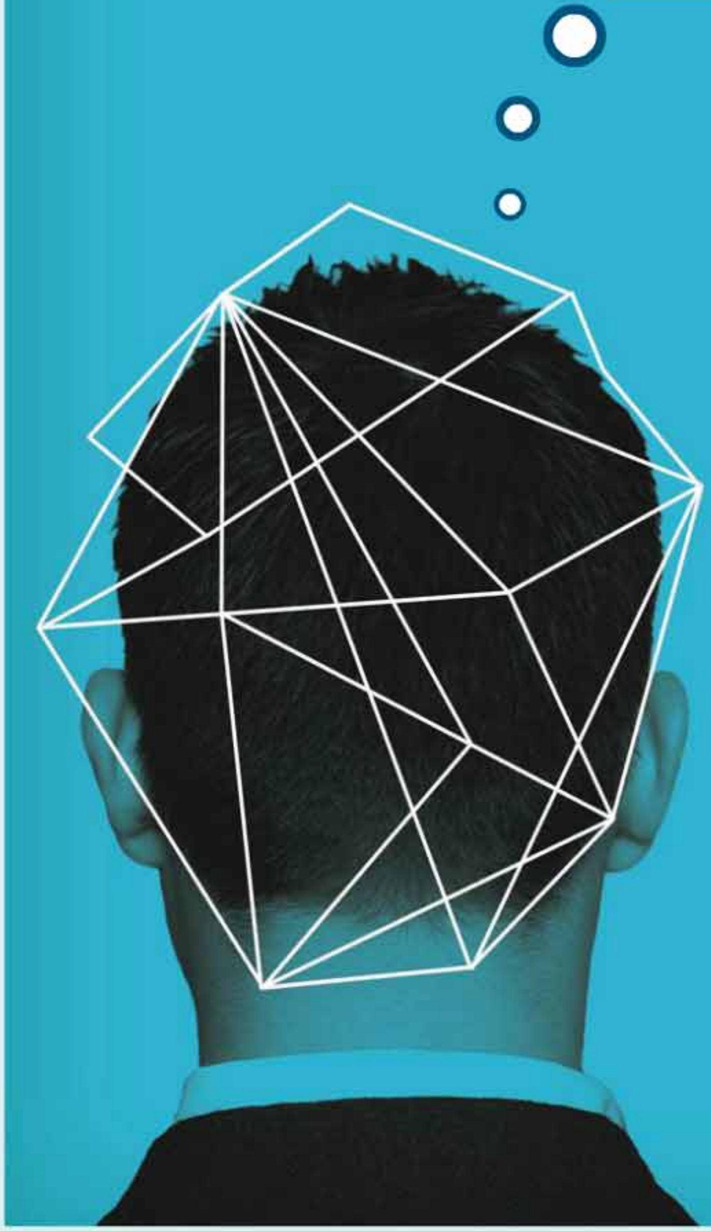
Information Security Leadership Development: Surviving as a Security Leader

Seminar Agenda

Start Time	Title	Presenter
8:30 AM	Introduction	
8:35 AM	Maturity Lifecycle of a Security Program	John Iatonna
9:10 AM	Building Your Team	Justin Peavey
9:40 AM	Role of the CISO: Influence & Decision Support	Derek Brink
10:15 AM	Break	
10:30 AM	Are You Fighting the Wrong Battles?	Bob Rudis
11:00 AM	CISO Roundtable: Security Intelligence Gathering for Leaders	Evan Wheeler (Moderator) Derek Brink James Burrell John Iatonna Dave Notch Bob Rudis
11:30 AM	Seminar Adjourns	

RSACONFERENCE2013



OBSERVE and ABSORB: The State of the Dis(?)-Union

- Take stock of your assets – executive support? budget situation? staffed properly? technology readiness?
- Assess the organizational landscape – new leadership? solid financial footing? Risk appetite?
- Identify and learn your corporate culture
- Foster your key relationships (Legal, HR, GMs)
- Learn the power structure – where do the tough decisions get made? who has the political clout to get things done?

BEST LAID PLANS: Define the objective

- What are you trying to accomplish – HIPAA certification, ISO alignment, keep-your-job accreditation?

YOUR PRIMARY QUESTIONS

a. what information resides on your network?
b. where does it sit?
c. who has access to it?
d. who wants your data and how will they come after it?
e. what is the value of the data (and the cost if it's lost)?

COMMUNICATE, COMMUNICATE … then communicate again

- The credibility gap – demonstrate a clear and accurate relationship between risk and compensating control
- Speak the same language – how does your company 'talk' – connect on the issues that are important to your audience (business managers think $, CMOs think socially, etc.)
- The medium is the message (BUT: Millennials aren't reading your emails

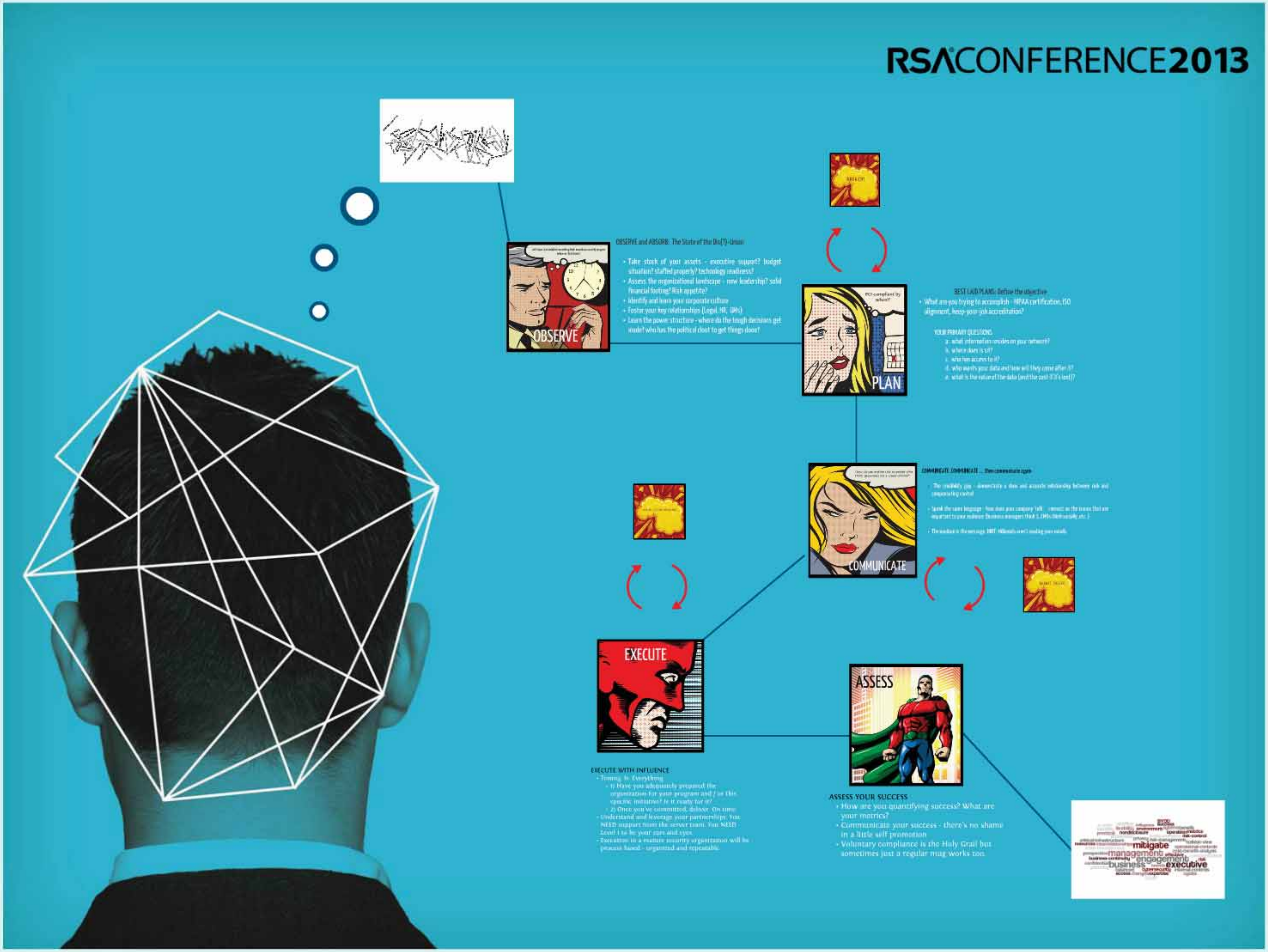
EXECUTE WITH INFLUENCE

- Timing Is Everything
  - 1) Have you adequately prepared the organization for your program and / or this specific initiative? Is it ready for it?
  - 2) Once you've committed, deliver. On time.
- Understand and leverage your partnerships. You NEED support from the senior team. You NEED Level 1 to be your ears and eyes.
- Execution in a mature security organization will be process based – organized and repeatable.

ASSESS YOUR SUCCESS

- How are you quantifying success? What are your metrics?
- Communicate your success – there's no shame in a little self promotion.
- Voluntary compliance is the Holy Grail but sometimes just a regular mug works too.

RSACONFERENCE2013



OBSERVE and ABSORB: The State of the Dis(?)-Union

- Take stock of your assets - executive support? budget situation? staffed properly? technology readiness?
- Assess the organizational landscape - new leadership? solid financial footing? Risk appetite?
- Identify and learn your corporate culture
- Foster your key relationships (Legal, HR, GMs)
- Learn the power structure - where do the tough decisions get made? who has the political clout to get things done?

BEST LAID PLANS: Define the objective

- What are you trying to accomplish - HIPAA certification, ISO alignment, keep-your-job accreditation?

YOUR PRIMARY QUESTIONS

a. what information resides on your network?
b. where does is sit?
c. who has access to it?
d. who wants your data and how will they come after it?
e. what is the value of the data (and the cost if it's lost)?

COMMUNICATE, COMMUNICATE ... then communicate again

- The credibility gap - demonstrate a clear and accurate relationship between risk and compensating control
- Speak the same language - how does your company 'talk' - connect on the issues that are important to your audience (business managers think $, CMOs think socially, etc.)
- The medium is the message. BUT: Millennials aren't reading your emails

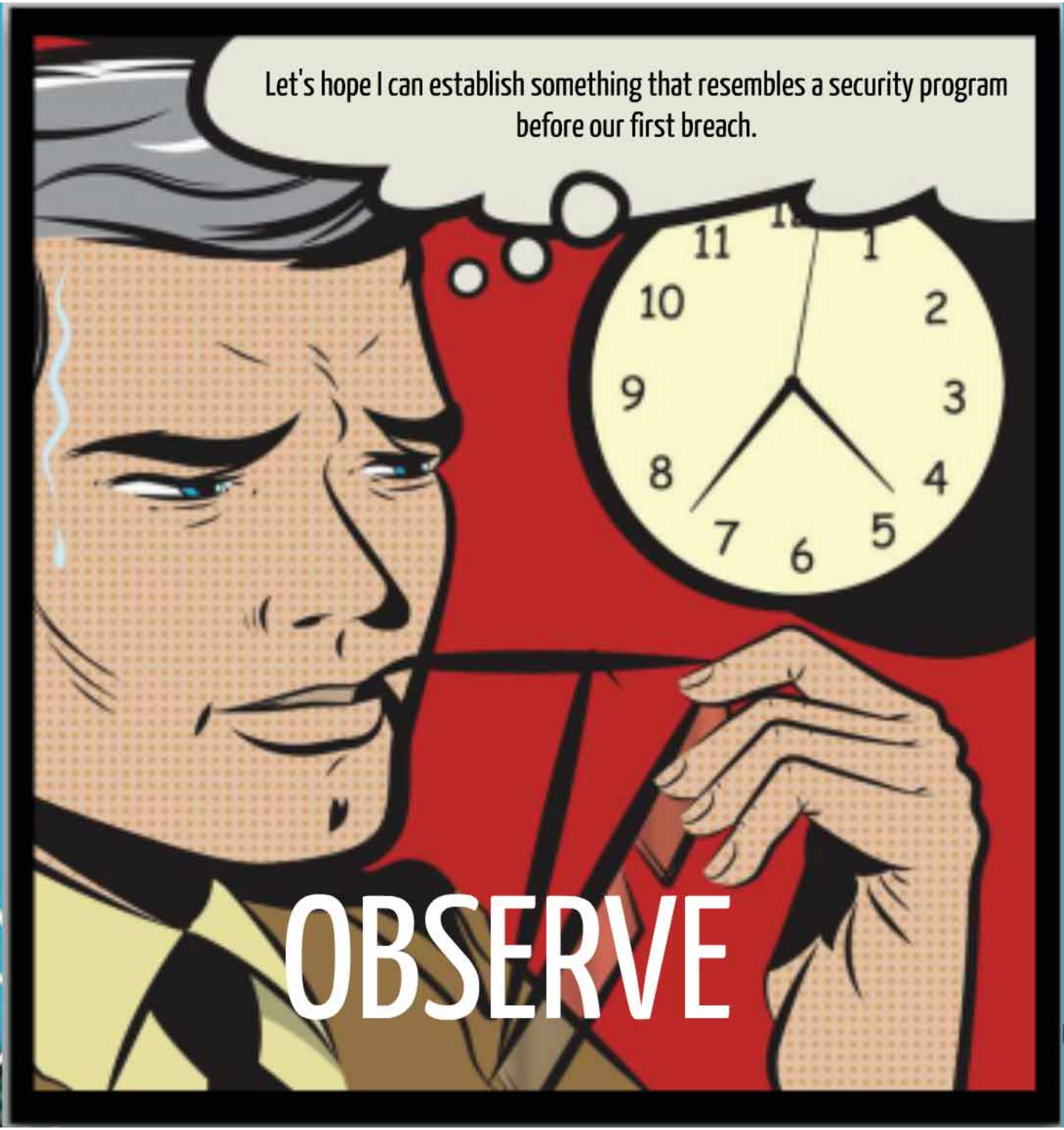
EXECUTE WITH INFLUENCE

- Timing Is Everything
  - 1) Have you adequately prepared the organization for your program and / or this specific initiative? Is it ready for it?
  - 2) Once you've committed, deliver. On time.
- Understand and leverage your partnerships. You NEED support from the server team. You NEED Level 1 to be your ears and eyes.
- Execution in a mature security organization will be process based - organized and repeatable.

ASSESS YOUR SUCCESS

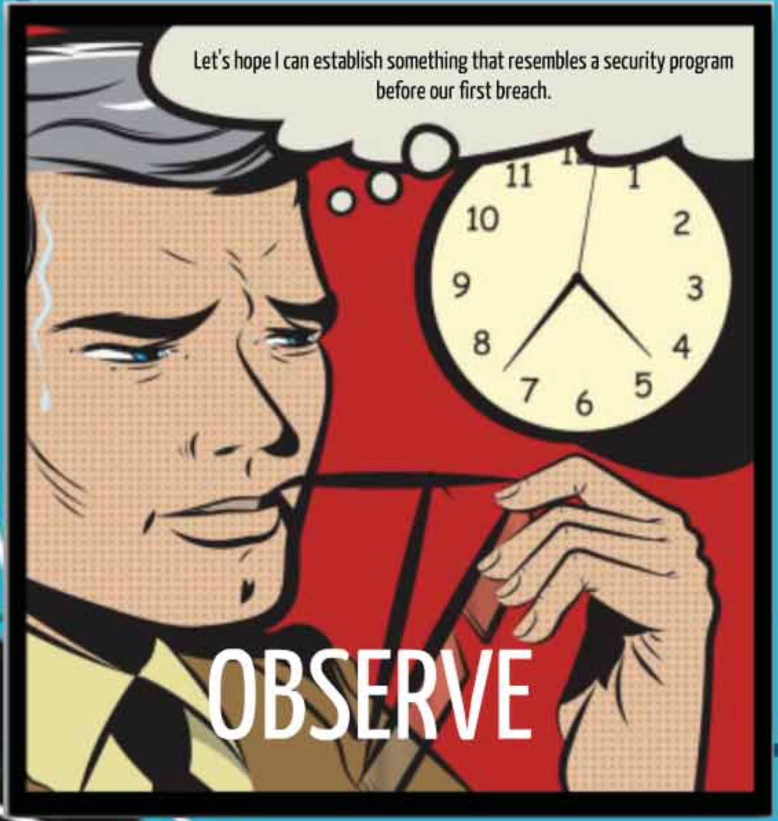
- How are you quantifying success? What are your metrics?
- Communicate your success - there's no shame in a little self promotion
- Voluntary compliance is the Holy Grail but sometimes just a regular mug works too.

internal-controls
patching
holistic-view
legal-advice
exploits
case-by-case-basis
systems
critical-infrastructure
PII
TCOR
indemnification
practical
crisis
Privacy
PHI
continuity
exposure
cycles
confidential-information
staffing
institutionalize
Sarbanes-Oxley
protection
insurance
hacker
influence
operation
FBI
operational-controls
access
disaster-recovery
cybersecurity
social-engineering
subpoena
trends
effective
expertise
operational
expense
metrics
averse
interrelationships
botnets
agency
changes
DHS
PCI
organizations
check-the-box-exercise
BYOD
perspective
environment
identity
liability
balanced
executive
communication
control
success
ISO/IEC
flexibility
c-suite
privacy
cyberespionage
nation-state-actors
ad-hoc
resources
nondisclosure
breach
government
benefit
cost-benefit-analysis


Let's hope I can establish something that resembles a security program before our first breach.
OBSERVE

OBSERV

- Ta
  si
- As
  fi
- Id
- Fo
- Le
  m


Let's hope I can establish something that resembles a security program before our first breach.
OBSERVE

OBSERVE and ABSORB: The State of the Dis(?)-Union

- Take stock of your assets - executive support? budget situation? staffed properly? technology readiness?
- Assess the organizational landscape - new leadership? solid financial footing? Risk appetite?
- Identify and learn your corporate culture
- Foster your key relationships (Legal, HR, GMs)
- Learn the power structure - where do the tough decisions get made? who has the political clout to get things done?

t

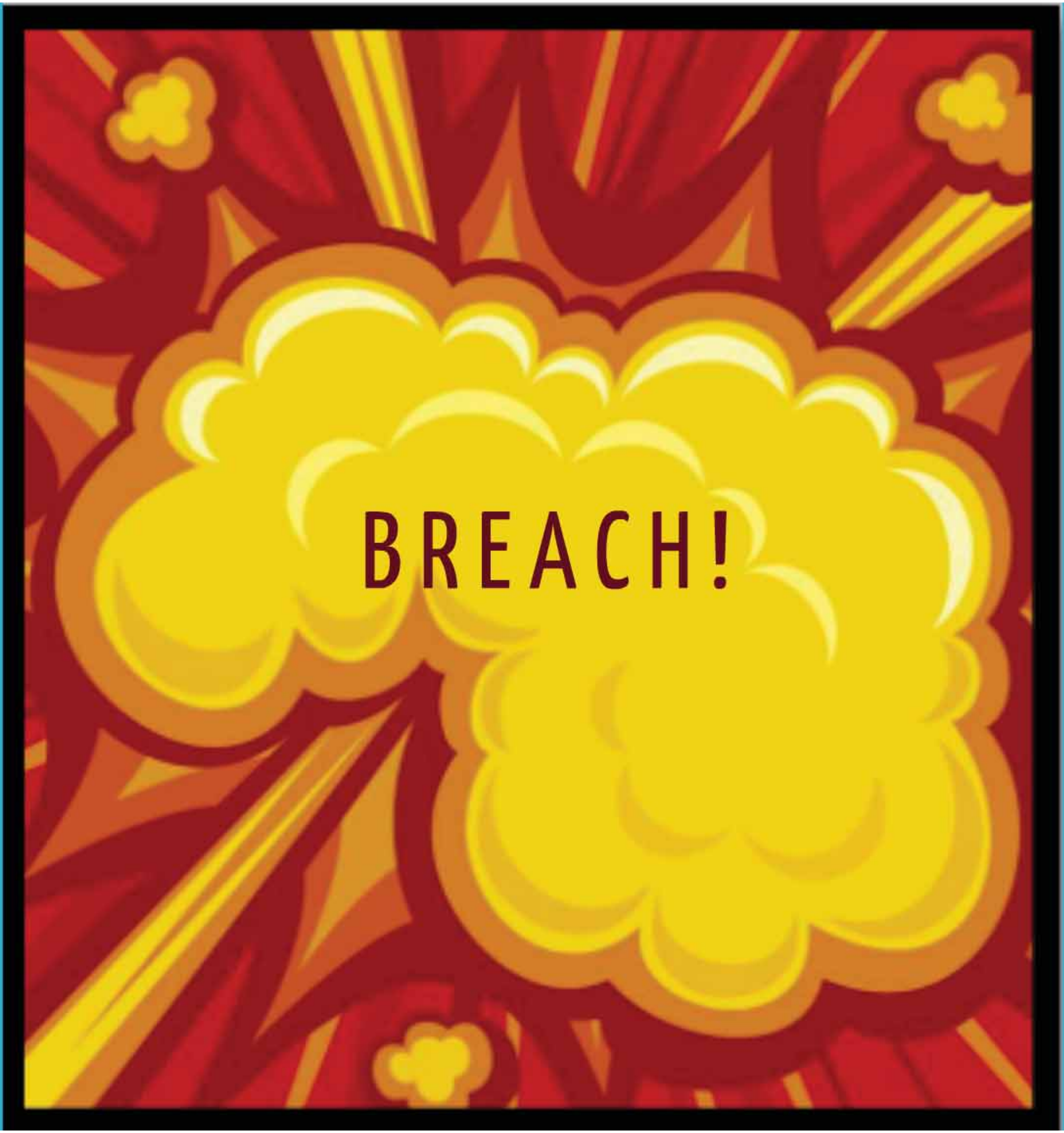
- W
al

BEST LAID PLANS: Define the objective

- What are you trying to accomplish - HIPAA certification, ISO alignment, keep-your-job accreditation?

YOUR PRIMARY QUESTIONS

a. what information resides on your network?
b. where does is sit?
c. who has access to it?
d. who wants your data and how will they come after it?
e. what is the value of the data (and the cost if it's lost)?



BREACH!

t

- W al

How do you explain risk to people who think passwords are a waste of time?
COMMUNICATE

COMMUNI

- The
comp

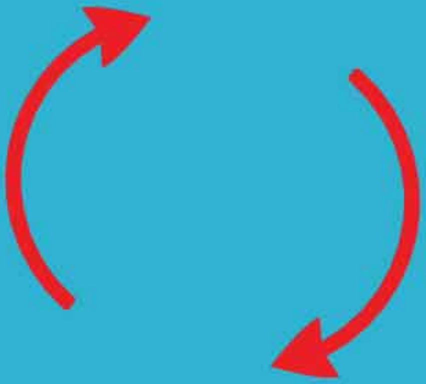
- Spea
impo

- The

How do you explain risk to people who think passwords are a waste of time?
COMMUNICATE

COMMUNICATE, COMMUNICATE .... then communicate again

- The credibility gap - demonstrate a clear and accurate relationship between risk and compensating control
- Speak the same language - how does your company 'talk', connect on the issues that are important to your audience (business managers think $, CMOs think socially, etc.)
- The medium is the message. HINT: Millenials aren't reading your emails.



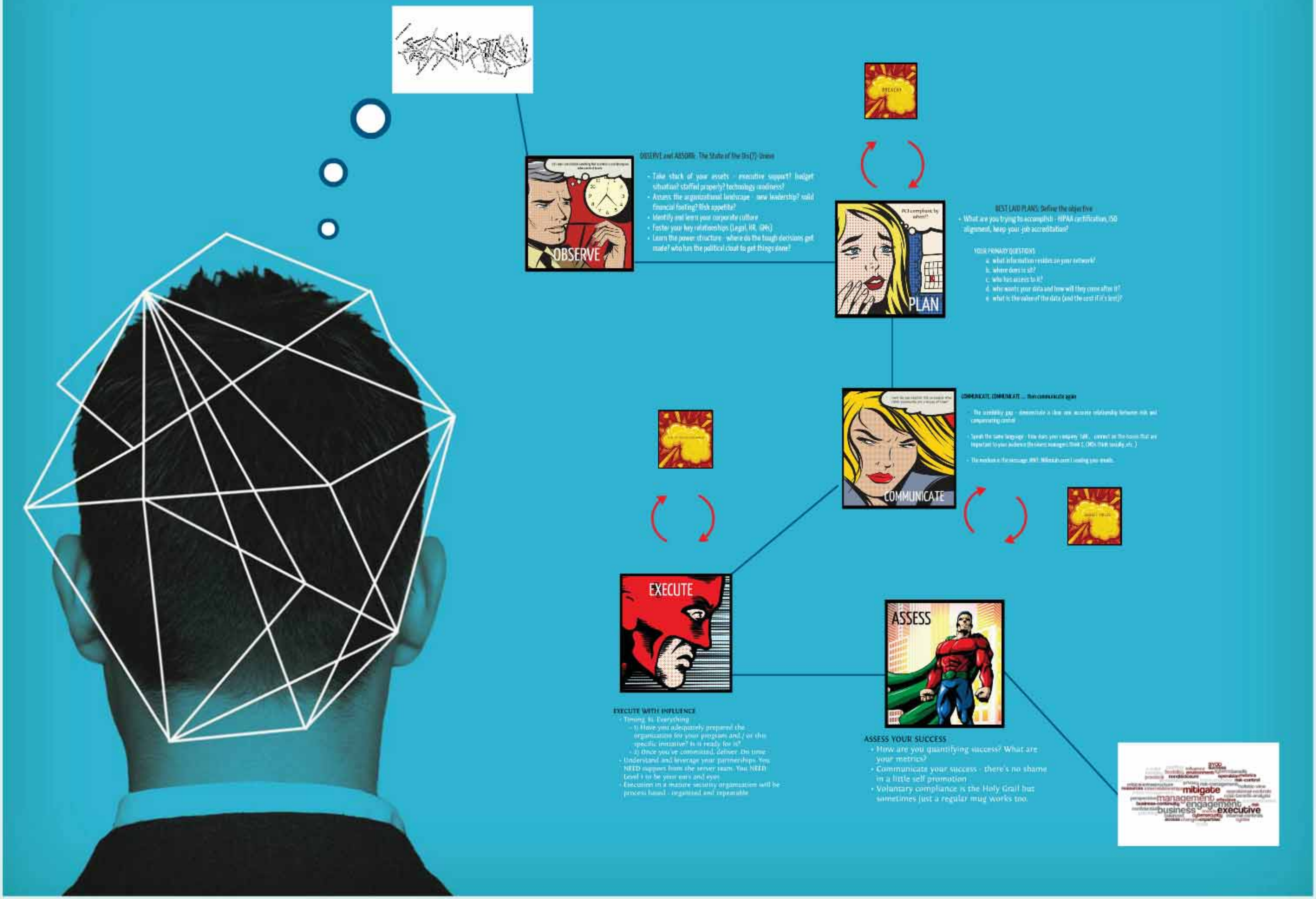
BUDGET FREEZE

How do you explain risk to people who think passwords are a waste of time?
COMMUNICATE

COMMUNI

- The com
- Spea impo
- The

RSACONFERENCE2013



OBSERVE and ABSORB: The State of the Dis(?) Union

- Take stock of your assets – executive support? budget situation? staffed properly? technology readiness?
- Assess the organizational landscape – new leadership? solid financial footing? Risk appetite?
- Identify and learn your corporate culture
- Foster your key relationships (Legal, HR, GMs)
- Learn the power structure – where do the tough decisions get made? who has the political clout to get things done?

BEST LAID PLANS: Define the objective

- What are you trying to accomplish – HIPAA certification, ISO alignment, keep your job accreditation?

YOUR PRIMARY QUESTIONS

a. what information resides on your network?
b. where does it sit?
c. who has access to it?
d. who wants your data and how will they come after it?
e. what is the value of the data (and the cost if it's lost)?

COMMUNICATE, COMMUNICATE … then communicate again

- The credibility gap – demonstrate a clear and accurate relationship between risk and compensating control
- Speak the same language – how does your company 'talk' … connect on the issues that are important to your audience (business managers think $, CXOs think [illegible], etc.)
- The medium is the message. [illegible] Millennials aren't reading your emails.

EXECUTE WITH INFLUENCE

- Timing Is Everything
  - 1) Have you adequately prepared the organization for your program and / or this specific initiative? Is it ready for it?
  - 2) Once you've committed, deliver. On time.
- Understand and leverage your partnerships. You NEED support from the server team. You NEED Level 1 to be your ears and eyes.
- Execution in a mature security organization will be process based – organized and repeatable

ASSESS YOUR SUCCESS

- How are you quantifying success? What are your metrics?
- Communicate your success – there's no shame in a little self promotion
- Voluntary compliance is the Holy Grail but sometimes just a regular mug works too.

EXECUTE

EXECUTE WITH INFLUENCE

- Timing. Is. Everything.
    - 1) Have you adequately prepared the organization for your program and / or this specific initiative? Is it ready for it?
    - 2) Once you've committed, deliver. On time.
- Understand and leverage your partnerships. You NEED support from the server team. You NEED Level 1 to be your ears and eyes.
- Execution in a mature security organization will be process based - organized and repeatable.

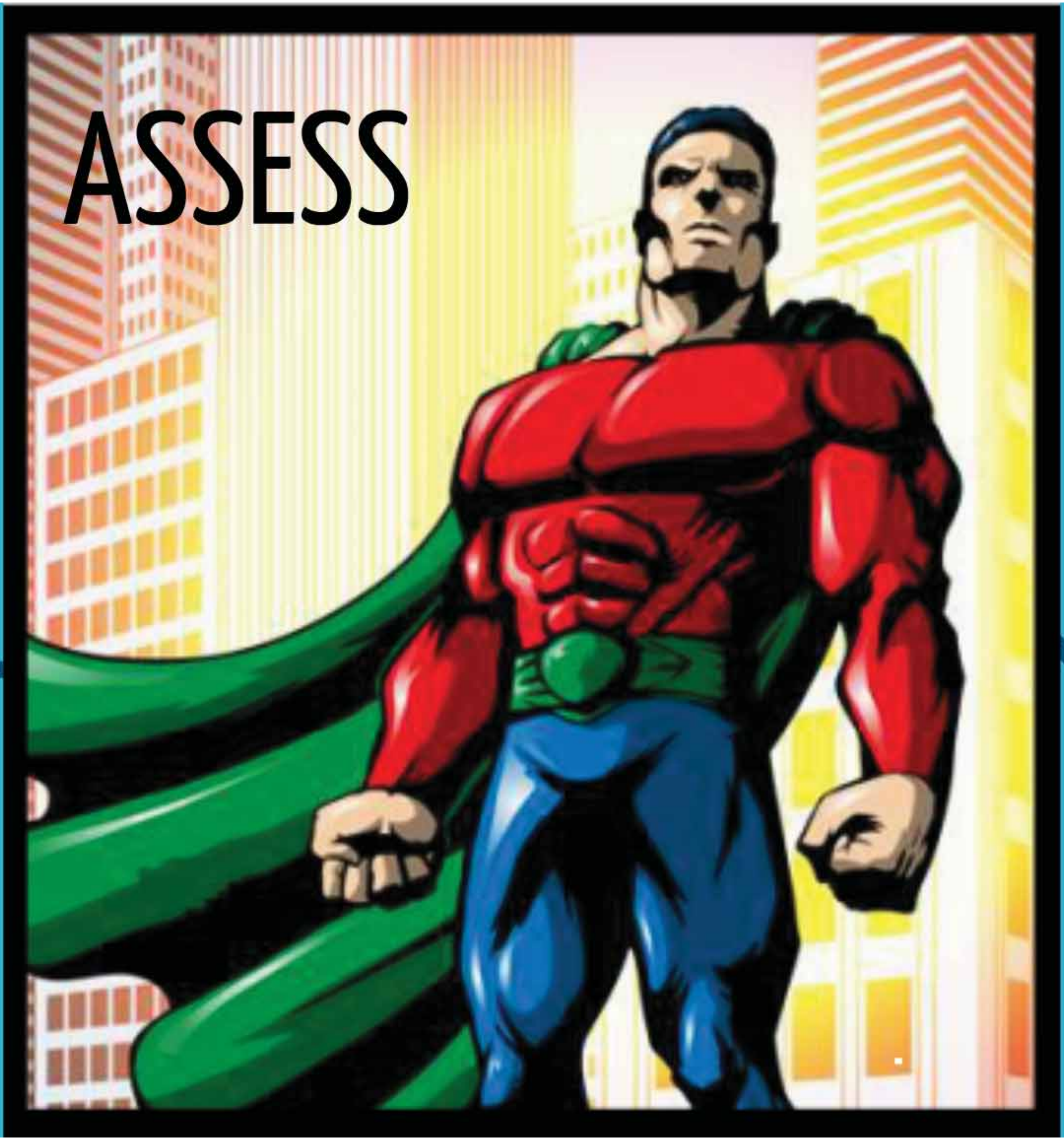
NEW CEO - STRATEGIC REALIGNMENT

t

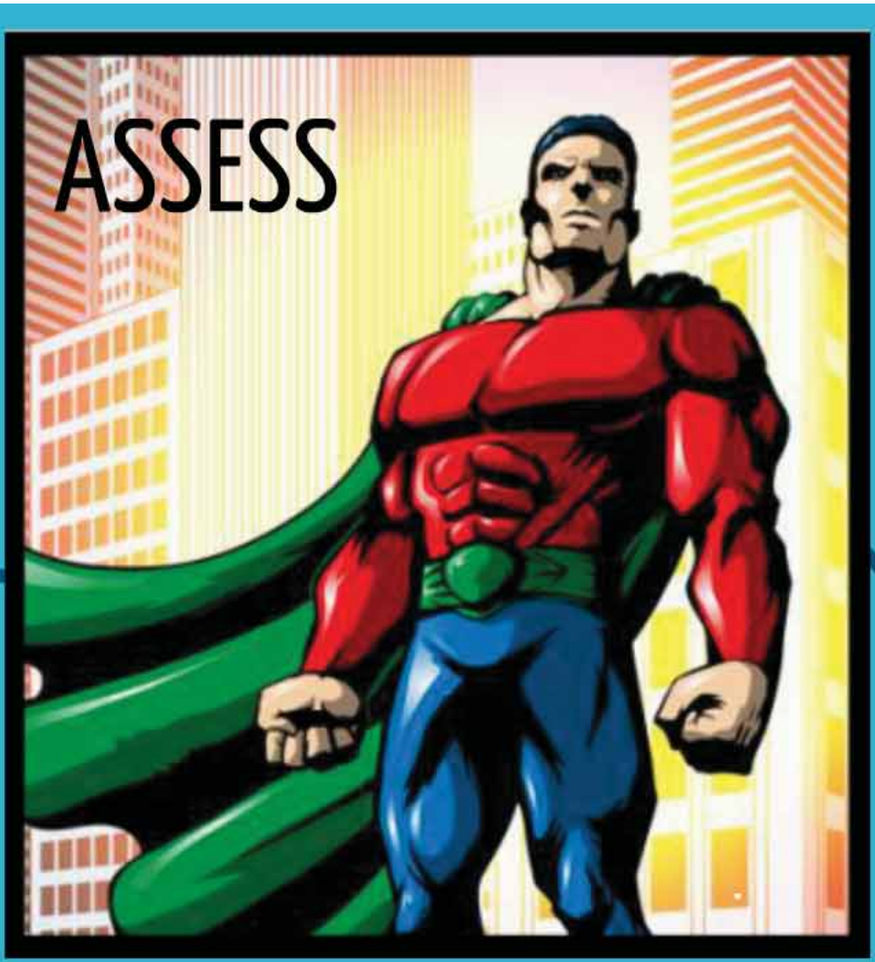
- W
al

EXECUTE

ASSESS



or, more accurately …

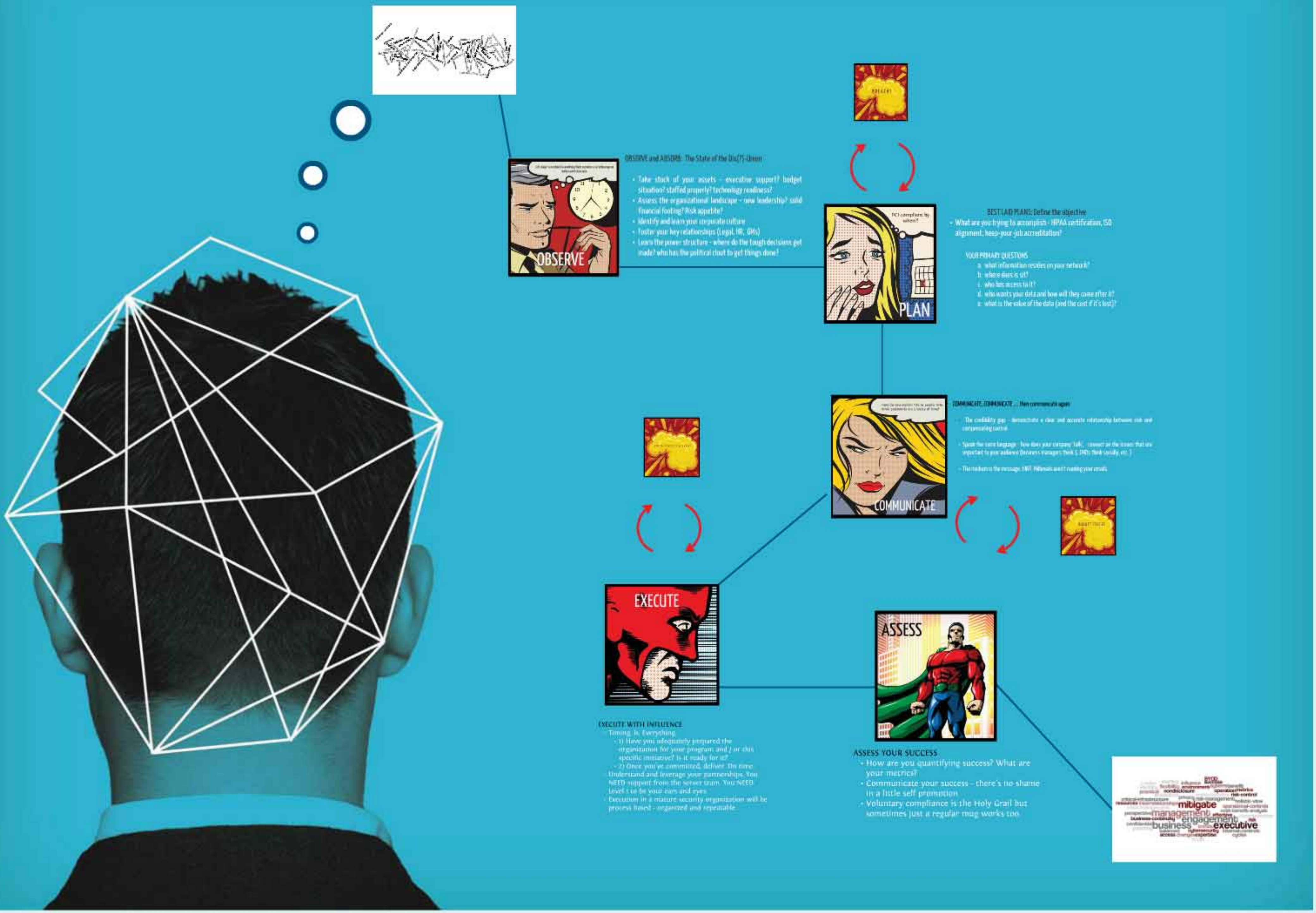


ASSESS YOUR SUCCESS

- How are you quantifying success? What are your metrics?
- Communicate your success - there's no shame in a little self promotion
- Voluntary compliance is the Holy Grail but sometimes just a regular mug works too.

BYOD
c-suite
staffing
influence
success
identity
flexibility
environment
sytems
benefit
practical
nondisclosure
operation
metrics
protection
institutionalize
risk-control
critical-infrastructure
privacy
risk-management
holistic-view
resources
interrelationships
mitigate
crisis-management
operational-controls
perspective
management
cost-benefit-analysis
effective
communication
business-continuity
engagement
risk
confidential
business
trends
executive
patching
balanced
cybersecurity
internal-controls
access
changes
expertise
cycles
TCOR

RSACONFERENCE2013



OBSERVE and ABSORB: The State of the Dis(?)-Union

- Take stock of your assets - executive support? budget situation? staffed properly? technology readiness?
- Assess the organizational landscape - new leadership? solid financial footing? Risk appetite?
- Identify and learn your corporate culture
- Foster your key relationships (Legal, HR, GMs)
- Learn the power structure - where do the tough decisions get made? who has the political clout to get things done?

BEST LAID PLANS: Define the objective

- What are you trying to accomplish - HIPAA certification, ISO alignment, keep-your-job accreditation?

YOUR PRIMARY QUESTIONS

a. what information resides on your network?
b. where does is sit?
c. who has access to it?
d. who wants your data and how will they come after it?
e. what is the value of the data (and the cost if it's lost)?

COMMUNICATE, COMMUNICATE … then communicate again

- The credibility gap - demonstrate a clear and accurate relationship between risk and compensating control
- Speak the same language - how does your company 'talk'… connect on the issues that are important to your audience (business managers think $, CMOs think socially, etc.)
- The medium is the message. HINT: Millennials aren't reading your emails

EXECUTE WITH INFLUENCE

- Timing Is Everything
  - 1) Have you adequately prepared the organization for your program and / or this specific initiative? Is it ready for it?
  - 2) Once you've committed, deliver. On time.
- Understand and leverage your partnerships. You NEED support from the server team. You NEED level 1 to be your ears and eyes.
- Execution in a mature security organization will be process based - organized and repeatable.

ASSESS YOUR SUCCESS

- How are you quantifying success? What are your metrics?
- Communicate your success - there's no shame in a little self promotion
- Voluntary compliance is the Holy Grail but sometimes just a regular mug works too

Security in knowledge

Building Your Team

Five lessons from the trenches

Justin Peavey

RSACONFERENCE2013

Session ID: SEM-003

Session Classification:

Lesson 1:

- In security, it's always an away game

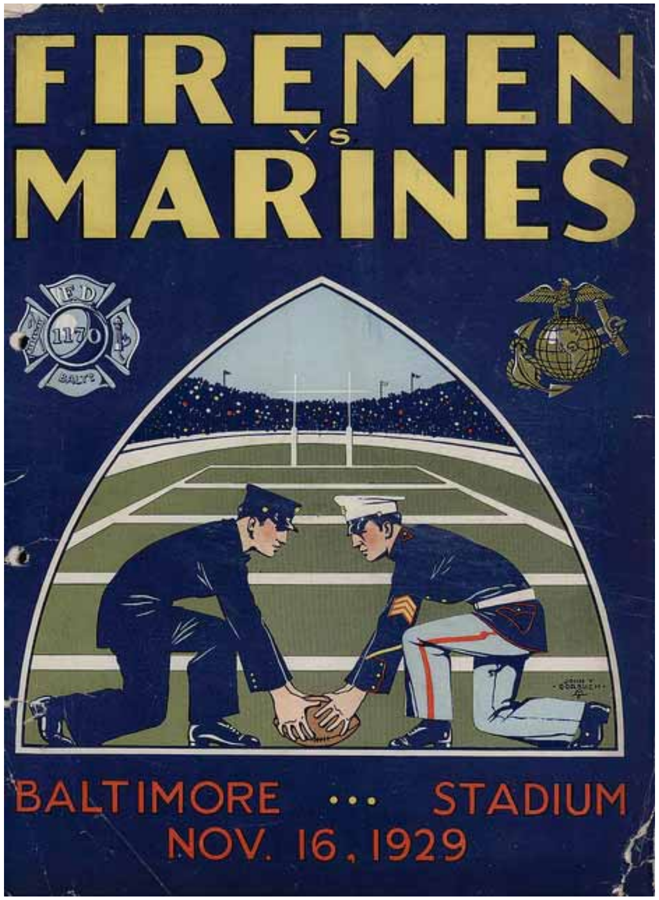


Image © Marine Corps Archives & Special Collections **(CC BY 2.0)**

Lesson 2:

- Some skills you can teach, some you can't (or maybe shouldn't)

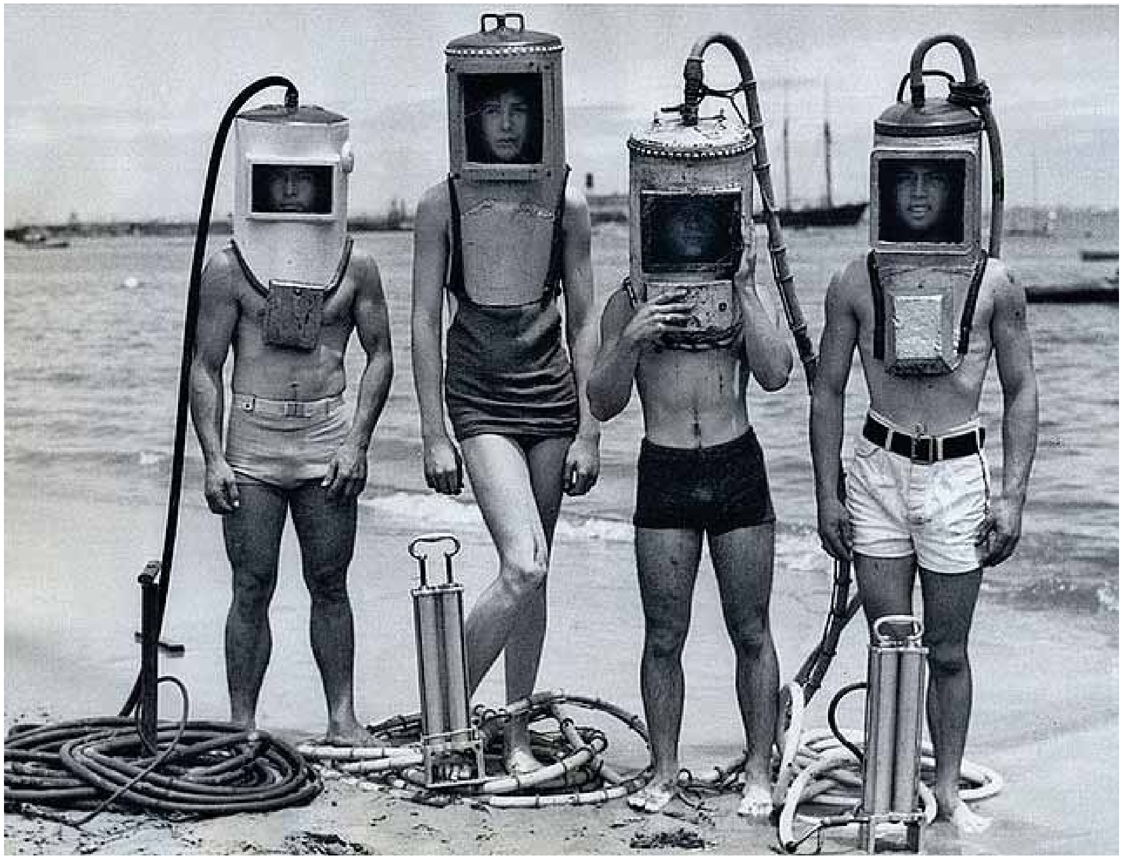


Image ©x-ray delta 1 (Flickr) . **CC BY-SA 2.0**

[redacted]

Lesson 3:

- Everybody has their issues

Image © Heather Rose. **CC BY-ND 2.0**

Lesson 4:

- Size does matter, at least to your CFO

Image ©Peter Taylor **(CC BY 2.0)**

Lesson 5:

- In business, it’s becoming nearly always an away game.

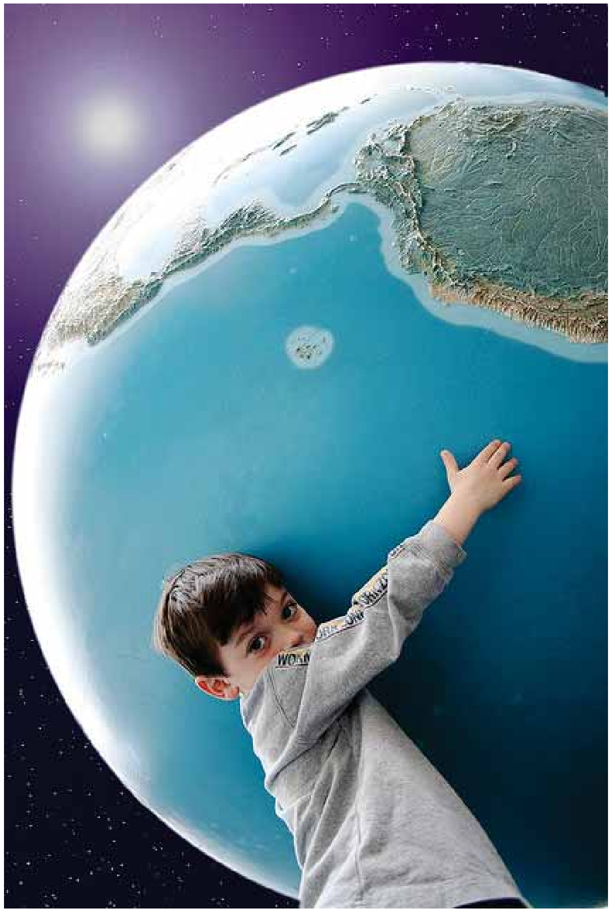


Image ©woodleywonderworks (Flickr) **(CC BY 2.0)**

Security in knowledge

RSACONFERENCE2013

Security in knowledge

Role of the CISO: Influence and Decision Support

Derek E. Brink, CISSP

Vice President and Research Fellow, IT Security and IT GRC

Aberdeen Group, a Harte-Hanks Company

www.linkedin.com/in/derekbrink

Session ID: SEM-003

Does Security Speak Make a Sound?

If what's being transmitted isn't heard, then it isn't making a sound

- "The 2012 CyLab Governance survey results indicate a serious lack of attention at the top."
  - Jody R. Westby, Carnegie Mellon CyLab, third bi-annual survey on how Boards of Directors and senior executives from the Forbes Global 2000 are governing security and privacy for their corporate information assets – at RSA Conference 2012

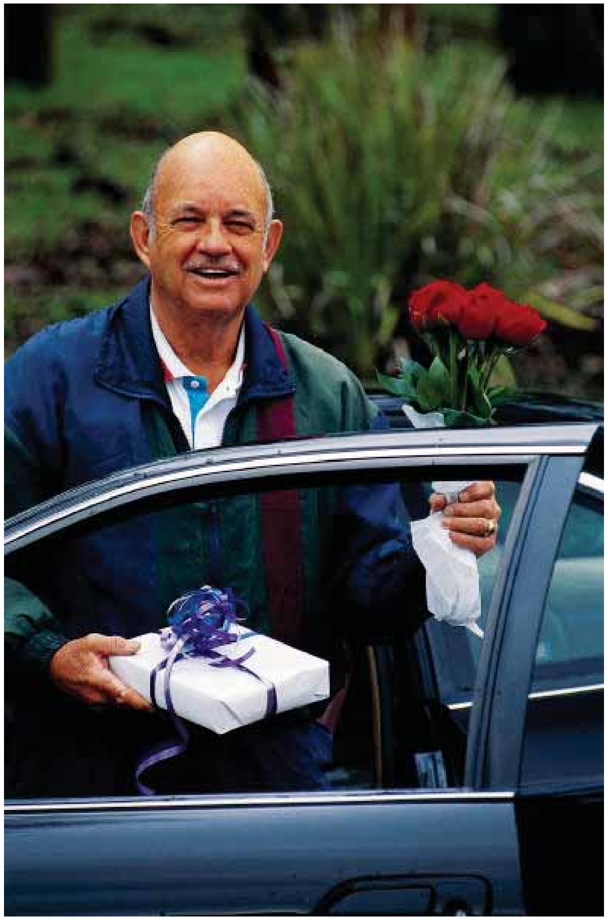
http://blogs.aberdeen.com/it-security/does-it-security-and-compliance-make-a-sound/ (6 March 2012)

The CISO is an Apologist for Security

The CISO is an Apologist for Security

- No, not in the sense of saying “I’m sorry” …

- … although there were plenty of public disclosures of Security to be sorry about since the last RSA Conference …



And the Beat Goes On . . .

- LinkedIn, eHarmony
- Yahoo
- Certificates signed with MD5
- Barnes & Noble
- United Technologies (Onity)
- South Carolina Department of Revenue
- Saudi Aramco
- Java vulnerabilities
  - NY Times, Wall Street Journal
  - Twitter, Facebook
- The Works Bakery Café
- …

TD Bank (drilldown)

TD Bank

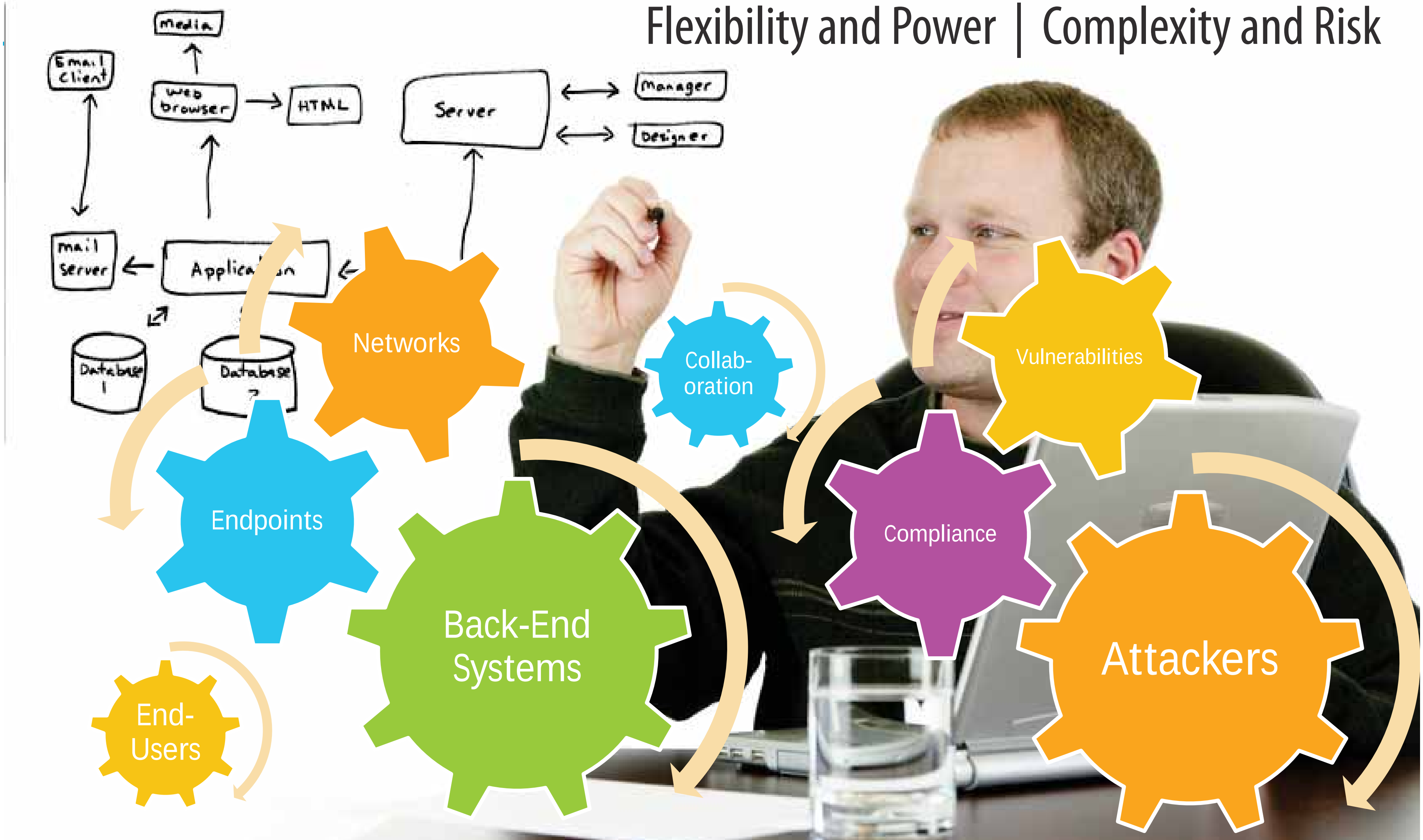
America's Most Convenient Bank®

- What bothers me most is the smarmy, disingenuous language that a Chief Privacy Officer at TD Bank uses in communicating about this incident to its customers:
  - "At TD Bank, we realize the importance of keeping you informed when it comes to your banking." *But we still waited six months.*
  - "That's why we're committed to notifying you about events that might affect your accounts." *Not just your accounts with us, of course, but your entire digital identity.*
  - "Today, we're writing to let you know about an incident involving your personal information." *We still haven't figured out what happened … and we're silent on whether or not we've taken any steps to prevent it from happening again.*
  - "At TD Bank, protecting our Customers' personal information is a top priority and something we take very seriously." *Except we didn't implement the basic best practice of encrypting our backup tapes, and we don't have controls in place to understand what happened to them even after an investigation of more than six months.*
- But perhaps the most painfully ironic is this: "We sincerely regret any concern or inconvenience this may cause you." *Written on letterhead with the tagline "America's Most Convenient Bank."*

http://blogs.aberdeen.com/it-security/td-fumbles-tapes-not-encrypted-customers-lose/ (19 October 2012)

Over just the past 3-4 years, a dramatic change in business context for CISOs

Flexibility and Power | Complexity and Risk



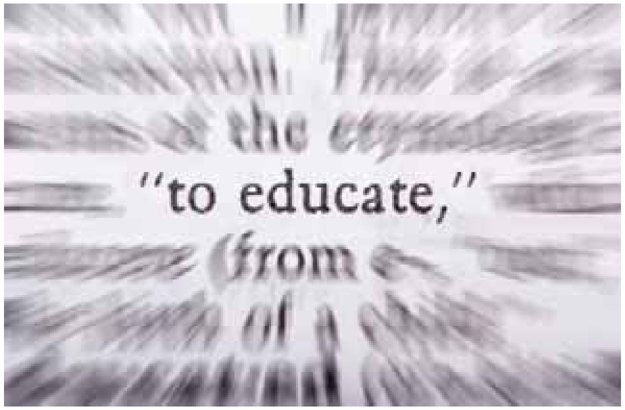
http://blogs.aberdeen.com/it-security/we-have-met-the-enemy-and-he-is-____/ (3 February 2012)

The CISO is an Apologist for Security

- An **apologist**, as in "a person who makes a case, in speech or in writing, for a belief or idea"
- The other side of the coin for **evangelist**, as in “an enthusiastic advocate”
  - Usually these terms are used in an *ecclesiastical* context …
  - … and in fact I often find many ecclesiastical parallels and inspiration for my own work …

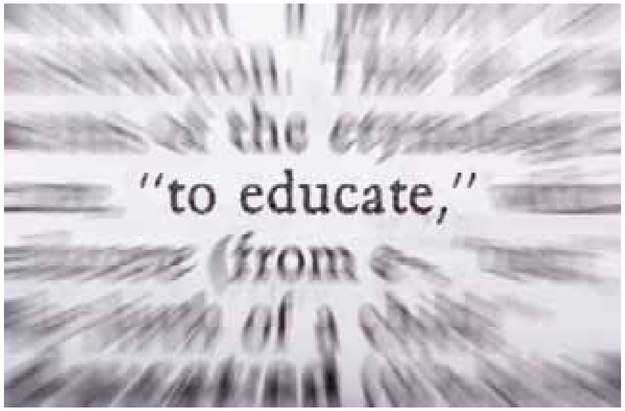
The Devil's Dictionary for IT and Security

- *The Devil's Dictionary* – also known as *The Cynic's Word Book* – by Ambrose Bierce was first published over 100 years ago
- Examples of his cynical, satirical "definitions" include:
  - **Absurdity** – a statement of belief manifestly inconsistent with one's own opinion
  - **Accident** – an inevitable occurrence resulting from the action of immutable natural laws
  - **Congratulations** – the civility of envy



The Devil's Dictionary for IT and Security

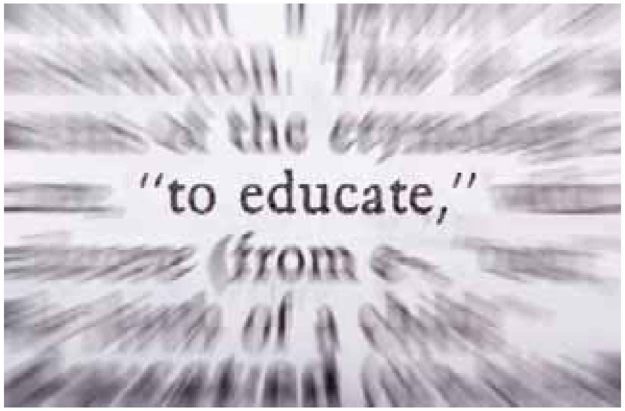
- **Advanced Persistent Threat (APT)** – an undocumented guest user, accessing valuable enterprise resources. See *Illegal Immigrant*.



http://blogs.aberdeen.com/it-infrastructure/the-devils-dictionary-for-it-and-it-security-eleven-initial-entries/ (27 November 2012)

The Devil's Dictionary for IT and Security

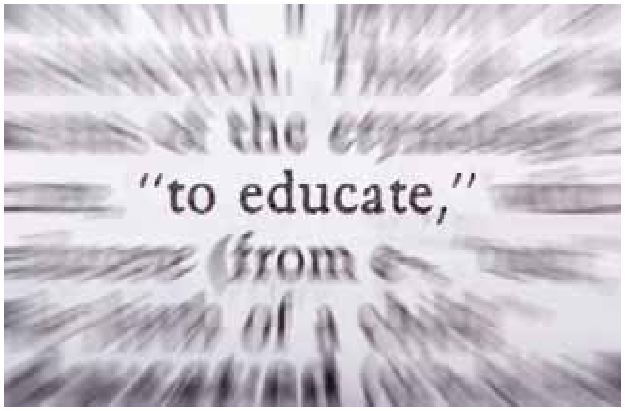
- **Consumerization** – an excuse frequently offered by enterprise IT and Security staffs for their lack of leadership, and their increasing risk of irrelevance



http://blogs.aberdeen.com/it-security/moron-consumer-file-sharing/ (27 April 2012)
http://blogs.aberdeen.com/it-infrastructure/the-devils-dictionary-for-it-and-it-security-eleven-initial-entries/ (27 November 2012)

The Devil's Dictionary for IT and Security

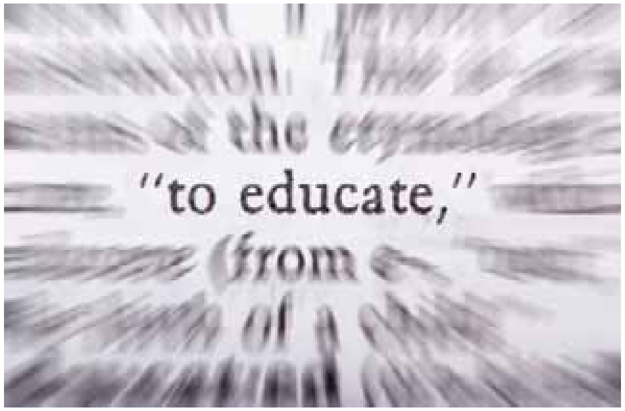
- **Deny by default** – the traditional enterprise security policy of denying everything except that which is specifically permitted, as opposed to proactively identifying and enabling the capabilities that support the rapidly changing needs of the business (see also *Consumerization* and *Dr. No*)



http://blogs.aberdeen.com/it-infrastructure/the-devils-dictionary-for-it-and-it-security-eleven-initial-entries/ (27 November 2012)

The Devil's Dictionary for IT and Security

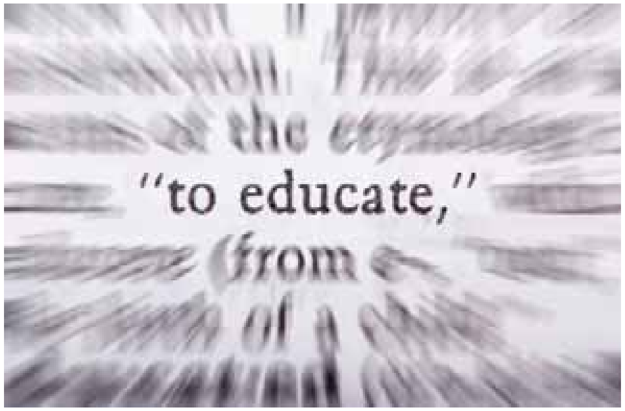
- **Security Breach Notification** – an opportunity for management to try to shift the blame for a security breach to someone else, and to position the company as the actual victim; an opportunity for management to remind its valued customers, whose information it has just allowed to be compromised,
  that the company takes the security of its customers' information very seriously



http://blogs.aberdeen.com/it-infrastructure/the-devils-dictionary-for-it-and-it-security-eleven-initial-entries/ (27 November 2012)

The Devil's Dictionary for IT and Security

- **Risk-based decisions** – the process by which enterprises with world-class brands fail to implement the most basic best practices and protections for user identities and data; the indifference, incompetence or calculation by which industry in general appears to be incapable of self-regulation in matters of security and continues to invite stronger regulatory mandates



http://blogs.aberdeen.com/it-infrastructure/the-devils-dictionary-for-it-and-it-security-eleven-initial-entries/ (27 November 2012)

Where is the Invisible Hand, or at least the Visible Hand of Management? Where is the Influence of the CISO?

- Are companies *capable* of self-regulation on security matters?
- Or will corporate profit motives / ignorance / indifference / incompetence continue to result in similar security breaches … and invite stronger *regulatory* mandates?

The Very Visible Hand of Regulation

- Isn’t the answer right in front of us?
- Each of the complex matrix of regulatory requirements was put in place because neither the invisible hand
  of the market,
  nor the visible hand
  of management,
  was deemed to be adequate …

The Larger Question

- The question is magnified when it gets applied to critical infrastructure – i.e.,
  - Power plants
  - Utilities
  - Pipelines
  - Transportation networks
  - Telecommunications networks
  - Hospitals
  - Financial systems
  - Other systems that people and businesses rely on for the essentials of daily life

CIOs Who Responded to Sen. Rockefeller's Letter *(September 2012 – about 300 of 500 companies responded)*

- Senator Rockefeller's staff published a 6-page memo on 28 Jan 2013 with their summary of industry feedback, along with 13 pages of verbatims from the written responses. Staff conclusions include:
  - "Many companies supported a voluntary program to protect critical infrastructure, so long as it would not become mandatory."
  - "Concerns related to the proposed voluntary program were primarily related to the potential development of an inflexible, "one-size-fits-all" set of best practices."
  - "Other common concerns included the need to adequately protect the confidentiality of information shared with the federal government during cyber threat assessments."
  - "The responses showed that you should continue working to advance cybersecurity legislation in the 113th Congress."
- *Confirmation bias* among the Senator's staff? **Worth your own read!**

President Obama's Executive Order

(February 2013) The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure

- to enhance the security and resilience of the Nation's critical infrastructure
- to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity
- while promoting safety, security, business confidentiality, privacy, and civil liberties
- through a partnership with the owners and operators of critical infrastructure to
  - improve cyber security information-sharing
  - and collaboratively develop and implement risk-based standards

Devil in the Details:

Agreement on "critical"

Conditions on information-sharing

Yet another framework

Voluntary adoption – at first

Again, I recommend that you read the verbatims

http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity (12 February 2013)

Evidence of Progress: Management's Discussion of Risk

Analysis of Dow Jones Industrial Average (30 companies) SEC 10-K Filings

- Four years ago, I wrote that discussion of IT-related risks were **not even showing up** in the SEC 10-K filings for leading US high-tech firms … my review of the 2012 filings of the DJIA shows some interesting new patterns

Company	Walt Disney	Johnson & Johnson	Microsoft	United Technologies	Bank of America	General Electric	Pfizer	Procter & Gamble	Coca-Cola	Travelers Companies	UnitedHealth	3M	AT&T	Exxon Mobil	Hewlett-Packard	JPMorgan Chase	Merck	Verizon	Wal-Mart	Intel	McDonald's	Boeing	Caterpillar	Home Depot	IBM	Alcoa	American Express	Du Pont	Chevron	Cisco Systems
Compromise of confidential information	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					
Compromise of intellectual property	X	X	X	X																X	X					X	X	X		
Disruption from reliance on IT infrastructure	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X										X	X
Disruption from reliance on third-party i/s	X				X	X	X	X	X	X	X																			

- 25 out of 30 identify the risk of compromise of confidential company / partner / customer information … but just 9 out of 30 explicitly discuss risks to their intellectual property and trade secrets
- 21 out of 30 identify the risks of disruptions in their IT infrastructure … but just 8 out of 30 explicitly discuss risks from their reliance on third-party infrastructure (e.g., managed services, cloud service providers)

http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm (13 October 2011)

Speaking the Language(s) of Risk

Review of the SEC 10-K language shows that companies are starting to bridge the gap in their discussions of risk

Types of Risk	Unrewarded	Rewarded
Risk Management Objectives	▪ Protect value ▪ Defend assets ▪ Minimize downside	▪ Create value ▪ Enable assets ▪ Maximize upside
Example Areas of Focus	▪ Security vulnerabilities and threats ▪ Regulatory compliance	▪ Innovation and growth initiatives ▪ Operational efficiencies
Associated Assets	▪ Identities and access ▪ Applications and data ▪ IT infrastructure ▪ Physical infrastructure ▪ Personnel safety	▪ Revenue streams ▪ Distribution channels ▪ Products and services ▪ Operations and supply chain ▪ Reputation and brand

Insane IT

Keep doing what you've always done, keep getting what you've always got

- "Insanity is doing the same thing over and over again but expecting different results."
  - Commonly attributed to Albert Einstein (Germany, 1879)
- "Good judgment comes from experience, and often experience comes from bad judgment."
  - Rita Mae Brown (US, 1944)

Insane IT – Examples? (1 of 2)

- Relying solely on traditional signature-based approaches
  - E.g., network security only traditional firewalls; endpoint security only anti-virus
- Applying traditional, centralized endpoint management approaches to smart phones and tablets
  - E.g., a focus on devices, as opposed to a focus on applications and data
- Scanning and testing as a primary strategy for application security
  - I.e., not necessarily fixing, or not developing applications with fewer vulnerabilities in the first place

Insane IT – Examples? (2 of 2)

- Leveraging the "big data" and "analytics" of security and compliance primarily for understanding "what happened"
  - I.e., as opposed to identifying, containing and responding to "what's abnormal" more quickly
- Communicating the value of IT Security solely in terms of prevention, avoidance, or "insurance"
- Enforcing policies to prevent end-users from using consumer-oriented tools, e.g., file-sharing
  - As opposed to providing them with supported, enterprise-class alternatives
- Investing millions in security technologies, but not investing in security awareness and education for end-users

Service to the Organization (Past … and Present)

Committed, faithful, honorable … unrecognized, and underappreciated

- *We live in a world that has walls, and those walls have to be guarded … Who's gonna do it? You? … I have a greater responsibility than you can possibly fathom … My existence, while grotesque and incomprehensible to you, saves lives … deep down in places you don't talk about at cocktail parties, you want me on that wall, you need me on that wall … I have neither the time nor the inclination to explain myself to a man who rises and sleeps under the blanket of the very freedom that I provide, and then questions the manner in which I provide it. I would rather you just said thank you, and went on your way.*

"You can't handle the truth!"

http://blogs.aberdeen.com/it-security/the-information-security-servant-leader-3/ (5 October 2012)

Service to the Organization (Present and Future)

CISOs as Servant-Leaders – a fundamentally different approach

Servant-Leaders are characterized as excellent:

- **Communicators**, with the ability to:
  - Listen
  - Empathize
  - Heal
  - Persuade / build consensus
- **Strategists**, with strengths in:
  - Awareness
  - Conceptualization
  - Forward-thinking
- **Builders**, with a commitment to:
  - Stewardship
  - Growth of people
  - Growth of community

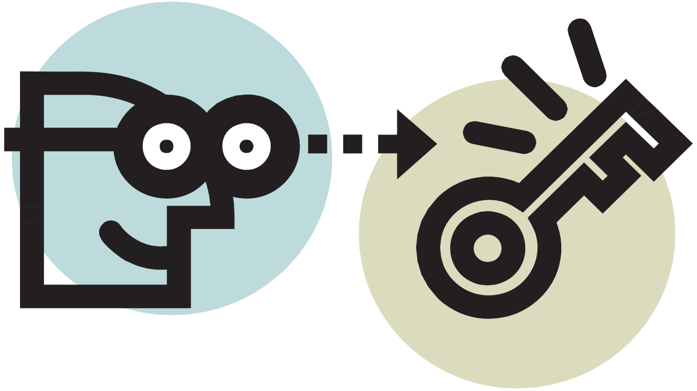
Source: *Character and Servant-Leadership: Ten Characteristics of Effective, Carding Leaders*, Larry C. Spears

The CISO is an Apologist for Security

Influence and Decision Support = Servant-Leadership

- **Understand** the business to **support** the business
  - Security and compliance objectives support strategic objectives …
    - Collaboration
    - Agility and productivity
    - Efficiency, innovation and growth
  - … by managing its risks and playing within the rules

  - Connect to concepts and projects that are understood and accepted
    - Compromised data or IP is compromised, regardless of how
    - Disrupted operations are disrupted, regardless of how



The CISO is an Apologist for Security

Influence and Decision Support = Servant-Leadership

- Build **influence** by building **relationships**
  - Finance, Audit, Legal, HR, Marketing, Lines of Business, Risk, Privacy, Business Continuity …
  - Solve their problems; establish your credibility; gain their trust, e.g.,
    - Finance and SEC filings
    - Audit and compliance deficiencies
    - Legal and IP protection
    - HR and onboarding
    - Marketing and data / privacy protections
    - Lines of Business and secure file sharing
  - End-users (employees)?
  - End-users (business partners, customers)?

The CISO is an Apologist for Security

Influence and Decision Support = Servant-Leadership

- Listen, empathize, heal, persuade
- Inform, educate, coach, connect
  - Public disclosures are opportunities
  - Awareness and training is ongoing
  - Decisions will increasingly be affected, both directly and indirectly

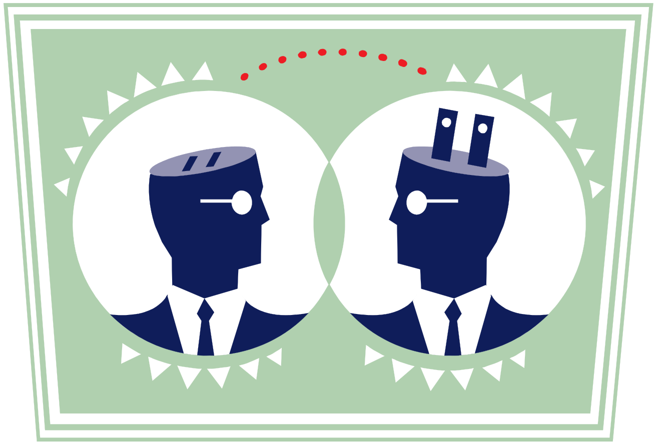
The CISO is an Apologist for Security

Influence and Decision Support = Servant-Leadership

- Communicate, in the right language for the target audience

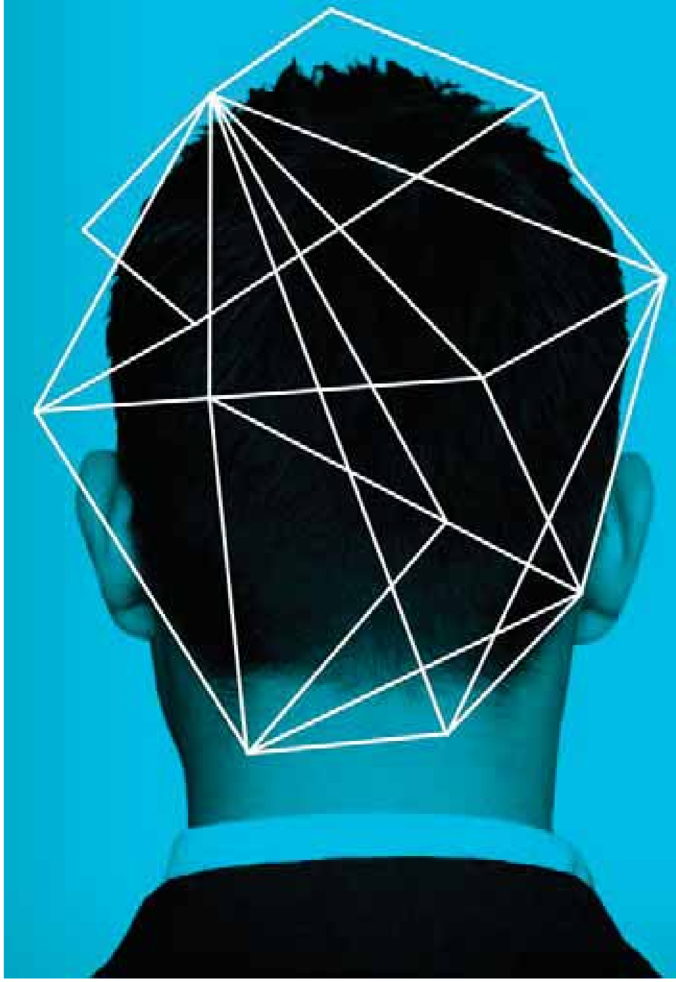
- Bridge the gaps
  - Between technology and business
  - Between the two types of risk
  - Between policies (management's intent) and administration

- "Act as if"
  - CISO as a business leadership role, not a technology support role



Role of the CISO: Influence and Decision Support

- Some situations cry out for change …
- Not everyone will necessarily like it



For More Information

Derek E. Brink, BS, MBA, CISSP
Vice President and Research Fellow,
IT Security and IT GRC
dbrink@mba1991.hbs.edu
www.linkedin.com/in/derekbrink

Research publications:
http://aberdeen.com/_aberdeen/it-security/ITSA/practice.aspx

Blogs:
http://blogs.aberdeen.com/category/it-security/

On-demand webcasts:
https://www.brighttalk.com/channel/290

INFORMATION SECURITY LEADERSHIP DEVELOPMENT
SURVIVING AS A SECURITY LEADER

ARE YOU FIGHTING THE WRONG BATTLES?

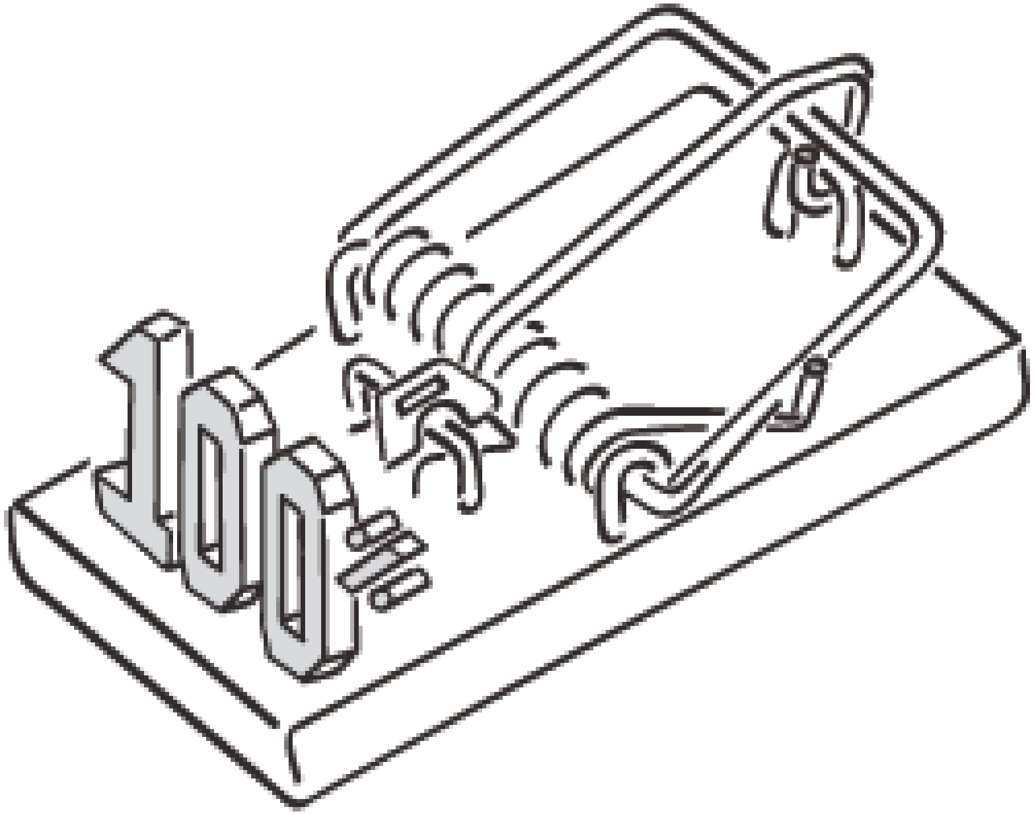
Bob Rudis

Liberty Mutual Insurance

Session ID: SEM-001

Session Classification: Seminars

IT'S A TRAP!!!

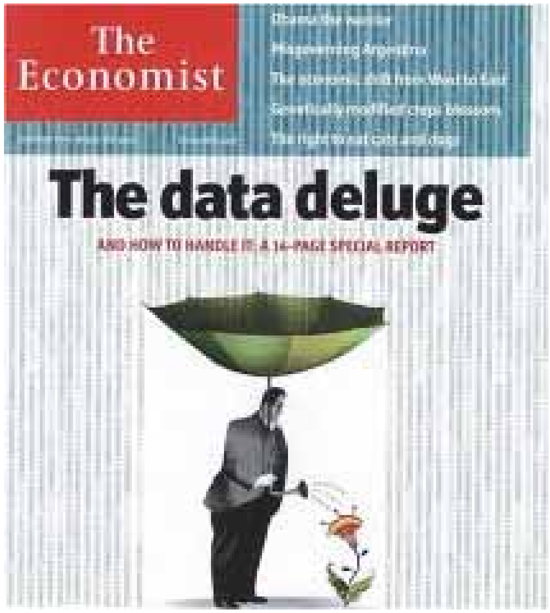


www.nicoledextras.com

[SCAN | PATCH | PEN TEST | LOG | RISK ASSESS | CONFIG CHECK | BLOCK | …]

SECURITY AWARENESS

- Steer clear of CBTs
- Do not use stock photography
- Tailor messages to specific audience
- Integrate training into daily workflow
- Create opportunities for live demos
- Think like Facebook/Twitter/Pinterest
- Use incentives (carrots vs sticks)
- Make messages personal


The Economist
Obama the warrior
Misgoverning Argentina
The economic shift from West to East
Genetically modified crops blossom
The right to eat cats and dogs
The data deluge
AND HOW TO HANDLE IT: A 14-PAGE SPECIAL REPORT

INFORMATION SECURITY POLICY

- Let things go!
- Gone…but not forgotten
- Issues
- Vulnerabilities
- Risks

If in doubt, Peregrin Took, always follow [***your users*** *|*
the business *]!*

pci

HIPAA

Sarbanes - Oxley

WHAT HAVE YOU DONE FOR ME LATELY?

- Empowered your users
- Enabled the business to do more/new
- Addressed emerging risks
- Made systems & processes more resilient
- Decreased application issues
- Deployed foundational security capabilities
- Created security allies in other areas

The
Turn Of A
Friendly Card
K
K
K
K

Security in knowledge

RSACONFERENCE2013

CISO ROUNDTABLE: SECURITY INTELLIGENCE GATHERING FOR LEADERS

MODERATOR:

Evan Wheeler

Omgeo

PANELISTS:

Bob Rudis

Liberty Mutual Insurance

John Iatonna

Edelman

James Burrell

Federal Bureau of Investigation

Derek Brink

Aberdeen Group

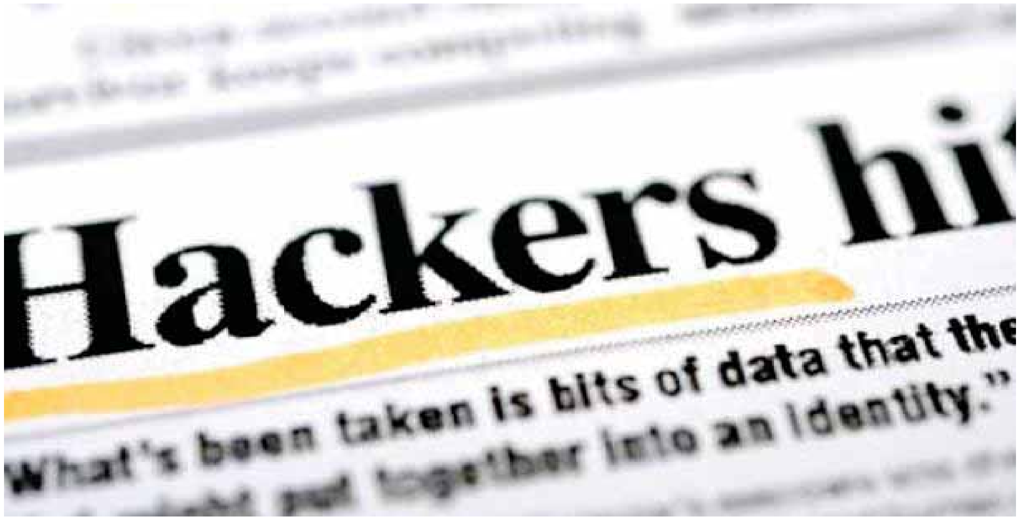
Dave Notch

Intensity Analytics

:

RSACONFERENCE2013

Discussion Topics


Hackers hi
What's been taken is bits of data that the
might put together into an identity."