

VIEW FROM THE CISO - DEMONSTRATING WINS

Michael Doucet

Executive Director, Office of the CISO

Michael.doucet@Optiv.com

(613)899-7169



Agenda

- ❖ Complexity in our Environment
- ❖ Changing Perspective
- ❖ Cyber Program Goals
- ❖ Six Forces of Security Strategy Influencers
- ❖ Security Domains
- ❖ **Optimized Security Program**
- ❖ Wrap up

COMPLEXITY

Billions of
Threats and
Vulnerabilities

100's of
Regulations
and Standards

2,500+ Security
Technology
Vendors

SECURITY PROGRAM

- Business aligned
- Right sized for the organization
- Prioritized
- Never completed



This is

THE CISO CONUNDRUM



“As a CISO, you have a choice: **either become the strategy guy, or the scapegoat.**”

*I’m criticized by execs as the guy who always says “no.” **How do I become the guy who says “yes”?***

*My CapEx costs are too high, due to investments in **products that are ineffective or never deployed.***

*There are **too many opinions**, too much information, too many experts and too little time. Everyone keeps telling me how many “things” they have – researchers, endpoints, found attacks. But none of that helps me with my problem.*

+ THE CISO CONCERNS

“This year, more than ever, I need to step back, take inventory and rationalize what we have, what’s working and what’s not. I need to focus on optimizing our current environment.”

*My CFO continues to ask me to show them the **measures and metrics** proving we are safe with the investments we have made. The vendors won’t do this.*

*“I have 17 Security agents deployed on our Desktop. **I know I don’t need all of these**, but who do I trust to guide to which are needed and which are redundant?”*

*25 – 30% of everything I have bought has not yet been deployed. **Do I even need it?** The Vendor pitch on the problem and the solution seemed to make sense?*



+ THE CISO CHALLENGES

Back to Basics

Inventory

Rationalize

Optimize

Demonstrate



CHANGING PERSPECTIVE

The perimeter no longer exists

Security purview must widen to meet the challenge

The path forward is unique for every business

Frameworks and blueprints can be used **but must be tailored**

There is an embarrassment of riches in technology

Technology must be mindfully selected and integrated for a proven purpose

Cyber Program goals



Align Security Initiatives with Your Business Goals



Determine specific threats against your organization. Identify requirements to elevate your defense and response



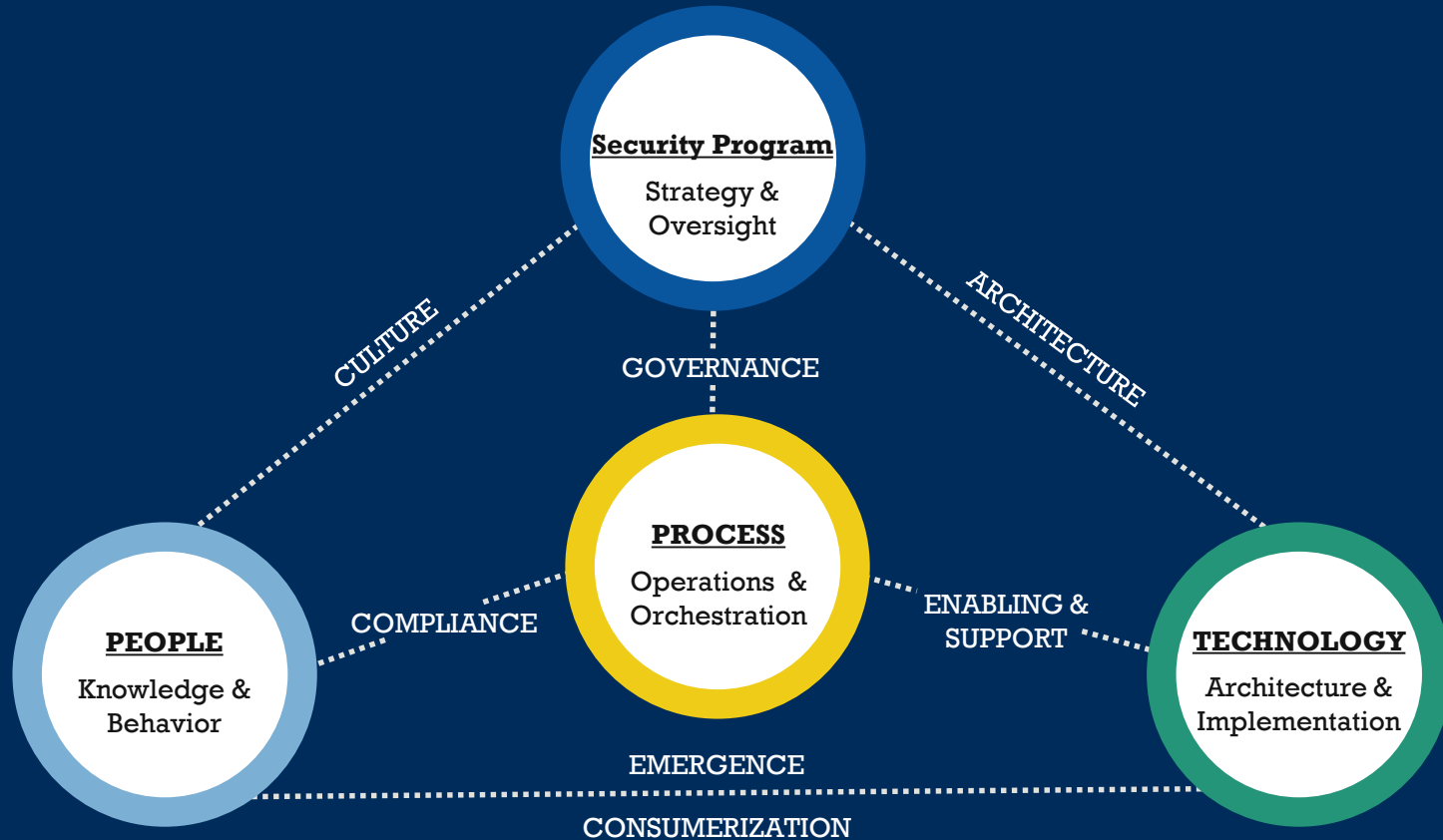
Map Controls in Place to Protect Your Business



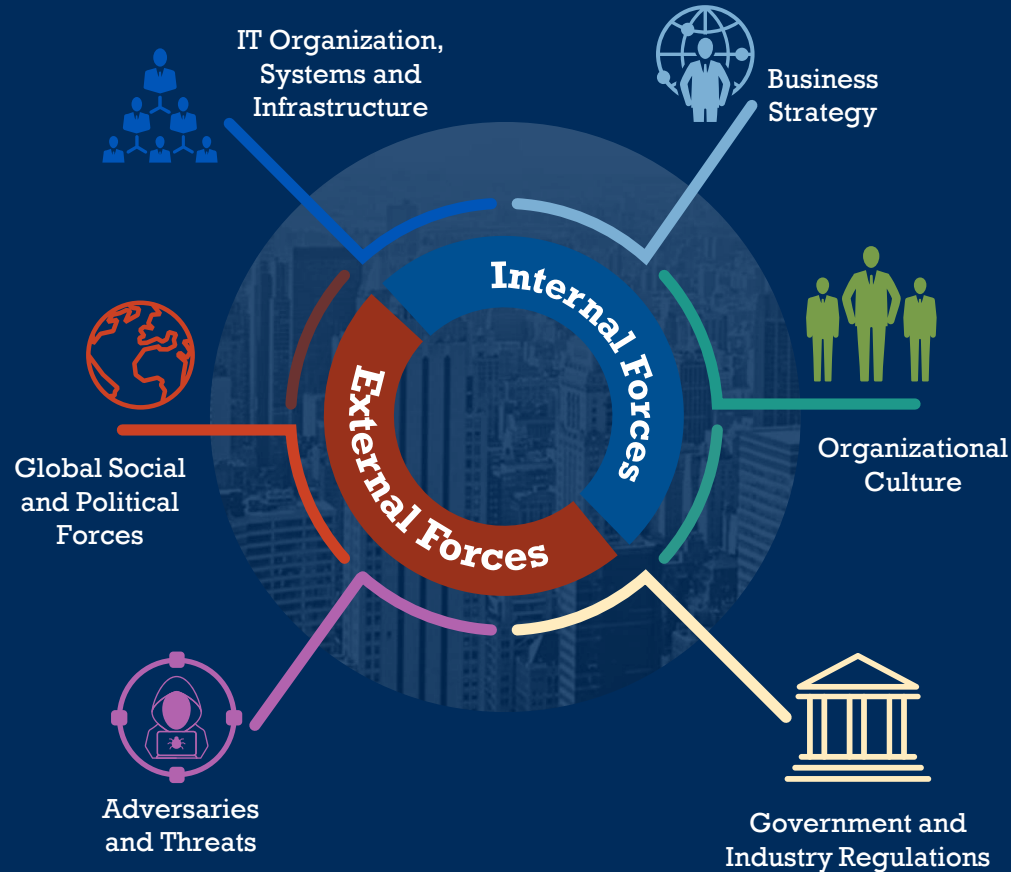
Build a Business Aligned Security Program



Business Model of Information Security



Six Forces of Security: Security Influencers



SECURITY DOMAINS

RISK MANAGEMENT AND TRANSFORMATION

Privacy and Governance

Cyber Resilience

Risk Optimization

Cyber Assurance

CYBER DIGITAL TRANSFORMATION

Cloud Security

Product Security

Analytics/Big Data

Orchestration and
Automation

THREAT MANAGEMENT

Secure Infrastructure

Adversarial Emulation
(Exposure Mgmt)

Threat Detection
and Response

CYBER OPERATIONS

Intelligence Operations

Cyber-as-a-Service

Advanced Fusion Center
Operations (MDR)

Managed Security Services
(MSS)

Cyber Authorized
Support Services

IDENTITY AND DATA MANAGEMENT

Identity Governance

Access Management

Data Governance
and Protection

INTEGRATION AND INNOVATION

Applied Research

Design Innovation Services

Integration Services



The security program is aligned with the business



The members of the security team believed they were valuable to the organization and had an impact



The security program made progress over time in its risk mitigation goals and strategy


WHAT DOES IT MEAN TO BE “OPTIMIZED”?



Board of Director and executive leadership interaction with the security leader



The executives of the organization saw value in the security program



Technology was one part of many components of the security program

OPTIMIZED PROGRAMS



Single, Identifiable, **Executive Sponsor** or Advocate



Develop a **Risk Steering Committee**



Leverage a **Control Framework**



Targeted **High Maturity** in Some Controls



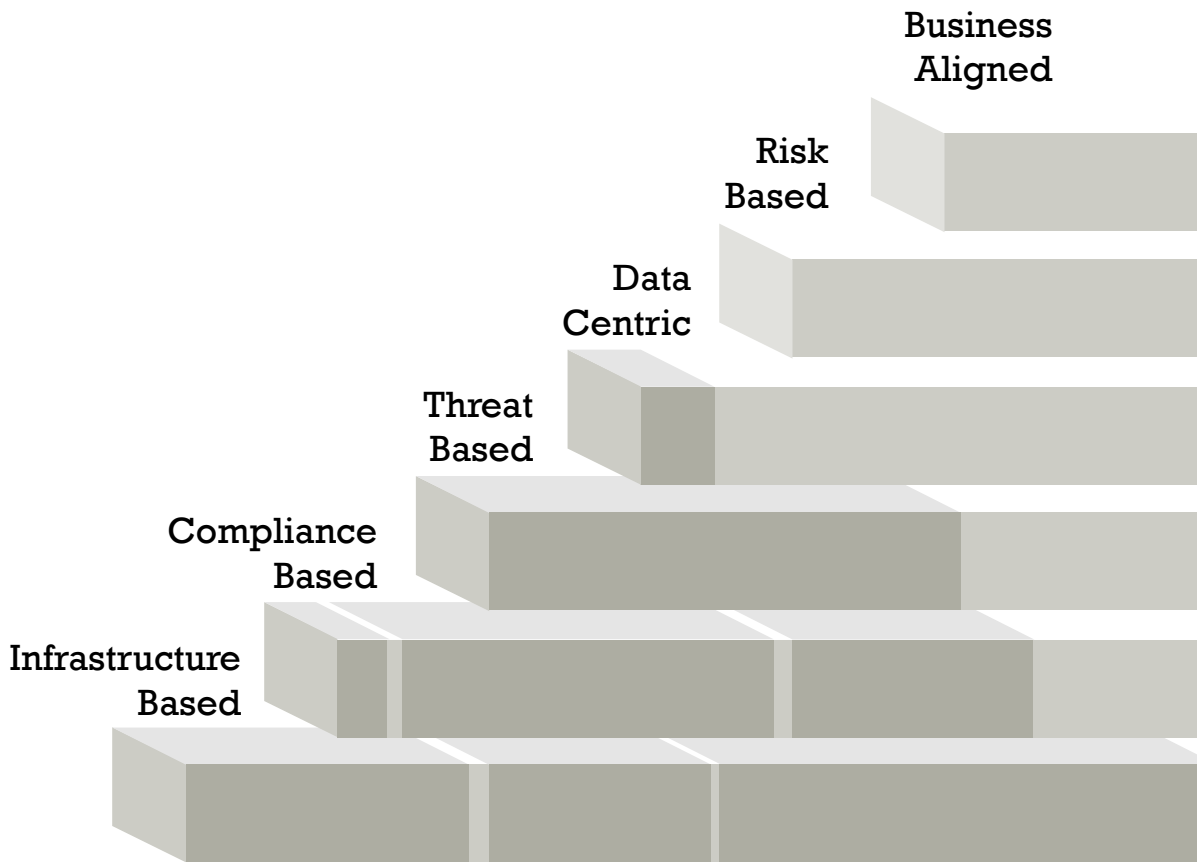
Thoughtful Deployment of Technology



Work with **Great People**



**THIS IS A
JOURNEY**

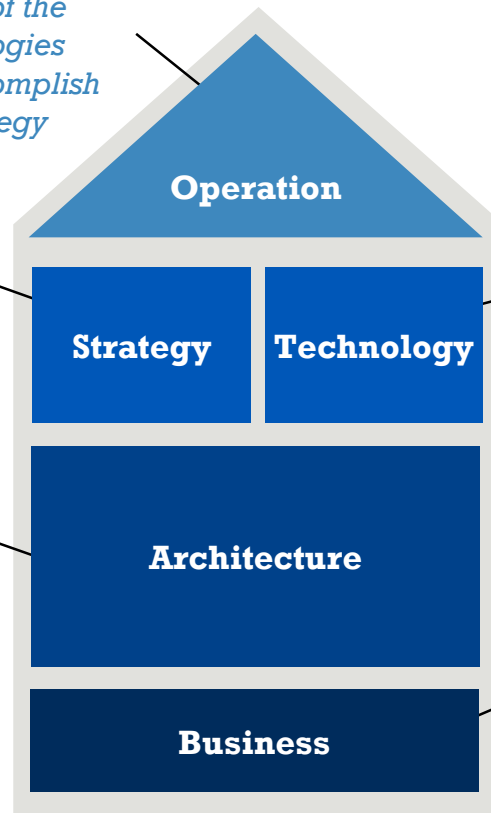


WITH THE RIGHT BUILDING BLOCKS

The day-to-day of the security technologies deployed to accomplish the security strategy

protecting the business from threats

security controls designed to accomplish the security strategy

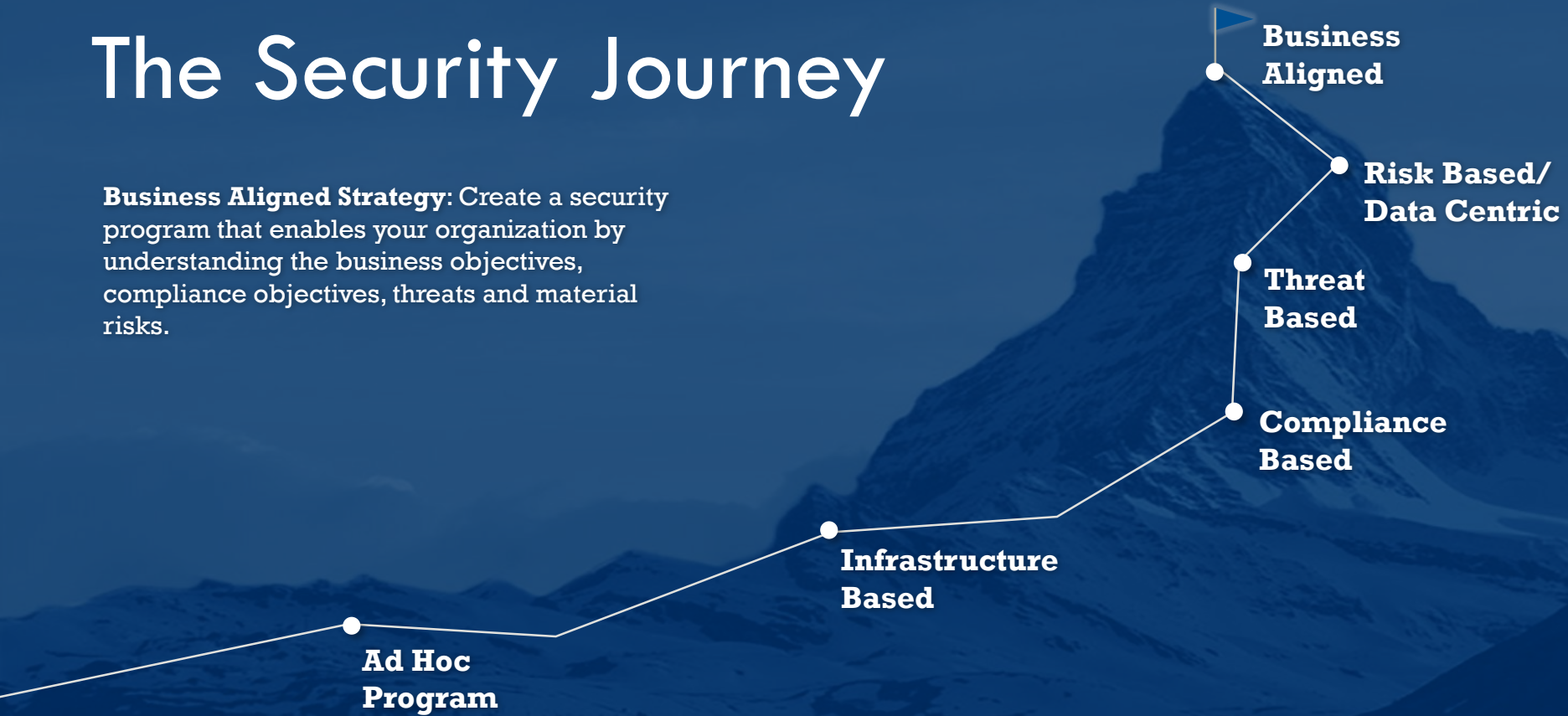


employed by the business to accomplish its goals

what industry, and how it operates

The Security Journey

Business Aligned Strategy: Create a security program that enables your organization by understanding the business objectives, compliance objectives, threats and material risks.



In Conclusion...how good are we?

- ❖ Complexity in our Environment
- ❖ Changing Perspective
- ❖ Cyber Program Goals
- ❖ Six Forces of Security Strategy Influencers
- ❖ Security Domains
- ❖ **Optimized Security Program**
- ❖ Wrap up

VIEW FROM THE CISO - DEMONSTRATING WINS

Michael Doucet

Executive Director, Office of the CISO

Michael.doucet@Optiv.com



CHANGING PERSPECTIVE

OUTCOME TARGETED

“Inside-Out”

The path forward is
unique for every
business

There is an
embarrassment of
riches in technology

Security purview must widen
to meet business needs and
outcomes

Frameworks and blueprints can
be used **but must be tailored**

Technology must be mindfully
selected and integrated for a
proven purpose