RSA Conference 2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: CRWD-T07

Hacking the CEO: Ninja Mind Tricks and other Ruses to Get Security $$$'s

John B. Dickson, CISSP

Principal
Denim Group
@johnbdickson

Agenda

- Background
- The Very Real Problem with Security
- How CEOs Think
- Ninja Mind Tricks & Ruses
- Questions and Answers

I Wear Two Hats – #1 The Security Guy Hat

- Armored “hat” (i.e., helmet) of a security guy
- Ex-Air Force guy
- 20+ years in the field
- World view heavily influenced by security mindset

I Wear Two Hats - #2 Business Guy Hat

- Serial Entrepreneur & MBA
- Interact with other business leaders and execs
- Understand how much fun the “onus of responsibility” can be
- Fully aware of across-the-board risk issues.

Background: Getting Your Security Budget Approved Without FUD

- Exploit Pet Projects
- Account for Culture
- Tailor to Your Specific Vertical
- Consciously Cultivate Credibility and Relationships
- Capitalize on Timely Events
- Capture Successes & Over-Communicate

Source: RSA 2014 “Getting Your Security Budget Approved Without FUD

Two Concepts that We'll Talk More about…

- Exploit Pet Projects
- Account for Culture
- Tailor to Your Specific Vertical
- Consciously Cultivate Credibility and Relationships
- Capitalize on Timely Events
- Capture Successes & Over-Communicate

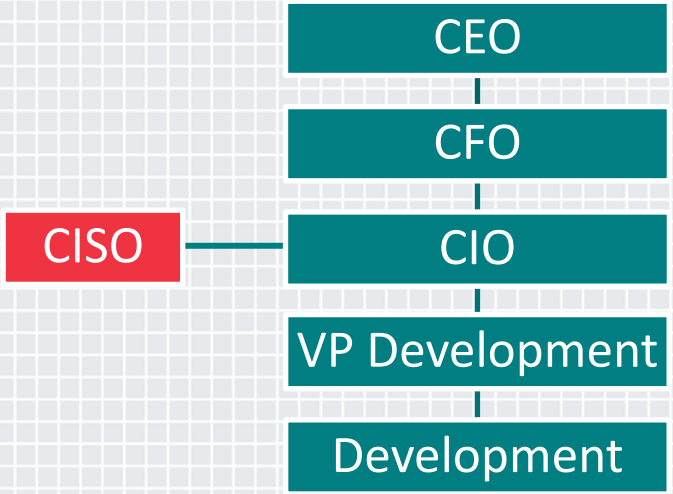
Security Budgets: The Starting Point

- Some have lost the game before getting on the field
- Competing Against:
  - Line of business pet projects – expansion of production
  - Executive level visibility or utility – e.g., new corporate jet
  - Things that product more tangible ROI
- Information security as the “silent service” – Rich Baich, Wells Fargo CISO
  - Source: “Winning as a CISO,” Rich Baich

Source: RSA 2014 Podcast The Savvy Security Leader: Using Guerrilla Tactics to ID Security Program Resources

Security Leaders Are at A Structural Disadvantage

- They have a staff advisory role and not a “line” operator role
- They have different world views that drive their perspective
- They talk differently
- They have less power

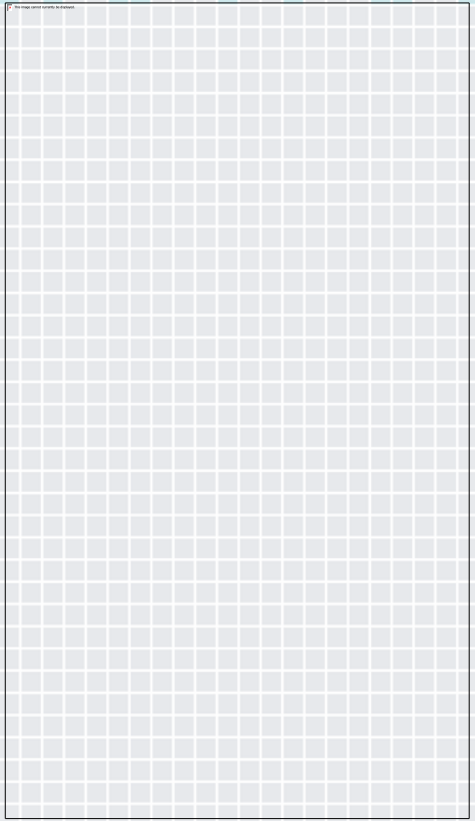


CEO's, Though Worried, Are FUD Resistant

- Is it like selling insurance?
- The security industry is struggling for parallel models and metaphors
- FUD Distorts the Process

CEO Concerns

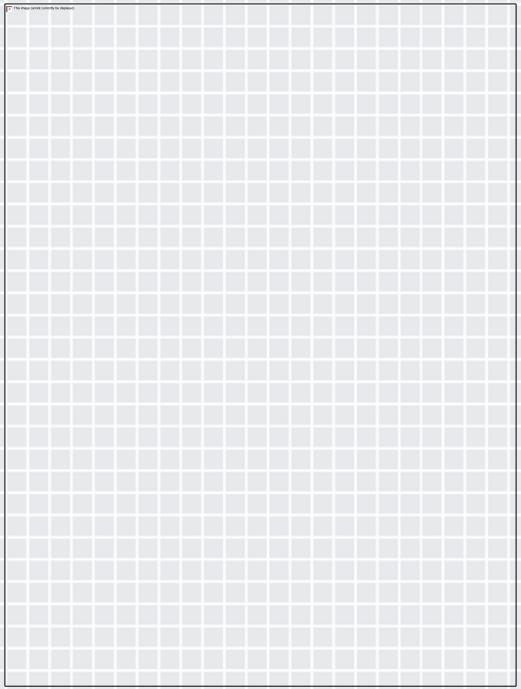
- Talent Management
- Operating in a Global Marketplace
- Regulation and Legislation
- Keeping Energy Costs Under Control
- Implementation of Healthcare Reform
- Regulatory Uncertainty
- Consumer Spending
- Currency Risk



Sources: WSJ and HBR Reports

CEO Concerns (Continued)

- Airplanes Falling out of the Sky
- Terrorism
- Oil Workers Getting Kidnapped in Nigeria
- North Korea (kind of…)
- Netflix if you were Blockbuster
- You Get the Picture



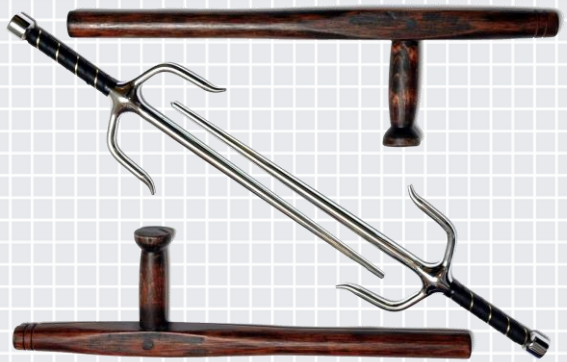
CEO's Stakeholders (Field of Play)

Inside

- Management Team
- Employees
- Unions

Outside

- Board of Directors
- Shareholders
- Public Opinion
- Auditors
- Regulators
- Unions
- Vendor Partners



Ninja Mind Trick #1 – Exploit CEO Pet Projects

- Key Strategy Concepts
  - Identify key corporate projects and bake in security
  - CEO-level sponsorship
  - Less scrutiny than “out year” operational budgets
  - Numbers are big
- Potential Success Patterns
  - Merger or acquisitions
  - Entry into new markets
  - New products

Ninja Mind Trick #2 - Consciously Cultivate Credibility and Relationships

- Key Strategy Concepts
  - Meet with your CEO when you don't need to…
  - Regular meetings without "asks"
  - Clarification for Audit Committee or Board of Directors
  - Build up a Surplus of Credibility, then ask for $$$'s
- Potential Success Patterns
  - Providing clarity on risk issues CEOs rarely understand
  - Providing voice of sanity on compliance matters
  - Pushing back on overzealous 3rd parties

Ninja Mind Trick #3 – Shine at the Board of Directors Meeting

- Key Strategy Concepts
  - The Board of Directors is the CEO's domain
  - Boards of Directors are now most interested in cyber security issues
  - Security is an issue CEO's are largely ill-equipped to address
  - Score cool points for your CEO with her board
  - Regularly address the Board on a recurring basis
- Potential Success Patterns
  - Defusing a tough security question from thorny board members
  - Providing security context for potential new business ventures

Ninja Mind Trick #4 – Enable New Markets or Products

- Key Strategy Concepts
  - I abhor terms like “alignment” or “enabling the business” however….
  - Providing enough confidence to conduct commerce or enter new markets allows CEO to expand top line
  - Security context allows CEOs to make calculated risks in new markets or products
  - Can communicate these calculated risks to internal and external stakeholders, raising level of confidence
  - Consistently helps

Ninja Mind Trick #4 – Enable New Markets or Products (Continued)

- Potential Success Patterns
  - Will privacy controls allow me to directly sell to end customers and cut out the middle man increasing our profit per transaction?
  - Will fraud detection tool allow me to better understand patterns of buy behavior so we can optimize their experience and cross-sell them more products?
  - Will security baked in to our mobile applications allow our clients to conduct more transactions and increase loyalty to our brand?
  - Will encryption and security controls allow me to sell into China and not worry about my intellectual property issues?

Ninja Mind Trick #4 – Enable New Markets or Products – Security Guy Perspective

- Potential Success Patterns
  - Will privacy controls allow me to directly sell to end customers and cut out the middle man increasing our profit per transaction?
  - Will fraud detection tools allow me to better understand patterns of buying behavior so we can optimize their experience and cross-sell them more products?
  - Will security baked in to our mobile applications allow our clients to conduct more transactions and increase loyalty to our brand?
  - Will encryption and security controls allow me to sell into China and not worry about my intellectual property issues?

Ninja Mind Trick #4 – Enable New Markets or Products – CEO Perspective

- Potential Success Patterns
  - Will privacy controls allow me to directly sell to end customers and cut out the middle man increasing our profit per transaction?
  - Will fraud detection tools allow me to better understand patterns of buying behavior so we can optimize their experience and cross-sell them more products?
  - Will security baked in to our mobile applications allow our clients to conduct more transactions and increase loyalty to our brand?
  - Will encryption and security controls allow me to sell into China and not worry about my intellectual property issues?

Ninja Mind Trick #5 – Positively Influence Share Price

- Key Strategy Concepts
  - If publicly traded…
- Potential Success Patterns
  - Confidence around a stream of new projects, products, and markets that create new and large revenue streams
  - Keeping your company out of the news
  - When public incidents do occur, reacting with confidence to stabilize the stock price

Ninja Mind Trick #6 – Prevent the CEO from Getting Fired

- Truism - A truism is a claim that is so obvious or self-evident as to be hardly worth mentioning, except as a reminder or as a rhetorical or literary device, and is the opposite of falsism.

Source: Wikipedia

Resources

- Source: RSA 2014 “Getting Your Security Budget Approved Without FUD,” http://www.rsaconference.com/writable/presentations/file_upload/ciso-w04a-getting-your-security-budget-approved-without-fud.pdf
- “The Savvy Security Leader: Using Guerrilla Tactics to ID Security Program Resources,” RSA Podcast http://www.rsaconference.com/media/the-savvy-security-leader-using-guerrilla-tactics-to-id-security-program-resources
- “The 3 Things CEOs Worry About the Most,” Harvard Business Review, https://hbr.org/2015/03/the-3-things-ceos-worry-about-the-most
- “5 Things CEOs are worried about in 2014”, Wall Street Journal, http://blogs.wsj.com/briefly/2014/01/03/5-things-ceos-are-worried-about-in-2014/
- “Winning as a CISO,” Baich, Rich
- Wikipedia

Contact

John B. Dickson, CISSP

Principal, Denim Group

john@denimgroup.com

@johnbdickson