
ATRION

Closing Keynote: Prevent Customers from Following the Herd

- Running existing IT security programs are complicated due to the active nature of threats and regulatory changes. Security-focused solution providers and MSPs must work closely on two fronts: starting a security program from scratch or take an existing one to a more mature level. Either path requires expanding existing services while meeting budget demands, protecting the organization and senior executives, and meeting the dynamic external pressures facing everyone. This session will focus on the following: the typical functions needed to meet threats and regulations within an information security program, how to examine these functions critically to reduce costs, and to stop customers from following the heard to create a unique strategy. The key to success is developing such a strategy that safely meets business objectives for solution provider customers or prospects.

CYBER AXIOMS

1. Technology **does not solve** the cyber problems businesses face today

2. Companies are managing more digital assets than they did a decade ago, and the value of these assets (Crown Jewels) is not realized

3. Corporate culture is fragmented and roles are ineffective

HORRIBLE CYBER ANALOGIES

1. “Networks are like candy bars: Hard and crunchy on the outside, but soft and gooey on the inside.”
2. “Two hikers in the woods and a hungry bear.”
3. “You don’t want to be the next XYZ do you?”
4. “Security controls are like a seat belt.”

FORGET THE HYPE

Does your company walk the talk

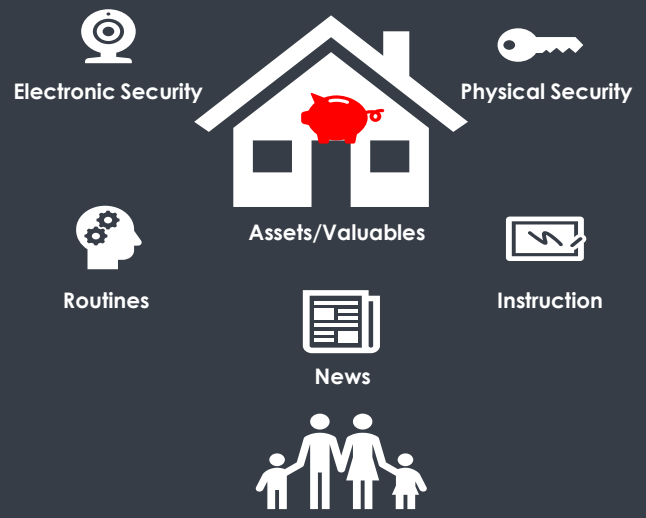
- Can your organization define cyber risks clearly?
- Do you know who is liable for a security incident, breach, or compliance failure?
- Don’t be bullied by FEAR (False Evidence Appearing Real) – Crying wolf

CYBER IS NOT MAGIC

T = Threats
V = Vulnerabilities
A = Assets

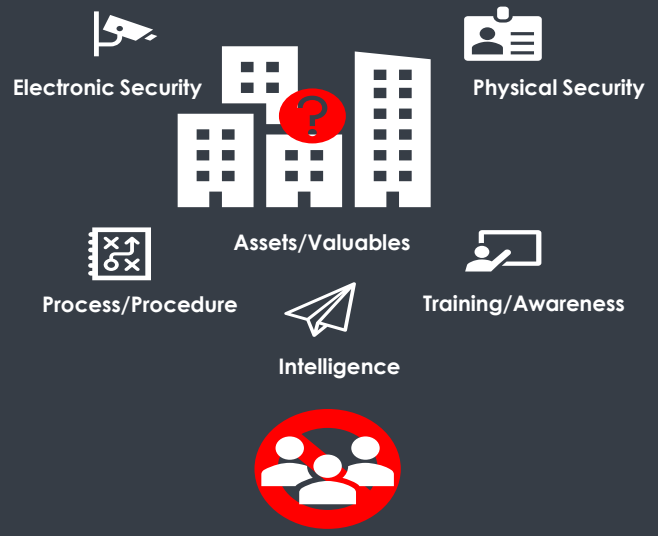
Home

1. Vested Interest in protecting valuables
2. Uses basic physical and electronic security measures
3. Routines are inherent/subconscious
4. We instruct everyone in the house how to keep it safe
5. News about others losses makes us improve our own security measures and is directed to a single source to make changes.



Organizations

1. Limited vested Interest in protecting assets and not sure what they are.
2. Uses sophisticated physical and electronic security measures
3. Routines become procedures and are formally documented
4. We attempt to train and make other aware of how to keep organization safe
5. Intelligence about threats and losses does not always find the right source due to how the information comes into the organization



Time

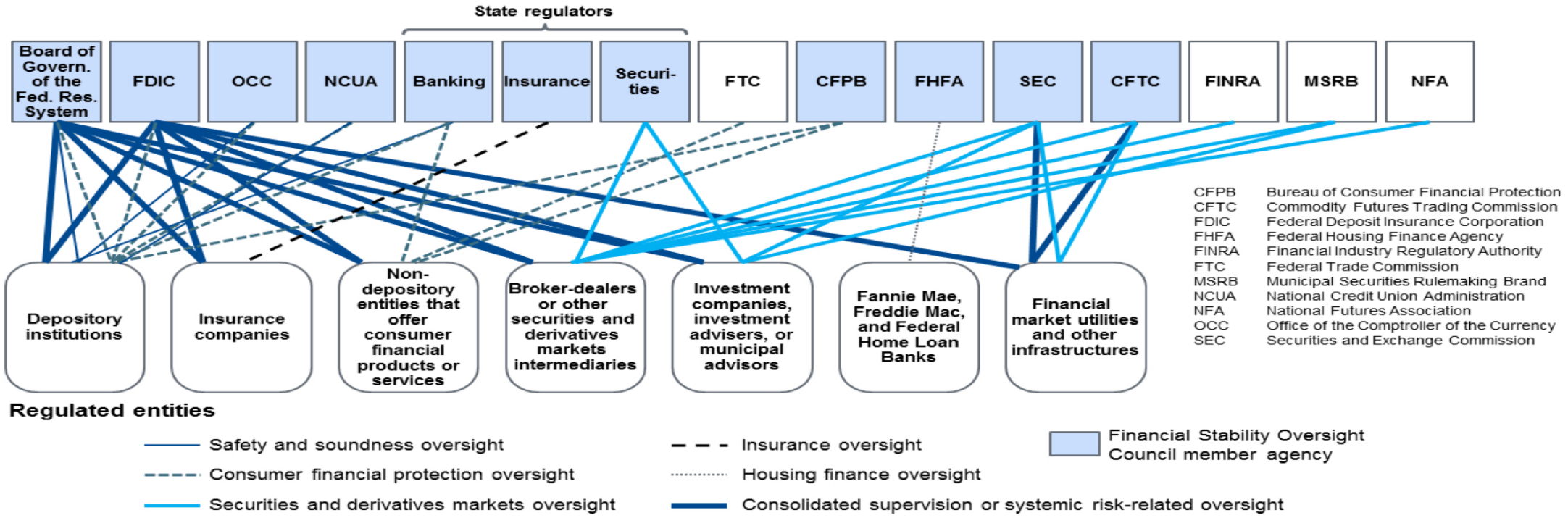
Security & Technology Executives tend to have a plethora of critical items on their minds. How can this be alleviated?

Cyber Hygiene

Transformational Business Objectives

The U.S. Financial Services Regulatory Structure (2017)

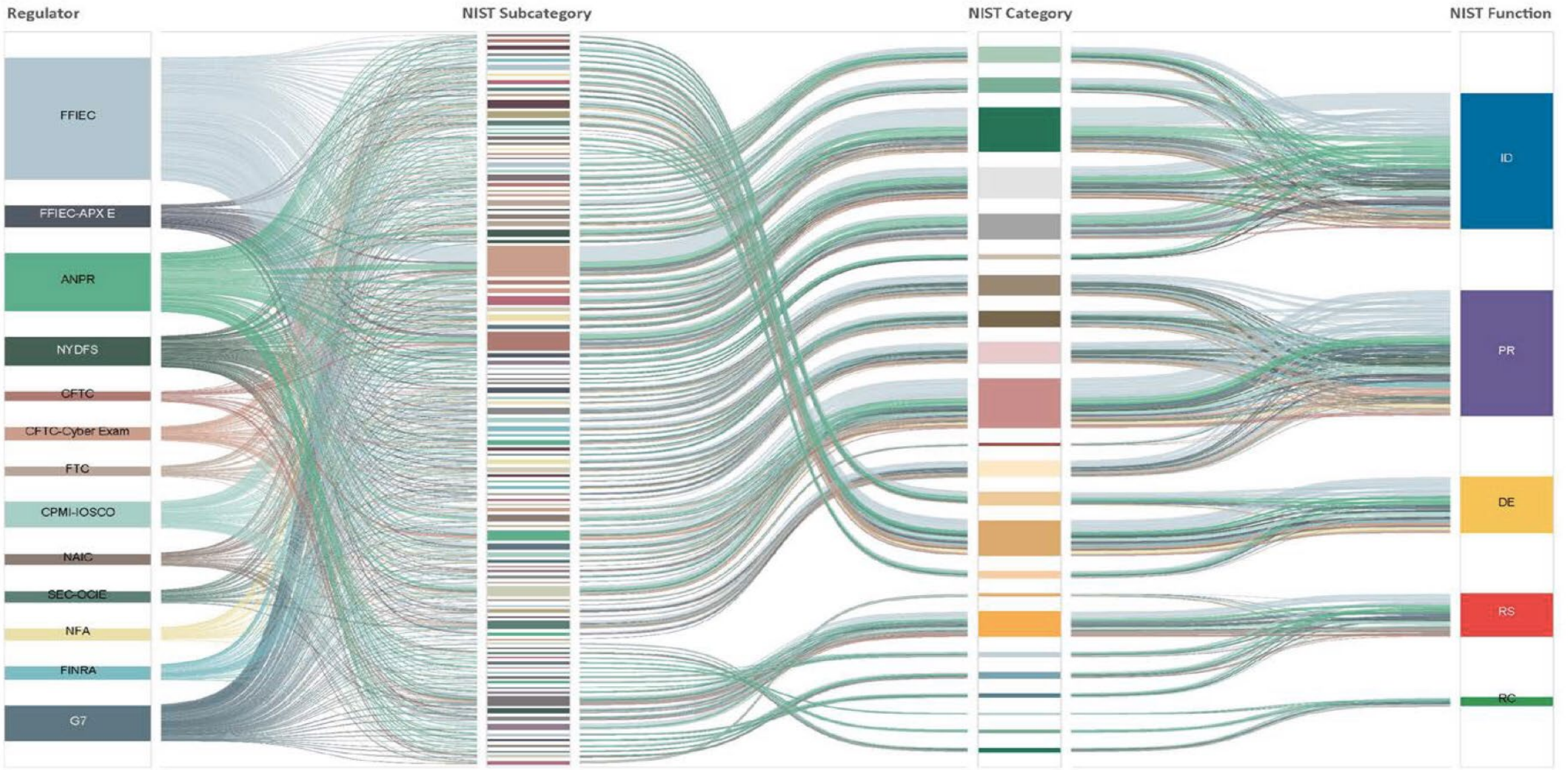
Federal and State Financial Services Regulatory and Oversight Agencies and Self-Regulatory Organi-zations



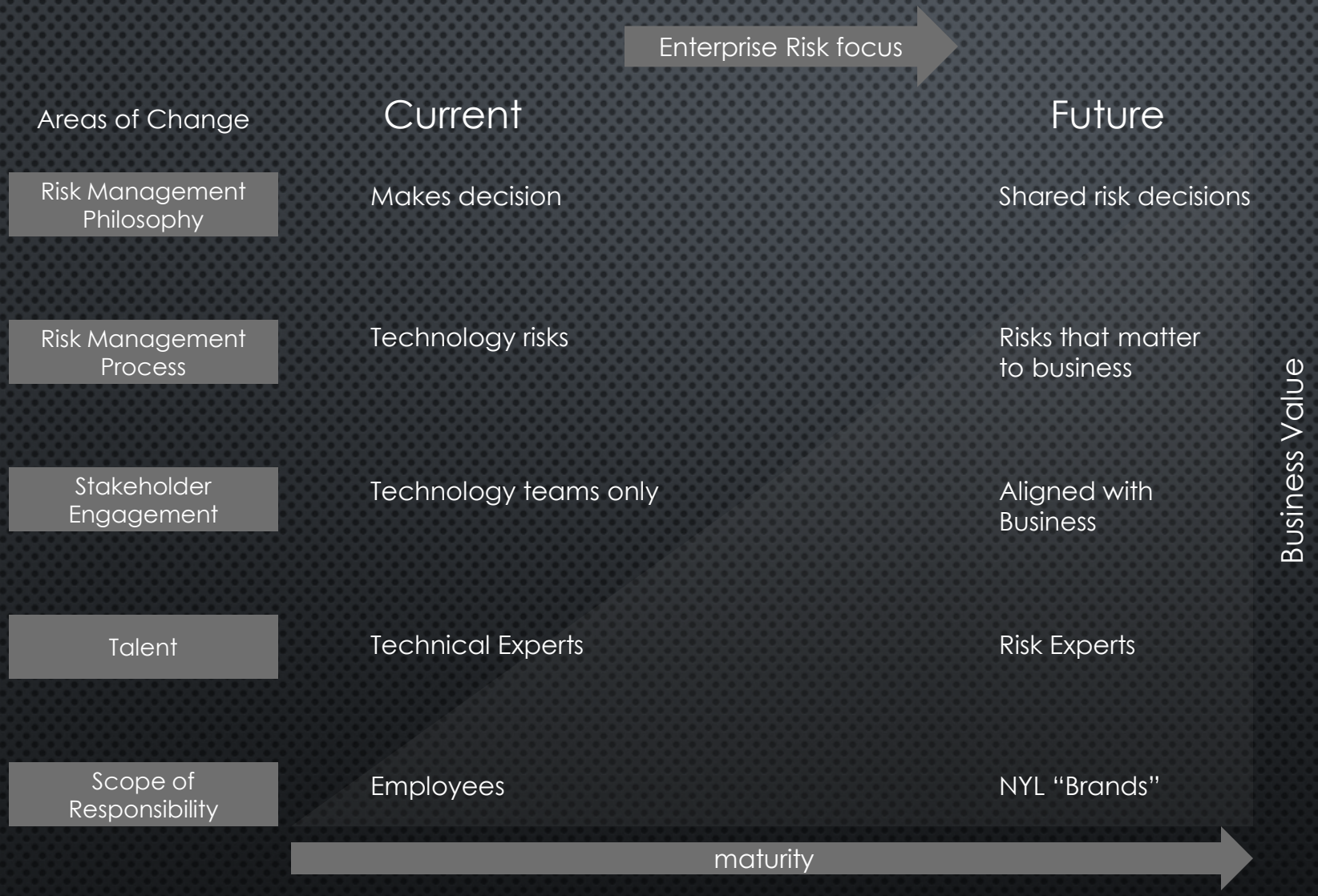
Additional Cyber Agencies

- White House (EOP, NSC/ NEC, OSTP)
- OMB
- U.S. Treasury (OFAC, FinCEN)
- DHS (ISAOs)
- Dept of Commerce (NIST, BIS)
- Federal Communications Commission
- Dept of State
- Law Enforcement Agencies (DOJ, USSS, FBI)

Note: The figure depicts the primary regulators in the US financial regulatory structure, as well as their primary oversight responsibilities. "Regulators" generally refers to entities that have rulemaking, supervisory, and enforcement authorities over financial institutions or entities. There are additional agencies involved in regulating the financial markets and there may be other possible regulatory connections than those depicted in this figure
Source: GAO; GAO-16-175


Regulator
NIST Subcategory
NIST Category
NIST Function
FFIEC
FFIEC-APX E
ANPR
NYDFS
CFTC
CFTC-Cyber Exam
FTC
CPMI-IOSCO
NAIC
SEC-OCIE
NFA
FINRA
G7
ID
PR
DE
RS
RC

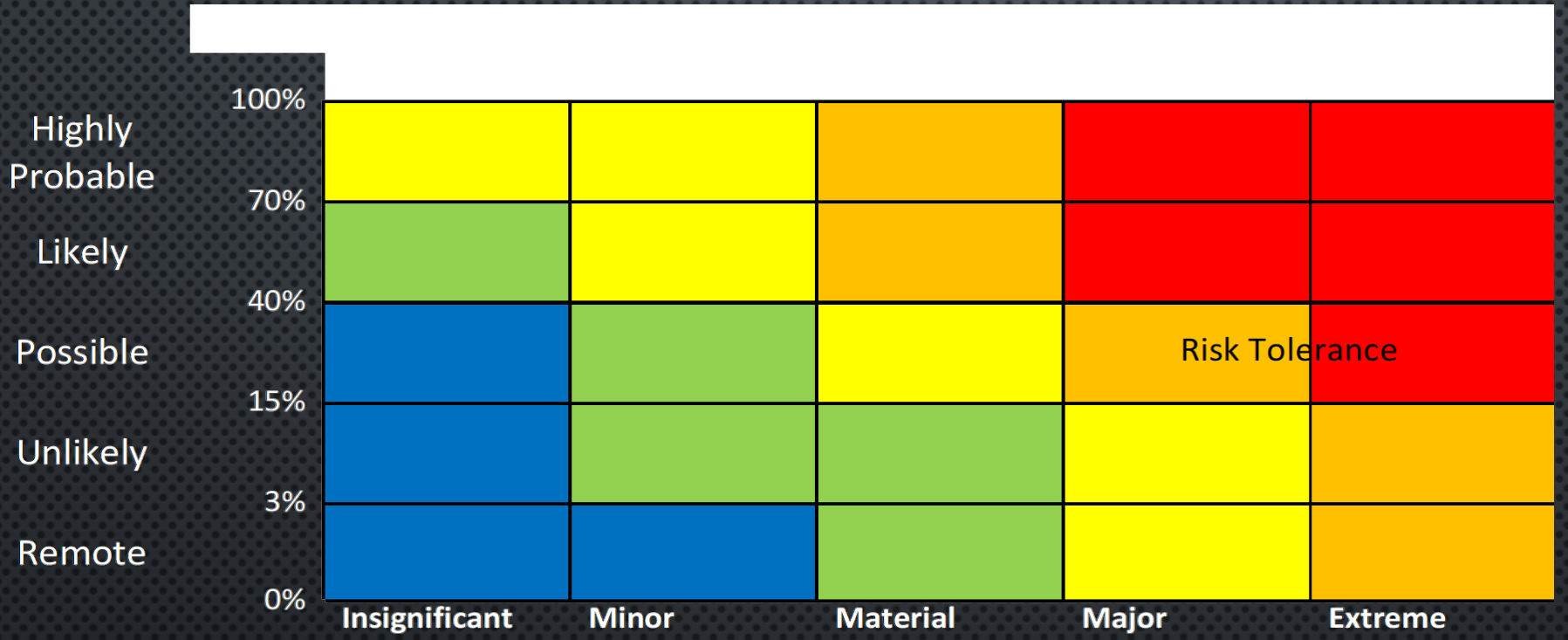
CHANGING THE VALUE



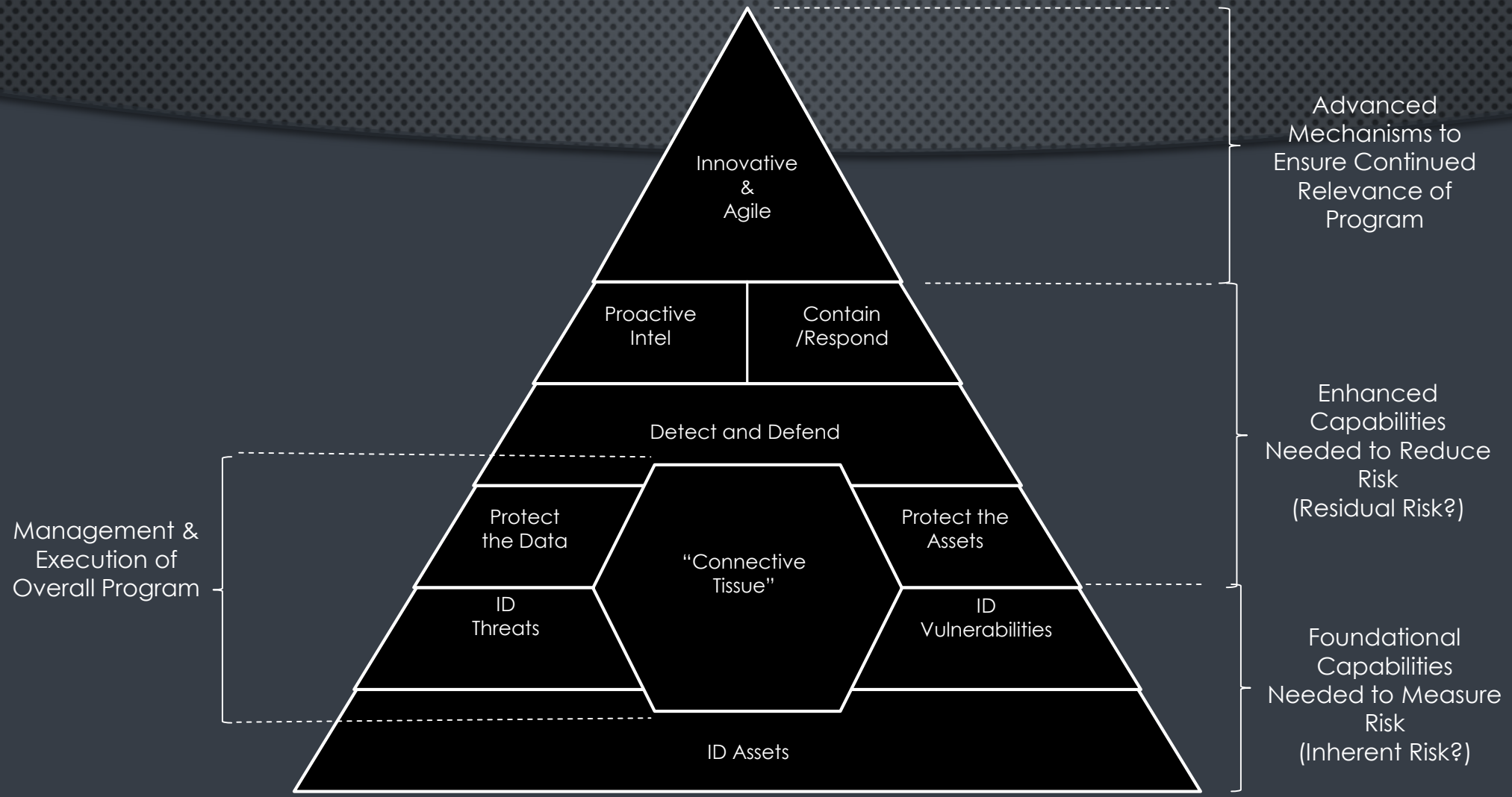
TALK BUSINESS RISK

Consequences

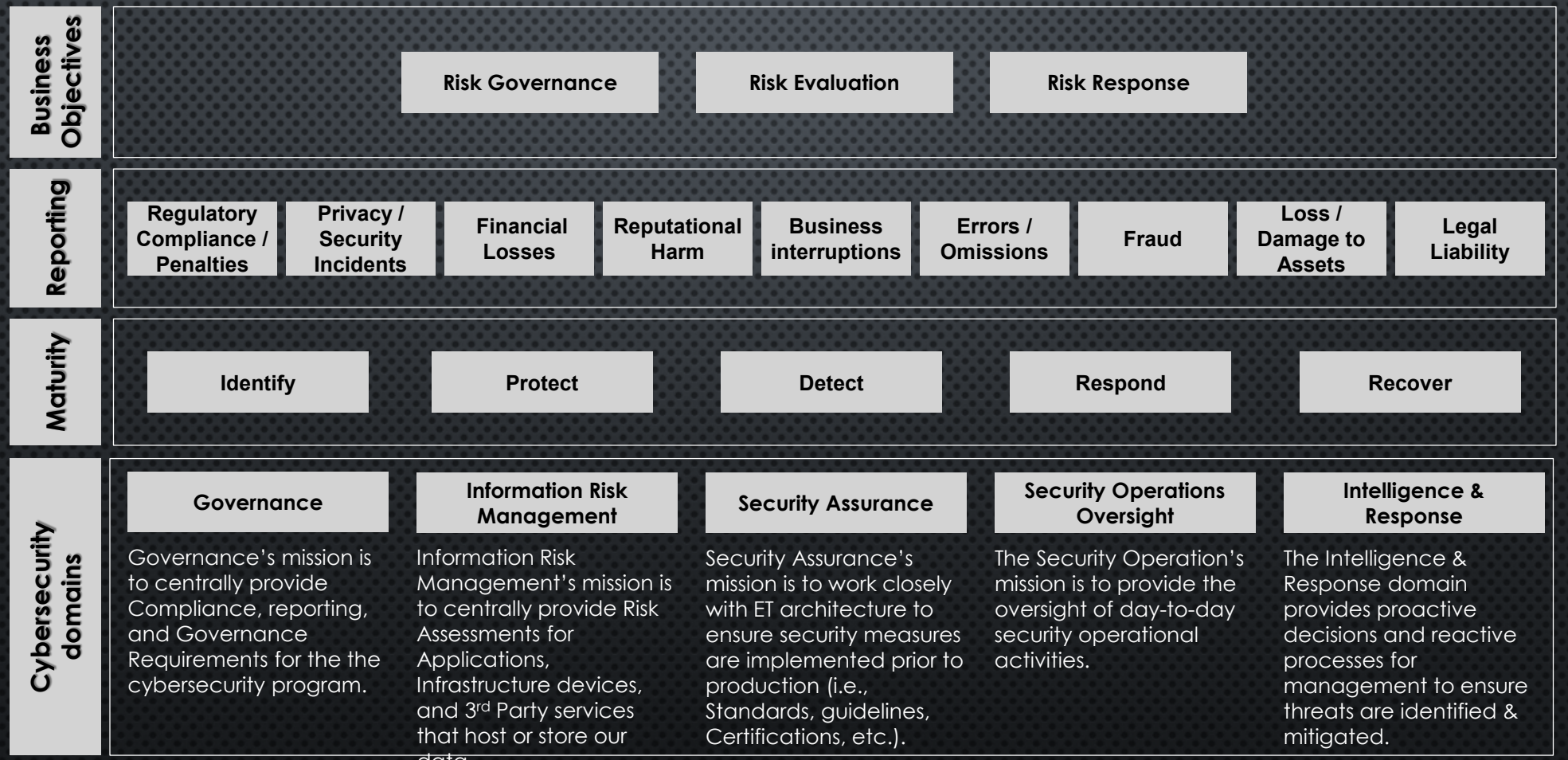
THE DEPRIVED VALUE



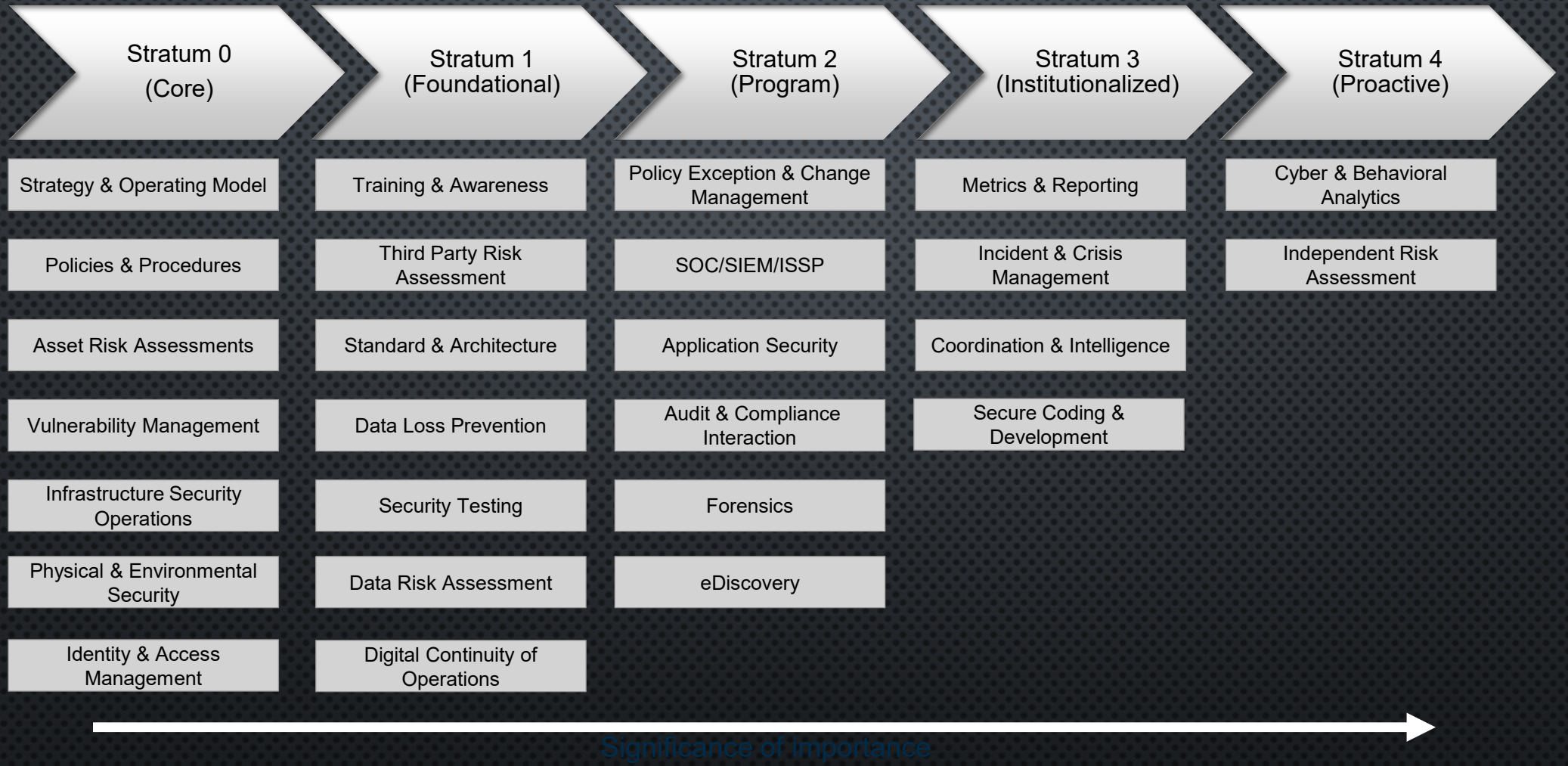
Score	Level	Financial Loss %	Statutory Capital Loss %
0	No impact	No Impact	No Impact
1	Insignificant	<2% Annual Earnings	<1%
2	Minor	1-5% Annual Earnings	1-5%
3	Material	5-15% Annual Earnings	5-10%
4	Major	15-100% Annual Earnings	10% up to amount of Free Surplus
5	Extreme	>100% Annual Earnings	Amount Exceeding Free Surplus


Innovative
&
Agile
Proactive
Intel
Contain
/Respond
Detect and Defend
Protect
the Data
"Connective
Tissue"
Protect the
Assets
ID
Threats
ID
Vulnerabilities
ID Assets
Management &
Execution of
Overall Program
Advanced
Mechanisms to
Ensure Continued
Relevance of
Program
Enhanced
Capabilities
Needed to Reduce
Risk
(Residual Risk?)
Foundational
Capabilities
Needed to Measure
Risk
(Inherent Risk?)

Designing an operationally focused program of service offerings to assist organizations in the transformation process of their organization's cybersecurity program and to facilitate an effective integration into the company's overall enterprise risk management functions, as well as to assist in identifying and closing existing gaps in their cyber risk oversight. Gives business the ability to make decisions regarding the maturity and effectiveness of their program.



CYBERSECURITY PROGRAM CAPABILITY MATURITY



*Note: Capabilities can reside in either 1st Line or 2nd Line (2nd Line view preferred).
Additionally, capabilities may depend on risk appetites and/or size of company/geography

Talent

RISK; POLICY; STRATEGY; TRAINING & AWARENESS

THREAT & VULNERABILITY MANAGEMENT

PROVISIONING

SOLUTION OPERATIONS

SOLUTION DEVELOPMENT

Last thoughts on final solutions

1. Improve and stabilize

   Provide a technology environment that is consistent, agile, reliable, secure, compliant, high performing, easy to use and sustainable (either directly or indirectly)

2. Reduce exposure to privacy breaches

   Optimized minimum baseline controls, technology, awareness, processes, clear obligatory contractual terms, and monitoring (prevent/detect/respond/recover)

3. Expand capability

   Enable agencies and field force to be resilient to unforeseen events (Crisis, BCP, DR) – access data from anywhere/any device

4. Collaborate and Partner for Sustainability

   Implement cross functional team across business, IT, and corporate assurance areas to prioritize, monitor, and maintain compliance in alignment with appetite/tolerance

CONCLUSION

Don’t “FEAR” the cyber black-box

Need a senior executive to effectively speak with Board or Senior Management about cyber

Need a security program that interacts with Technology and Business

Contact Information

Richard Moore
800-601-0563
rmoore@nthnet.net