Life is rough for a security leader! The security product landscape is increasingly complicated but seems to always lag behind malicious actor capabilities. Organizations need proven security programs that demonstrate visible ROI, but once-vaulted security concepts have been sacrificed upon the altars of speed and mobility. Organizational leadership-level involvement has never been greater, offering access to increased funding but greatly complicating risk tolerance, needed capabilities, and desired levels of maturity in action. How can we not only maintain our capabilities but evolve them to address the in-flight needs of the business? In this session we will discuss current risk transformation needs, addressing topics such as the ongoing evolution of privacy and governance obligations, the definition of control activities that combine effectiveness and operational resilience, and the optimization of ongoing business-integrated risk management.
RISK TRANSFORMATION

• The Industry Problem
• Privacy and Governance
• Cyber Resilience
• Risk Transformation and Optimization
THE INDUSTRY PROBLEM
TRANSFORMATION?

We Are Being Outpaced

Technology
Heuristics, Threat Modeling, SIEM “Death”, Hybrid Solutions

Data
Modeling, Aggregation, Machine Learning, SOAR

Platform
Managed Security, “As-A-Service”, Cloud (Willing or Otherwise), Mobility
CURRENT STATE
Digital transformation initiatives are pushing new frontiers in cyber security, requiring stronger resilience in people, process and technology along with new, risk-based strategies and creating new challenges.

LACK OF RISK GOVERNANCE
Organizations lack some fundamentals of risk: how to classify assets, which definitions are most appropriate, how to align requirements to business objectives.

VOLUME AND VELOCITY OF CHANGE
As organizations balance digital transformation initiatives with concern about the next security threat or regulation, security teams struggle to keep up.

DIFFICULTY ARTICULATING HEALTH
As security initiatives move to the forefront within organizations, security teams are challenged to be able to articulate risk and security performance in business terms.
INDUSTRY CHALLENGE – THE OLD WAYS FAIL

Companies conduct assessments and get recommendations every year

- Why don’t the gaps get closed?
- Why do companies struggle with how to address problems rather than symptoms?
- Why do the same things show up again and again?

Because:

- Are they even gaps that demonstrate risk reduction
- Solutions are not integrated*
- Execution requires more than just the people to do the work. It requires:
SEEKING BALANCE

- Organizations are adopting new risk and compliance principles to achieve business resilience.
- IT risk management is evolving to operational risk and integrating into the fabric of the organization.
- Adaptive risk-based decision making is core to business agility and resilience.
AN APPROACH TO INTEGRATED RISK

RISK TRANSFORMATION AND OPTIMIZATION:
Optimize risk capabilities to effectively report security posture in order to influence better decision-making and improve overall business health

- Program Performance Management
- Third-Party Risk Management
- Continuous Risk Monitoring
- Program Optimization and Continuous Improvement

PRIVACY AND GOVERNANCE:
Align strategies to business objectives, consistent with regulations, in order to manage risk

- Business Alignment
- Compliance and Privacy Obligations
- Program and Control Status
- Maturity and Capability Definition

CYBER RESILIENCE:
Adapt to volume and velocity of change through sustainable and well-structured risk management capabilities

- Risk Transformation
- Cyber Program Development
- Vulnerability Management
- Staff Development and Training
PRIVACY AND GOVERNANCE
PRIVACY AND GOVERNANCE

- Business Alignment
  - Put Effort Where It Matters

- Compliance and Privacy Obligations
  - Understand What You Must Do

- Program and Control Status
  - Know What You Need To Do

- Maturity and Capability Definition
  - Define Goal States That You Want ... REGARDLESS OF APPEARANCES
Overview
- Business Alignment
- Compliance and Privacy Obligations
- Program and Control Status
- Maturity and Capability Definition

Outcome
- **Align strategies to business objectives**, protecting the organization’s critical needs while minimizing noise
- **Understand the true security requirements** of the organization’s legal, regulatory, industry, and contractual obligations
- **Understand current capabilities** from a performance-based point of view
- **Define goals based upon requirements** that will define not only what is done, but also how well it must be executed and what outcomes should be realized

Use Case
**Situation**
Private equity firm needed to understand the security posture and GDPR readiness of their 75 portfolio companies. Constraints included completion within four months and no use of intrusive agents or procedures for analysis.

**Approach**
- Develop a **tiered ranking system** to identify critical metrics that aligned to the business and compliance needs
- **Inside-Out analysis** with robust set of semi-automated questionnaires and direct interviews to establish control state
- **Technological Validation** - Offline GPO reviews, an external threat intelligence service, and Internet-based data leakage analysis
- **Final Outcome**: risk-based reports for each individual portfolio company as well as a detailed roll-up report showing trends across all 75 organizations
CYBER RESILIENCE
**CYBER RESILIENCE**

- Integrated Risk Management
  - Create Baselines of Decision Making

- Cyber Program Development
  - Develop a Comprehensive Controls Framework and Program

- Continuous Vulnerability Management
  - Settle in for the Long Game

- Dynamic Staff Development and Training
  - Put More Eyes on the Targets
## Overview
- Integrated Risk Management
- Cyber Program Development
- Continuous Vulnerability Management
- Dynamic Staff Development and Training

## Outcome
- **Risk-based decision making capabilities** are aligned with daily planning and execution goals, resulting in a connected approach that demonstrates ROI while securing the business
- **Security program activities** are defined and implemented to address outcomes rather than activities, enabling forward-looking growth to address change
- **Operational risk management practices** that allow for resilience in people, process and technology

## Use Case
### Situation
Company was focused on moving critical infrastructure to the cloud, but was unable to adequately develop a strategy to identify and monitor risks associated with such a move. In addition, the organization struggled to retain talent and keep in-house subject matter experts to support security initiatives.

### Approach
- Developed a **strategy aligned to business objectives**
- Validated details of existing security management capabilities and developed project plans for prioritized workstreams
- Developed **Adaptive Security Management procedures** and leveraged existing security requirements
- Proper **cloud security** was protected and customer security principles were maintained
RISK TRANSFORMATION AND OPTIMIZATION

- Program Performance Management
  - Implement **Truthful Metrics**
- Third-Party Risk Management
  - Address **All** Security Actors
- Continuous Risk Monitoring
  - **Redefine** Reality Daily
- Program Optimization and Continuous Development
  - Demand **Constant Improvement**
## RISK TRANSFORMATION AND OPTIMIZATION

<table>
<thead>
<tr>
<th>Overview</th>
<th>Outcome</th>
<th>Use Case</th>
</tr>
</thead>
</table>
| • Program Performance Management  
• Third-Party Risk Management  
• Continuous Risk Monitoring  
• Program Optimization and Continuous Improvement | • Applied evaluation of security program activities using tailored metrics to determine effectiveness  
• Equivalent security control capabilities applied to both internal and external agents  
• Increased understanding of organizational risk capabilities to effectively report security posture and influence better decision making and improve overall business health  
• Continuous cycle of improvement that establishes a pattern of needed change to address morphing requirements | **Situation**  
Due to recent staff losses, an organization’s security team was struggling to maintain day-to-day operations. In addition, poor patch management and ineffective incident response communications led to a targeted malware attack with widespread infection.  
**Approach**  
• Team facilitated root-cause analysis and developed actionable remediation plans  
• Optimized patch management procedures and a more robust incident communications process were developed to remedy future incidents  
• Supplementary workflows were added to the GRC Platform allowing for greater automation of vulnerability identification and classification |
IN SUMMARY

Establish Those Baselines that Align Security to the Business

Build and Include Those Most Critical Aspects

The “Noble Eightfold Path” of Security

Integration
Guide Through Inclusion and Partnership

Privacy and Governance

Cyber Resilience

Risk Transformation
THANK YOU!

Chris Gray

Director, Service Delivery Canada
Email: chris.gray@optiv.com
Phone: 647.242.9115