Utilizing the NIST Framework to Improve Cybersecurity

Jeff Olejnik, Director
Risk Advisory Services
Agenda

- Cybersecurity Industry Developments
- Executive Order 13636
- NIST Cybersecurity Framework
- Using the NIST Framework to Improve Preparedness
Our Mission

We are advisors with a relentless commitment to creating value and securing the future of our clients, their businesses and the communities we live in and serve.
Comprehensive Governance, Risk, Compliance and Testing
Notable Data Breaches

- AOL
- Target
- Anthem
- OpenSSL
- Apple
- Neiman Marcus
- Home Depot
- Michaels
- Jimmy John's
- CHS Community Health Systems
- Sony
- P.F. Chang's
- Johns Hopkins University
- Supervalu
ATM Cash-out

- Criminals compromised bank network to raise amount of funds available
- Obtained cards
- $40M withdrawn from ATMs in 24 countries in a 10 hour period
Distributed Denial of Service (DDoS)
Account Hijacking

Email Received by Victim or Victim Visits a Legitimate Website
Attachment contains malware or malicious script is on website

Work Station Compromised
Victim is infected with credential stealing software and banking credentials are stolen

Hacker Engages
Hacker receives banking credentials and remotes into victim’s computer via a compromised proxy and logs into victim’s online banking service

Mules receive stolen funds and retain percentage

Stolen Funds

Money Transferred to Fraudulent Companies

Money laundered

Money moved offshore

Cycle Repeats
Good Morning,

Can you please update me with the available balance in my account and also the information needed to complete an outgoing wire transfer for me today? I am on my way to my nephew funeral service but I will check my mail often for your response.

Thanks.
Cryptolocker Ransomware

- Employee clicks on email
- Personal files encrypted
- Virus spreads to other computers
- Ransom demand to provide key to decrypt
- Ransom demand increases after 72 hrs. passed
Reality check

- **Cybercrime is big business.** There is a well-organized and well-funded underground economy for stealing and selling corporate data.

- **100% protection is not possible.** There are thousands of ways attackers can compromise security and they need only be successful once.

- **Cyber incidents will happen.** How quickly and effectively organizations detect and respond makes all the difference.
Current Challenges

- Communication of cybersecurity readiness with senior management and the Board of Directors
- Gaps in layered controls
- IT audit effectiveness and thoroughness
“Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.”
Critical Infrastructure - assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
16 Critical Infrastructure Sectors

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy

Financial Services
Food & Agriculture
Government Facilities
Healthcare & Public Health
Information Technology
Nuclear Reactors, Materials and Waste
Transportation System
Waste and Wastewater
Executive Order 13636
February 12, 2013

- Information sharing & collaboration
- Develop a baseline framework of cybersecurity standards and best practices - NIST
- Establish consultative process
- Identify high priority infrastructure
- Incentives for voluntary participation
- Review / assess regulatory requirements
- Incorporate privacy and civil liberties
Executive Order 13636 Timeline

- **DHS Information Sharing**: Feb. 2013
- **NIST Cybersecurity Framework**: Jun. 2013
- **Framework Effectiveness Assessment**: Oct. 2013

**Days**:
- 30
- 120
- 150
- 210
- 240
- 365
- 455
- 1095

**Steps**:
- "At Greatest Risk" Assessment
- Sector Reports on Participation
- Positive Incentives
- Privacy Impact Assessment
- Regulatory Requirements Sufficiency Analysis

**Timeline**:
- Preliminary: Feb. 2013
1. **Identify**: An understanding of how to manage cybersecurity risk to systems, assets, data and capabilities.

2. **Protect**: The controls and safeguards to protect or deter cybersecurity threats.

3. **Detect**: Continuous monitoring to provide proactive real-time alerts to cybersecurity-related events.

4. **Respond**: Incident response activities.

5. **Recover**: Business continuity plans to maintain resilience and recover capabilities after a data breach.
2. NIST Cybersecurity Framework – TIERS

- **Tier 1 (Partial)** Risk management is “ad hoc” with limited awareness of risk and no collaboration with others.

- **Tier 2 (Risk Informed)** – Risk Management processes and programs are in place but not integrated enterprise-wide. Collaboration is understood but lacks formal capabilities.

- **Tier 3 (Repeatable)** Formal policies for risk-management processes and programs are in place enterprise-wide, with partial external collaboration.

- **Tier 4 (Adaptive)** – Risk management processes and programs are based on lessons learned and embedded in the culture, with proactive collaboration.
<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness &amp; Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes &amp; Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies &amp; Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
Category: Risk Assessment

The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Asset vulnerabilities are identified and documented *

- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization

Threat and vulnerability information is received from information sharing forums and sources *

- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization

Threats, both internal and external, are identified and documented *

- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization

Potential business impacts and likelihoods are identified *
Category: Access Control

Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Identities and credentials are managed for authorized devices and users *
- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization

Physical access to assets is managed and protected *
- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization

Remote access is managed *
- Adaptive
- Repeatable
- Risk Informed
- Partial
- Not At My Organization
Your Overall Risk Factor

265

Overall Risk Factor by Function

Each Function, as a percentage of your Overall Risk Factor.
The pie chart indicates how much each Function is contributing to your Overall Risk Factor. Larger slices indicate Function areas where you want to focus mitigation efforts.
<table>
<thead>
<tr>
<th>Critical Security Controls - Ver. 5</th>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC #1: Inventory Devices</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 5</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #2: Inventory Software</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 5</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #3: Hardening Hardware &amp; Software</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 3</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #4: Continuous Vuln Asmt &amp; Remediation</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 12</td>
</tr>
<tr>
<td>CC #5: Malware Defenses</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 8</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #6: Application Software Security</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 3</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #7: Wireless Device Control</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 7</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #8: Data Recovery Capability</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 8</td>
</tr>
<tr>
<td>CC #9: Security Skills Asmt &amp; add Training</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 11</td>
</tr>
<tr>
<td>CC #10: Hardening Network Devices</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 3</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #11: Restrict Ntkw Ports, Prots &amp; Svcs</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 3</td>
<td>T4: 11</td>
</tr>
<tr>
<td>CC #12: Control Use of Admin Privileges</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 3</td>
<td>T4: 2</td>
</tr>
<tr>
<td>CC #13: Boundary Defense</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 8</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #14: Audit Logs - Maint, Monitor &amp; Analysis</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 15</td>
</tr>
<tr>
<td>CC #15: Controlled Access - Need to Know</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 7</td>
</tr>
<tr>
<td>CC #16: Account Monitoring &amp; Control</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 6</td>
<td>T4: 15</td>
</tr>
<tr>
<td>CC #17: Data Loss Prevention</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 1</td>
<td>T4: 0</td>
</tr>
<tr>
<td>CC #18: Incident Response &amp; Mgmt</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 14</td>
</tr>
<tr>
<td>CC #19: Secure Network Engineering</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 2</td>
<td>T4: 13</td>
</tr>
<tr>
<td>CC #20: Penetration / Attack Tests</td>
<td>T0: 0</td>
<td>T1: 0</td>
<td>T2: 0</td>
<td>T3: 1</td>
<td>T4: 14</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework – Key Points

- NIST Released Cybersecurity Framework V 1.0 – Feb 2014
  - “Living” Document – Ongoing Updates Expected and Necessary

- Provides a structure that organizations of all types can use to create, guide, assess or improve comprehensive cybersecurity programs

- Currently used as benchmark by regulators
How to use the Framework

1. Baseline Current State
2. Assess Risk
3. Create a Target Profile
4. Determine, Analyze and Prioritize Gaps
5. Implement Action Plan
Reasons to Adopt the Cybersecurity Framework

- **Improve communication**
  - Senior management and board
  - External parties

- **Identify “gaps”**
  - Create plans and track progress

- **Build effective audit plans**

- **Legal and regulatory advantages**
  - “De facto” standard for cybersecurity and privacy
Cybersecurity Assessment Areas of Focus for Financial Institutions

Risk Management and Oversight
  • Document Information Security Program
  • Training and Awareness

Threat Intelligence
  • External – FS-ISAC
  • Internal – Security Assessments / IT Audits

Cybersecurity Controls
  • Identify, Protect, Detect, Response, Recover (NIST Cybersecurity Controls)

3rd Party / Vendor Management
  • Process / Data Flow
  • Vendor Management Program

Cyber Incident Response and Resilience
  • IR Program Development
  • Tabletop exercises (include senior management team)
What should we be doing now?

- Get familiar with framework and create a baseline
- Document / Update / Create Information Security Program
- Identify Blind Spots
- Evolve Testing
  - Social Engineering, Penetration Testing, Web application pen test
- REALLY assess key vendors
- Participate in Threat Intelligence Group – FS-ISAC, Infragard
- Train your Employees
● FREE Cybersecurity Framework Survey
www.assurityriver.com/csfsurvey

● NIST Cybersecurity Framework

● OCIE Cybersecurity Initiative

● National Cybersecurity Awareness Month
http://www.staysafeonline.org/ncsam/
Contact Information

Jeff Olejnik, Director
Wipfli LLP
7601 France Avenue South, Ste. 400
Minneapolis, MN 55435

Direct: 952.230.6488
E-mail: jolejnik@wipfli.com
LinkedIn: www.linkedin.com/in/jeffolejnik