Sloan Information Security Plan

MANAGEMENT
SLOAN SCHOOL

June 2018

NIST Cyber Security Framework

NIST Cybersecurity Framework

- **Sloan's Information Security Program uses the NIST Cybersecurity Framework**
  - Established in accordance with Executive Order 13636
  - Wide adoption across many sectors
- **Structure**
  - Five Functions
    - Identify, Protect, Detect, Respond, Recover
  - 20 Categories
  - 94 Subcategories

Self Assessment

- **Sloan conducted a self assessment using the NIST framework**
- **This initial self assessment was a high level review of the existing information security controls**
- **Each of the 94 subcategories were rated by:**
  - Importance: how critical is a particular subcategory to Sloan
  - Maturity: how mature is Sloan's current implementation
- **Scale ranged from 0 to 4**

- **Results helped guide and prioritize Sloan's infosec program**

Self Assessment - Example

- **Recover is the least complex function**
  - Only five subcategories
- **Importance – Maturity = Priority**

Function	Category	Subcategory	ID	Importance	Maturity	Priority
Recover	Recovery Planning	Recovery plan is executed	RC.RP-1	2	0	2
Recover	Improvements	Plans are updated with lessons learned	RC.IM-1	2	1	1
Recover	Improvements	Recovery strategy is updated	RC.IM-2	2	0	2
Recover	Communications	Public Relations are managed	RC.CO-1	1	0	1
Recover	Communications	Reputation after an event is repaired	RC.CO-2	1	0	1

Self Assessment – Summary

Area	Importance	Maturity
Identify	2.27	1.00
Protect	1.78	0.92
Detect	0.76	0.76
Respond	1.36	0.64
Recover	1.40	0.20

Self Assessment – Summary

Category	Importance	Maturity
Asset Management	3.17	1.17
Business Environment	2.75	2.00
Governance	3.00	1.00
Risk Assessment	0.80	0.00
Risk Management	1.33	1.00
Access Control	2.80	1.60
Awareness and Training	3.00	0.60
Data Security	1.56	1.33
Information Protection	1.55	0.36
Maintenance	0.50	2.00
Protective Technology	1.00	0.60
Anomalies and Events	0.60	0.60
Security Continuous Monitoring	0.29	0.57
Detection Processes	1.60	1.20
Response Planning	2.00	1.00
Communications	1.14	0.29
Analysis	1.25	1.00
Mitigation	1.00	1.00
Improvements	1.75	0.25
Recovery Planning	2.00	0.00

Security Matters

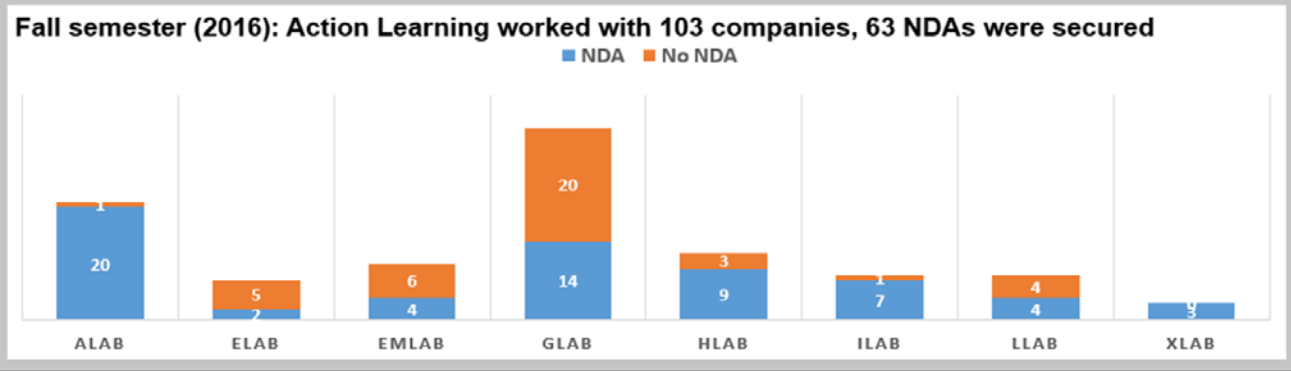
Sloan's Information Security Program

By Will Hedglon
Sloan Technology Services

Sloan's mission, **to develop principled, innovative leaders who improve the world and to generate ideas that advance management practice**, depends on securing and maintaining access to private information

Core Values

- Augment MIT WISP
- Enable Innovation
- Operational Excellence



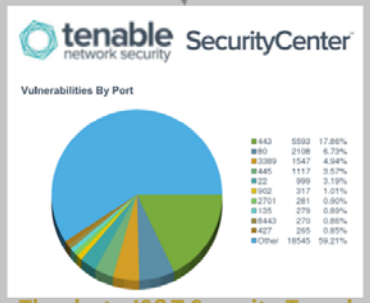
NIST Cybersecurity Framework

Broad Perspective

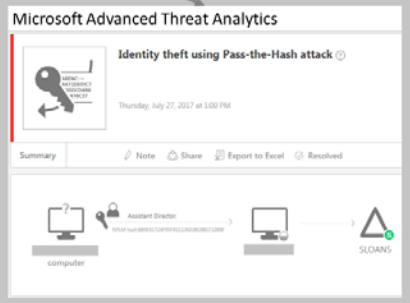
Area	Importance	Maturity
Identify	2.27	1.12
Protect	1.78	1.05
Detect	1.76	0.76
Respond	1.36	0.64
Recover	1.40	0.20

Granular Perspective

Area	Category	Subcategory	Importance	Maturity
Identify	Governance	Organizational information security policy is established	4	0
Identify	Asset Management	Resources are prioritized	4	1
Protect	Awareness and Training	General users are informed and trained	4	1
Protect	Access Control	Access permissions are managed	4	1
Protect	Awareness and Training	Senior executives understand roles & responsibilities	4	1
Protect	Awareness and Training	Privileged users understand roles & responsibilities	3	0
Identify	Asset Management	The organizational communication and data flow is mapped	4	1
Identify	Asset Management	Physical devices and systems within the organization are inventoried	4	2
Identify	Business Environment	Priorities for organizational mission, objectives, and activities are established	4	2
Identify	Business Environment	Dependencies and critical functions for delivery of critical services are established	4	2



Thanks to IS&T Security Team!



Thanks to MIT HR Learning Services Team!

Executive Committee

- Function: sponsor policy
- Membership: Deputy Dean, Senior Associate Dean for Undergraduate and Master's Programs, Senior Associate Dean for Administration

Working Group

- Function: craft policy, scope cost/benefit, communicate to users
- Membership: Contact Administration, CTO, ExecEd, Faculty & Research, Finance, HR, OC, Student Services, AD IOS

Faculty Collaboration | IS&T | MIT Audit | Sloan ITAG