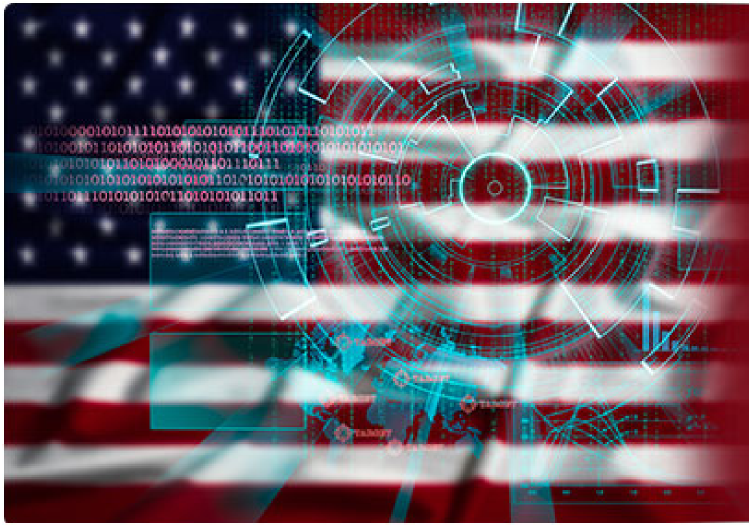


CYBER RESILIENCE SUMMIT

SECURING SYSTEMS INSIDE THE PERIMETER

Hyatt Reston Town Center
March 21, 2017 Reston, VA, USA

CO-PRODUCED BY:

CISQ
CONSORTIUM FOR IT SOFTWARE QUALITY

INFORMATION TECHNOLOGY ACQUISITION ADVISORY COUNCIL
ITAAC

“What’s Holding Us Back?”

Dr. Dale Meyerrose
Major General, U.S. Air Force, Retired

MeyerRose

Short answer: we don't tell the truth about #cybersecurity

- DoD Inspector General Report
  - "…87% of intruders into DoD information systems were either employees or others internal to the organization."
- Kroll Advisory Solutions
  - Company insiders, <u>not outside hackers</u> are responsible for 70% of all cyber cases involving theft

Today's cybersecurity threats are largely an inside-out proposition with insider behavior playing the dominant role. Tomorrow's threats will likely be the same!!

Examples of not telling the truth about #cybersecurity?

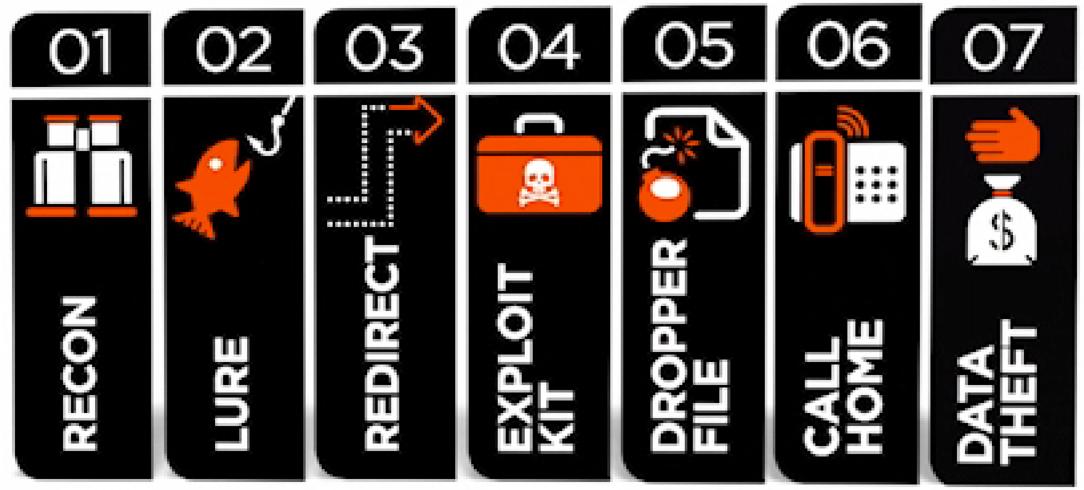
Myth	**Reality**
Biggest threat: Outsiders	Insider behavior
Means: High-tech hacking	Low-tech infiltration
Tool of choice: Malware	Social engineering
Most attacks ever: this yr	2012
Breaches getting bigger	Breaches more targeted
Victims/targets are helpless	90% victims already had ability to prevent attacks

Cybersecurity industry doesn’t want to; media isn’t capable; public is low information and has short attention span; Governments.........?

Today's #cybersecurity industry ignores the "cyber attack chain"

- Traditional cybersecurity measures fail to address most, if not all, of today's threat
- Stuck in the signature-based "mentality" rut of intrusion detection

*



Guarding a cyber perimeter that no longer exists—today's workforce exists and operates from beyond a network firewall

*Websense—Raytheon kill chain

We aren’t honest about ourselves

- CIO survey says*
  - 60 days to detect infiltration
  - 30 days to remediate
- Reality says**
  - 256 days to detect infiltration
  - 90-120 days to remediate

A breach is an organizational crisis—not a cybersecurity incident; nothing “incidental” about the impact

*2016 survey of 500 UK companies

**2016 Ponemon Inst research

Re-think @ how we approach #cybersecurity

- Cyber is a means to an outcome or human desire—therefore, cybersecurity IS NOT the goal
- Cybersecurity: what you do; not something you have
- Proactive beats reactive—hunting over responding—improved over restoral—built-in versus add-on
- All connected humans & objects need to be continuously monitored, measured, analyzed, optimized, controlled, & social engineered in terms of organizational value/risk

The real job is to protect organizational value proposition and activities; not just securing cyber and technical systems

Conclusion: we must be incompetent

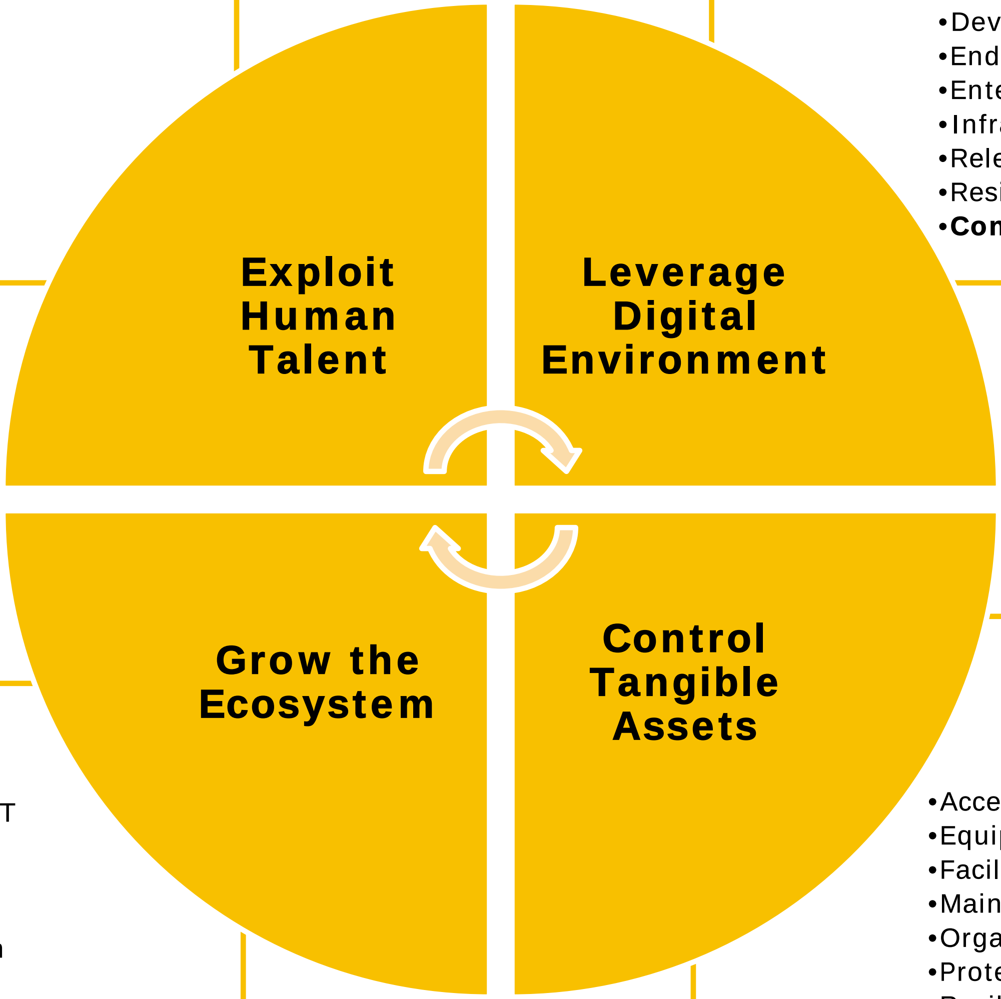
- Insider behavior (70% compromises) worsened by wider employee/third-party data access
- Continued failure to monitor access and activity around email/file systems – where most confidential/sensitive data moves/lives
- Most organizations don’t #encrypt data or segment/containerize their enterprise
- Security applications (add-ons)have to be pre-configured; can’t respond dynamically

Most data loss and cyber theft due to factors that can be controlled

*Ponemon Institute 2016 study for Varonis

MeyerRose

Top-rate #cybersecurity programs are ones of CONVERGING disciplines



Exploit Human Talent

- Customers
- New hires
- Out-sourced
- Partners
- Salaried
- Succession plan/resilience
- Technical competence
- Third-party suppliers
- **Continuous assessment**

Leverage Digital Environment

- Analytics
- Data rights management
- DevOps/standards
- Endpoint performance
- Enterprise architecture
- Infrastructure
- Relevant threat analysis
- Resilience
- **Continuous assessment**

Grow the Ecosystem

- Business intelligence/SWOT
- Governance
- Intellectual property
- Policies/accountabilities
- Priority/resource allocation
- Strategy/resilience
- Value proposition
- **Continuous assessment**

Control Tangible Assets

- Access/exposure
- Equipment/hardware
- Facilities
- Maintenance
- Organizational footprint
- Protection/safety
- Resilience
- **Continuous assessment**

Before calling the cyber folks stupid

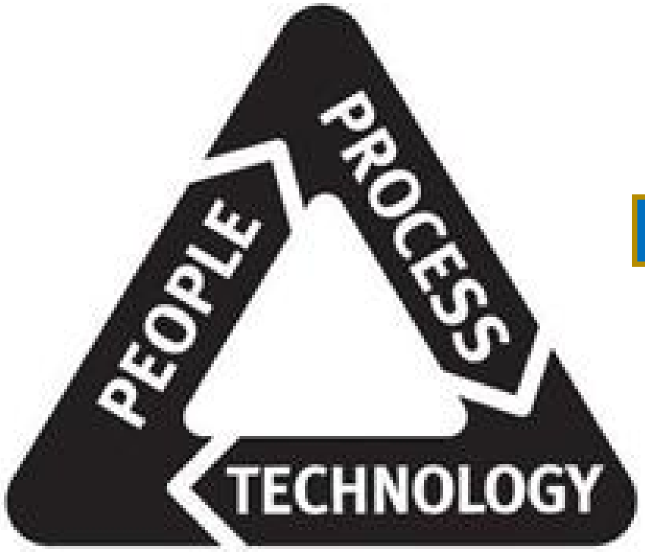
The GAO attributes the problems with IT programs to "...a lack of disciplined and effective management and inadequate executive-level oversight."

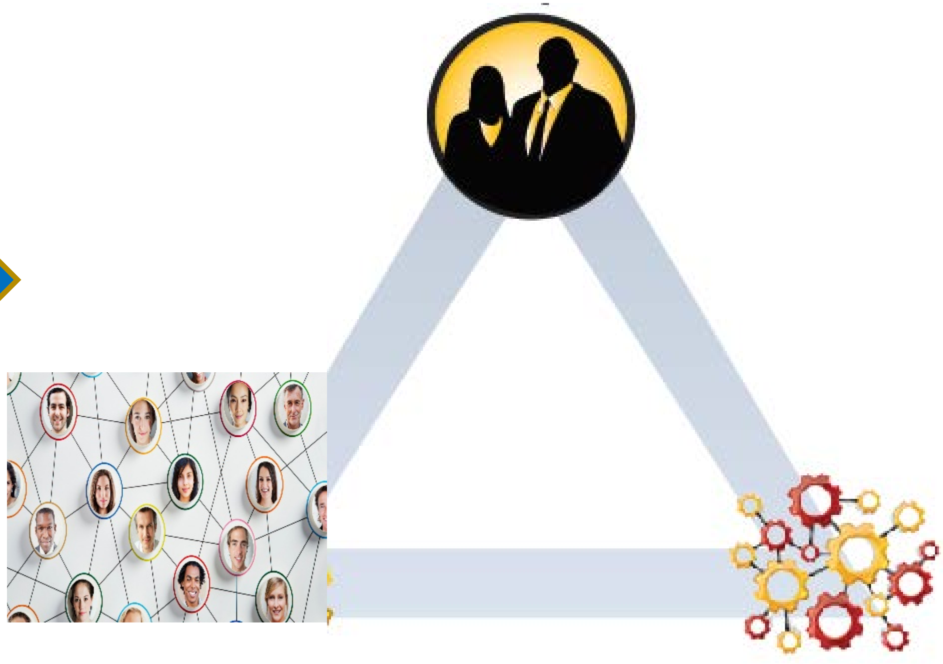
IT acquisition focused on process not programmatic success

▪ User	→	Usability
▪ IT	→	Maintainability
▪ Management	→	Budget
▪ Contracting	→	Process
▪ Legal	→	Justifiable
▪ Contractor	→	$$

- Adversarial relationships start early—persist and never go away
- >85% of USG IT initiatives fail to meet budget and timeline—many never come on line

Our focus on process is self-defeating





Talent

Customers

Outcomes

“You never change things by fighting the existing reality. To change something, build a new model that makes the existing model obsolete” R. Buckminster Fuller

Why do we debate what the world has already decided?

- Currently, over half of the companies in North America have a “cloud first” strategy
  - By the end of this decade, almost all will have a “cloud only” one
- The Internet of Things is already here
  - 60% of companies already employ #IOT constructs

We need to worry about the next billion digital connections—not the last billion

*Gartner

“Leadership buy-in” hoax

- “Bureaucratic placebo”
  - CYA
  - Delegation of process but not important decisions
  - Governance ‘restraint’ provided through councils/committees and policies
- *Faux* support
  - Approval vice commitment
  - Conundrum: spend $$$ with no assurances
  - “Dwell time” reflection of real priorities

Leadership participation is the #1 clue of something’s importance—one nurtures that which matters

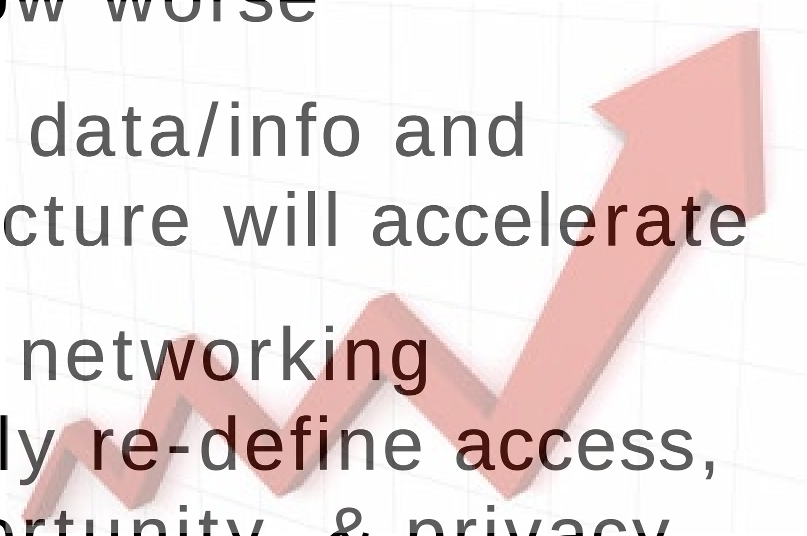
We trivialize IT/cyber contributions

- Dispersed, incremental decision making—process introduces “late-to-need”
- Workable standards/frameworks exist—not followed or enforced
- Acquisition process disconnected from program accountability
- Regarded as commodity in lieu of a strategy
- Measure/analyze the wrong things—activity vs outcomes

And often fail due to a lack of imagination

MeyerRose

Cyber / IT "drivers" for the next decade



- Scarcity of talent will grow worse
- Expanding digitization of data/info and virtualization of infrastructure will accelerate
- Technology-based social networking continually will continually re-define access, crime, law, liability, opportunity, & privacy
- Internet of Things will drive all industries
- Threats will not diminish or remain static

Forces outside of the "cyber/IT bubble" will determine what happens inside

The real threat inside our perimeters

Are you effective at telling the compelling #cybersecurity story to your senior leadership?

www.meyerrose.com

Questions?

Never completely trust sources that stand to benefit from the advice/information they give you

IF you were wondering about the #s, ask a Millennial