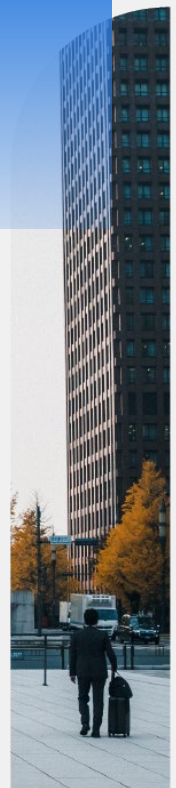
# A Foot in Both Camps: A Different Perspective on Cyber

Jim Richberg, Public Sector Field CISO and VP of Information Security

November 2021



# I learned a lot about Cyber while in Government…

**34 years** at multiple levels of the U.S. Intelligence Community

- **14 years** with the Director of US National Intelligence (DNI)
  - National Intelligence Manager for Cyber setting strategy and priorities for 17 Departments with an ~$80B operating budget, senior advisor to DNI on cyber, led cyber threat intelligence
  - Monitored & coordinated national cybersecurity (CNCI) for two Presidents
  - Ran national counterintelligence (insider and cyber threats)
- **20 years** at CIA in intelligence analysis, field operations, and technology management

But I didn't fully appreciate when/why the public and private sector talk past each other, nor the impact of AI/ML-powered automation on commercial cybersecurity capabilities

# Agenda

1. Common Misunderstandings
2. Implications and Advice for Operating in “the New Normal”
3. Cyber Metrics: measuring what we can vs. what we should
4. Final Thoughts

# Threat is often misunderstood in the Private Sector

- Cyber offense is harder than it looks!
  - **Advanced threats** (APT's) have resource constraints and only use their Varsity playbook if needed
  - **Supply chain threats**: "bad news, good news"
- The **criminal cyber criminal ecosystem** features more 'Darwin Award winners' than Professor Moriarty-like criminal masterminds
- **Targeted threats are less common** than 'opportunistic' ones ($)
- Increasing **convergence between outsider** and **insider threat**
- Damage from insider **risk** is often greater than from insider **threat**
- **Cyber Threat Intelligence**

# Trends not well understood by Government

- “Digital Transformation” has been embraced more aggressively by the private sector
- The intentional convergence of corporate Information Technology and corporate Operational Technology (IT and OT)
- The convergence between the adoption of reprogrammable software-defined devices and increasing connectivity directly to the Internet
    - For example, the growth of Software Defined Networking (SD WAN)

The Internet of Things (IOT) cuts across all three trends

*COVID has dramatically accelerated Government learning and adoption!*

# …and the Behavioral Aspect of Human-Machine Interaction is not well understood by either side

**Deception** (decoys and honeypots) has an impact beyond serving as a tripwire

- Influences both adversary speed and behavior
- Impact occurs even when this technology is present in an organization but not deployed everywhere
  - placebo effect
  - herd immunity

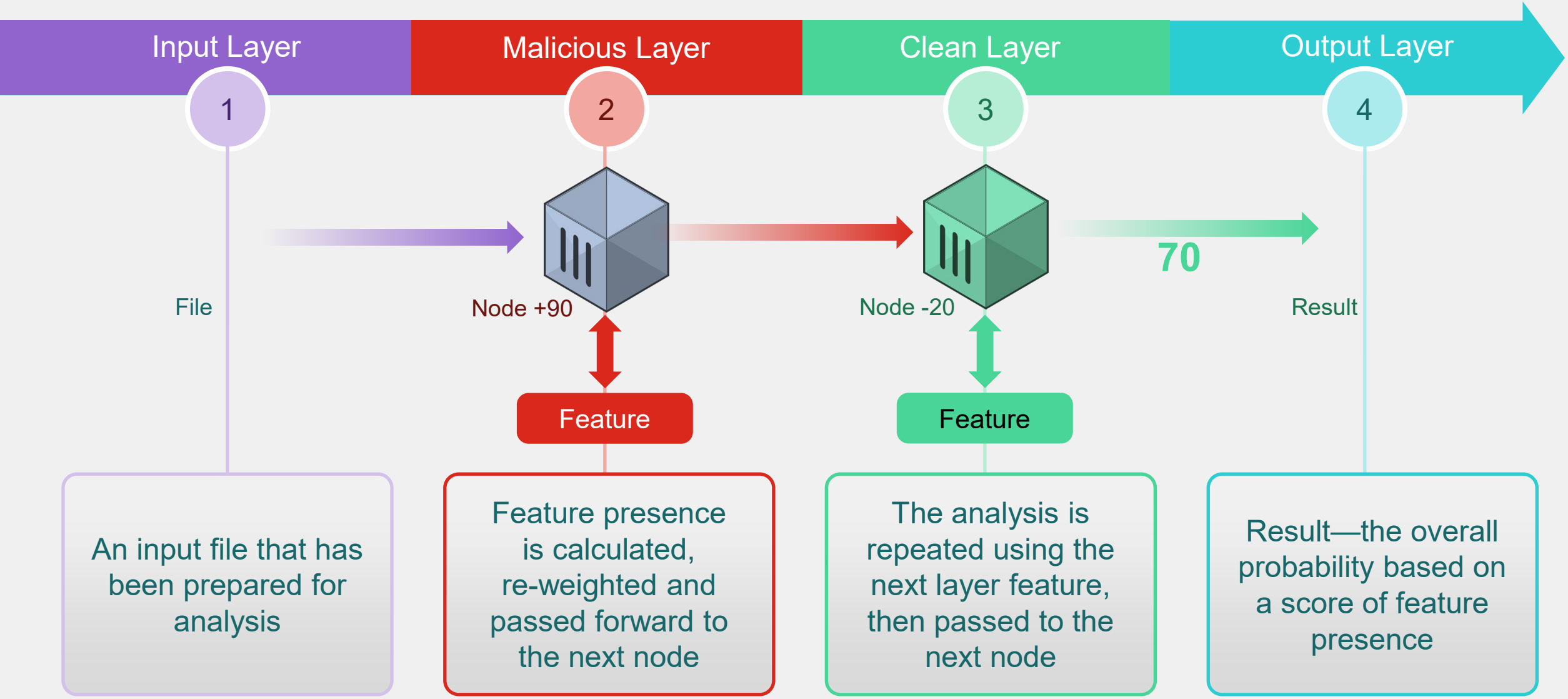
**This is especially relevant for organizations such as the SSA**

# …neither is the Breadth of the Impact of AI/ML

This affects Continuous Diagnostics and Monitoring (CDM) in Government

- Our definition of “Continuous” in Government has changed over time …along with our approach to cyber instrumentation and analysis
  - The Comprehensive National Cybersecurity Initiative (CNCI) of 2008 was predicated on **Shared situational awareness, Common Operating Picture, “response at machine speed**”
- Industry has developed cyber Big Data Analytics (**AI/ML**) and enterprise-focused approaches to policy-driven **automation**, and unified capability families or **platforms** that present **viable options as COTS solutions or contributors to CDM**

# How does it work Conceptually: Malware Analysis based on Features & Weights



# AI/ML in the Cybersecurity Industry

- Vendors have been using AL/ML (Artificial Intelligence and Machine Learning) in threat detection for **over 10 years**
  - Malware analysis, website evaluation, user behavioral analytics, ‘sandboxing’, and threat intelligence
- Virtually all threat detection at many cybersecurity firms generated by AI/ML
- Using all three modes of AI/ML (supervised, unstructured, reinforcement)
- Growing maturity of deep learning/neural network capability enable new use options including standalone deployment use within Agency IT networks or in OT environments

# Common Reasons Cybersecurity is hard…

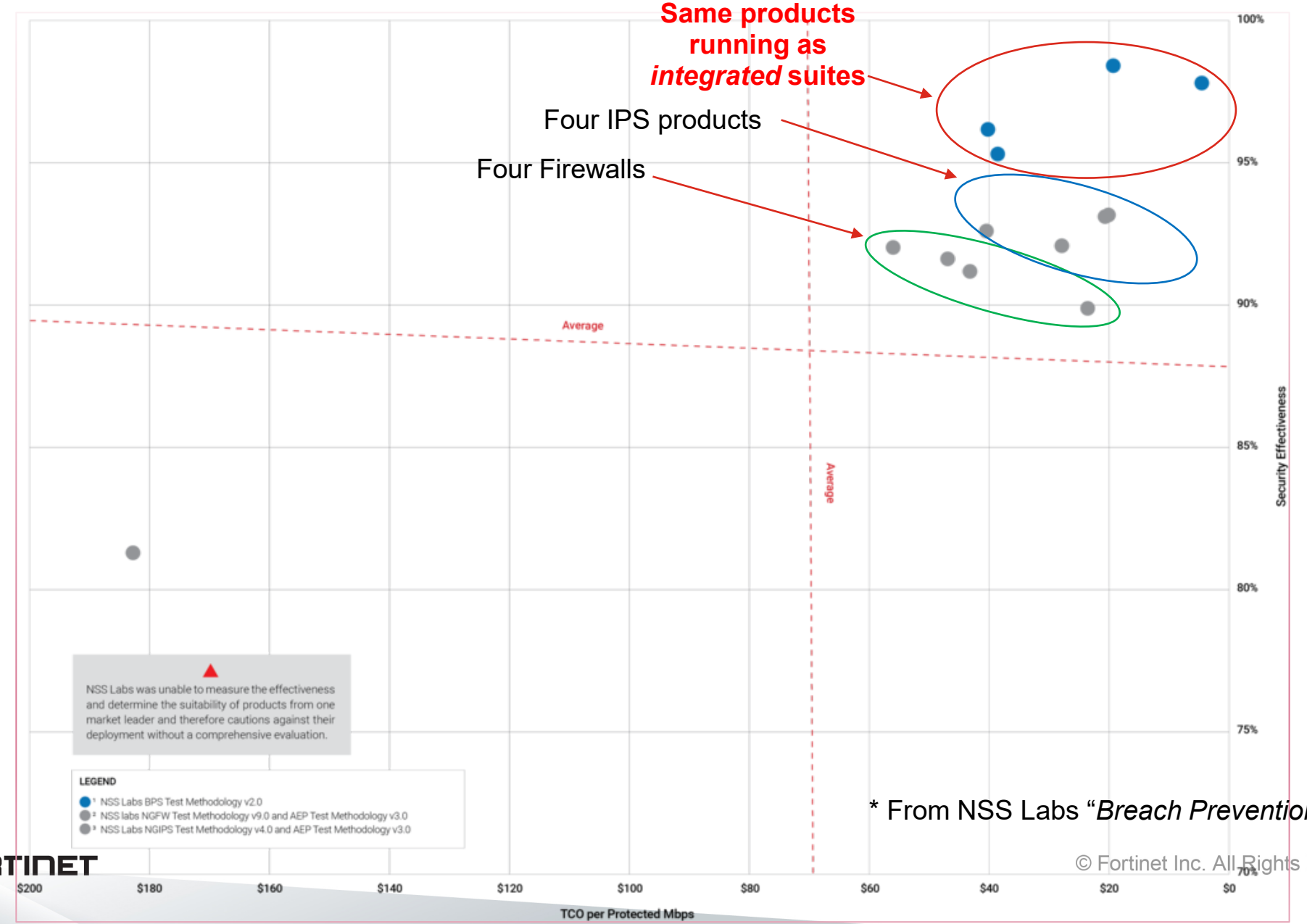
Because of:

- The growing attack or vulnerability surface of networks
- The workforce shortage (size and skills)
- Data and solution overload

**But *what if* you instrument the key parts of the digital surface** with devices that are both sensors and control devices?

- i.e., **produce a security platform or fabric**

# Independent Validation* of the Effectiveness of this Approach




* From NSS Labs "*Breach Prevention Systems*" test August 2019

# We are on the Cusp of a Revolution in Capability…

Driven by this **convergence** between **unified technology platforms** *(the source of sensor and controls)* and **AI/ML** (*decision engine*)

- Has the potential to **take away attacker's advantages** of stealth & speed
- **Big Data** is the 'fuel' and defenders typically have more than attackers
- Defenders benefit from **insight** gleaned from activity **against other targets**
- **Enables automation** that can offset the workforce/skills shortage
- ***Visibility*** and ***control*** and **speed/scale** enable dynamic/granular Zero Trust

# Recommendation: ***Add a 'third P' to Purchase Criteria***

## In addition to **Performance** and **Price**, consider **Platform** affiliation

- Products unified in a common platform typically outperform even 'best in class' non-integrated solutions
- Not all platforms are equal in coverage, power, or openness
- Splitting investment across platform families does not increase defense in depth, it minimizes synergy
- ***Not all solutions need to come from a single vendor to reap the benefits of platform integration and performance***

# We face a continued period of Transition and Hybrid Activity

- Further expansion of hybrid work patterns and locations
- Continued growth in hybrid modes of delivery of customer/citizen-services, use of OT and RPA
- Hybridization of the threats we face
- What does this mean for IT and Security architectures?

## And What Can Government Organizations Do In Response?

# Organizations are Coping with this Dynamic by "Spending Smarter"

***…but what does that mean in practice?***

- Look to ***lessons learned from others***
- Leverage the ***platform approach*** to cybersecurity
- Develop and leverage ***trusted partnerships***

# Learning from the Experiences of others

*There is no 'free lunch' – Improvement will require increased spending*

***61% of firms surveyed planned to increase IT spending***

- *Focused on enhancing resilience via more bandwidth & staff, more flexible architectures (esp. Cloud, Software Defined Networking)*
- *Hiring priorities: security architects, network engineers, developers*

***66% plan to raise security budgets***

- *Top focus areas: Secure Remote Access, Zero Trust*
- *Increase in outsourcing' of complex functions (e.g., SOAR, advanced SIEM, SOC-as-a-Service)*

# Modernization: an *Opportunity* to Accelerate Digital Transformation

Leverage increased **automation and efficiency** of offerings in key areas such as Software-Defined Networking and Cloud services

- Software Defined Networking (e.g., SD WAN) offers greater bandwidth, is cheaper, more flexible, and can provide a better user experience

- Government-validated guidance and best practices are emerging in key areas (e.g, CISA Cloud Security Technical Reference Architecture) and apply across cloud environments (types and number)

**"Bake in" security** by looking for *dual use or multi-purpose* IT options where security is an *integral* function

- e.g., Secure SD WAN: Multi-purpose products are not only more cost-effective, they are often more advanced in *each* discrete capability

# Recommendation: Partnerships Matter!
## …'Going it alone' is not an Attractive Option

Develop and use ***trusted*** **partnerships**

- Find **strategic advisors**/thought leaders
- Optimize your consumption of **cyber threat intelligence**
- Leverage **high performing technology partners**
  - Don't re-invent the wheel!

# Measuring Cyber Performance

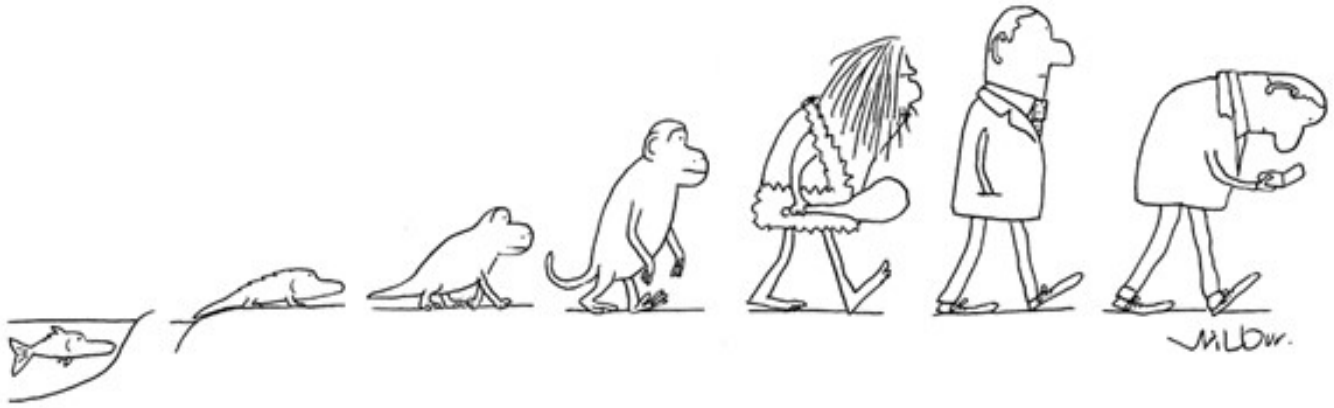
Why do we do Cybersecurity?

Why do we measure Cybersecurity?

*What does the term "Cyber Metrics" even mean?*

In my opinion **Metrics** are the Achilles Heel of Cybersecurity

# My 15 year Evolution in Measuring Cybersecurity Performance



**Seven stages of Cyber Measurement:**

1. **INPUT**: how many resources?

   ***(*Measures: *what did I spend?)***

2. **OUTPUT**: cyber goods and services

   ***(*Measures*: what did I get?)***

3. **OUTCOME**: simple (one dimension)
4. **OUTCOME**: multi-dimensional (time!)

***(*Measures *or* metrics: *what did it do?)***

5. **IMPACT**: on *information*
6. **IMPACT**: on the *organization*
7. **IMPACT**: on *Risk* Management

***(*Metrics*: what difference did it make?)***

# Final Thoughts

SSA's IT Modernization Plan Provides an Opportunity to:

- Implement a consistent security design philosophy (e.g., platforms) to leverage automation and AI (efficiency and cost savings)
- Embrace functional consolidation of security and networking, prepare for continued technology change (5G, edge computing)
  - Software Defined Networking, securing Cloud operations ("SASE")
- Implement Zero Trust principles consistent with importance of SSA data ("crown jewels") and services
  - Need for "Full spectrum" (deterrence and defense)
  - Leverage Robotic Process and Intelligent Automation (start/stay small?)

# Questions?

Jrichberg@Fortinet.com