Surviving as a CISO in a World of Zombie Auditors, Twitter Twits, and Cavity Searches

Eddie Schwartz

RSA, The Security Division of EMC

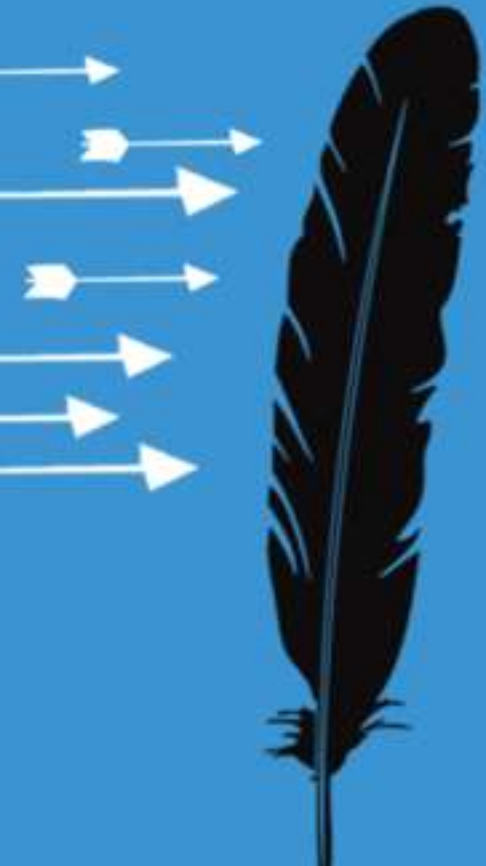
Session ID: GRC-309

Session Classification: Intermediate

RSACONFERENCE EUROPE 2012

Agenda

- The Changing Role of the CISO
  - Oh, the good old days
  - Welcome to the (social) media circus
  - A few words about zombie auditors, twits, and anal probes
- Surviving as a CISO Today
  - Things for your survival list
  - Apply slide
- Discussion



The Changing Role of the CISO

CISO - 1990's Vintage - Personal Experience

- Nationwide Insurance – first CISO
- Many new audit "network" findings
- Policies and standards were thin
- No security SDLC or standard control framework
- Roles and responsibilities unclear
- Compliance ruled (banking dereg, privacy, etc.)
- Adversary space – fraudulent employees and agents, "hackers" (who?), "viruses"

Surviving as a CISO in the 1990's

- Kill off the most egregious audit findings to make the audit committee happy and keep my job
- Get CEO buy-in and focus on root cause
- Implement BS7799 (sort of), SSE-CMM-style SDLC and QM approaches
- CIRT, more firewalls, AV, and IDS
- Figure out Windows security and compliance
- Basic collaboration via FS-ISAC
- eSecurityOnline.com
- Life was GOOD!!! ☺

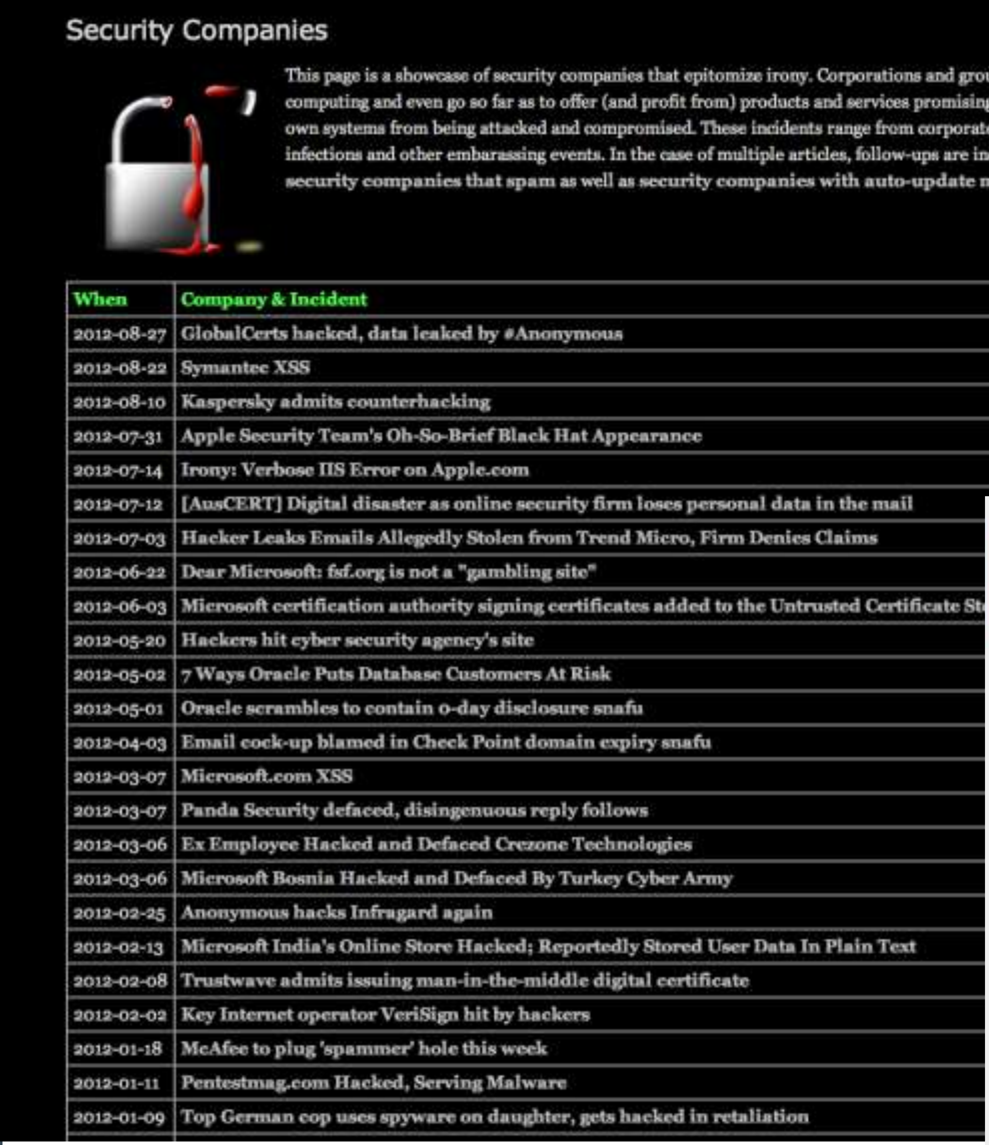
Fast Forward 10 or 15 Years – What Has Changed?

CISOs - 2012 Vintage - In the eyes of pundits, the media, and certain morons

NOT BREACHED!!

BREACHED!!

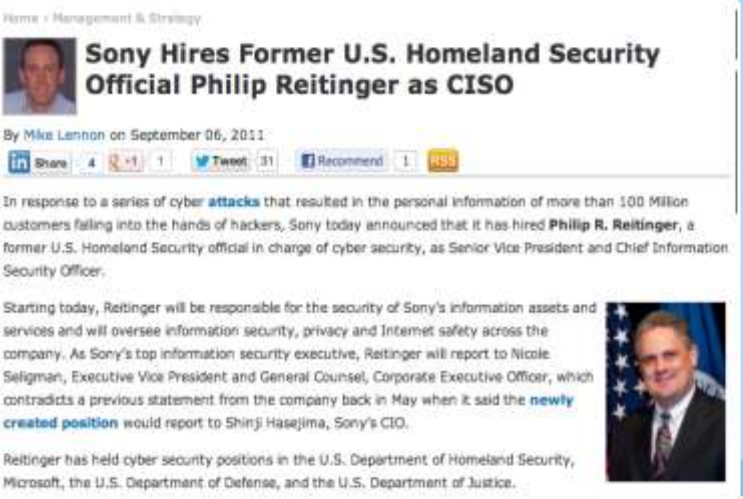
Is breach the right metric? It depends…



Security Companies

This page is a showcase of security companies that epitomize irony. Corporations and groups that espouse the ide computing and even go so far as to offer (and profit from) products and services promising such security, while un own systems from being attacked and compromised. These incidents range from corporate web defacements to vi infections and other embarassing events. In the case of multiple articles, follow-ups are included below. We also m security companies that spam as well as security companies with auto-update mechanism problems.

When	Company & Incident
2012-08-27	GlobalCerts hacked, data leaked by #Anonymous
2012-08-22	Symantec XSS
2012-08-10	Kaspersky admits counterhacking
2012-07-31	Apple Security Team's Oh-So-Brief Black Hat Appearance
2012-07-14	Irony: Verbose IIS Error on Apple.com
2012-07-12	[AusCERT] Digital disaster as online security firm loses personal data in the mail
2012-07-03	Hacker Leaks Emails Allegedly Stolen from Trend Micro, Firm Denies Claims
2012-06-22	Dear Microsoft: fsf.org is not a "gambling site"
2012-06-03	Microsoft certification authority signing certificates added to the Untrusted Certificate St
2012-05-20	Hackers hit cyber security agency's site
2012-05-02	7 Ways Oracle Puts Database Customers At Risk
2012-05-01	Oracle scrambles to contain 0-day disclosure snafu
2012-04-03	Email cock-up blamed in Check Point domain expiry snafu
2012-03-07	Microsoft.com XSS
2012-03-07	Panda Security defaced, disingenuous reply follows
2012-03-06	Ex Employee Hacked and Defaced Crezone Technologies
2012-03-06	Microsoft Bosnia Hacked and Defaced By Turkey Cyber Army
2012-02-25	Anonymous hacks Infragard again
2012-02-13	Microsoft India's Online Store Hacked; Reportedly Stored User Data In Plain Text
2012-02-08	Trustwave admits issuing man-in-the-middle digital certificate
2012-02-02	Key Internet operator VeriSign hit by hackers
2012-01-18	McAfee to plug 'spammer' hole this week
2012-01-11	Pentestmag.com Hacked, Serving Malware
2012-01-09	Top German cop uses spyware on daughter, gets hacked in retaliation



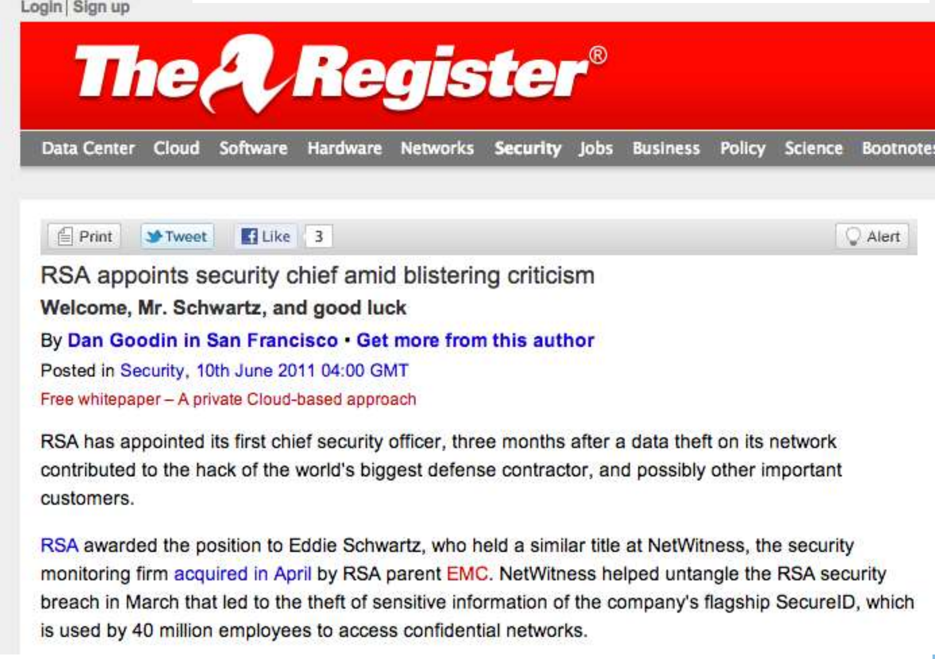
Sony Hires Former U.S. Homeland Security Official Philip Reitinger as CISO

By Mike Lennon on September 06, 2011

In response to a series of cyber **attacks** that resulted in the personal information of more than 100 Million customers falling into the hands of hackers, Sony today announced that it has hired **Philip R. Reitinger**, a former U.S. Homeland Security official in charge of cyber security, as Senior Vice President and Chief Information Security Officer.

Starting today, Reitinger will be responsible for the security of Sony's information assets and services and will oversee information security, privacy and Internet safety across the company. As Sony's top information security executive, Reitinger will report to Nicole Seligman, Executive Vice President and General Counsel, Corporate Executive Officer, which contradicts a previous statement from the company back in May when it said the **newly created position** would report to Shinji Hasejima, Sony's CIO.

Reitinger has held cyber security positions in the U.S. Department of Homeland Security, Microsoft, the U.S. Department of Defense, and the U.S. Department of Justice.



RSA appoints security chief amid blistering criticism

Welcome, Mr. Schwartz, and good luck

By Dan Goodin in San Francisco • Get more from this author

Posted in Security, 10th June 2011 04:00 GMT

Free whitepaper – A private Cloud-based approach

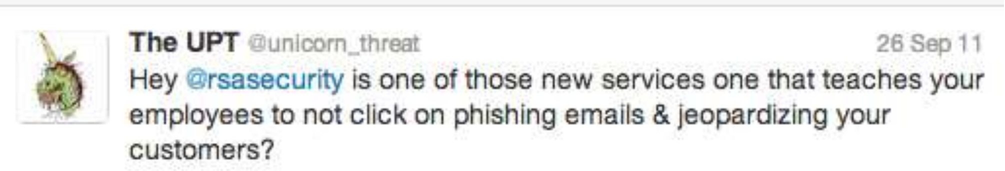
RSA has appointed its first chief security officer, three months after a data theft on its network contributed to the hack of the world's biggest defense contractor, and possibly other important customers.

RSA awarded the position to Eddie Schwartz, who held a similar title at NetWitness, the security monitoring firm acquired in April by RSA parent EMC. NetWitness helped untangle the RSA security breach in March that led to the theft of sensitive information of the company's flagship SecureID, which is used by 40 million employees to access confidential networks.

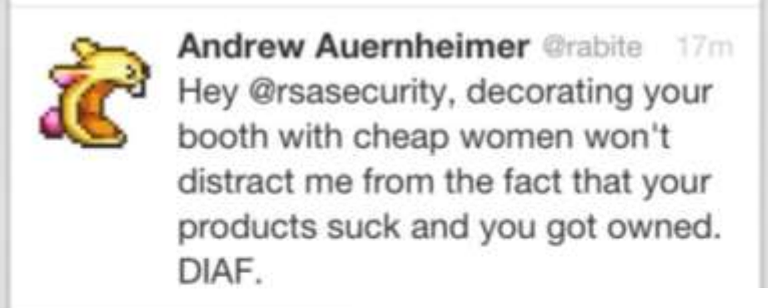
Welcome to the Club – You Don't Want to be a Member…

No End to the Critics

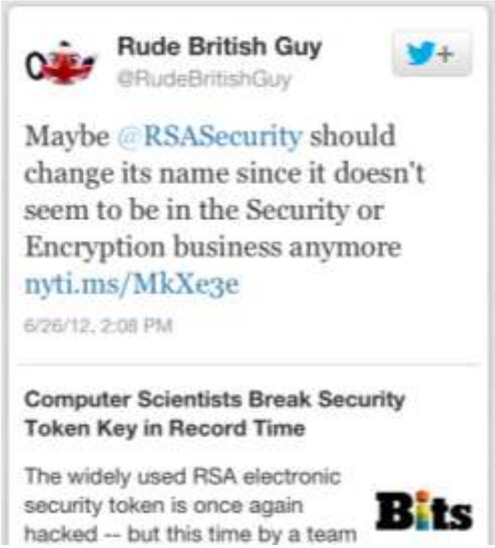
HEY! @rsasecurity you just can't handle all the reality up in here! Boom goes the dynamite! we're on a podcast!


The UPT @unicorn_threat 26 Sep 11

Hey @rsasecurity is one of those new services one that teaches your employees to not click on phishing emails & jeopardizing your customers?


Andrew Auernheimer @rabite 17m

Hey @rsasecurity, decorating your booth with cheap women won't distract me from the fact that your products suck and you got owned. DIAF.

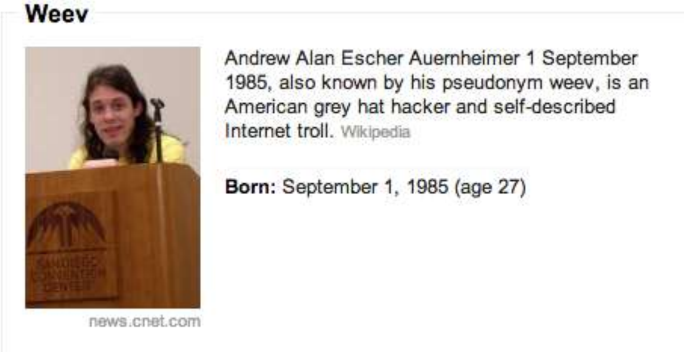

Rude British Guy @RudeBritishGuy

Maybe @RSASecurity should change its name since it doesn't seem to be in the Security or Encryption business anymore nyti.ms/MkXe3e

6/26/12, 2:08 PM

Computer Scientists Break Security Token Key in Record Time

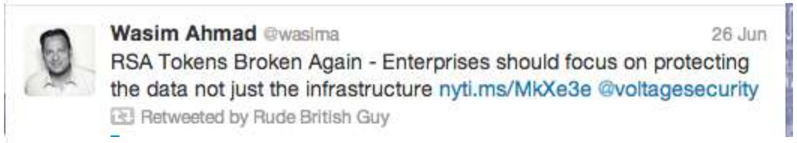
The widely used RSA electronic security token is once again hacked -- but this time by a team


Weev

Andrew Alan Escher Auernheimer 1 September 1985, also known by his pseudonym weev, is an American grey hat hacker and self-described Internet troll. Wikipedia

Born: September 1, 1985 (age 27)

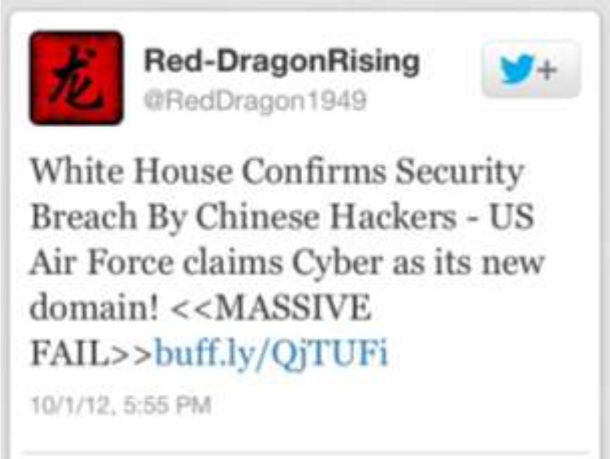
news.cnet.com


Wasim Ahmad @wasima 26 Jun

RSA Tokens Broken Again - Enterprises should focus on protecting the data not just the infrastructure nyti.ms/MkXe3e @voltagesecurity

Retweeted by Rude British Guy

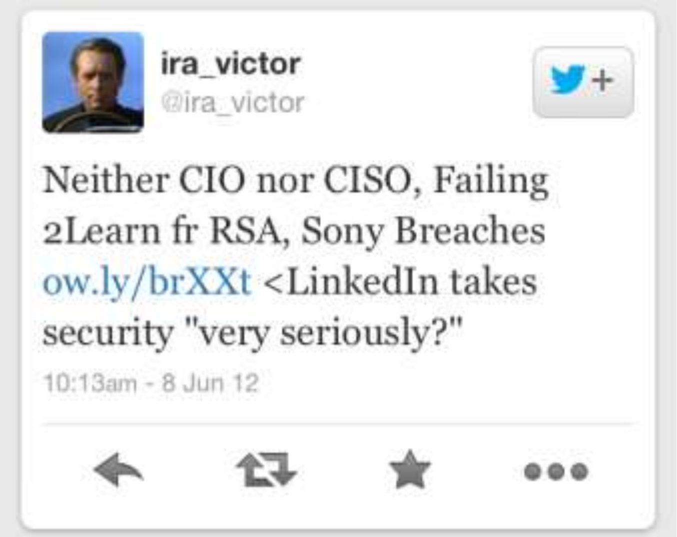
Oh, you think it's just RSA?



Red-DragonRising
@RedDragon1949

White House Confirms Security Breach By Chinese Hackers - US Air Force claims Cyber as its new domain! <<MASSIVE FAIL>>buff.ly/QjTUFi

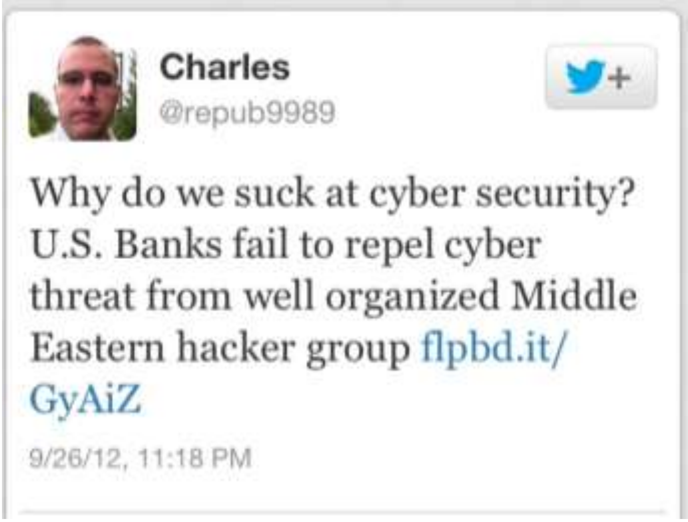
10/1/12, 5:55 PM



ira_victor
@ira_victor

Neither CIO nor CISO, Failing 2Learn fr RSA, Sony Breaches ow.ly/brXXt <LinkedIn takes security "very seriously?"

10:13am - 8 Jun 12

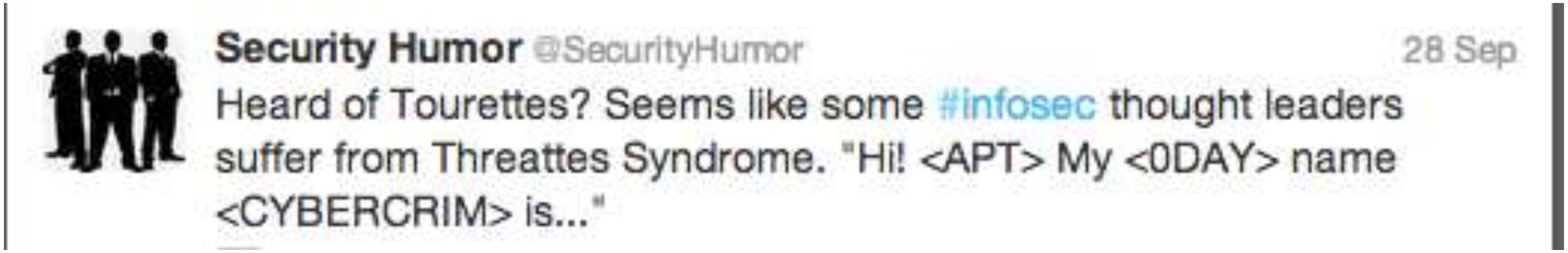


Charles
@repub9989

Why do we suck at cyber security? U.S. Banks fail to repel cyber threat from well organized Middle Eastern hacker group flpbd.it/GyAiZ

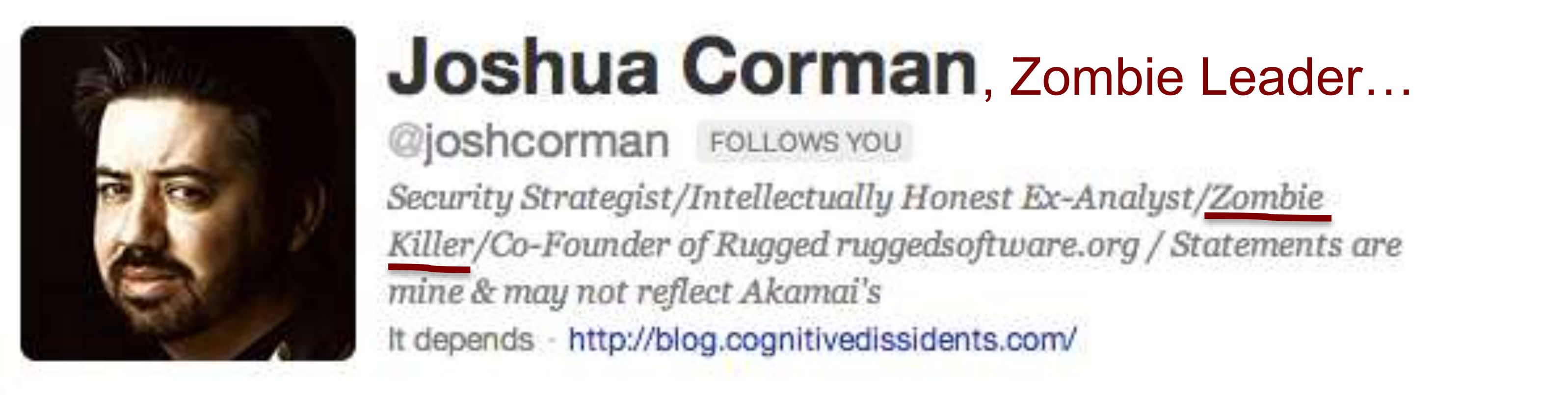
9/26/12, 11:18 PM

There is the occasional tweet that makes sense…



Security Humor @SecurityHumor 28 Sep

Heard of Tourettes? Seems like some #infosec thought leaders suffer from Threattes Syndrome. "Hi! <APT> My <0DAY> name <CYBERCRIM> is..."



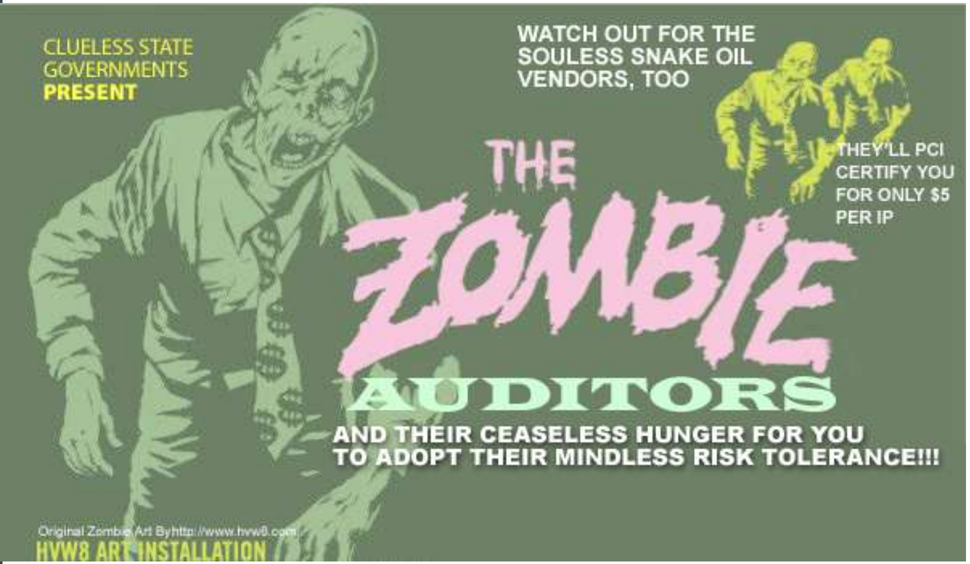
Joshua Corman, Zombie Leader…

@joshcorman FOLLOWS YOU

Security Strategist/Intellectually Honest Ex-Analyst/Zombie Killer/Co-Founder of Rugged ruggedsoftware.org / Statements are mine & may not reflect Akamai's

It depends · http://blog.cognitivedissidents.com/

Zombies vs. Auditors? Mmm…


CLUELESS STATE GOVERNMENTS PRESENT
WATCH OUT FOR THE SOULESS SNAKE OIL VENDORS, TOO
THEY'LL PCI CERTIFY YOU FOR ONLY $5 PER IP
THE ZOMBIE AUDITORS
AND THEIR CEASELESS HUNGER FOR YOU TO ADOPT THEIR MINDLESS RISK TOLERANCE!!!
Original Zombie Art By http://www.hvw8.com
HVW8 ART INSTALLATION

Zombies	Auditors
Tireless, flesh-eating creatures that attack unexpectedly	Work long hours, relentless, disruptive requests for useless information, short time frames
Easily distracted	Easily distracted
Seemingly endless armies with no end in sight	A new team for every policy, regulation, framework and customer
Keep you from living a normal, safe life	Keep you from focusing on business risk

ANAL PROBE

YOU'RE GONNA GET ONE.

Who Is Doing the Probing (and Worse)?

NATION STATE ACTORS

Nation states

Government, defense industrial base, IP rich organizations, waterholes

CRIMINALS

Petty criminals

Unsophisticated, but noisy

Organized crime

Organized, sophisticated supply chains (PII, PCI, financial services, retail)

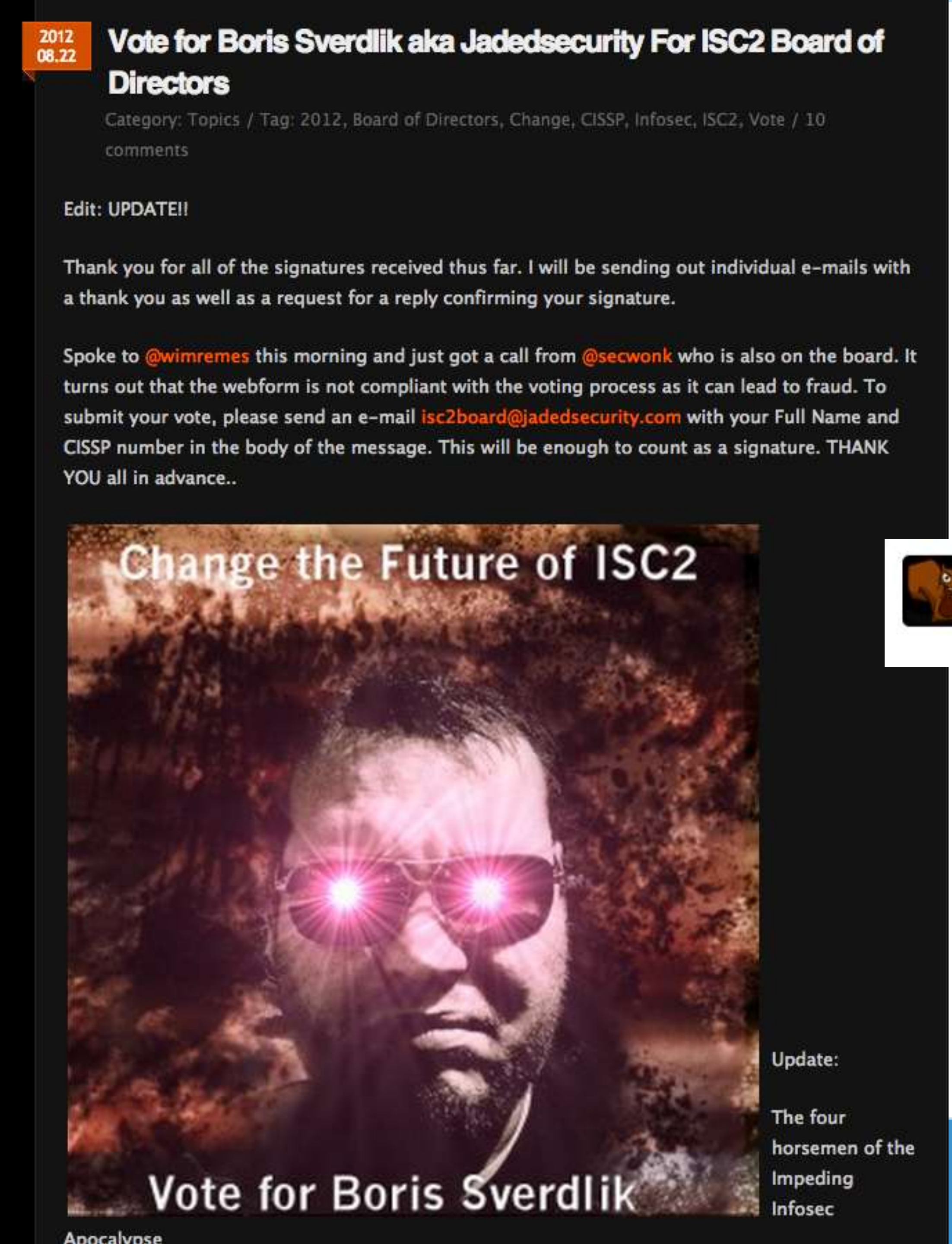
NON-STATE ACTORS

Insiders

Various reasons, including collaboration with the enemy

Cyber-terrorists / Hacktivists

Political targets of opportunity, mass disruption, mercenary



2012
08.22

Vote for Boris Sverdlik aka Jadedsecurity For ISC2 Board of Directors

Category: Topics / Tag: 2012, Board of Directors, Change, CISSP, Infosec, ISC2, Vote / 10 comments

Edit: UPDATE!!

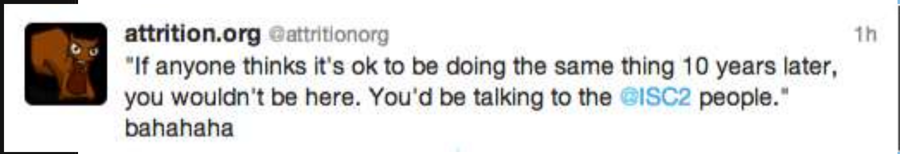
Thank you for all of the signatures received thus far. I will be sending out individual e-mails with a thank you as well as a request for a reply confirming your signature.

Spoke to @wimremes this morning and just got a call from @secwonk who is also on the board. It turns out that the webform is not compliant with the voting process as it can lead to fraud. To submit your vote, please send an e-mail isc2board@jadedsecurity.com with your Full Name and CISSP number in the body of the message. This will be enough to count as a signature. THANK YOU all in advance..

Update:

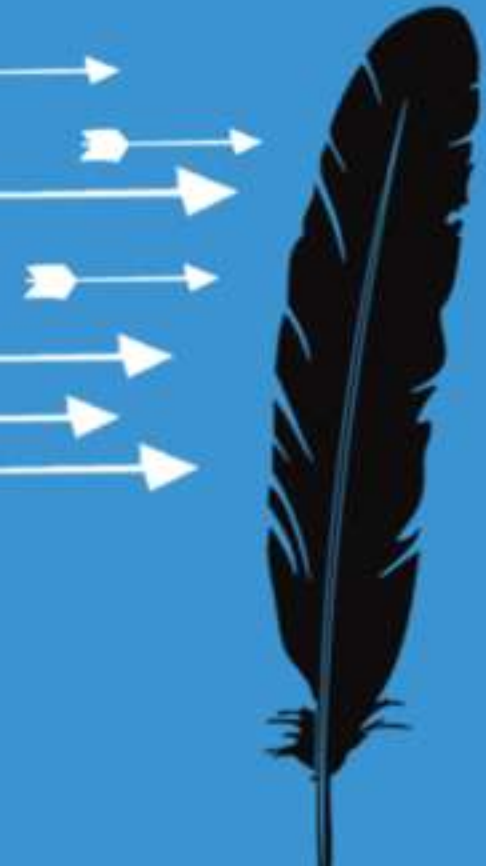
The four horsemen of the Impeding Infosec Apocalypse

Yes, everyone gets criticized, although some actually deserve the twits and the probing..



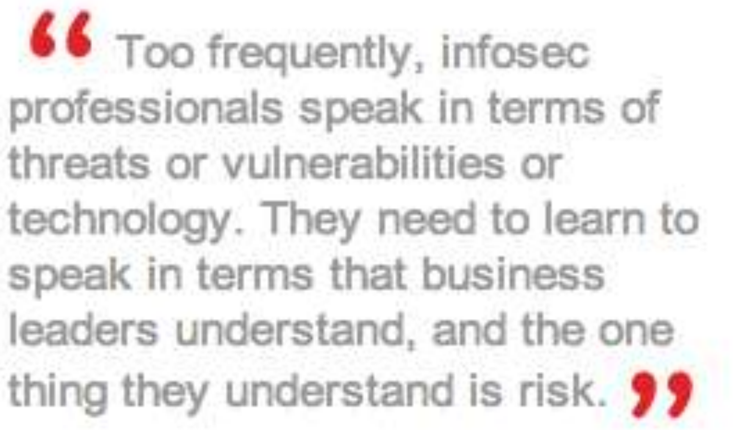
attrition.org @attritionorg 1h

"If anyone thinks it's ok to be doing the same thing 10 years later, you wouldn't be here. You'd be talking to the @ISC2 people." bahahaha



Surviving As a CISO Today

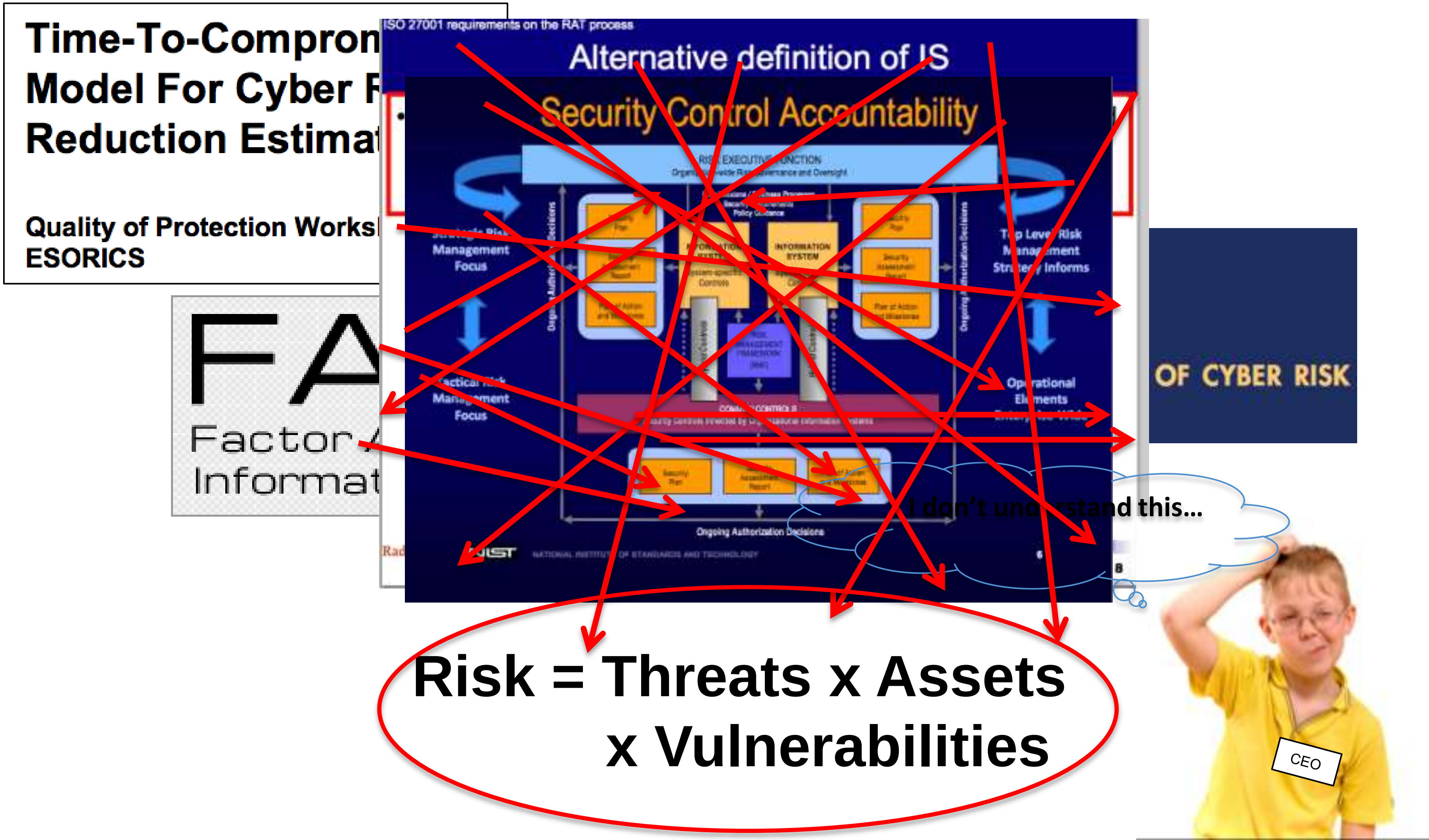
Attention CISOs! You Don’t Speak the “Language of Business”



“Too frequently, infosec professionals speak in terms of threats or vulnerabilities or technology. They need to learn to speak in terms that business leaders understand, and the one thing they understand is risk.”

- How many times have we heard this comment?
- What exactly is this mystery language?
  - Debits / Credits
  - Annual Loss Expectancy
  - ROI
  - Shareholder Value
- I know you all speak it and I don’t
- Many have gone down trying…

Greatest Hits - Not Wrong, Just Not Heard



Time-To-Compron
Model For Cyber F
Reduction Estimat
Quality of Protection Works
ESORICS
FA
Factor A
Informat
ISO 27001 requirements on the RAT process
Alternative definition of IS
Security Control Accountability
RISK EXECUTIVE FUNCTION
Organization-wide Risk Governance and Oversight
Strategic Risk Management Focus
Tactical Risk Management Focus
Top Level Risk Management Strategy Informs
Operational Elements
INFORMATION SYSTEM
COMMON CONTROLS
Ongoing Authorization Decisions
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
OF CYBER RISK
I don't understand this...
CEO

Risk = Threats x Assets x Vulnerabilities

Spending is Part of the Problem - Determine the right arithmetic here…

Enterprise Security Investment Profile:

Known threats and security hygiene ______

Advanced threats and analytics ______

Physical security and supply chain ______

Other stuff you should be doing ______

Total Budget %: 100%

Spending is Part of the Problem -- Determine the right arithmetic here…

Enterprise Security Investment Profile:	TODAY
Known threats and security hygiene	70%
Advanced threats and analytics	15%
Physical security and supply chain	5%
Other stuff you should be doing	10%
Total Budget %:	100%

Spending is Part of the Problem -- Determine the right arithmetic here…

Enterprise Security Investment Profile:	BETTER
Known threats and security hygiene	40%
Advanced threats and analytics	35%
Physical security and supply chain	12.5%
Other stuff you should be doing	12.5%
Total Budget %:	100%

Key Factors: 1. Process maturity and repeatability, secure development, lower costs; 2. Increased skills and technology; 3. Program focus, pervasive; 4. Aggressive vs. passive.

Risk = Threats x Assets x Vulnerabilities

BAD?

Risk =
- Material Assets You Really Can Protect
- Related to Your Real Attack Surface
- And the Adversaries that Want Those Assets

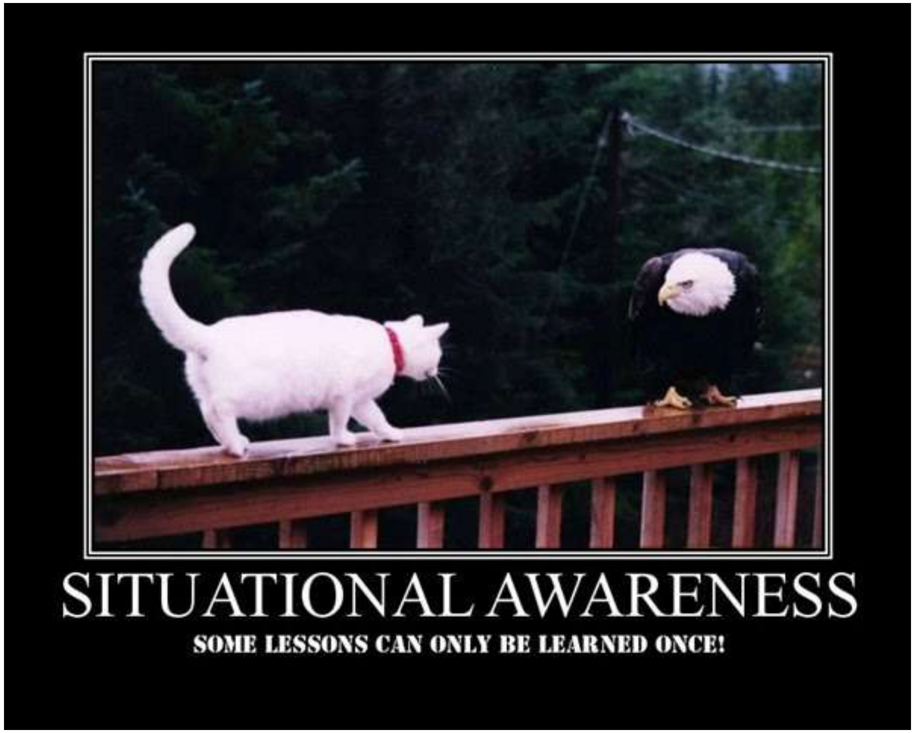
So, We Need to Rethink What We Are Doing

- Most of us are being targeted – many do not know it or will not believe it. Many will find out the hard way. Breaches are inevitable.
- We cannot protect all information and services equally -- nor do all information and services require / deserve equal protection.
- Current result -- organizations misallocate more than $1B in security-related spending each year.
- We have to rethink how we spend our security money and how we organize our security programs. Losses and defeat are not inevitable.

Source: Gartner, IT Expo 2011

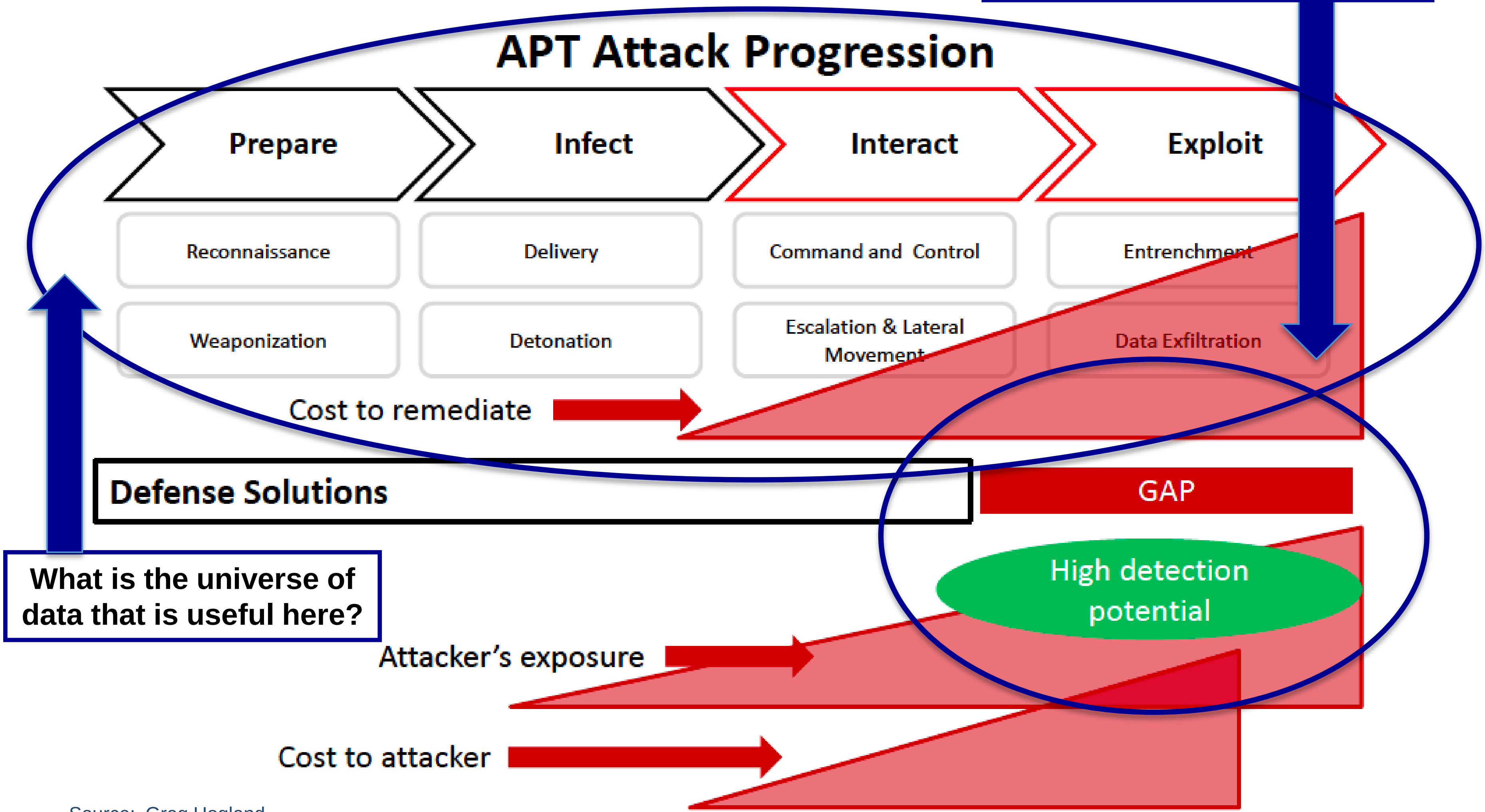
Top areas of focus

- Understanding adversarial attack phases
- Rethinking security infrastructure
- Big data and intelligence-driven security operations
- Segmentation and isolation
- Hire new people and create new processes
- SDLC, 3rd party assurance / supply chain security
- Don’t be a twit



Understand Adversarial Phases

What level of resources belongs RIGHT HERE??



APT Attack Progression

Prepare

Infect

Interact

Exploit

Reconnaissance

Weaponization

Delivery

Detonation

Command and Control

Escalation & Lateral Movement

Entrenchment

Data Exfiltration

Cost to remediate

Defense Solutions

GAP

High detection potential

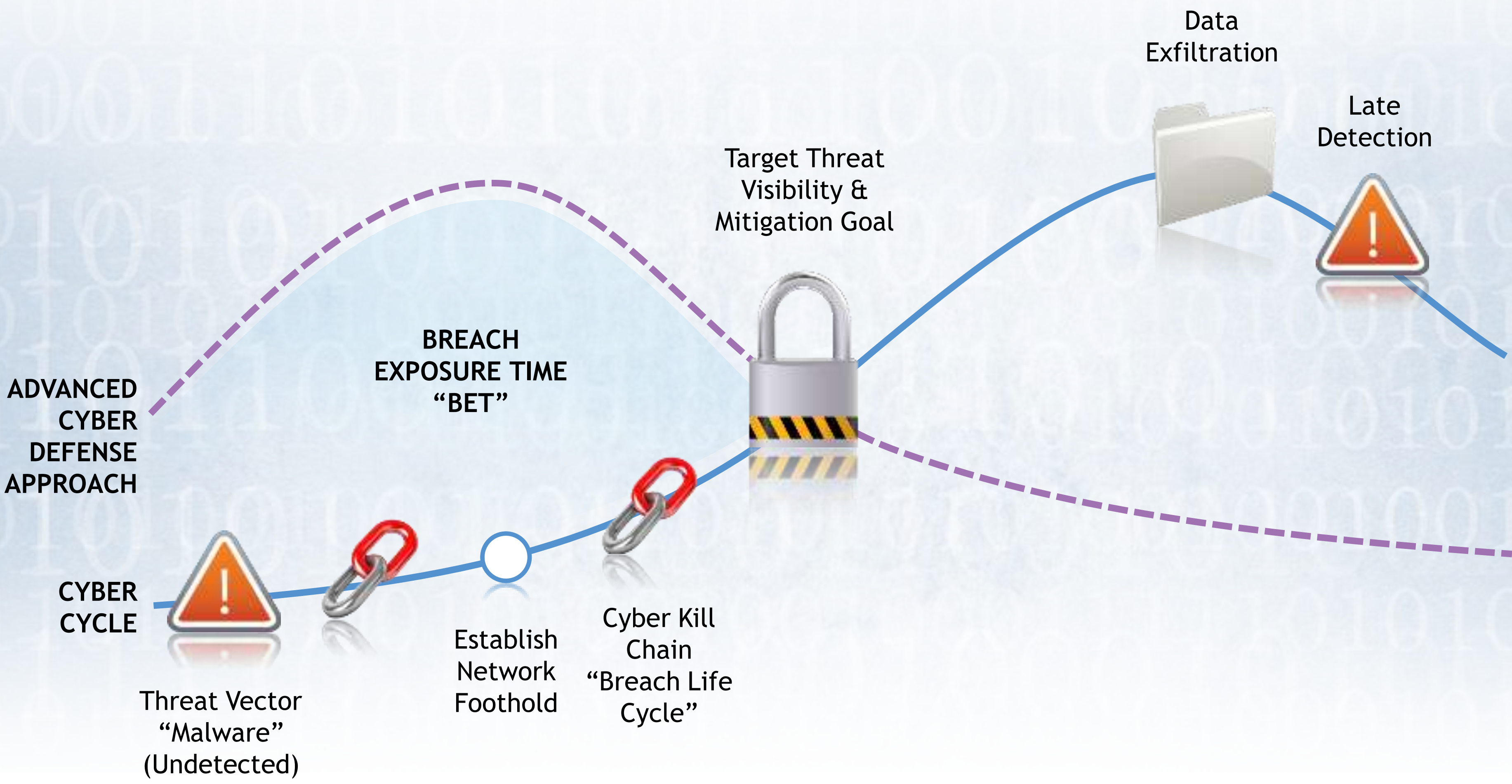
Attacker's exposure

Cost to attacker

What is the universe of data that is useful here?

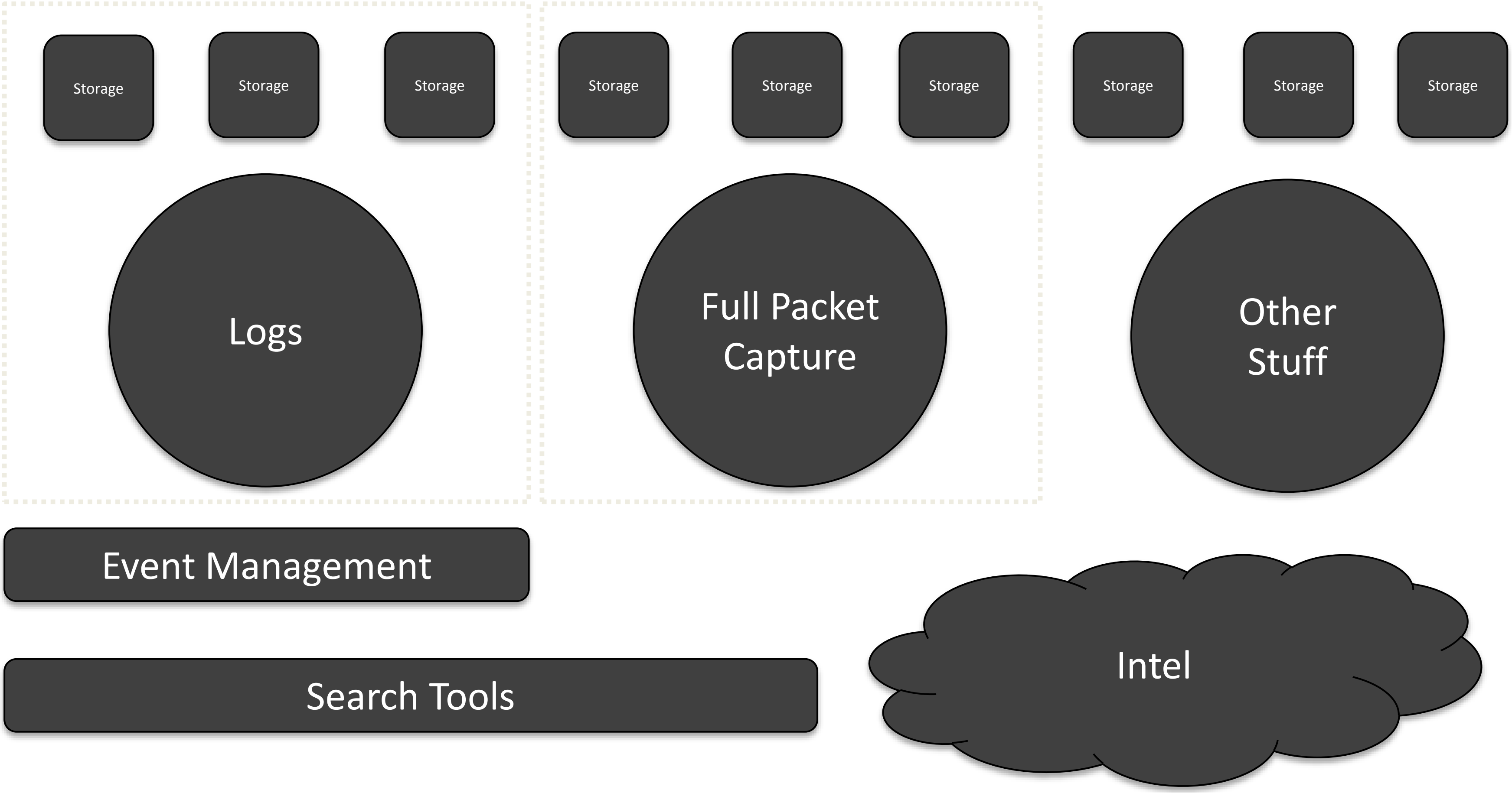
Source: Greg Hogland

Attack Kill Chain Life Cycle

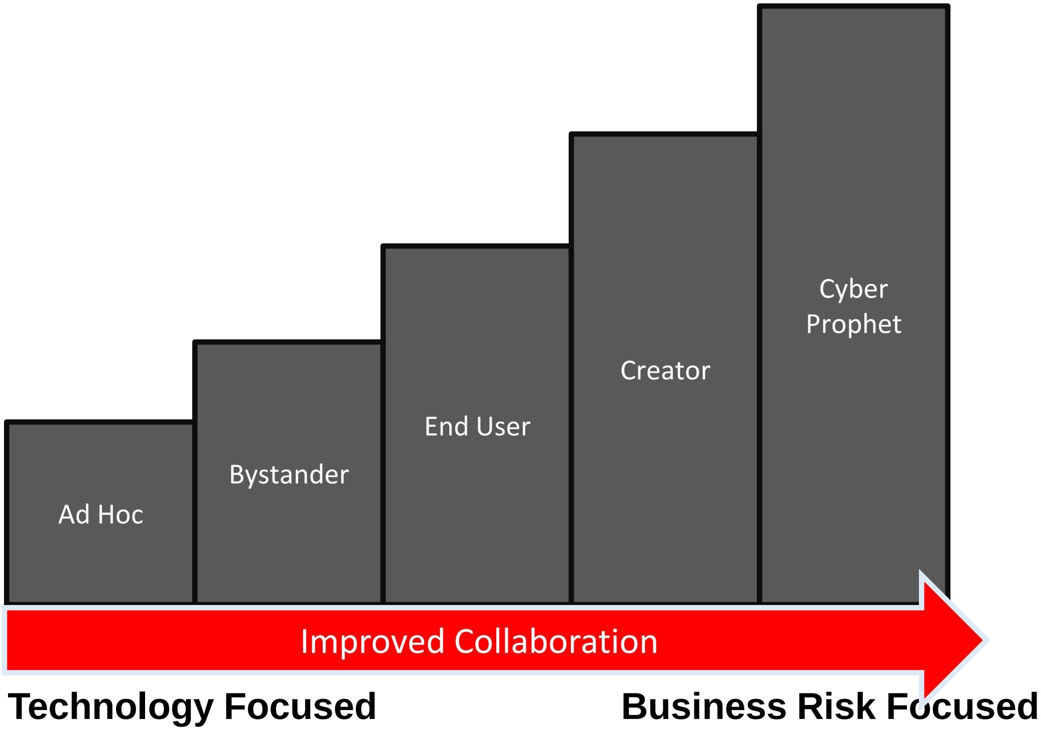


Data Exfiltration
Late Detection
Target Threat Visibility & Mitigation Goal
BREACH EXPOSURE TIME "BET"
ADVANCED CYBER DEFENSE APPROACH
CYBER CYCLE
Establish Network Foothold
Cyber Kill Chain "Breach Life Cycle"
Threat Vector "Malware" (Undetected)

Rethink Infrastructure - Disjoint Sets Are Messy and Do Not Help with TCO



Stop Living on an Island - Be Social!



Ad Hoc

Bystander

End User

Creator

Cyber Prophet

Improved Collaboration

Technology Focused

Business Risk Focused

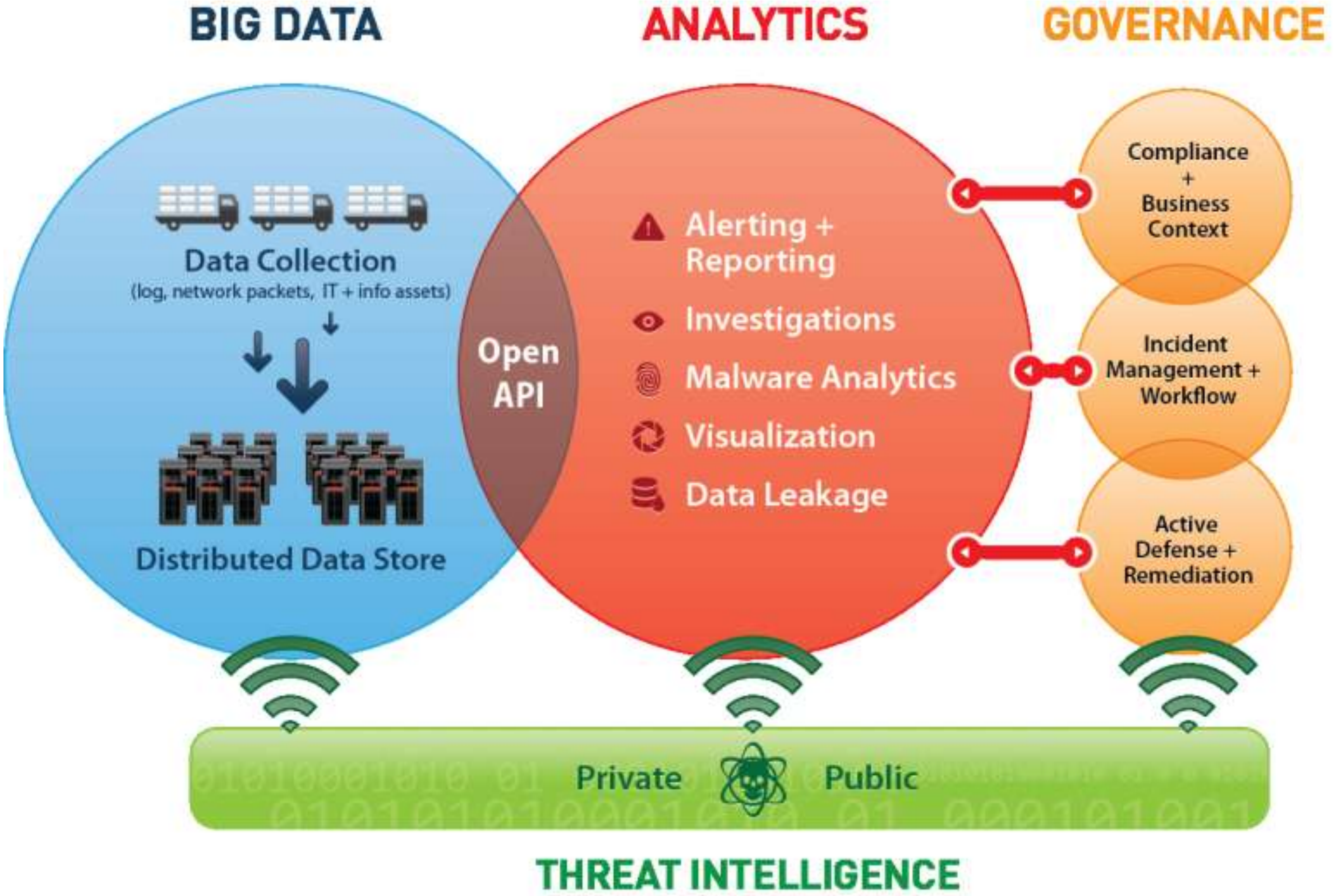
Big data / intelligence driven security operations

- Goals: Use big data to drive maximum situational awareness across various security use cases
- Requirements: I want it all – all the data that has security relevance to securing material assets – internal and external
- Reality: This approach entails a multi-year strategy associated with storage, data management, analytics, skill development, relationship building, etc.

Thinking in a big data context - we must be strategic

- Plan for True Scalability
  - Plan for large data volumes
  - Plan for higher data speeds
  - Plan for hyperextension and connectivity
- Plan for Agility
  - Openness is critical
  - Short term and long term objectives
  - Adapt to tomorrow’s adversary challenges
- Look for Automation and Risk-based
  - Pre-mining and clustered processing
  - Dynamic data feeds (ties to agility of data structures too)
  - Reporting and alerting
- External collaboration is CRITICAL – how do you get your hands on the right intel – what do you share?

Big Data + Good Intelligence = Situational Awareness



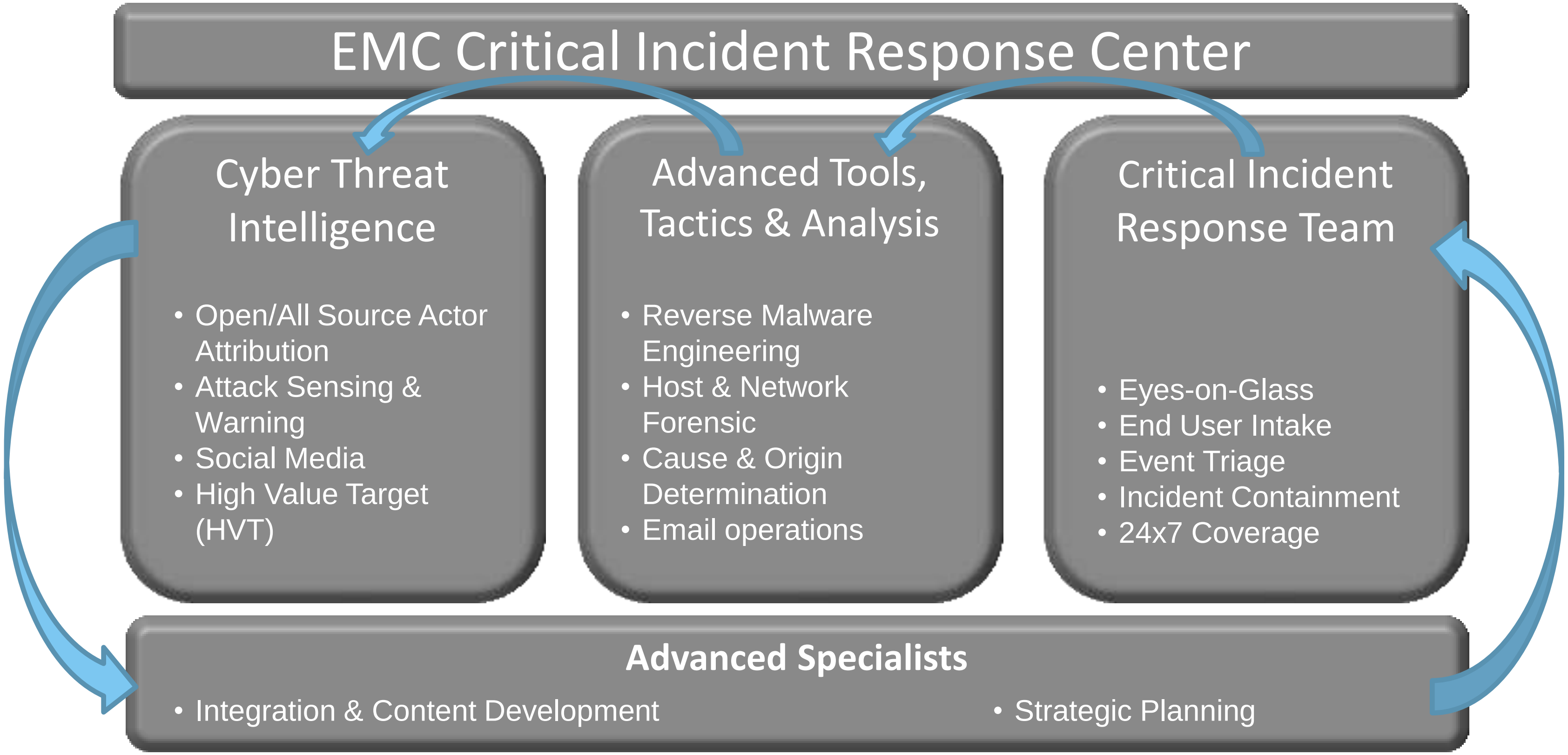
Segmentation and Isolation

- What does this have to do with being social? Nothing!
- It has to do with control. Well, I can’t get visibility without better control in some cases, and I can’t change the network fast enough – it’s too big and too messy
- Goal: But, we can transform high value and high risk processes and assets to create better segmentation and isolation – even if they are legacy environments…
- Requirements: Decide what really matters and what does not. Also, get everyone to be honest about what is polluting your network (e.g., unfettered access to the Internet)

Segmentation Current State

- Aggressive use of virtualization:
  - vdi for common business unit builds (sales, marketing, executives, engineering)
  - No “rich” featureset for certain vdi’s (no cut and paste for developers)
  - vdi builds for new acquisitions
  - Virtual environments for throw away Internet use
- Virtual environments and possible use of HSM and two man rule for high value/risk areas like code-signing and admin functions
- Hard network segmentation for manufacturing processes
- Monitor, monitor, monitor

Rethinking the SOC and Assembling Right Team Is Critical



EMC Critical Incident Response Center

Cyber Threat Intelligence

- Open/All Source Actor Attribution
- Attack Sensing & Warning
- Social Media
- High Value Target (HVT)

Advanced Tools, Tactics & Analysis

- Reverse Malware Engineering
- Host & Network Forensic
- Cause & Origin Determination
- Email operations

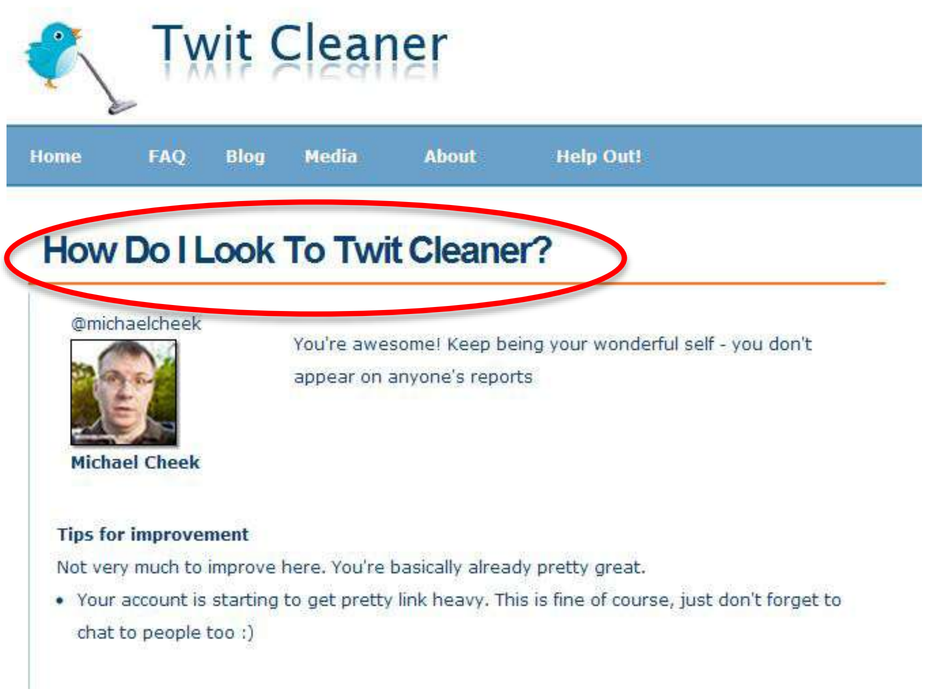
Critical Incident Response Team

- Eyes-on-Glass
- End User Intake
- Event Triage
- Incident Containment
- 24x7 Coverage

Advanced Specialists

- Integration & Content Development
- Strategic Planning

Stop Being Such a Twit!



How Do I Look To Twit Cleaner?

@michaelcheek

Michael Cheek

You're awesome! Keep being your wonderful self - you don't appear on anyone's reports

Tips for improvement

Not very much to improve here. You're basically already pretty great.

- Your account is starting to get pretty link heavy. This is fine of course, just don't forget to chat to people too :)

- Don’t you wish more security people asked themselves this question?
- Especially security people who actually don’t have real jobs like certain bloggers, pundits, self-appointed analysts, etc.
- Don’t be a twit – before you tweet think about what we are all trying to achieve

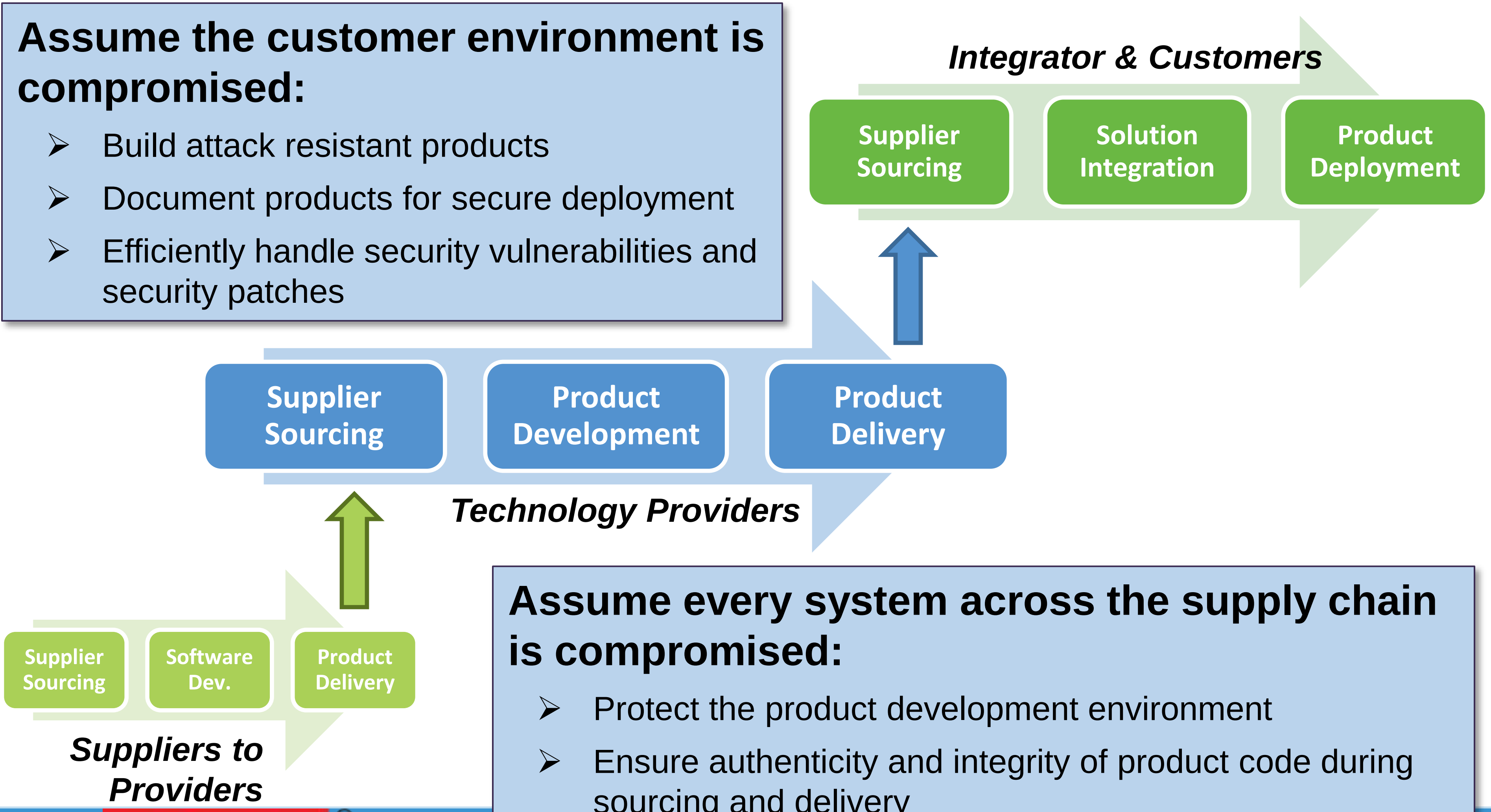
SDLC

- Goal: Achieve end-to-end assurance and visibility into the risks of software, systems, and networks
- Problems:
  - Disparate security groups (8) and processes (product security office focused on software assurance, global security office focused on corporate / shared security)
  - BU / Division-level security issues create gaps (e.g., I/T assets, manufacturing, BU-specific apps and processes

Rethinking Software Security …
… in the Context of the Supply Chain

Assume the customer environment is compromised:

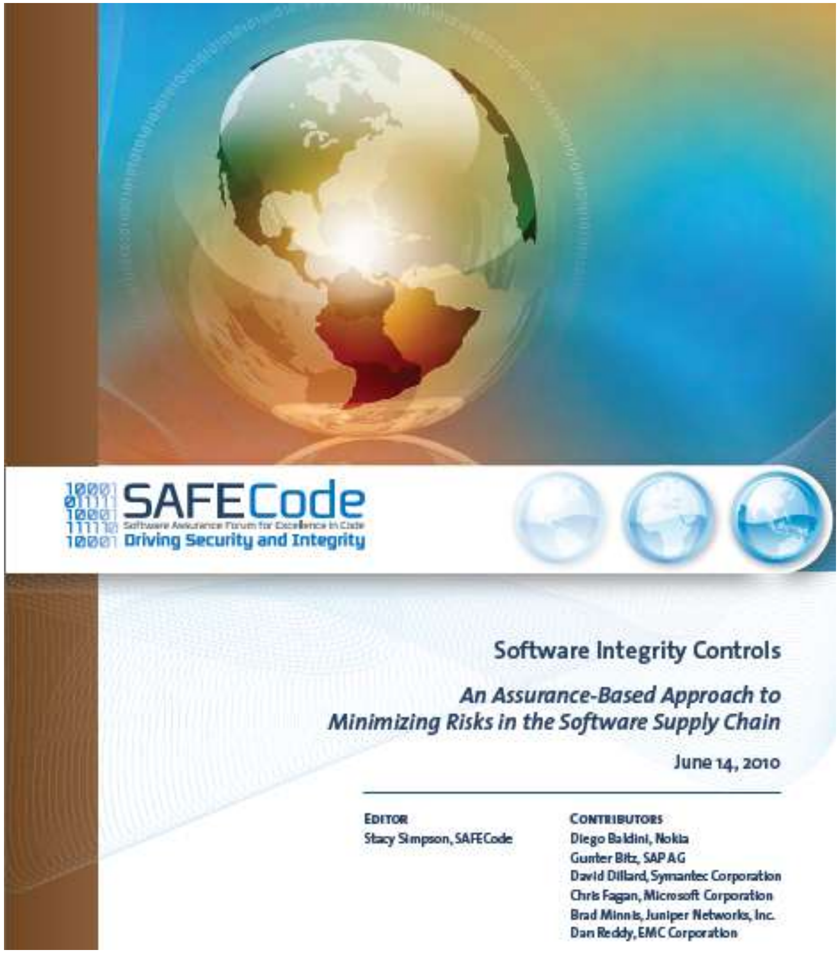
- Build attack resistant products
- Document products for secure deployment
- Efficiently handle security vulnerabilities and security patches



Assume every system across the supply chain is compromised:

- Protect the product development environment
- Ensure authenticity and integrity of product code during sourcing and delivery
- Build attack-aware products

SAFECode, a Global, Industry-led Effort to Promote Broad Adoption of Product Assurance Practices



SAFECode

Software Assurance Forum for Excellence in Code

Driving Security and Integrity

Software Integrity Controls

An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain

June 14, 2010

EDITOR

Stacy Simpson, SAFECode

CONTRIBUTORS

Diego Baldini, Nokia

Gunter Bitz, SAP AG

David Dillard, Symantec Corporation

Chris Fagan, Microsoft Corporation

Brad Minnis, Juniper Networks, Inc.

Dan Reddy, EMC Corporation

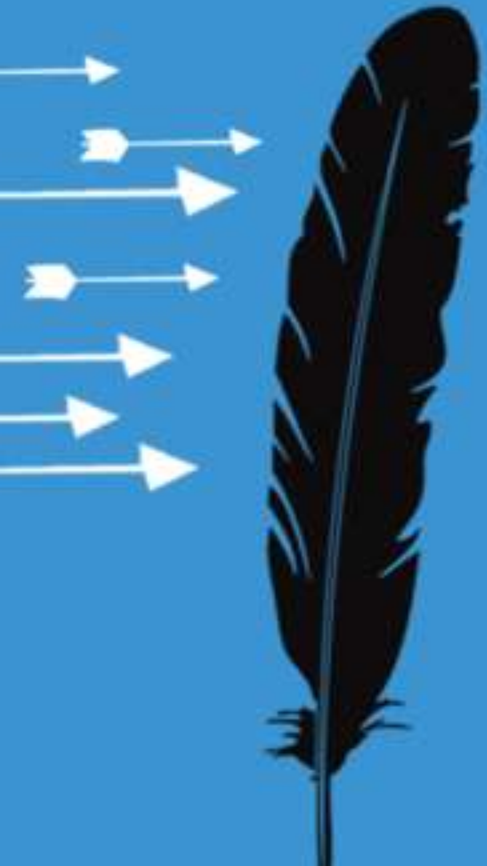
- Increase understanding of the secure development methods and integrity controls used by vendors
- Promote proven software assurance practices among vendors and customers to foster a more trusted ecosystem
- Catalyze action on key research and development initiatives in the area of software assurance

http://www.SAFECode.org

SIEMENS Juniper NETWORKS Adobe SAP Microsoft symantec. NOKIA EMC²

Apply Slide

- Timeframe: Now to 3 Months
  - Create a threat model mapping adversaries, to assets, to both strengths and weaknesses in terms of visibility and control
  - Conduct a threat assessment for all high value assets using this new threat model
  - Identify gaps
- Timeframe: 3 Months to 1 Year
  - Develop a multi-year roadmap for transforming the following areas: skills, incident management, security process maturity, security architecture and infrastructure
  - Link roadmap to funding and program metrics



THANK YOU

Eddie Schwartz
eddie.schwartz@rsa.com
@eddieschwartz
http://www.linkedin.com/in/eddieschwartz