NIST Cybersecurity Framework – A Practical Approach to Risk Assessments and Assessing Security Posture

Presenter
Victoria Gabbai, CISA, MS  Sr. IT Auditor  Johns Hopkins Institutions

2017
ANNUAL CONFERENCE
PHOENIX, ARIZONA

Question Time
Who has heard of the NIST Cybersecurity Framework?
Has anyone aligned the Framework to their College/University or Academic Medical Center controls?

I have a question!
**Goals for Today**

- What is Cybersecurity?
- Provide a historical overview of the NIST Cybersecurity Framework (CSF)
- Discuss what the NIST CSF is designed to accomplish
- The components of the NIST CSF
- Discuss Johns Hopkins Institutions’ approach for conducting a gap analysis using the CSF

**What is Cybersecurity?**

Techtarget.com defines Cybersecurity as:

the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cybersecurity and physical security.

Data Source: [http://whatis.techtarget.com/definition/cybersecurity](http://whatis.techtarget.com/definition/cybersecurity)
History of the NIST Cybersecurity Framework

Then...

- Executive Order 13636
  "Improving Critical Infrastructure Cybersecurity"
  - Signed: February 12, 2013
  - 3 key areas: Information sharing, privacy, and adoption of cybersecurity practices

Request for Information
- What did they want to see?
- What would be valuable?

Workshops
- April 2013 to November 2013
- 5 workshops in 5 cities

Draft release/request for comments/draft release
- Throughout the workshop process

NIST Framework
- Framework for Improving Critical Infrastructure Cybersecurity v.1.0 (Feb. 2014)

Now...
- Draft update: January 10, 2017 version 1.1 (under review)

What is the NIST Cybersecurity Framework?

- Voluntary guidance, based on existing standards, guidelines, and practices
- Not a one-size-fits-all approach
- A guideline
- Complements your risk management process and cybersecurity program
- Better manage and reduce cybersecurity risk
- A good tool to assess your cybersecurity maturity
The Components of the NIST Cybersecurity Framework – AKA Informative References

Council on CyberSecurity (CCS) Top 20 Critical Security Controls (CSC)

ISACA - COBIT 5


NIST - Special Publication: Security and Privacy Controls for Federal Information Systems and Organizations – NIST SP 800-53 Rev. 4

The Maturity Model –
Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework:

Tier 1 (Partial) – Grade “F/D”
Tier 2 (Risk Informed) – Grade “C”
Tier 3 (Repeatable) – Grade “B”
Tier 4 (Adaptive) – Grade “A”

The activities, outcomes and references
• Five Functions: Identify, Protect, Detect, Respond, Recover

Components of the NIST Cybersecurity Framework

An assessment of your current and target profile – where you are and where you want to be
Why would you want to use the Framework?

- It’s a tool you can use to:
  - Describe the current cybersecurity posture
  - Describe where you want to be
  - Identify gaps and weaknesses of your controls
  - Assess progress toward the target state (where you wanted to be)
  - Communicate among internal and external stakeholders about cybersecurity risk.
  - Create an action plan

Data Source: https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-virtual-events Cybersecurity Framework Webcast, Day 1, Part 1

Who Can Use the Framework?

Everyone
The Johns Hopkins Institutions’ Approach

Our NIST Cybersecurity Framework Project

How It All Began – Project Background

In the Summer of 2014...

- The Sr. VP of Finance and Administration of JHU requested that the Office of Hopkins Internal Audit (OHIA) IT Audit team assist the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) in the area of Cybersecurity.

- Our previous Chief Audit Executive (CAE) had asked if the IT Audit Team could look into Cybersecurity practices and where the institution was headed.

- The OHIA IT Audit Team decided to conduct a gap analysis of the institution using the NIST Cybersecurity Framework
  - CIO and CISO buy-in
How It All Began – Project Background

• Kicked-off project in August 2014
• Purpose of project: To provide assistance to the CISO and help augment the 3-year security plan by documenting risks and Cybersecurity posture if and when Centers for Medicare/Medicaid (CMS) audits Johns Hopkins.

Project Team

• Chief Information Security Officer (CISO)
• IT Manager, IT@JH Enterprise Services
• Director of IT Audit, Office of Hopkins Internal Audit (OHIA)
• 2 Senior IT Auditors, OHIA
NIST Cybersecurity Framework Approach

NIST CSF Approach

Prioritize and Scope ➔ Orient ➔ Current Profile ➔ Risk Assessment ➔ Target Profile ➔ Determine, Analyze, and Prioritize Gaps ➔ Action Plan

Johns Hopkins University/Johns Hopkins Medicine Approach

Prioritize and Scope ➔ Orient ➔ Risk Assessment ➔ Current Profile ➔ Target Profile ➔ Determine, Analyze, and Prioritize Gaps ➔ Action Plan

NIST Steps

Step 1: Prioritize & Scope
- Identify objectives and priorities
- Make decisions regarding cybersecurity implementations
- Determine the scope of systems and assets that support the selected business line or process

Step 2: Orient
- Organization identifies:
  - systems and assets
  - regulatory requirements
  - overall risk approach
- Identify threats and vulnerabilities of systems and assets.

**NIST Steps**

*Step 4: Conduct Risk Assessment*

- Organization’s overall risk management process
- Analyze the operational environment
  - Don’t forget – include emerging risks and threat and vulnerability data


---

**Risk Assessment**

- Met 2 times week with CISO and IT Manager and IT Audit team (Late October 2014 to November 2014)
  - Determined methodology to conduct Risk Assessment
  - Determined risks & assigned values to probability and severity
  - Determined current controls & future controls to mitigate each listed risk
  - Presented Draft Risk Assessment to IT Policy Committee (mid-November 2014), Institutional Computing Standards Committees (ICSC), Information Security Advisory Committee, Institutional and Enterprise Risk Management groups
  - CISO presented to CIO and Chief Risk Officer

Approximate Time Spent: 120 (3 auditors)
Example Risk Assessment

<table>
<thead>
<tr>
<th>#</th>
<th>Risk Name</th>
<th>Threat</th>
<th>Probability</th>
<th>Severity</th>
<th>Current Description</th>
<th>Hopkins Controls</th>
<th>Quality</th>
<th>Future Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>Internally published on the Internet of Restricted information</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>3 (Minor) – 5 (Significant, long-lasting losses)</td>
<td>1 (None) – 5 (Full Controls + Leadership)</td>
<td>10 - Impersonation/spoofing</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Internal use of unencrypted Restricted information</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>Intentional compromise</td>
<td>1 (Remote &lt;5% chance) – 5 (Very Likely &gt; 95% chance)</td>
<td>17 - Environmental hazards</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Intentional compromise of major restricted database application (more than 50K records)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>External monitoring for potential exfiltration attempts</td>
<td>1 (Few Controls) – 5 (Full Controls + Leadership)</td>
<td>5 - Sophisticated Hacktivists</td>
<td></td>
</tr>
</tbody>
</table>

Potential Risks That Your Organization Might Face

<table>
<thead>
<tr>
<th>Potential Risks</th>
<th>Principle Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intentional compromise of major Restricted Application (greater than 50K records)</td>
<td>Standard cyber-security controls (e.g. firewalls, IPS, multi-factor authentication, security testing, patching, continuous surveillance, Website testing, surveillance)</td>
</tr>
<tr>
<td>Intentional compromise of major Restricted Application (fewer than 50K records)</td>
<td></td>
</tr>
<tr>
<td>Web application attacks</td>
<td></td>
</tr>
<tr>
<td>External cloud-based infrastructure compromise</td>
<td></td>
</tr>
<tr>
<td>Inadvertent publication of Restricted information on the Internet</td>
<td></td>
</tr>
<tr>
<td>Inappropriate use or abuse by insiders</td>
<td>Training and awareness, surveillance</td>
</tr>
<tr>
<td>Physical loss or theft of a laptop</td>
<td>Encryption, host management, surveillance</td>
</tr>
<tr>
<td>Physical loss or theft of a Restricted server</td>
<td>Data centers, encryption, virtualization</td>
</tr>
</tbody>
</table>
NIST Steps

Step 3: Create Current Profile
• Develop Current Profile by reviewing controls achieved by each Category and Subcategory

Step 5: Create a Target Profile
• The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories

Step 6: Determine, Analyze, and Prioritize Gaps
• The organization compares the Current Profile and the Target Profile to determine gaps

Current Profile, Target Profile & Determine, Analyze, and Prioritize Gaps
• Met 2 times week with CISO and IT Manager and IT Audit team (Between November/December 2014 – June 2015)
  • Divided each Cybersecurity Framework category (under Identify, Protect, Detect, Respond, Recover) of the NIST Cyber-security Framework among the team
  • Involved various IT points of contact to understand processes
  • Developed narratives of current controls to each category – 95 pages!
  • Team review of Cybersecurity narratives

Approximate Time Spent: 335 (3 auditors)

Framework Core

- Approach much like an audit program or risk and control matrix
### NIST Narrative AKA Profiles

<table>
<thead>
<tr>
<th>ID. RA-2, 3</th>
<th>Threat and vulnerability information is received from information sharing forums and sources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Threats, both internal and external, are identified and documented</td>
</tr>
</tbody>
</table>

#### Current Controls

- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
- xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

#### Planned Enhancements

- Expand the number of individuals in security participating in these information sharing groups.

#### Challenges

- Although we have multiple information sources, it is difficult to correlate the impact of relevant sources to Hopkins.

#### Maturity Tiers

- The organizational risk management criteria is Tier 4 (Adaptive) widely deployed. Almost fully achieved.

#### Cross-References

- ICSC Purpose (http://www.it.johnshopkins.edu/about/committees/icsc)
- Incident Response Procedure

---

A word from our CISO...
**NIST Steps**

Step 7: Implement Action Plan

- The organization determines which actions to take in regards to any identified gaps.

---

**CISO Action Plan**

<table>
<thead>
<tr>
<th>2015</th>
<th>Present</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand deployments of multi-factor authentication</td>
<td>Continue to deploy and enhance efforts</td>
</tr>
<tr>
<td>Deploy Palo Alto Next Generation firewall</td>
<td>Done</td>
</tr>
<tr>
<td>Broaden server scanning and vulnerability management for servers and clients</td>
<td>- Tenable agents have been deployed to servers</td>
</tr>
<tr>
<td>• Continue scanning/testing for web and mobile application vulnerabilities</td>
<td>- Netsparker to Acunetix for web vulnerability assessments</td>
</tr>
<tr>
<td>Focus on data security through two initiatives by focusing on database activity logging, data risk minimization and encryption</td>
<td>- Core Impact and home grown Python scripts for Penetration testing</td>
</tr>
<tr>
<td>Focus on directed training for secure server administration for both IT@JH and beyond</td>
<td>Data Trust Initiative created for Johns Hopkins Medicine (JHM) – 9 different committees (in the areas of research, operations, privacy/security)</td>
</tr>
<tr>
<td>Replicate privacy and security liaison programs</td>
<td>Now it’s both on the JHM &amp; JHU side</td>
</tr>
<tr>
<td>Deploy specialized incident response staff</td>
<td>Just hired 2 specialized incident response staff starting in Mid September and one in October.</td>
</tr>
<tr>
<td>Increase sensitivity on our monitoring tools for more sophisticated attacks</td>
<td>100 gigs of daily logs to 600 gigs of daily logs</td>
</tr>
</tbody>
</table>
Risk Assessment/NIST Cybersecurity Framework
Introduction Document

• Met between June/July 2015 - August 2015
  • This overview document was created to present to Centers for Medicare/Medicaid (CMS) or any external 3rd parties coming in to audit us.
    • Includes: Our overall security posture, risk assessment and remediation, objectives-based project management, security frameworks, regulatory compliance and maturity models, controls compared to peers both in the industry and others, audits and 3rd party evaluations, X Factors – visibility, sensitivity and specificity.
  • Created by the CISO and reviewed as a team

Approximate Time Spent: 96 (3 auditors)

Reporting the Results

• Internal audit aided in the creation, review and/or feedback of:
  • Risk Assessment
  • Cybersecurity Framework
  • CSF Intro
• Internal audit also reviewed files the CISO wrote that accompanied the previously discussed documents:
  • Johns Hopkins Institutions – High-Level 3-Year Information Security IT Risk Management Plan (ISRMP)
  • Johns Hopkins HIPAA Risk Assessment - Security Compliance Matrix 2015
    • Maps Health Insurance Portability and Accountability Act (HIPAA) standards to applicable IT@JH policies & description of that policy
  • Johns Hopkins Information Security Assessment July 2015 - Information Security Controls Compendium
    • compares technologies of our peers in Academic Medical Centers/University's to ourselves
Key Project Takeaways

- Risk Assessment: OHIA will continue to assist the CISO in future years on the IT risk assessment.
- NIST Cybersecurity Framework: Process will be repeated every 3 years between Internal Audit, CISO and his team (including our current FY18).

Questions?
Putting Our Work Into Action

• Someone had a laptop stolen overseas which contained Electronic Patient Health Information (ePHI).
• Security documentation reviewed by outside council before submitting to our documentation to the Office of Civil Rights (OCR) for their review.
• The Johns Hopkins Risk Assessment did not conform to the NIST 800-30 standards (Guide for Conducting Risk Assessments).
• The Johns Hopkins CISO immediately contacted our office asking for assistance.
• Our risk assessment had all the right components required by NIST, but we needed to convert the existing IT risk assessment document to conform to the NIST 800-30 standard.
• Three weeks later (OHIA working with the CISO) the document was completed and included in a package to OCR.

Total time spent: 16 hours

Adversarial Risk

• Adversarial Risk – Intentional
  • Intentional compromise of major Restricted Database Application (>50k records)
  • Intentional compromise of major Restricted Database Application (<50k records)
  • Physical loss or theft of a laptop computer with unencrypted Restricted information
  • Major Ransomware Outbreak
  • Physical theft of a Restricted server
  • Major breach of primary directory
  • Hacktivism type attack
  • Denial of Service
  • Inappropriate use or abuse by insiders
  • Web application attacks (SQL injection, XSS)
  • Rogue administrator
  • Physical loss or theft of a workstation or other equipment with unencrypted Restricted information
  • Point of Sale (POS) compromise
  • Massive malware infection
# NIST 800-30 Results: Adversarial Risks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Intentional compromise of major Restricted Database Application (&gt;50k records)</td>
<td>Individual, Group, Organization, Nation State</td>
<td>High</td>
<td>Very High</td>
<td>High</td>
<td>Expected</td>
<td>Very High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Intentional compromise of major Restricted Database Application (&lt;50k records)</td>
<td>Individual, Group, Organization, Nation State</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Confirmed</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Physical loss or theft of a laptop computer with unencrypted Restricted information</td>
<td>Individual</td>
<td>Low</td>
<td>Low</td>
<td>Very Low</td>
<td>Confirmed</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

## Non-Adversarial Risk

- **Non-Adversarial Risk – Unintentional**
  - Inadvertent publication on the Internet of Restricted information
  - Physical loss or theft of a laptop computer with unencrypted Restricted information
  - Inappropriate use or abuse by insiders
  - Rogue administrator
  - Physical loss or theft of a workstation or other equipment with unencrypted Restricted information
  - Mishandling of file sharing services
  - Environmental hazards
  - Physical loss or theft of unencrypted back-up media
  - Loss or theft of portable media and devices with unencrypted Restricted information
  - Compliance issues (e-discovery, FISMA, 21 CFR Part 11, PCI, Meaningful Use, copyright issues, intellectual property)
  - Poor disposal of equipment including workstations / copiers
  - Missent transmissions
  - Web publication of email lists and other information that could be sensitive when aggregated
# NIST 800-30 Results: Non-Adversarial Risks

## Table

<table>
<thead>
<tr>
<th>Threat Event</th>
<th>Threat Sources (D-2)</th>
<th>Range of Effects (D-4)</th>
<th>Relevance (D-6)</th>
<th>Vulnerabilities and Predisposing Conditions (F-2)</th>
<th>Likelihood of Event Occurring (G-2)</th>
<th>Severity and Pervasiveness (F-5)</th>
<th>Likelihood Event Results in Adverse Impact (G-4)</th>
<th>Overall Likelihood (G-5)</th>
<th>Level of Impact (H-3)</th>
<th>Risk (I-2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inadvertent publication on the Internet of Restricted information</td>
<td>Individual, Insider</td>
<td>Moderate</td>
<td>Confirmed</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Physical loss or theft of a laptop computer with unencrypted Restricted information</td>
<td>Individual</td>
<td>Low</td>
<td>Confirmed</td>
<td>Very High</td>
<td>High</td>
<td>Moderate</td>
<td>Very High</td>
<td>Moderate</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Inappropriate use or abuse by insiders</td>
<td>Individual, Insider</td>
<td>Low</td>
<td>Confirmed</td>
<td>Very High</td>
<td>Very High</td>
<td>Moderate</td>
<td>Very High</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

## Final Results

- The final risk assessment was shared with the CIO and Information Systems Advisory Committee and was overwhelmingly approved and accepted.
- Johns Hopkins updated all of their security documents (plan, HIPAA, etc.) stating that "John Hopkins conforms to the NIST 800-30 standard, Guide for Conducting Risk Assessments")
- All security documentation was given to the OCR for their review.
  - They acknowledged the documentation received
  - Commented on the adequacy of the documentation
  - The CISO was informed there was no further need for investigation.
Contact Information

Victoria Gabbai
Sr. IT Auditor
☎ Phone: 443-997-3117
✉ vgabbai1@jhu.edu

Biography
Victoria Gabbai is a Senior IT Auditor at the Johns Hopkins Institutions. She has conducted Information Systems audits, analyzing the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of data and programs on computer and communication systems within Johns Hopkins University and Johns Hopkins Medicine for the last 5 ½ years.

Vicky is a graduate of Stevenson University in Stevenson, MD with a B.S. in Business Information Systems and M.S. in Forensic Studies with a Computer Forensics concentration. Prior to Hopkins, Vicky worked at Clifton Gunderson/CliftonLarsonAllen in Timonium, MD for 5 years as an IT Auditor. She performed SAS-70/SSAE 16, SOX IT compliance, GLBA, PCI readiness, Red Flag, vulnerability, security reviews/assessments, computer forensic investigations and information technology general controls (ITGCs) reviews of public companies, banks, credit unions, state and local governments, community colleges, and non-profits.

She earned the Certified Information Systems Auditor (CISA) designation in March 2012 and is a member of the ISACA’s Central Maryland Chapter.