

# CYBER SECURITY INFORMATION SHARING & COLLABORATION

David N. Saul  
Senior Vice President & Chief Scientist



STATE STREET®

28 June 2013

# Discussion Flow

**The Evolving Threat Environment**

---

**Drivers That Shape Our Information Security Policy**

---

**Sources of Security Threat Information**

---

**State Street Multi-Layered Security Model**

---

**Financial Services Information Sharing and Analysis Center**

---

**Advanced Cyber Security Center**

---

**ACSC Working Group Top Consensus Priorities**

---

**Questions**

---

## Strengthening Our Information Security Program to Protect Against an Evolving Threat Environment






Cyber-threats grow more frequent and sophisticated every day

- State-sponsored criminals, “hacktivists” and internal threats on the rise
- No shortage of data breach case studies – RSA, Sony, LinkedIn, Global Payments Inc.
- A constant battle against malware, social engineering and “advanced persistent threats”



# Profiling Threat Actors

From Verizon's 2013 DATA BREACH INVESTIGATIONS REPORT

|   | ORGANIZED CRIME   | STATE-AFFILIATED   | ACTIVISTS  |
|---|---|--|--|
| <b>VICTIM INDUSTRY</b><br>     | Finance<br>Retail<br>Food   | Manufacturing<br>Professional<br>Transportation  | Information<br>Public<br>Other Services  |
| <b>REGION OF OPERATION</b><br> | Eastern Europe<br>North America   | East Asia (China)  | Western Europe<br>North America  |
| <b>COMMON ACTIONS</b><br>      | Tampering (Physical)<br>Brute force (Hacking)<br>Spyware (Malware)<br>Capture stored data (Malware)<br>Adminware (Malware)<br>RAM Scraper (Malware) | Backdoor (Malware)<br>Phishing (Social)<br>Command/Control (C2) (Malware, Hacking)<br>Export data (Malware)<br>Password dumper (Malware)<br>Downloader (Malware)<br>Stolen creds (Hacking) | SQLi (Hacking)<br>Stolen creds (Hacking)<br>Brute force (Hacking)<br>RFI (Hacking)<br>Backdoor (Malware) |
| <b>TARGETED ASSETS</b><br>    | ATM<br>POS controller<br>POS terminal<br>Database<br>Desktop  | Laptop/desktop<br>File server<br>Mail server<br>Directory server   | Web application<br>Database<br>Mail server   |
| <b>DESIRED DATA</b><br>      | Payment cards<br>Credentials<br>Bank account info   | Credentials<br>Internal organization data<br>Trade secrets<br>System info  | Personal info<br>Credentials<br>Internal organization data   |

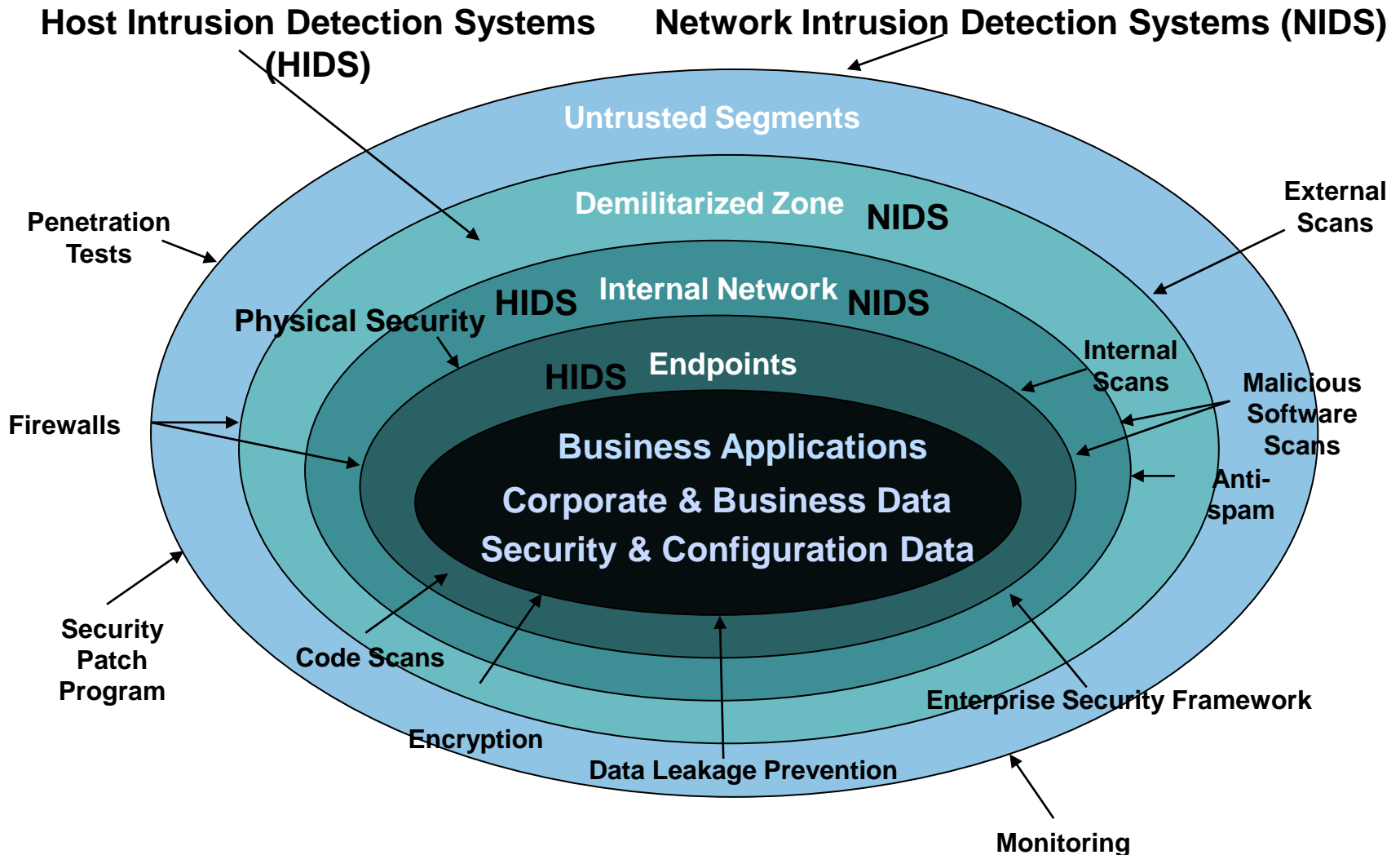
## Drivers That Shape Our Information Security Policy

- **Client Concerns** - Recent waves of distributed denial-of-service (DDoS) attacks have generated considerable press and sharpened focus on the banking sector's ability to sustain attacks of increasing data volume and sophistication.
- **Advanced Persistent Threats (APT)** - Typically a group, such as a foreign government, with both the capability and motivation to persistently attack using increasingly sophisticated tools. A global "cyber arms" race exists, with several nation-states very active in developing world-class offensive cyber capabilities. Sophisticated malware is filtering down from the nation-state attacks to cyber-criminals.
- **Insider Threats** - Trusted resources such as employees or contractors, whose actions may, knowingly or unknowingly, compromise internal systems.
- **Social Engineering** - Increasingly sophisticated social engineering attacks continue to threaten our systems, networks and data. Targeted phishing attacks use email or malicious websites to elicit certain behaviors from users that could compromise our data or disrupt business operations.
- **Regulatory Directives** - Government regulators are increasing pressure on the financial sector to strengthen cyber security standards.

## Sources of Security Threat Information

- Active threats at State Street are identified in a number of ways, with most threats identified by the IBM Security Operations Center and FireEye as part of our 24 x7 monitoring
- Corporate Information Security (CIS) receives threat intelligence from the following sources:
  - **Verisign iDefense Security Intelligence Services**
  - **Financial Services Information Sharing and Analysis Center**: industry forum for collaboration on critical security threats facing the financial services sector
  - **Advanced Cyber Security Center**: a cross-sector collaboration established by leading industry executives, university experts and public officials with focus on responding to advanced cyber threats
  - **IBM X-Force**: researches and monitors the latest Internet threat trends
  - **Verizon Data Breach report** including data from the Secret Service
  - **Department of Homeland Security**: U.S. CERT and Industrial Control Systems
  - **FBI and US Cyber Command**

# State Street Multi-Layered Security Model



## Financial Services Information Sharing and Analysis Center (FS-ISAC)

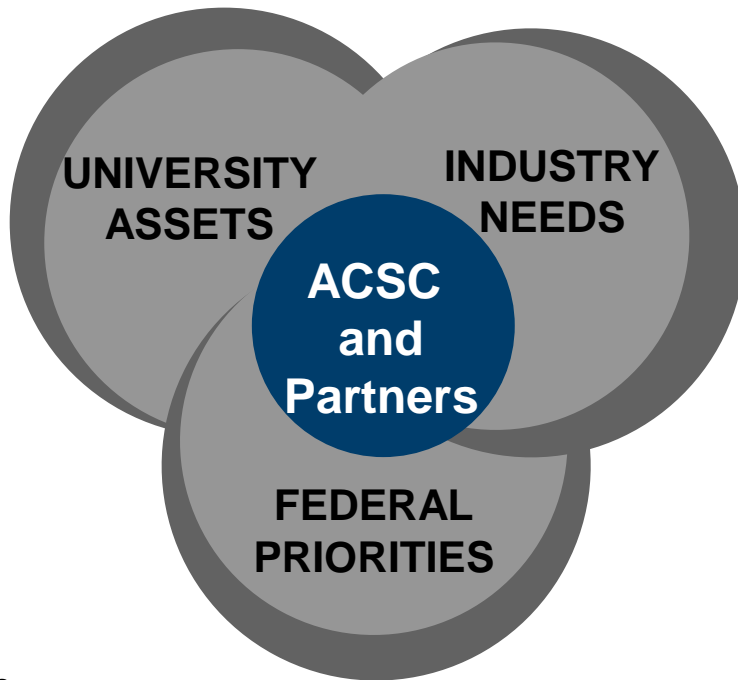
- The FS-ISAC was established in 1999 by the financial services sector in response to Presidential Directive 63.
- Mandates that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.
- Constantly gathers reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources.
- Uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information including analysis and recommended solutions from leading industry experts.
- Both Treasury and Department of Homeland Security rely on the FS-ISAC to disseminate critical information to the financial services sector in times of crisis.





## Advanced Cyber Security Center (ACSC)

- The Advanced Cyber Security Center (ACSC) brings together industry, university, and government organizations to address the most advanced cyber threats.
- State Street is a charter member of the Advanced Cyber Security Center, and actively collaborates with member organizations to share leading threat indicators and exchange insights on emerging APT activity.
- Through its regional leadership ACSC bridges the space for partnerships between university, industry and government.



# Advanced Cyber Security Center Key Initiatives

The Advanced Cyber Security Center is a **cross-sector collaboration** organized to help protect the region's organizations from the rapidly evolving advanced and persistent cyber threats...

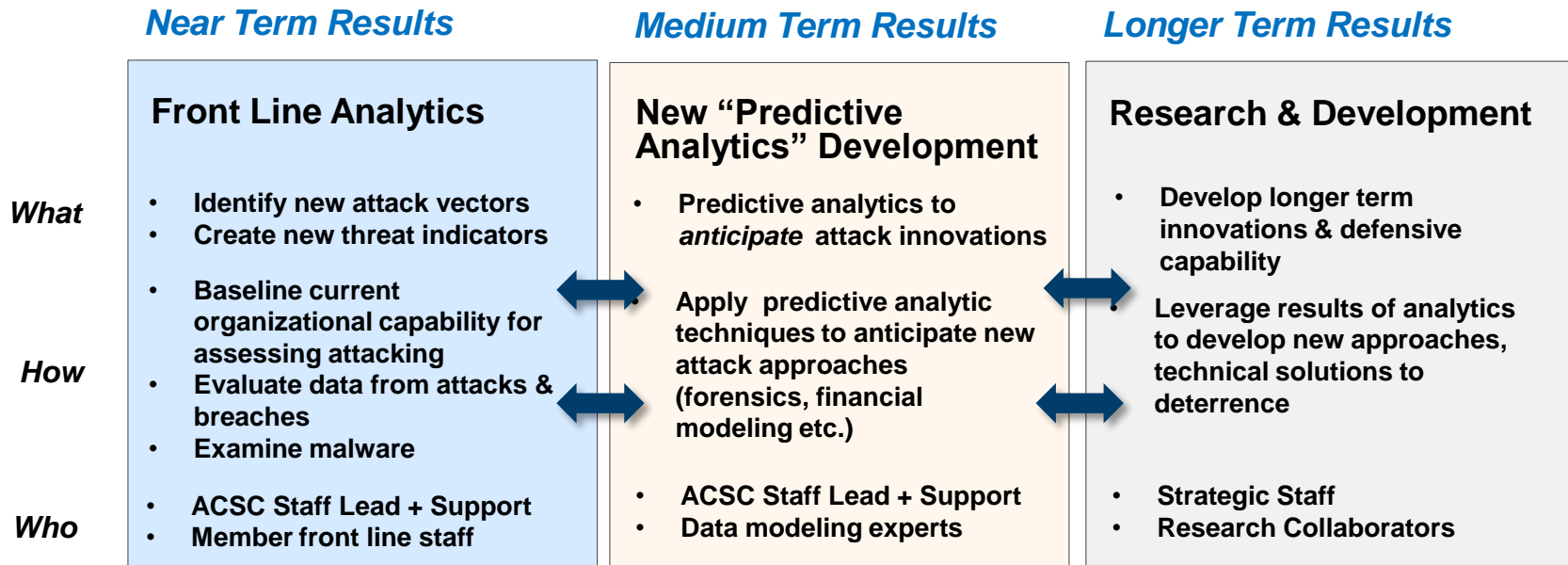
.....and to **support New England's role as a center for cyber security R+D, education, talent and jobs.**

## Three Key Initiatives:



# ACSC Strengthens Short-Term Defenses and Long-Term Capability

The ACSC will deliver actionable intelligence to bolster an organization's defenses in the short term and generate new defensive strategies and R+D in the longer tem.



**Data & Information Sharing**

## ACSC Working Group Top Consensus Priorities:

### 1. **Develop next generation resilient systems with the capacity to recover from attacks and failures**

Integrate cognitive psychology, controls, and complex network design for systems that mitigate the impact of cyber attacks, maintain operation during attacks, and automatically recover

### 2. **Develop “Big Data” security solutions responding to analytic, privacy and regulatory challenges**

Establish policies, processes and technology for the collection, storage, aggregation, integration, processing, analysis and reporting of large data sets across multiple platforms, jurisdictions and languages while ensuring privacy and security

### 3. **As the Internet and IT systems “go mobile”, develop the security that users demand**

Assess the economic and risk trade-offs associated with minimizing device size and maximizing battery for the user vs. the mix of security and operating applications, users apps and data storage that can be supported.

Determine how to incorporate more efficient advanced authentication mechanisms and security into mobile, virtual desktop and "bring your own device to work" environments.

## ACSC Working Group Top Consensus Priorities:

### **4. Develop automated real time threat sharing networks inside and between organizations that provide for federated intelligence-driven defense against cyber attacks.**

Develop policies and agreements for sharing data amongst organizations, and then design standards and structure for automated feeds that enable the automated collection of disparate data sets from disparate systems and data sets, protecting privacy and proprietary information through effective protocols and technology solutions.

### **5. Develop cyber security risk frameworks and integrate with enterprise risk frameworks.**

Assess the probabilities of different levels of cyber security risk and determine the policies, human resources support and economics to mitigate.

## Key Messages

- State Street is executing a long-term, risk-based information security strategy that evolves to meet an ever-changing threat environment
- We are utilizing multiple channels of external intelligence to share information, improve threat awareness and develop responses to advanced cyber threats
- Participation in the FS-Information Sharing and Analysis Center and Advanced Cyber Security Center enables collaboration with peer financial services organizations, universities, and government agencies
- The constant flow of new information and solutions enables us to strengthen our security controls and respond to new threats quickly

# Thank You

# Questions