Agenda

- Threat Landscape
- Response
- Information Security Organization
- Evolution of Services
If targeted by a well-funded and determined adversary it is nearly impossible for an organization to prevent an intrusion regardless of the level of security controls = BREACHES WILL HAPPEN.
Threats

- **Maintaining Staff & Skillset**
  - Retention, recruiting & training of staff

- **System Lifecycle**
  - Challenge including security policy throughout the entire lifecycle, conception, design, build/acquire, operate, & sunset

- **Foundation**
  - Challenge maintaining/enhancing foundational or fundamental controls such as appropriate change, asset, compliance, and identity & authentication management

- **Culture of Trust**
  - Especially in relation to insider threat

- **Targeted/ Advanced Persistent Threat**
  - Custom, tailored attacks bypass traditional controls & countermeasures
    - Common signature vs. unique, noisy vs. stealth, IS vectors vs. multidisciplinary

- **Information Leakage**
  - Exposure with increasing use of the Internet or outside service providers

- **Third Party Reliance**
  - Especially in regard to FRS performance

- **Proliferation & Consumerization of Technology**
  - Feature rich with lack of appropriate controls
Response

Strategic
- Planning, scorecards, trends
- Integrate with business & IT strategy
- Architecture & design
- Security governance

Proactive
- IT Lifecycle focused
- Policies & standards
- Design
- Application & Vendor security assurance
- Security Awareness & Training

Foundational
- Defense in Depth
- Vulnerability & Threat management
- Reactive incident response
- Compliance management
- Identity & Access Management
ISNY: Information Security Teams

Strategic

Business

Risk Assessment

Architecture and Strategic Oversight Team

Risk Mgmt. & Policy

Operational

Threat Mgmt.

Vulnerability Mgmt. & Incident Response

Security Engineering & Controls

National IT Information Security Infrastructure, Policy and Operations
Evolution of Information Security

- **6 years ago**
  - Foundational, commodity services centric
  - Almost organized like a help desk

- **3 years ago**
  - Moved some of the focus toward engineering & National
  - Starting to build a stronger policy & security assessment team

- **Current**
  - Focusing on supporting National control development, National service management, security assessments, developing a strategic architecture team
  - Outsourcing commodity services, last mile support still a challenge

- **Future**
  - Stay ahead of emerging threats, further develop a combined strategy & policy team with tighter business strategy integration
  - Focus: Risk Management, Policy, Awareness & Education, Personnel and Insider investigations, Cyber Resilience, Compliance
  - Continually evaluate services, staffing & skillset relative to threat landscape