Apr 13

Awareness is Essential

- ◆ Cybersecurity is no longer solely an I.T. risk
 - ◆ Potential loss of revenue, customers, reputation, IP, PII
 - ◆ Regulatory responsibility
- ◆ Significant risks to organizations
 - ◆ Network size and complexity makes defense near impossible
 - ◆ Evolving threat landscape
 - ◆ Shortage of suitably qualified/skilled/experienced professionals
- ◆ General lack of cyber awareness among executives
 - ◆ Cybersecurity knowledge based on headlines & vendors
 - ◆ Awareness closely linked to organizational cyber security maturity

Awareness & Maturity



Maturity level credit: Lance Spitzner, Sans

One Size Does Not Fit All

- ◆ Variety of factors will influence program:
 - ◆ Size of organization
 - ◆ Security maturity
 - ◆ Industry
 - ◆ Perceived threat
 - ◆ Data loss experience
 - ◆ Criticality of data at risk
 - ◆ Time available
 - ◆ Level of interest



Scope and Considerations

- ◆ Which executives need awareness briefings and what is their existing level of awareness?
- ◆ What does the executive need to know?
- ◆ Tailored to the individual executive or generic?
- ◆ Where do these briefings fit into wider cyber security strategy priorities?
- ◆ How will program be structured and scheduled?
- ◆ Who will deliver the briefings?



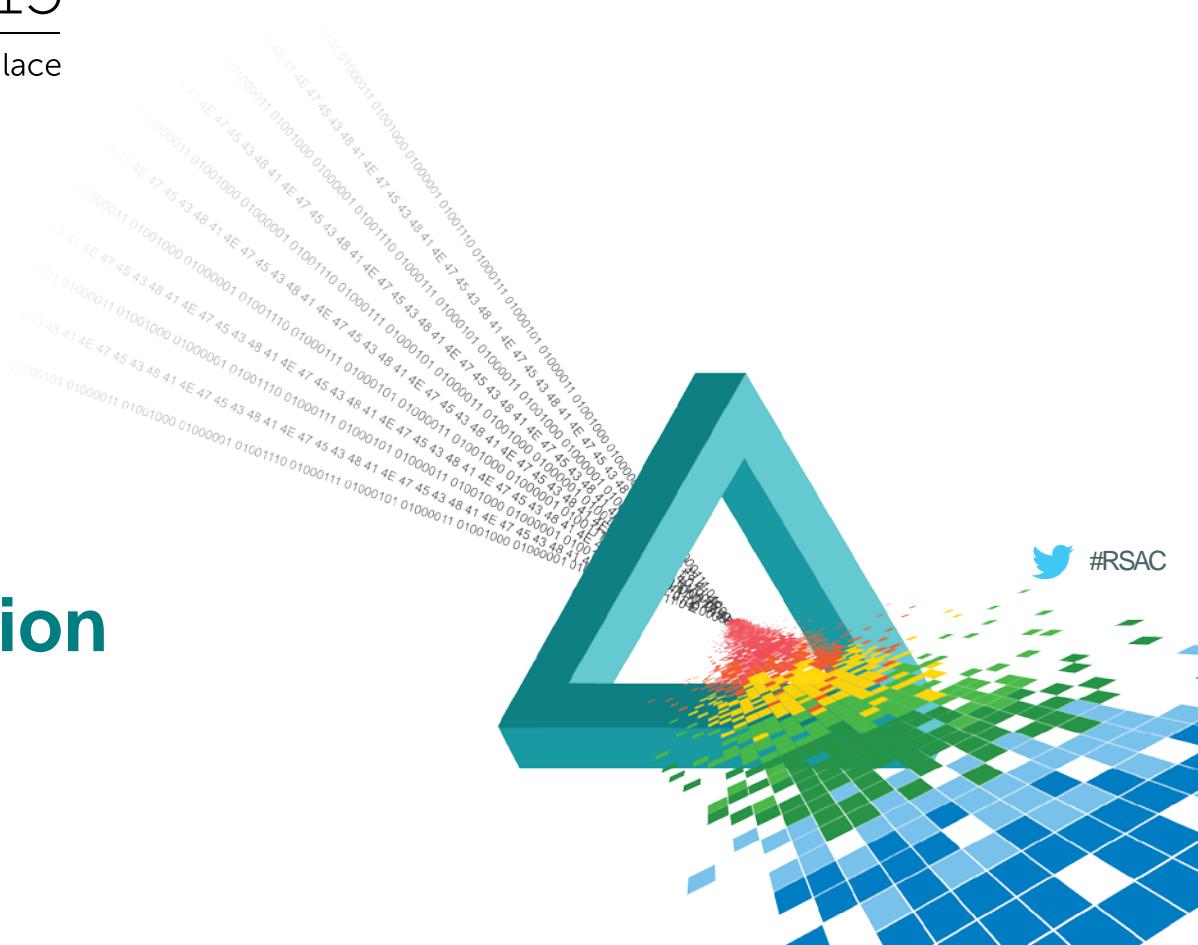
Pre-requisites

- ◆ Establish the critical data assets of the organization and the defenses in place to protect them
- ◆ Collect evidence of previous compromises, data breaches, and impact. Repeat for peer organizations
- ◆ Perform a gap analysis to establish the true state of cyber preparedness
- ◆ Understand the executive and their focus, the hardware / software they use, and their current level of awareness

RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

Practical Application



Cyber Hygiene

- ◆ The executive must understand that they are at heightened risk of being targeted themselves
- ◆ Basic protective security advice in line with that provided to the wider user community, complemented with tailored assistance depending on their devices
- ◆ Visual examples of the social engineering and phishing attacks to highlight reasons for suspicion
- ◆ Executive support in case of issues
- ◆ Annual refresher and/or ad hoc alerts



DOW JONES



Cyber Hygiene

- ◆ Key points for delivery:
 - ◆ Understand how the individual executive likes to consume information
 - ◆ Use professional materials and provide a takeaway sheet
 - ◆ Be led by the executive
 - ◆ Do not focus on the tech
 - ◆ Keep it short and to the point
 - ◆ This is hygiene, not vaccination



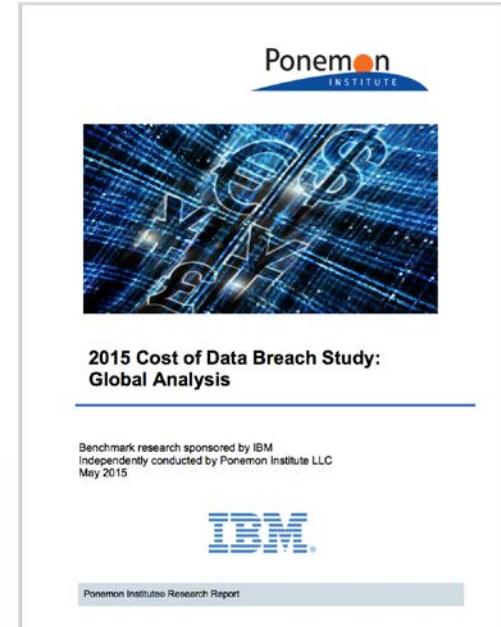
Threat Landscape

- ◆ The executive needs to understand the threat actors and their capabilities
- ◆ What data does your organization have that threat actors might target and for what purpose?
- ◆ Has your organization or industry been targeted by cyber threat actors? What was the impact?
- ◆ How is the organization getting better insight into the landscape?



Threat Landscape

- ◆ Key points for delivery:
 - ◆ Do not resort to FUD
 - ◆ Keep it relevant to your industry
 - ◆ Include statistics and their sources
 - ◆ Use example incidents from your organization and focus on the business, not the tech
 - ◆ Exploit vendor materials, open source, and government reports
 - ◆ Brief at least annually, supplemented with ad hoc relevant briefings to highlight incidents and landscape trends



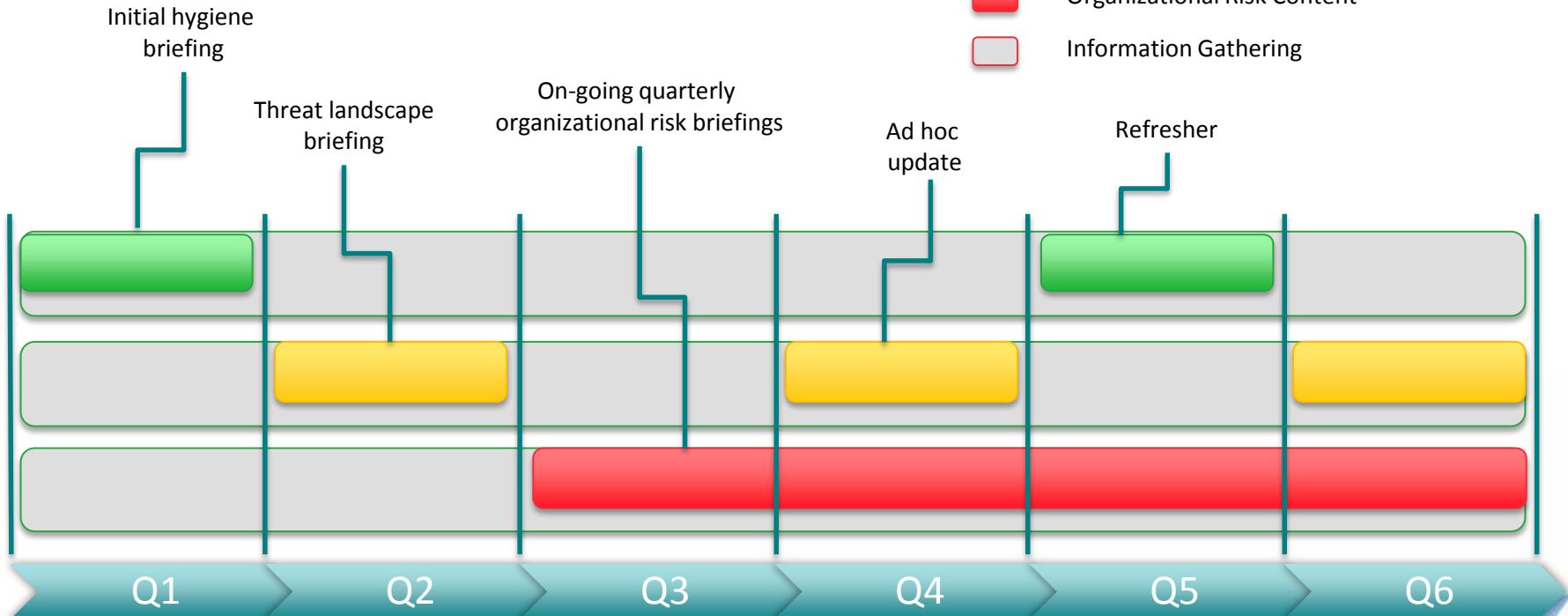
Organizational Risk

- ◆ This is the heart of the awareness program. Understanding risk and potential impact, and measures to deal with it
- ◆ Significant preparatory work may be necessary including third party consultancy engagements
 - ◆ Risk assessment
 - ◆ Threat assessment
 - ◆ Gap analysis
- ◆ Internal regular engagement with legal, marketing, comms, business leads, risk owners, IT, and internal experts
- ◆ Executives require a clear picture of critical data risk exposure against the current level of investment and staffing

Organizational Risk

- ◆ Risk = Threat x Vulnerability x Cost
- ◆ Ultimate outcome is the ability to reduce and track risk with metrics
 - ◆ Number of attacks detected
 - ◆ Number of successful compromises
 - ◆ Impact of compromises
 - ◆ Quantification of risk
- ◆ Compliance with regulations and adoption of standards
- ◆ The maturity of the cyber security program will aid the tracking of risk and vice versa

Cyber Awareness Timeline

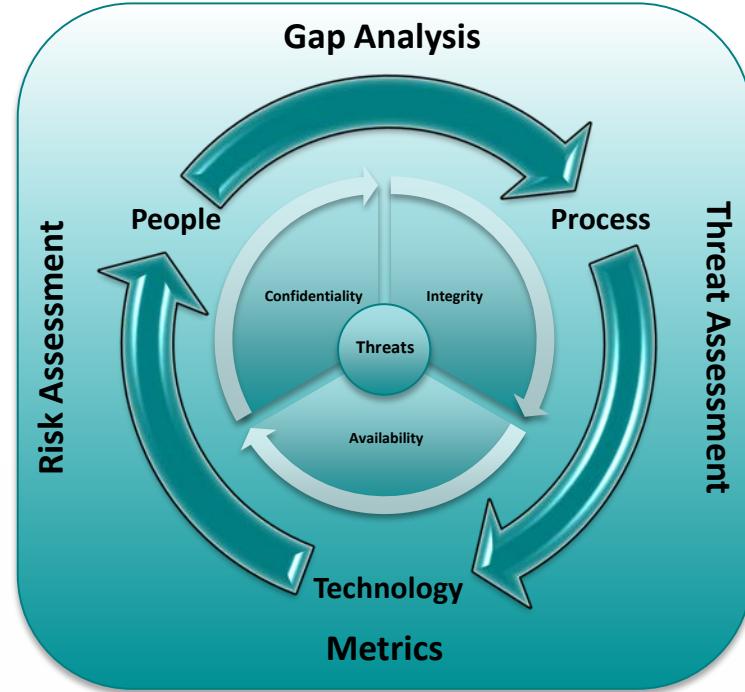


Outcomes & Benefits

- ◆ Immediate benefits:
 - ◆ Cyber security strategy strengthened with high-level buy-in and leadership
 - ◆ Recognition of cyber as a business risk
 - ◆ Decision-making based on subject matter familiarity
 - ◆ Stronger tactical/strategic response to breaches
- ◆ Longer term benefits:
 - ◆ Support for security mission drives investment
 - ◆ Potential for new lines of business
 - ◆ Organizational and personal advantages

Initial Steps

- ◆ Establish awareness gaps
- ◆ Collect requirements for cyber briefings from individual executives
- ◆ Budget for projects to determine exposure to threat and risk
- ◆ Set responsibility for tracking landscape evolution and cyber hygiene



Final Thought

Cyber security is everyone's responsibility,
but leadership starts at the top

RSA® Conference 2015

Abu Dhabi | 4–5 November | Emirates Palace

Questions

