Doug Meier

Owner, Meier Information Design, LLC

National Director, Information Security & Data Governance
Gordon Rees Scully & Mansukhani

Slipping Behind the Curve of Reality

Good Reasons To NOT Build a Security Program

Part 1

Security has a believability problem

“I don’t believe in Security”

-- VP of Enterprise Systems, 2013

(Internet firm, $1B annual revenue)

WAH
quickmeme.com

My journey adjusting to “I don’t believe in Security…”

- **Be offended** (experience outrage)
- **Empathize** (walk a mile in their shoes)
- **Bend** (adjust to business realities)

LET IT
GO
imgflip.com

“Security is not very important”

http://www.dtc.umn.edu/~odlyzko/doc/cyberinsecurity.pdf

Andrew Olydzko

mathematician and a former head of the University of Minnesota's Digital Technology Center and of the Minnesota Supercomputing Institute. He began his career in 1975 at Bell Telephone Laboratories, where he stayed for 26 years (wikipedia)

Realities

“The digital Armegeddon has not appeared; There are risks much greater than cyberrisks.”

“It is very hard for technologists to give up the idea of absolute cybersecurity… they are not used to thinking that even a sieve can hold water to an extent adequate for many purposes.”

“People are creatures who are not amenable to reengineering, and are *only very slightly amenable to reasoning and education.*”

“Most criminals ... have no interest in destroying the system they are abusing. They just want to exploit it, to extract value for themselves.”

Andrew Olydzko

Your security program probably doesn’t...

- Develop, integrate, test, release product ? -- Eng / Mfg Ops
- Generate leads / Close deals ? -- Sales
- Develop strategic partnerships ? -- Alliances
- Settle lawsuits, complete M&A work ? -- Legal
- Rollout HRIS in the cloud to the company ? -- HR
- Migrate enterprise apps from VMs to Containers ? -- Infra
- Revenue Recognition automations ? -- RevOps
- Salesforce BI integration -? - SalesOps

Security is inconvenient and annoying

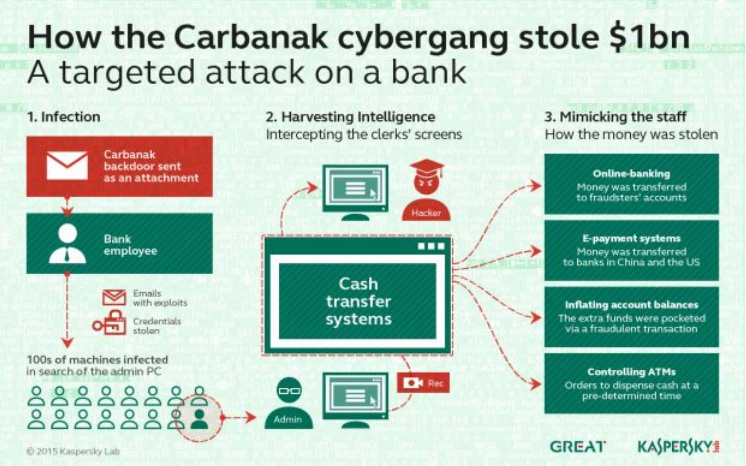
The CISO's Commandments

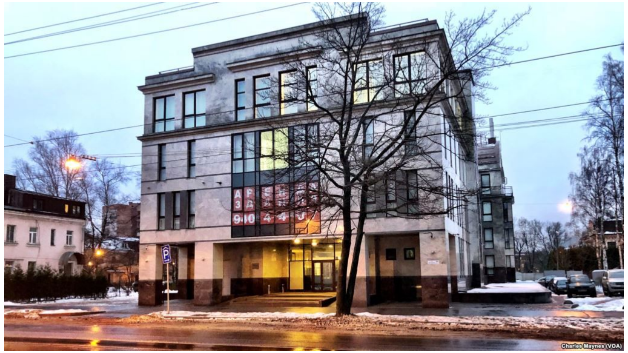
Thou shalt:

- Two-factor gladfully each day
- Receive urgent messages to update your endpoint's OS immediately!
- Be required to complete OWASP training
- Use Captcha to prove to Google that you are human
- Purchase cyberinsurance that may or may not cover all risks
- Be successfully phished by your IT dept
- Segment the network for regulatory compliance reasons
- Allow IT to install endpoint mgmt software on your personal cell phone
- Be admonished for someone else tailgating into the building behind you
- Provide evidence of access reviews and vuln remediations over the last five months

Security Theater

Security Reality

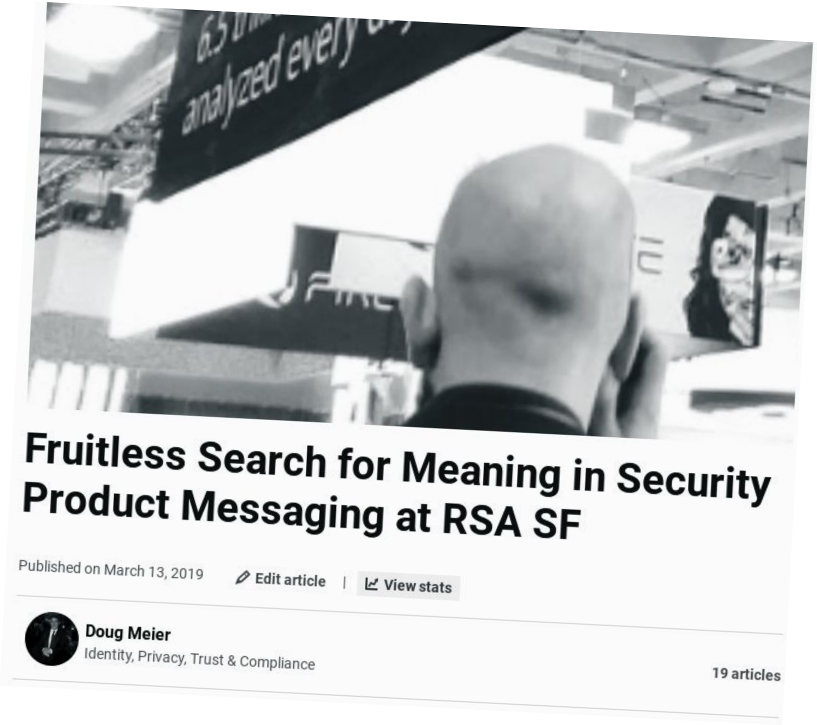

How the Carbanak cybergang stole $1bn
A targeted attack on a bank
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected in search of the admin PC
Admin
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
© 2015 Kaspersky Lab
GREAT
KASPERSKY



https://www.linkedin.com/pulse/rsa-sf-2019-walkabout-doug-meier/

linkedin.com/in/dougmeier

Security Hype



Fruitless Search for Meaning in Security Product Messaging at RSA SF

Published on March 13, 2019

Doug Meier
Identity, Privacy, Trust & Compliance

19 articles

Real hype from the RSA Expo floor

- Comcast Business: ***Beyond fast.***
- Cisco Systems: ***Security on top of everything.***
- Cisco Systems again: ***Security above everything.***
- Infoblox's Secureville: ***Giving you the comfort of yesterday in today's complex world.***
- Proofpoint: ***Don't let cloud threats rain on your parade.***
- Endgame: ***Military grade endpoint protection.***
- SolarWinds: ***Security just got real.***
- Overheard on the floor: ***The great thing is you'll receive continuous alert notifications as they happen.***

RIP Internet Trust (1969 - 2019)

- 1990s: **Trust, by verify**
- 2012ish: **Never trust, always verify**
- 2016: Current: **Zero trust**
- 2020 **Post-Trust**
- Evolving into: **Persistent distrust**

YOU KEEP USING THAT WORD SECURITY
IT DOES NOT MEME WHAT YOU THINK IT MEMES
imgflip.com

Internet Security: Mission Impossible

“Resolved: the Internet is no place for critical infrastructure”

https://queue.acm.org/detail.cfm?id=2479677

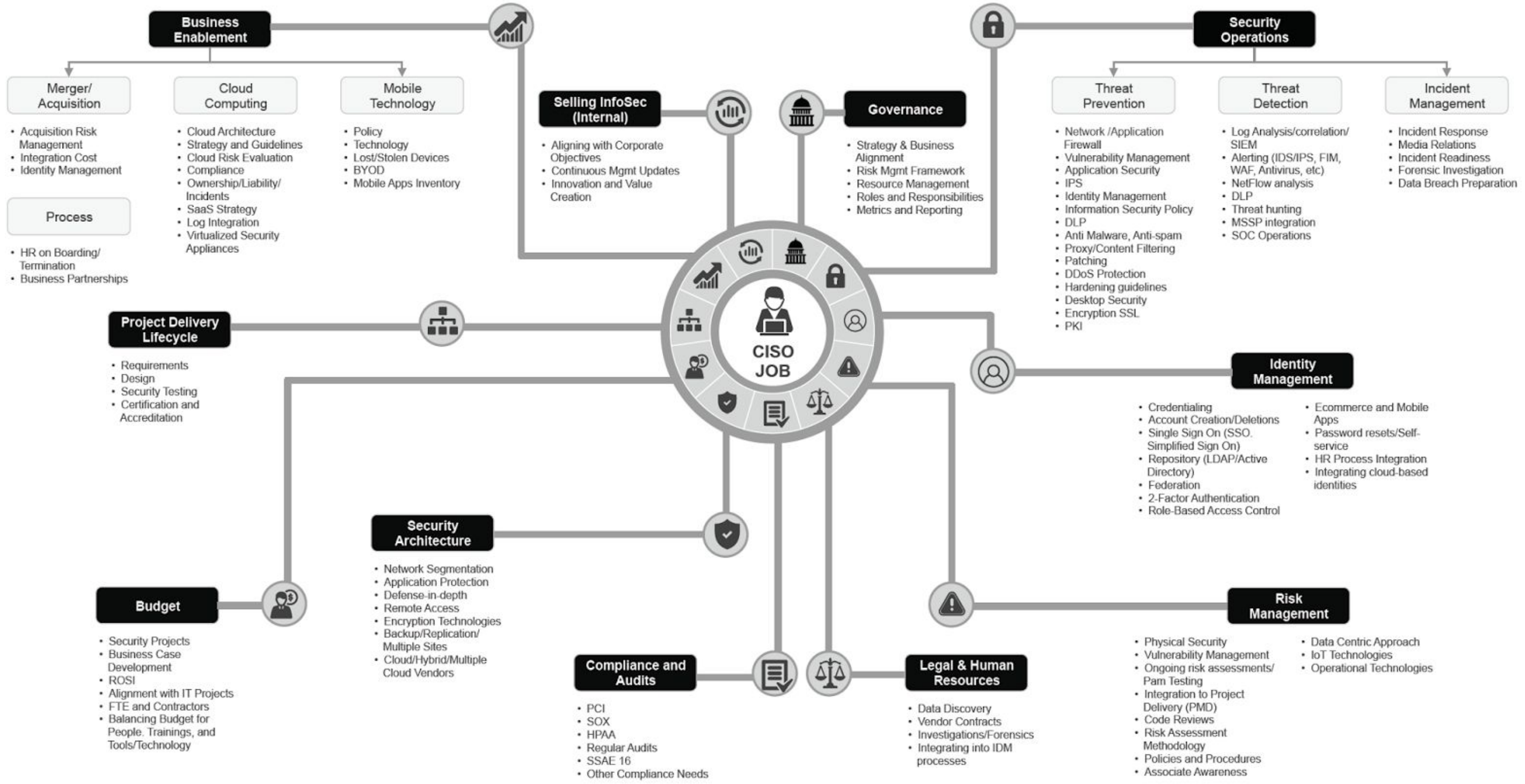
Dan Geer

chief information security officer for In-Q-Tel, a not-for-profit venture capital firm that invests in technology to support the Central Intelligence Agency.
Recognized for raising awareness of critical computer and network security issues before the risks were widely understood, and for ground-breaking work on the economics of security.

Part 2

Security doesn’t fit in

CISO Mind Map: An Overview of The Responsibilities and Ever Expanding Role of The CISO



CISO JOB

Business Enablement

Merger/ Acquisition
- Acquisition Risk Management
- Integration Cost
- Identity Management

Process
- HR on Boarding/ Termination
- Business Partnerships

Cloud Computing
- Cloud Architecture
- Strategy and Guidelines
- Cloud Risk Evaluation
- Compliance
- Ownership/Liability/ Incidents
- SaaS Strategy
- Log Integration
- Virtualized Security Appliances

Mobile Technology
- Policy
- Technology
- Lost/Stolen Devices
- BYOD
- Mobile Apps Inventory

Selling InfoSec (Internal)
- Aligning with Corporate Objectives
- Continuous Mgmt Updates
- Innovation and Value Creation

Governance
- Strategy & Business Alignment
- Risk Mgmt Framework
- Resource Management
- Roles and Responsibilities
- Metrics and Reporting

Security Operations

Threat Prevention
- Network /Application Firewall
- Vulnerability Management
- Application Security
- IPS
- Identity Management
- Information Security Policy
- DLP
- Anti Malware, Anti-spam
- Proxy/Content Filtering
- Patching
- DDoS Protection
- Hardening guidelines
- Desktop Security
- Encryption SSL
- PKI

Threat Detection
- Log Analysis/correlation/ SIEM
- Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
- NetFlow analysis
- DLP
- Threat hunting
- MSSP integration
- SOC Operations

Incident Management
- Incident Response
- Media Relations
- Incident Readiness
- Forensic Investigation
- Data Breach Preparation

Project Delivery Lifecycle
- Requirements
- Design
- Security Testing
- Certification and Accreditation

Identity Management
- Credentialing
- Account Creation/Deletions
- Single Sign On (SSO, Simplified Sign On)
- Repository (LDAP/Active Directory)
- Federation
- 2-Factor Authentication
- Role-Based Access Control
- Ecommerce and Mobile Apps
- Password resets/Self-service
- HR Process Integration
- Integrating cloud-based identities

Security Architecture
- Network Segmentation
- Application Protection
- Defense-in-depth
- Remote Access
- Encryption Technologies
- Backup/Replication/ Multiple Sites
- Cloud/Hybrid/Multiple Cloud Vendors

Budget
- Security Projects
- Business Case Development
- ROSI
- Alignment with IT Projects
- FTE and Contractors
- Balancing Budget for People, Trainings, and Tools/Technology

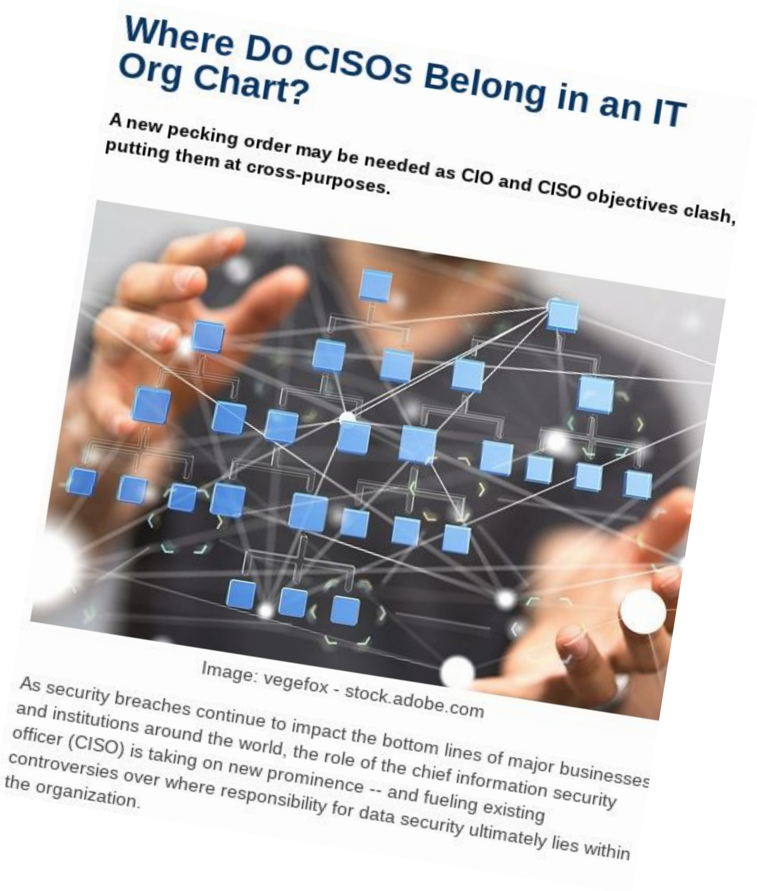
Compliance and Audits
- PCI
- SOX
- HPAA
- Regular Audits
- SSAE 16
- Other Compliance Needs

Legal & Human Resources
- Data Discovery
- Vendor Contracts
- Investigations/Forensics
- Integrating into IDM processes

Risk Management
- Physical Security
- Vulnerability Management
- Ongoing risk assessments/ Pam Testing
- Integration to Project Delivery (PMD)
- Code Reviews
- Risk Assessment Methodology
- Policies and Procedures
- Associate Awareness
- Data Centric Approach
- IoT Technologies
- Operational Technologies

Source: Rafeeq Rehman: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

Security, the orphan in the organization



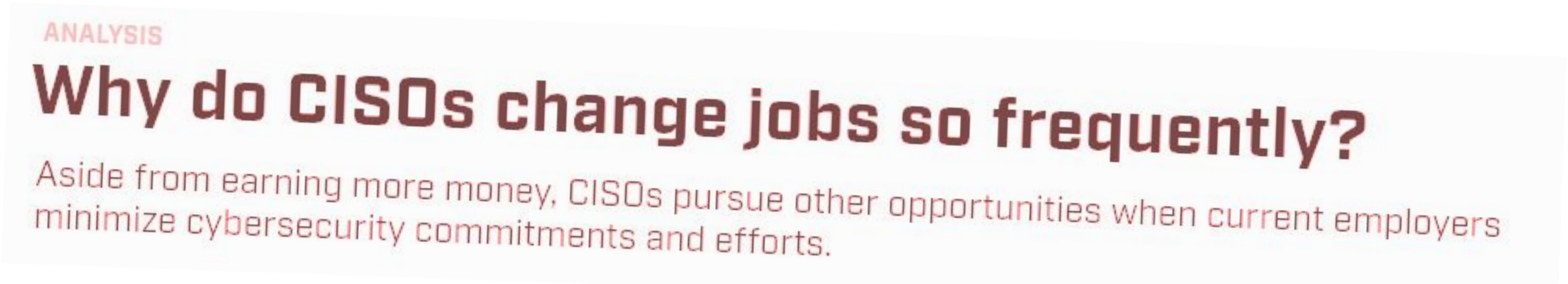
Where Do CISOs Belong in an IT Org Chart?

A new pecking order may be needed as CIO and CISO objectives clash, putting them at cross-purposes.

Image: vegefox - stock.adobe.com

As security breaches continue to impact the bottom lines of major businesses and institutions around the world, the role of the chief information security officer (CISO) is taking on new prominence -- and fueling existing controversies over where responsibility for data security ultimately lies within the organization.

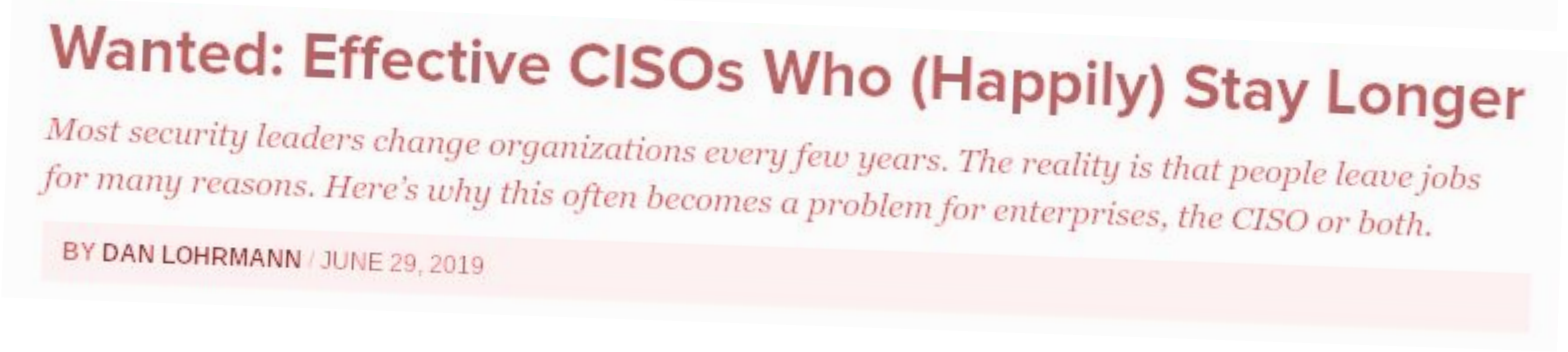
Average CISO tenure: 18 - 24 months



ANALYSIS

Why do CISOs change jobs so frequently?

Aside from earning more money, CISOs pursue other opportunities when current employers minimize cybersecurity commitments and efforts.



Wanted: Effective CISOs Who (Happily) Stay Longer

Most security leaders change organizations every few years. The reality is that people leave jobs for many reasons. Here's why this often becomes a problem for enterprises, the CISO or both.

BY DAN LOHRMANN / JUNE 29, 2019

Avoiding Failure

- **Focus on Risk Management:** The program needs a complete picture of the comprehensive risk landscape.
- **Sell the program internally:** Communicate successes in non-tech terms internally and externally.
- **Alignment with Strategic Objectives:** Continuous adjustments over time.
- **Understanding of Organizational Appetite for Security.** Could not suppress Ready Fire Aim impulses while problem solving.
- **Meaningful Successes to Build On.** Program demonstrates benefit of budget, resources, and support needed to accomplish risk management.

Part 3

Risk Management in the post-Truth, post-Trust Era

There is no such thing as Security...

… but Risk Management is definitely a thing

On Perceived Risk vs Actual Risk

“our job as risk managers is to understand that we over react to immediate threats and under react to long-term threats.”

On Risk Management vs Security

“when we … use the term "risk management," we don't want you to do it by trusting your gut. We want you to do risk management consciously and intelligently. This means balancing the costs and benefits of any security decision -- buying and installing a new technology, implementing a new procedure or forgoing a common precaution. ”

.

Bruce Schneier

Some ways CISO orgs may succeed

- Understand what the company does
- Understand the company’s appetite for risk.
- Align w the big business goals
- Maintain a Risk Register as your Source of Truth for Risk.
- Balance out techbro culture. Hire women.
- Be non-intrusive
- Communicate well
- Manage risk well at the vendor perimeter.
- Hold point solution vendors accountable..
- Get back to the basics: [SMB link]
- Be sensitive to security fatigue
- Recognize that compliance drives security

Risk Management IS important, because it’s ...

- understandable
- believable
- And aligns with survival

Any questions?