12TH ANNUAL
PEAK CYBER SYMPOSIUM
& CYBERSECURITY SUMMIT FOR SMALL BUSINESSES

ISSA
Information Systems Security Association
Colorado Springs Chapter

Colorado SBDC
TECHSOURCE
CYBER: Cover Your Assets™

9.14 - 9.16.22
COLORADO SPRINGS, CO

Today's Cyber Environment — Dealing with the Elephants in the Room

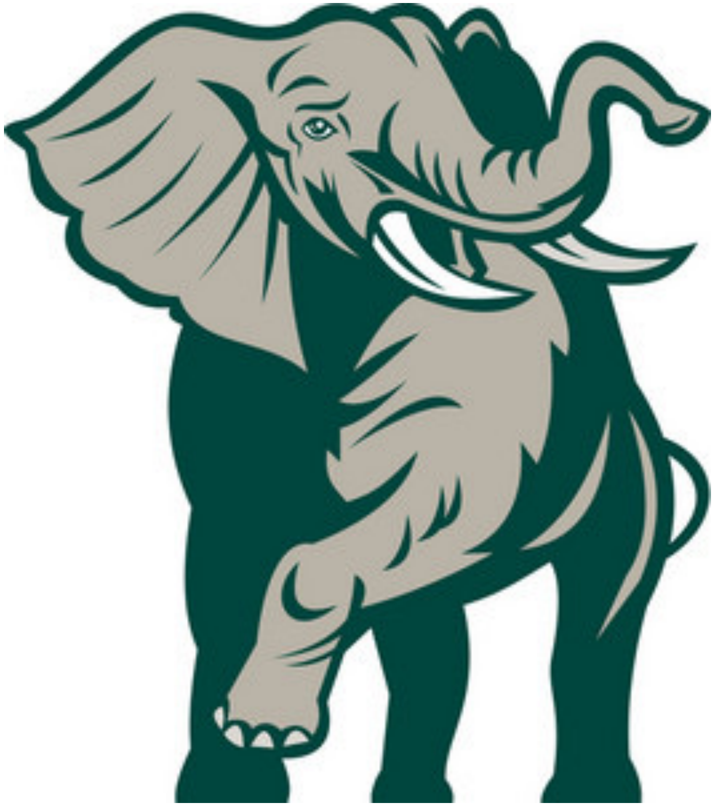
Dr. Dale Meyerrose, DPS
Major General, U.S. Air Force, Retired

September 15, 2022

MeyerRose

The "Elephants" of Cyber(security)

Information



Basics

First
Principles

Choices

Information

Don’t get tricked into stupid

Ideology & money influence the quality of information

NIH
GRANT
MACLEOD

"You are completely free to carry out whatever research you want, so long as you come to these conclusions."

The state of today’s information sources**

- 2.6M studies published yearly in 30K peer-reviewed journals
  - Good science: high level of integrity, transparency, and objectivity leads to findings that can be replicated by other researchers
  - Bad science: ideology-driven or industry-sponsored; not designed to advance knowledge, but to mislead for political or financial gain
  - “Sneer review” replacing peer review feeding cancel culture
- Researchers’ conclusions:
  - “What appears beyond dispute is that making absurd and horrible ideas sufficiently politically fashionable can get them validated at the highest level of academic grievance studies….”
  - “The discerning reader, whether scientist, academic, ethicist, journalist, or layperson, should realize: any asserted scientific “fact” or “conclusion” must be combined with common sense, a healthy skepticism, and a closer look at those who stand to profit or advance a position….”

Good information is the "nectar of knowledge"

- Methodologies
  - Research
  - Studies
  - Surveys
  - Theories
  - Modeling
  - Rumors & outbursts (social media)

- Before reading:
  - Author's employment & credentials
  - Triangulate sources
- As you read:
  - Challenge assumptions, assertions & facts
- Find related material & repeat

"Settled science" is a reflection of the speaker's stupidity, ignorance, or malevolence

Critical thinkers will change when faced with better information

- Don’t be cowered by people who argue like bullies
  - “Are you a doctor?”
  - Demean the person rather than refute the idea
  - Intolerant of dissenting views
- Don’t be fooled by “we can all agree…”
  - Common knowledge often not based on fact
  - Repetition of bad info more entrenched over time
  - Memories are short—cause & effect disconnected

“Right is right, even if everyone is against it, and wrong is wrong, even if everyone is for it.” William Penn

Basics

The keys to success

Observations of the "cheese" migration in our industry

- The pre-eminence of Cloud
- Legacy of on-premise
- Evolution of workflow and the human and digital workforces

Equal in scale and impact

Cloud security in 2022*

- 78% of identified attack paths use known vulnerabilities (CVEs) as an initial access attack vector
- 70% of organizations have a Kubernetes API server that is publicly accessible
- 58% of providers don’t use MFA
- 15% of cloud assets use software with vulnerabilities at least 10 years old

The average attack path only needs 3 steps to reach a “crown jewel asset” in a cloud architecture

*Orca Security 13 Sep 2022

On-premise infrastructure in 2022*

- Major surge in exploiting vulnerabilities in Internet-facing applications tied to the multiple, critical Exchange Server vulnerabilities
  - CVEs serve as attacker roadmaps—it only takes minutes for attackers to scan 1000s of systems with just-disclosed flaws
  - Attackers use legitimate tools and frameworks to collect data, escalate privileges, and execute commands
- Bottom line: threat actors will use exploits that work, following the path of least resistance. If there's a new remote code exploit on some O/S or APP, they'll flock to it and breach as many networks as they can before the systems are patched.

63% of attackers managed to stay unnoticed in a network for more than a month after gaining initial entry

*Palo Alto 8 Sep 2022

Human behavior remains central to credential compromises

- Individuals now have a single, unified digital life—blurring professional and personal boundaries—accelerated by reaction to pandemic*
  - 39% had malware on their personal devices
  - 59% had antivirus on their personal devices
  - 40% had their home IP address available for sale via online data brokers
  - 75% of personal computers are either totally unprotected or operating using default security settings
  - 68% were writing down their passwords on personal notebooks or storing them in their contacts list on the phone.
- Cybersecurity industry slow to adopt using a digital workforce
  - Expanded attack surfaces tasks scale workload beyond human capacity

*BlackCloak Aug 2022

Policy makers agree even if their policies don’t align (i.e. EO 13800)

John C. Inglis, National Cyber Director, EOP:

- 85% of security breaches prevented by:
  - Two-factor authentication
  - Data segmentation
  - Ruthless patching

Hard to sell cybersecurity products with this realization

In 2022 there are more cyber knowns than unknowns

- Threat vectors remain relatively unchanged
  - Physical & credential theft aided by inside(r) behavior
  - Nation-states & criminals target **$**, secrets, ideology, etc.
- Risk fundamentals are well understood—and still work in today's "changed world"
  - Stay true to value proposition
  - Leverage AI to continuously collect, analyze, and profile all data
  - Include human factors and linkages in risk assessments
  - Drive metrics to better inform decision making
  - Focus on outcomes over process

The real job is to sustain functionality and purpose—not just secure technology and systems

First Principles

Getting practical

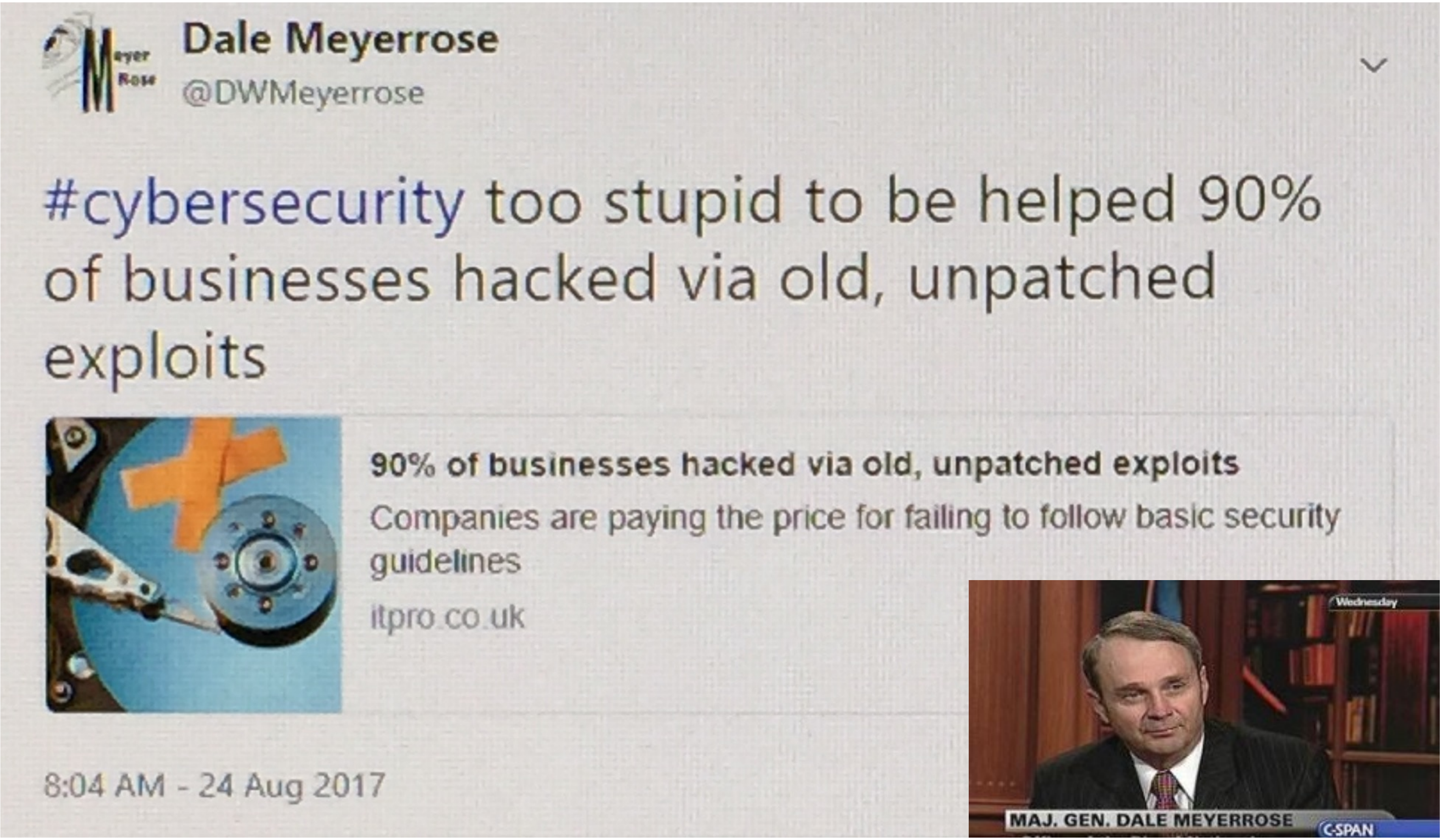
Has anything changed? Is anyone listening?

"We say we know the perimeter is dead. We say we know the adversary is on the inside, but we don't change our actions. We can't just apply some bling and hope that revolutionary technology will come save us. The security industry is broke at its core. We suffer from a lack of excellence."

Amit Yoran
CEO Tenable
Former RSA Pres

Part of the problem with research is convincing an organization that it's applicable to their situation

NO!



Dale Meyerrose
@DWMeyerrose

#cybersecurity too stupid to be helped 90% of businesses hacked via old, unpatched exploits

90% of businesses hacked via old, unpatched exploits
Companies are paying the price for failing to follow basic security guidelines
itpro.co.uk

8:04 AM - 24 Aug 2017

In its current form, cybersecurity is DOOMED for the trash pile of history!

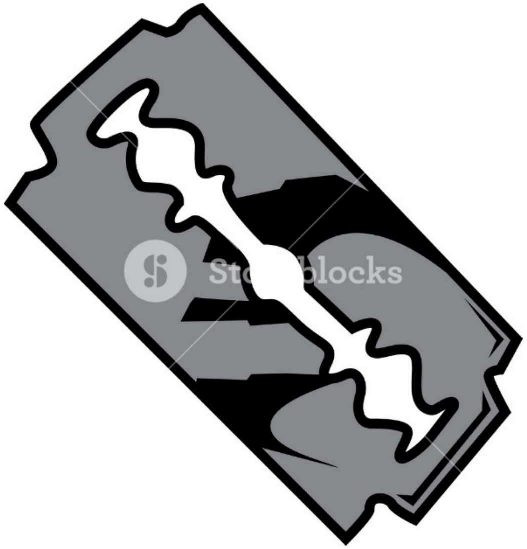
As professionals, we:

- Don’t drill down on the real, underlying threats
- Aren’t truthful @ our capability
- Rely on obsolete concepts
- Lack imagination and sense of direction
- Paralyzed by the fear-of-the-inevitable
- Can’t, by ourselves, meet the challenge
- Fail to tell the compelling story to senior leadership

Your network is your net worth. Tim Sanders

Ockham’s (also Occam’s) razor

- The principle in understanding a concept, analyzing a situation, or solving a problem, getting unnecessary information out of the way is the fastest way to the truth, best explanation, or potential solution



Know Your Numbers

- Sell ideas/proposals
  - Include contradictory indicators & uncertainty factors
- Counter urban myths by leveraging BIG analysis
- Understand all linkages
- Move beyond 80/20

Target what matters, vice what's merely important or interesting

Cybersecurity first principles

- Initial infiltration usually undetected
- Starts with credential compromise through social engineering or CVE
  - Followed by software/malware insertion
- Inside(r) behaviors play dominant role
- Not every threat is applicable to every situation/organization
- Data is the principle target of "evil doers"

Today's cybersecurity threats are an inside-out proposition with insider behavior playing the dominant role—unchanged for years—tomorrow's will likely be the same!!

Choices

Today’s cyber “victims” are universally complicit in their own “victimhood”

Determining essence should be the first step in problem solving

- Complexity clouds root causes, numbs the mind, and constipates decision-making
  - Large number of inter-related elements (scale)
  - Non-linear (speed)
  - Dynamic (changing baseline)
  - Evolutionary characteristics (trends hidden in nuances)
  - Uncertainty (zero-day)
  - Unordered nature (zero trust)

> Success is neither magical nor mysterious. Success is the natural consequence of consistently applying the basic fundamentals.” Jim Rohn

Warren Buffett’s “Institutional Imperatives”

Why do normally intelligent leaders make stupid decisions?

- “Target fixation” on the familiar, measurable, & interesting vice the consequential
- Behavior imitation of peer organizations
- Bureaucratic inertia nullifies rational thinking
  - *Stare decisis, p*rogram of record, etc.
- Process-emphasis in lieu outcome-focus
- “Cherry pick” data that reinforces pre-existing notions & ideologies—censoring dissenters

Be picky about the advice you follow

Cybersecurity Trends That We Can See

- AI, Cloud, & XaaS continue to dominate
- Cyber talent remains at a premium
- Data-driven solutions in lieu of system-centric security
- Legal and policy activities will lack currency
- Think BIG—analyze in detail
- “Big Brother” will harvest your data, monitor your behavior, and leverage it at every opportunity

“Perfect security” exists no where on earth—why should cyber be any different?

Thanks for the honor

www.meyerrose.com

Questions?

You want people to insist on you being one of a select, handful of individuals invited to solve a need—and then insist on not starting the meeting until you arrive if you happen to be running late