Enabling Digital Transformation
…a Personal Perspective

Jim Richberg
Head of Cyber Policy and Global Field CISO

March 2025

Agenda

Why me?

Level setting

My guiding principles

© Fortinet Inc. All Rights Reserved.

Why me?

33 years in the US Federal government…

- Oversaw whole-of-government cyber initiatives for two Presidents
- National Intelligence Manager for Cyber, setting priorities and cyber strategy for the 100,000 employees and 17 agencies of the US Intelligence Community
- Ran cyber operations and national threat intelligence analysis
- Supported national incident response, worked with private sector and international partners

6 years with Fortinet working with government and the private sector globally

During my years in government, I developed 'rules of thumb' for driving technology change that I refined during my time in the private sector

© Fortinet Inc. All Rights Reserved.

Level setting is invaluable:
Creating a common/shared understanding of goals

For example:

Cyber **resilience** is the ability to ***anticipate***, ***withstand***, ***recover*** from, and ***adapt*** to adverse conditions, stresses, attacks, or compromises

(source is US National Institute of Standards and Technology SP 800-172)

Other relevant forms of digital resilience in the public sector include:

- **Supply chain** for information and communications technology
- **Military** digital resilience
- **Cognitive** resilience against Mis, Dis, and Mal-information

Resiliency is intended to enable achievement of mission or business objectives that depend on these resources *(i.e., is a means to an end)*

The same applies to technology transformation

© Fortinet Inc. All Rights Reserved.

My Guiding Principles or Rules of Thumb for Supporting Transformation

1. When *everything* matters, start with the areas you are *responsible for*
2. Try to identify the *key questions* within those areas
3. Stay abreast of technology
4. Stay abreast of threat
5. Good solutions are multi-*function*, *great* ones are multi-*purpose*
6. Procurement is both an underappreciated *vulnerability* and a *lever*
7. The biggest problem is often metrics, not “people, process, or technology”

© Fortinet Inc. All Rights Reserved.

#1 Where to start…?

When *everything* matters, start with the areas you are responsible for *(or will be held accountable for when something goes wrong!)*

e.g., if you are accountable for resilience, what criteria are you judged by

- Demonstrable impact on continuity of operations when things go wrong (including non-cyber events)?
- Cost and efficiency?
- Other?

Regulation increasingly sets requirements or expectations and drives solutions (EU's DORA)

- The risk is of 'checking compliance boxes' vs. delivering actual impact

© Fortinet Inc. All Rights Reserved.

#2 Try to identify the key or core questions

- Within these areas of responsibility, try to find the key questions
  - For example– as governments wrestle with GenAI, the key questions are about supply and security, not solutions, i.e., it is not about *how should government use GenAI* but rather *how can it enable use* given energy/power constraints? And how can government drive greater security of AI use?
- How can you step back and find these key questions?
  - For example, in a world of cyber 'villains, victims, vendors, and visionaries' *how do you find the visionaries*?
    - Peers or trusted advisors
    - Blogs or newsfeeds
    - other…?
    - *Conscious and continuous investigation*

© Fortinet Inc. All Rights Reserved.

#3 Understand key technology trends…

1. ***Follow*** *where you* ***<u>can</u>***
2. ***Lead*** *where you* ***<u>must</u>***
3. ***<u>Don't</u> work against trends*** *without a compelling reason!*

Exemplar technology trends and capabilities:

- Cloud for data storage and processing, software, services (Xaas)
- Software Defined Networking (e.g. SD WAN)
- Edge computing (IoT and IIoT)
- High impact security-specific trends (e.g., Mesh Architectures ecosystems)
- Convergence of networking and security (e.g., SASE)
- GenAI for knowledge-focused problems
- *AI-powered automation*

© Fortinet Inc. All Rights Reserved.

#4 Continuous requirements and solutions against threats

Prepare for Advanced Persistent Threat (APT) actors who:

- Follow the weakest link by preference (unpatched vulnerabilities) but can deploy novel exploits (zero days)
- Are patient (move ‘low and slow’)
- Use ‘living off the land techniques’ (legitimate tools already on targets)
- Target civilian critical infrastructure along with government networks

Cyber due diligence for Critical Infrastructure includes

- Strong identity management and access control, network segmentation
- Ensuring that your security tools are *‘fit for purpose’*
- Leveraging *diversity* of defenses and sensors
- *Create and practice* contingency plans

Cyber Threat Intelligence is vital, it comes from many sources, and it may be curated/enriched in-house

Preparing for APT actors positions you to handle other cyber threats as well

© Fortinet Inc. All Rights Reserved.

#5 Good solutions are multi-function… great ones are multi-purpose

Good security solutions solve *multiple security problems*, are *cost-effective* and *high impact*

- **Replacement products** (e.g., Next Gen Firewalls) that are not only more powerful but can perform functions of multiple legacy security product types
- **Deception technology**—deters, degrades, discovers multiple types of threat (nation state, criminal, insider)

Great cyber solutions are also positioned to address non-cyber problems

- Security **products** that enhance networking, user experience, mission resilience, provide cost savings, etc.
- Security **concepts** presented from a *mission-enhancing* perspective, e.g., Zero Trust as expanding secure connectivity options between users, devices, data, and compute resources regardless of location

© Fortinet Inc. All Rights Reserved.

#6 Procurement is both a vulnerability and a lever

- Security controls are often a weakness in project specification and execution (esp. public sector infrastructure)
- Procurement requirements can be a powerful driver of change
  - Government mandated frameworks such as software and hardware Bills of Materials or the Secure Software Development Framework (SSDF)
- Look at voluntary approaches such as “Secure by Design” (SbD)

© Fortinet Inc. All Rights Reserved.

This was operationalized in ‘Secure by Design” white papers with Canadian input

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC
National Cyber Security Centre
OAS
NISC
CSA SINGAPORE
certnz
NSM NORWEGIAN NATIONAL CYBER SECURITY CENTRE
National Cyber and Information Security Agency
KISA KOREA INTERNET & SECURITY AGENCY
JPCERT CC®

© Fortinet Inc. All Rights Reserved.

#7: Metrics—the biggest problem (IMO) in Cybersecurity

We often measure to answer one of three cyber questions

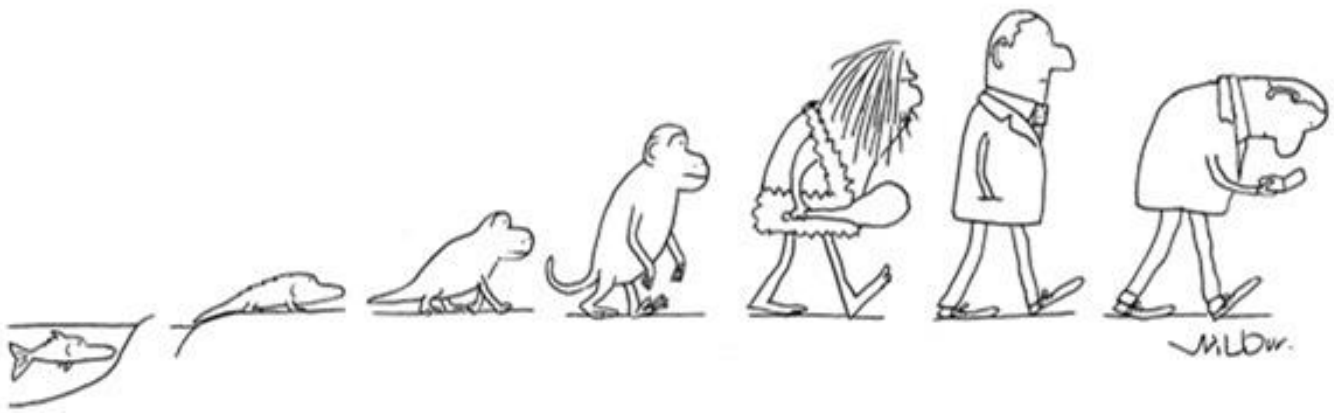
1. ***How am I doing?*** *(benchmarking)*
2. ***How can I prove it?*** *(compliance)*
3. ***How can I do better?*** *(gap analysis/sensitivity testing)*

Paradoxically, for a field that is inherently quantitative, we are hobbled by inadequate metrics. We are challenged to demonstrate:

- What works?
- What doesn't work—and why?
- What is the ROI?
- What should we do next?

© Fortinet Inc. All Rights Reserved.

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?)

© Fortinet Inc. All Rights Reserved.

Wrap up – *"The hard stuff is the soft stuff"*

We are drowning in technological change and new tools…
e.g., operational resilience enablers such as CEM, CLM, CM, DSP, GRC, and TPRM

In my opinion, *mindset* is more important than technical *mastery* in managing this change…

- When *everything* is important start with the areas you are *responsible for*
- Try to identify and focus on the *key questions* within those areas
- Stay abreast of technology and threat
- Think multi-dimensionally: good solutions are multi-*function*, great ones are multi-*purpose*
- Procurement is both part of the problem and a tool for public sector-driven change
- Having clear goals and measures of progress is often a greater problem that keeping up with technology

© Fortinet Inc. All Rights Reserved.

Thank you!

Jrichberg@Fortinet.com

or

Jim Richberg | LinkedIn

© Fortinet Inc. All Rights Reserved.


FORTINET