“#Cybersecurity, are we incompetent?”

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

MeyerRose

Ever listen to #cybersecurity professionals talk?

- It's not a matter of if you'll be breached, it's when
- Today's threat environment is more complex and dangerous
- The "evil doers" have the advantage and we can't seem to get in front of the threat
- Pessimism abounds: we can't guarantee security but might mitigate its impact

Why do we buy #cybersecurity products that don't seem to fix our organizational needs?

Are we as smart as we think we are?

As professionals:

1. Do we understand cyber threats?
2. Are we truthful @ our capabilities?
3. Do we rely on obsolete concepts regarding cyber?
4. Do we lack imagination and sense of direction?
5. Can, we by ourselves, meet the cyber challenge?

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

1. Think hackers are your biggest threat?—think again

- 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, not outside hackers 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!!

1. Threats/attacks are not single threaded events

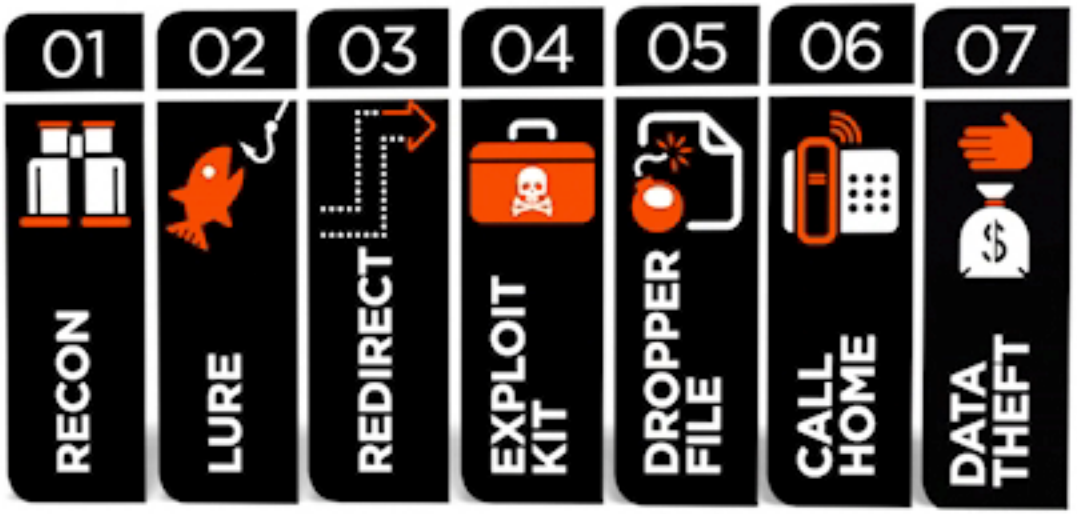
- Persistent over time, not a single incident or event—think in terms of "attack campaigns"
- An "inside-out" challenge—not an "outside-in one"
- Motivations: theft, espionage, retaliation
- Cyber is a means to an outcome—not the source of criminal motivation
- Multiple participants, roles, tools, domains, attempts—usually after data not your systems
- Attackers dynamically adjust to defender actions

"Evil doers" will take the path of least resistance to gain entry and then operate from the inside as an authorized user

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

- Traditional cybersecurity measures fail to address most, if not all, of today's threat
- Lack a value proposition for the real threat—stuck in signature-based "mentality" rut

*



*Websense—Raytheon kill chain

1. Attack vector landscape

- Multi-vector—almost always include DDoS component (80% of which are HTTP Floods)
- Preferred methodology: social engineering
- Main targets: email, web services, file systs

*

*blog.executivebiz.com

2. We can't tell the truth about #cybersecurity?

Myth	Reality
Biggest threat: Outsiders	Insider behavior
Means: High-tech hacking	Low-tech infiltration
Tool of choice: Malware	Credential theft
Most attacks ever: 2016	2012
Breaches getting bigger	Breaches more targeted
Victims/targets are helpless	90% victims 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……?

2. "Cyber Attack" = euphemism for aggressive human activity in cyber

- Deception
- Disruption
- Espionage
- Free speech
- Pranks
- Retribution
- Spying/surveillance
- Theft
- Unintentional human error
- Vandalism

Reality: A cyber "attack" is, more often than not, merely software preempting other software

2. We can't be trusted to be objective

- 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

MeyerRose

3. Hurdles to most #cybersecurity thinking

- There are only people issues and decisions—almost none are technical
- Talent is the only true competitive advantage
- Strategy is more about resolve than brilliance
- Defining success is the first task of a leader—the second is to adapt when one gets the first task wrong—with enough speed to matter
- Disruption usually comes from an unanticipated combination of "knowns"
- Emotion dominates logic in many decisions

Security—which should encompass #cybersecurity—is what you do, not something you buy

3. Obsolete thinking example 1: "Defense in Depth"

- Passive approach—field, then "wait and see"
- Assumes attacks come from outside; most actually start from inside
- Implication each layer engages sequentially; not how cyber activity/functions occur
- Premise that layers of defense attenuate threats; not so!
- Tiered security is a failed strategy; protected zone access gained thru less protected ones

Much of today's workforce exists and operates from beyond a network perimeter

3. Obsolete thinking example 2: "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

The cost of data breaches is not enough to convince companies to spend vastly more to bolster cybersecurity. eWeek 5.30.2016

4. We trivialize our cyber contribution

- Impact of dispersed, incremental decision making
- Obsess on the urgent, leave important to chance
- Treat like a technology in lieu of people and business/mission issues
- Regard as a utility rather than a discipline and a commodity rather than part of a strategy
- Account as overhead, cost/seat or transaction
- Amount of investment doesn't translate into competitive advantage—or battlefield dominance

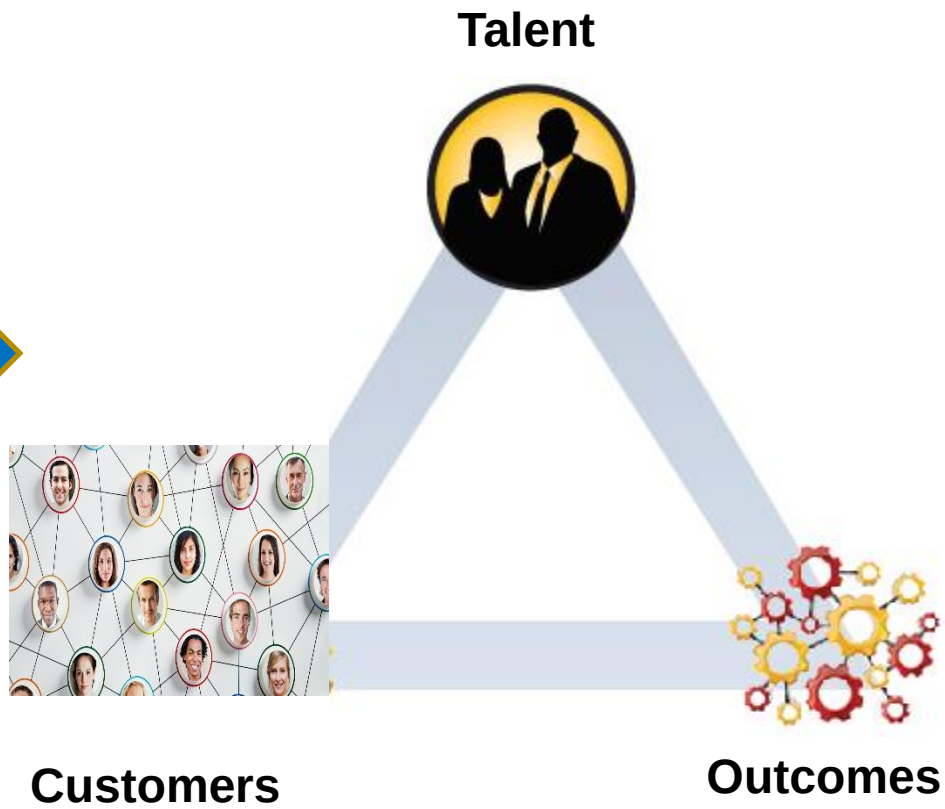
4. Why do we debate what the world has already decided?

- 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

Sadly, we lag not only the need, but reality itself

*Gartner

4. Challenge your usual perspective of inputs versus outputs



"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

5. If you have a #cybersecurity program, you are probably behind—and losing

- Not holistic
- Static in outlook
- Historically event-driven
- Led by security people
- Symptoms-based
- Reactionary

Security is about controlling an ecosystem—people, places, and things

5. Traits of the best security programs

- C-suite accountable office
- Designated Chief Security Officer vice Chief Information Security Officer
- Integral to business processes—not separately handled issues
- Measurements linked with outcomes
- Budgeted, resourced, planned
- Tested, evaluated, and adjusted
- Designated, trained response team

Sources: SANS Institute, Ponemon Institute

5. Most telling missteps

Strategic Shortcomings

- C-suite commitment
- Communications
- Duration
- Event scope
- Intelligence investments
- Legal considerations
- Resource allocation
- Response process

Technical Failures

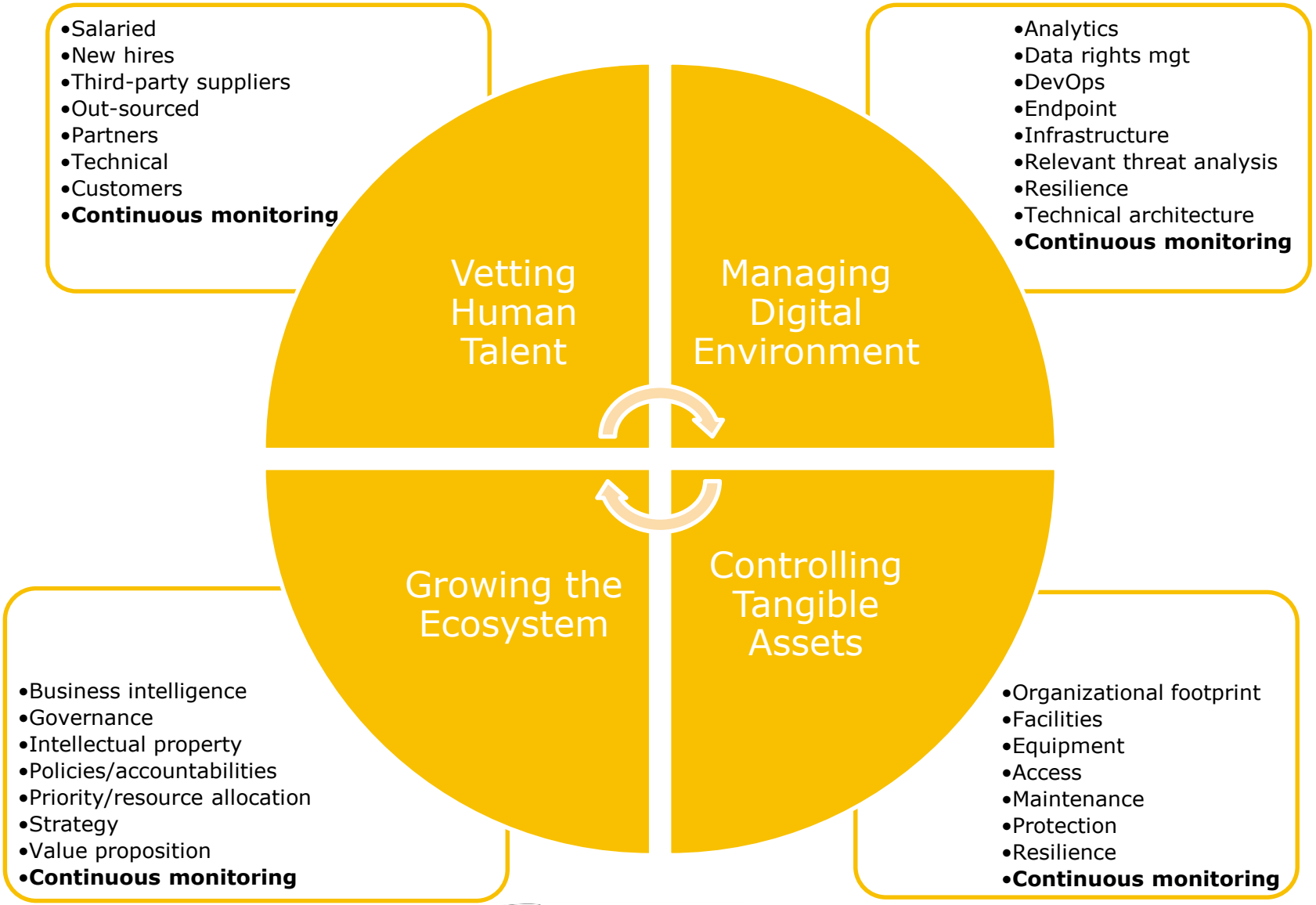
- Asset accountability
- Colleague cooperation
- Discerning cause/effect
- Documentation
- Leverage existing tools and analytics
- Monitoring internal communications
- Training/proficiency

It's crisis management—not a cybersecurity response

Sources: Tripwire; InfoSecurity Group

MeyerRose

5. Necessities for a top-rate security program—CONVERGING disciplines



MeyerRose

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 companies don't #encrypt data or segment/containerize their enterprise
- Deployed security applications 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

Which worldview matters?

- #C-suite*
  - Industry trends
  - Business disruptions
  - Potential markets
  - Consumer tastes
  - SWOT
- CIOs/CISOs**
  - Threats—next breach
  - Technology development
  - Technology competence
  - Program mgt
  - Minimizing risk

CEOs' focus = growth & profitability
Cyber professionals' focus = keeping the lights on

*McKinsey
**MeyerRose Group survey

MeyerRose

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
- Address human and technical vulnerabilities in context of applicability, priorities, liability, and risk
- Continuous monitoring applies to more than technology and processes
- All connected humans & objects need to be monitored, measured, analyzed, optimized, controlled, and social engineered in terms of value/risk

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

#Cybersecurity "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 "cybersecurity bubble" will determine what happens inside

One thing more—a favor, please

- Langley Cyber Attack—20th Anniversary
  - Jan – May 1997
  - One of the first major cyber attacks against USG
  - Story documented in civilian publications—USAF not so much
- Seeking to tell the "cyber story" of the people, era, and event
  - Need specific permission to use information/documentation/pictures

Contact: dale@meyerrose.com

MeyerRose

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