INTERESTING TIMES

Will Business Survive?

Ben Tomhave, MS, CISSP

DISCLAIMER

The views expressed during this talk are not representative of any employers, whether past, ~~present~~, or future.

LUTHER COLLEGE

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

ISSA
Information Systems Security Association

(CISSP)®

SIRA
Society of Information Risk Analysts

NRA RANGE SAFETY OFFICER

NRA CERTIFIED INSTRUCTOR

ABA AMERICAN BAR ASSOCIATION
SciTech Information Security Committee

HYPOTHESES

1. A traditional approach is insufficient and not commercially reasonable

2. A tech-heavy approach is not commercially reasonable

3. A legally defensible position requires changing the game

HISTORICAL PERSPECTIVE

"Those who cannot remember the past are condemned to repeat it."
(George Santayana)

HISTORICAL PERSPECTIVE

The Good…

1969 – First packet transmitted
1979 – Online transaction processing invented
1981 – First online home banking services (US)
… (lots of standards dev work) …
1990 – First Successful HTTP communication
1994 – First pizza ordered online
1994 – Amazon founded
1996 – NIST FIPS 161-2 EDI released; HTTP v1.0
1997 – First mobile commerce (SMS Coke)
1998 – PayPal launches, Google incorporated
2007 – iPhone released
2010 – Square releases first card reader product

HISTORICAL PERSPECTIVE

The Bad…

1962 – Malware invented
…
1981 – First widespread virus (Elk Cloner)
… (lots of activity over this period) …
1996 – CERT SYN Flood advisory
1998 – Forerunners of botnets emerge
2000 – DDoS attacks take down major sites
2001 – DoCoMo mobile malware outbreak
2003 – SQL Slammer wreaks havoc
2005 – First mobile worm (Commwarrior-A)
2008 – Cold Boot attack published
2012 – NFC exploits demonstrated

HISTORICAL PERSPECTIVE

The Ugly…

1980 – IDS concept emerges
1983 – Orange Book published
1988 – First paper on the firewall; X.509 issued
1989 – IBM releases Viruscan; COPS released
1991 – PGP created
1992 – ISS; first commercial disk encryption
1994 – First commercial NIDS, Netscape SSL
1995 – IPsec published (RFCs 1825, 1829)
2001 – Vontu (DLP) founded; ASLR defined
2002 – Mobile AV emerges (Symantec)
2005 – SIEM coined by Gartner
>2005 – ??? (evolution, but not innovation?)

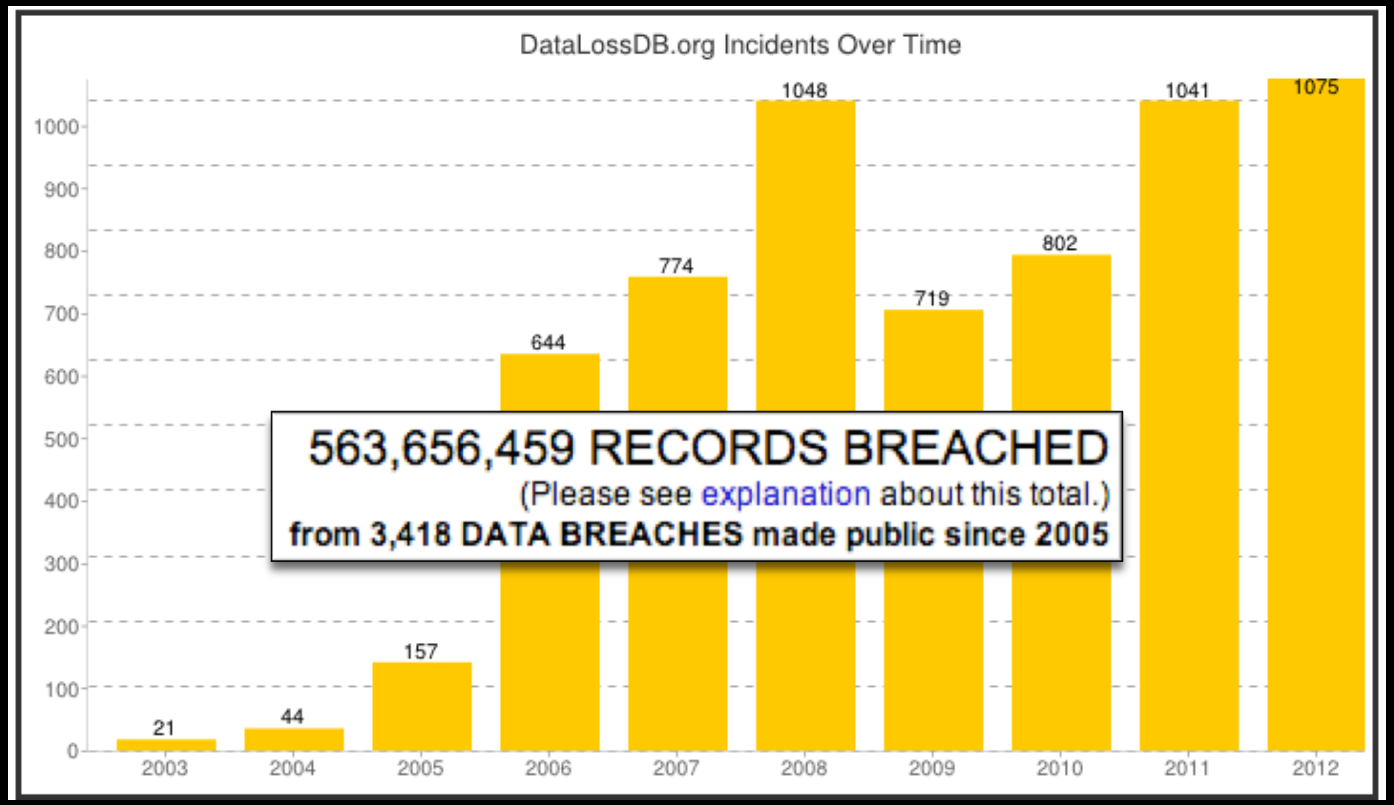
HISTORICAL PERSPECTIVE

The Uglier…

1934 – Communications Act
1973 - HEW Fair Information Practices
1974 – Privacy Act
1980 – OECD Privacy Principles
1986 – ECPA; CFAA
1994 – CFAA (networked abuses added)
1995 – EU Data Protection Directive
1996 – Telecom Act; HIPAA
1998 – PIPEDA (Canada); DMCA; COPPA
1999 – GLBA
2000 – ESIGN Act
2001 – USA PATRIOT Act; FERC Standard Market Design (Appendix G)
2002 – Homeland Security Act; FISMA; Sarbanes-Oxley
2003 – California SB 1386; FACTA
2004 – PCI DSS v1.0
2005 – FFIEC Guidance
2006 – Budapest Convention on Cybercrime
2009 – HITECH Act; EU Cookie Directive
2010 – Dodd-Frank; MA 201 CMR 17.00
2011 – SEC "cyber risk" disclosure guidance

HISTORICAL PERSPECTIVE

The Ugliest…



As of Oct. 9, 2012…

JUST HOW BAD IS IT?

How Apple and Amazon Security Flaws Led to My Epic Hacking

By Mat Honan August 6, 2012 | 8:01 pm | Categories: Miscellaneous

Cyber attack on RSA cost EMC $66 million

By Hayley Tsukayama

In its earnings call Tuesday, EMC disclosed that it spent $66 million in its second quarter to deal with a cyber attack that compromised its RSA Security division.

Symantec-Sponsored Ponemon Report Finds Negligent Employees Top Cause of Data Breaches in the U.S. While Malicious Attacks Most Costly

Share Tweet

MOUNTAIN VIEW, Calif. –Mar. 20, 2012 – Symantec Corp. (Nasdaq: SYMC) and the Ponemon Institute today released the findings of the 2011 Cost of Data Breach Study: United States, which reveals negligent insiders are the top cause of data breaches while malicious attacks are 25 percent more costly than other types. The study also found organizations which employ a chief information security officer (CISO) with enterprise-wide responsibility for data protection can reduce the cost of a data breach by 35 percent per compromised record. The organizational cost of a data breach was $5.5 million last year. The seventh annual Ponemon Cost of a Data Breach report is based on the actual data breach experiences of 49 U.S. companies from 14 different industry sectors.

INEVITABILITY

OUR APPROACH IS FLAWED

"A long habit of not thinking a thing wrong gives it a superficial appearance of being right." (Thomas Paine)

OUR APPROACH IS FLAWED

What's of value?

What control can we exert?

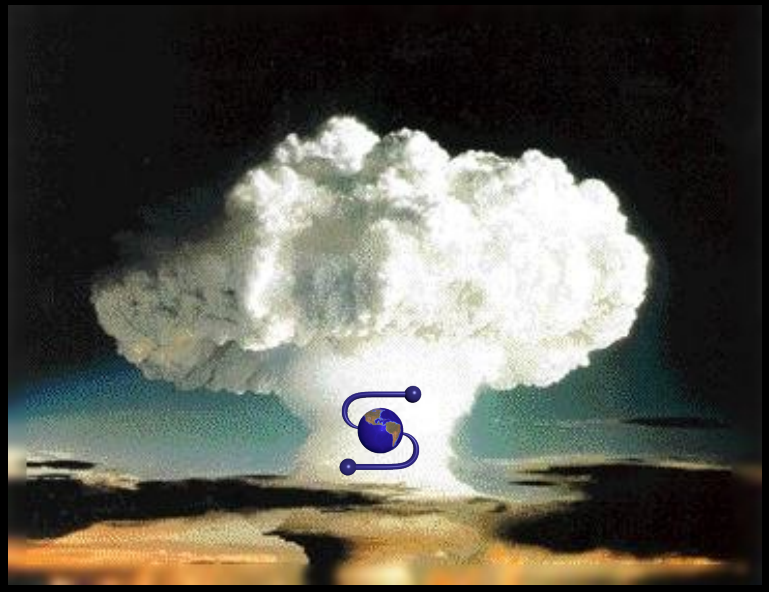
Where's the accountability?

http://www.flickr.com/photos/digitalcurrency/2438118655/sizes/m/in/photostream/
http://www.flickr.com/photos/global-jet/2124785243/sizes/m/in/photostream/
http://www.flickr.com/photos/ensh/6204837462/sizes/m/in/photostream/

HOW DID WE GET HERE?

"Never complain of that of which it is at all times in your power to rid yourself." (Adam Smith)

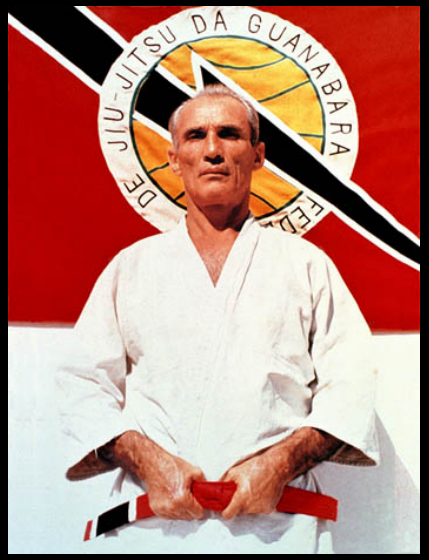
A LITTLE BIT OF EVOLUTION



Undefined → Emerging → Organized → Optimized → Managed

RISK MANAGEMENT FAILURES

Today…



Business Survival

Assets

BLIND LEADING THE BLIND?

It takes a generation…

Big data…

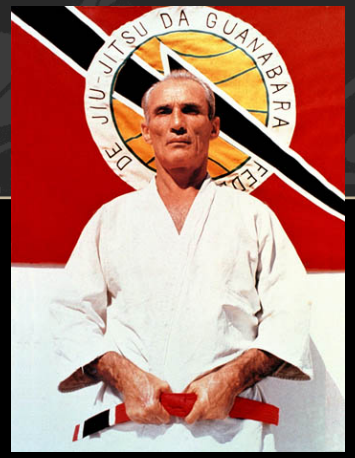
Rapidly changing environment

http://www.flickr.com/photos/cmogle/2907198746/sizes/m/in/photostream/
http://www.flickr.com/photos/nakrnsm/3898384586/sizes/m/in/photostream/
CSA Guide 3.0. "NIST Visual Model of Cloud Computing Definition"
http://www.flickr.com/photos/25692668@N06/3428784441/sizes/m/in/photostream/

WHAT NOW?

"We have it in our power to begin the world over again." (Thomas Paine)

WHAT NOW?



Objective 1: Jump to the next curve – a mature GRC program

Objective 2: Jump to the next curve – better "security" awareness

Objective 3: Establish a culture of accountability

3 STEPS FORWARD

"Common sense is seeing things as they are; and doing things as they ought to be." (Harriet Beecher Stowe)

1. GRC PROGRAM BUILD-OUT

1. Elevate it

2. True, legally defensible enterprise risk management

3. Return security operations to IT, governing accordingly

2. AGGRESSIVE AWARENESS

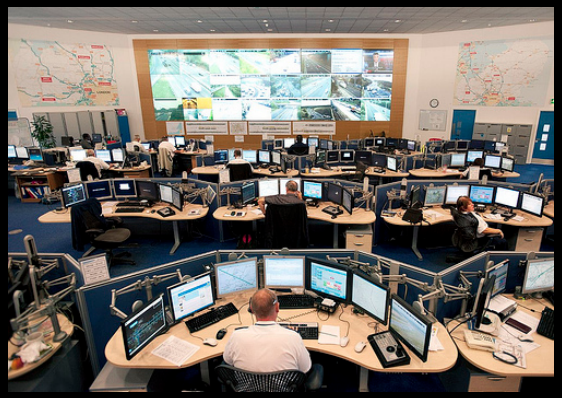
For Business Leaders

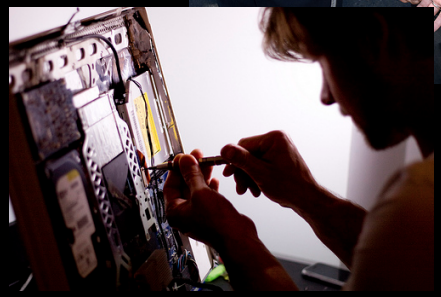
For Legal

For Everyone

http://cache.marriott.com/propertyimages/l/laxcv/phototour/laxcv_phototour20.jpg?Log=1
http://www.flickr.com/photos/crobj/4312159033/sizes/m/in/photostream/
http://www.flickr.com/photos/jurvetson/2487910168/sizes/m/in/photostream/

3. ACCOUNTABILITY FOR ALL





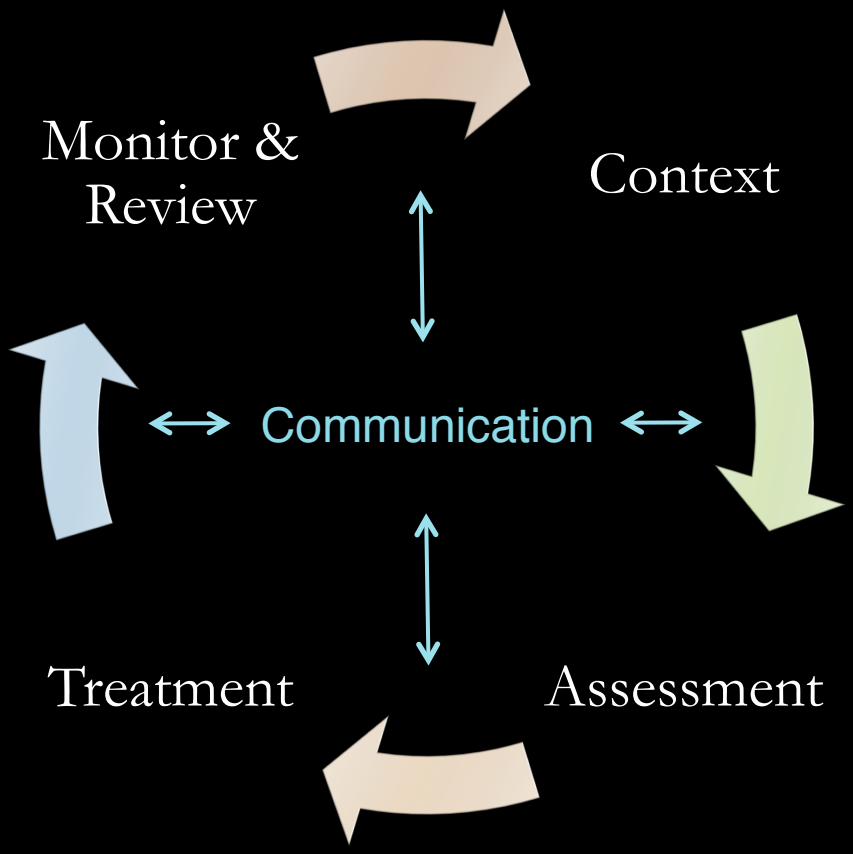
Monitor

Detect

Correct

http://www.flickr.com/photos/highwaysagency/6281302040/sizes/m/in/photostream/
http://www.flickr.com/photos/reneeviehmann/4320360120/sizes/m/in/photostream/
http://www.flickr.com/photos/cefeida/4714238826/sizes/m/in/photostream/
http://www.flickr.com/photos/oregondot/3853990076/sizes/m/in/photostream/

DEVOPS, RM, AND THE 3 WAYS



Images: http://itrevolution.com/

THE THREE WAYS

The First Way: Systems Thinking

Holistic, No Silos, Understand Value Streams

The Second Way: Amplifying Feedback Loops

Communication, Rapid Response, Embed Knowledge

The Third Way: Culture of Continual Experimentation & Learning

Innovate, Fail Fast / Learn Fast, “Freedom & Responsibility”

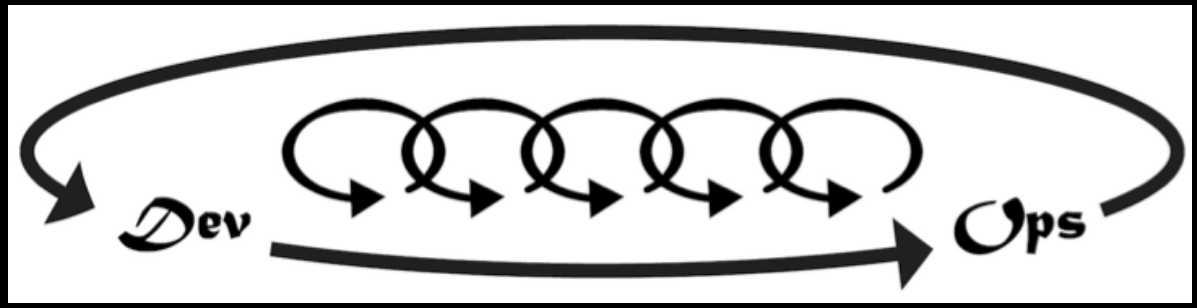
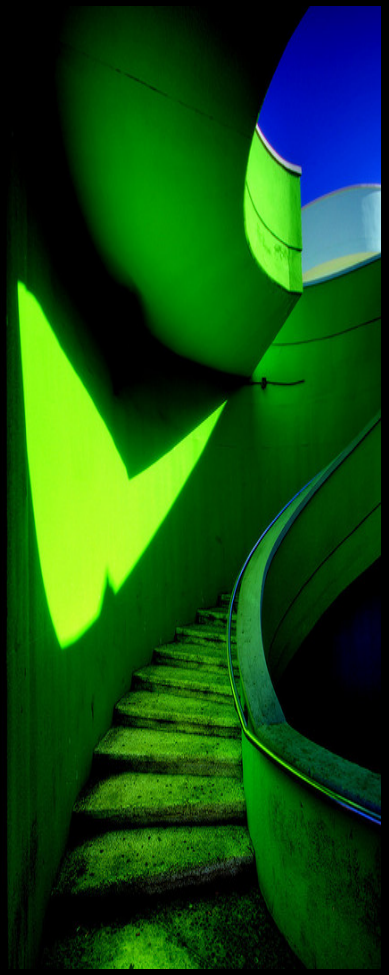


Image: http://itrevolution.com/the-three-ways-principles-underpinning-devops/

IN SUMMARY

"The mind once enlightened cannot again become dark." (Thomas Paine)

IN SUMMARY



The status quo is undermining business survivability.

It's (past) time to jump the curve – we cannot wait any longer.

3 Steps Forward:

1. "GRC" Program Build-Out
2. Aggressive Awareness
3. Accountability

http://www.flickr.com/photos/extranoise/3509011033/sizes/z/in/photostream/

Thank You!

Ben Tomhave

@falconsview

www.secureconsulting.net