SCRAM

Secure Cyber Risk Aggregation and Measurement

Internet Policy Research Initiative
Massachusetts Institute of Technology

Backgrounder:
Loss attribution - Process

SCRAM
Secure Cyber Risk Aggregation and Measurement

Review: Losses linked to control failures

Losses (last 2 years, >$5,000 per incident)

$250,000 (2020)	1.04 20.02 5.04 3.04 14.06
$1,300,000 (2020)	14.08 13.08 17.08 12.11
$35,000 (2021)	12.03 2.01 7.05 18.07 7.01
(…)	

Can choose up to 5 control failures (of lack of implementation) that led to the loss

Include any information security losses of greater than $5,000 that happened over the past 2 years

SCRAM
Secure Cyber Risk Aggregation and Measurement

Loss attribution: Concept and framework

Concept: Linking an economic loss ($) back to specific implemented controls that failed or non-implemented controls that would have helped if they had been adopted/implemented

<u>2 possibilities</u>

- Implemented and failed
- Not implemented but would have stopped

Limit of 5 implications per incident

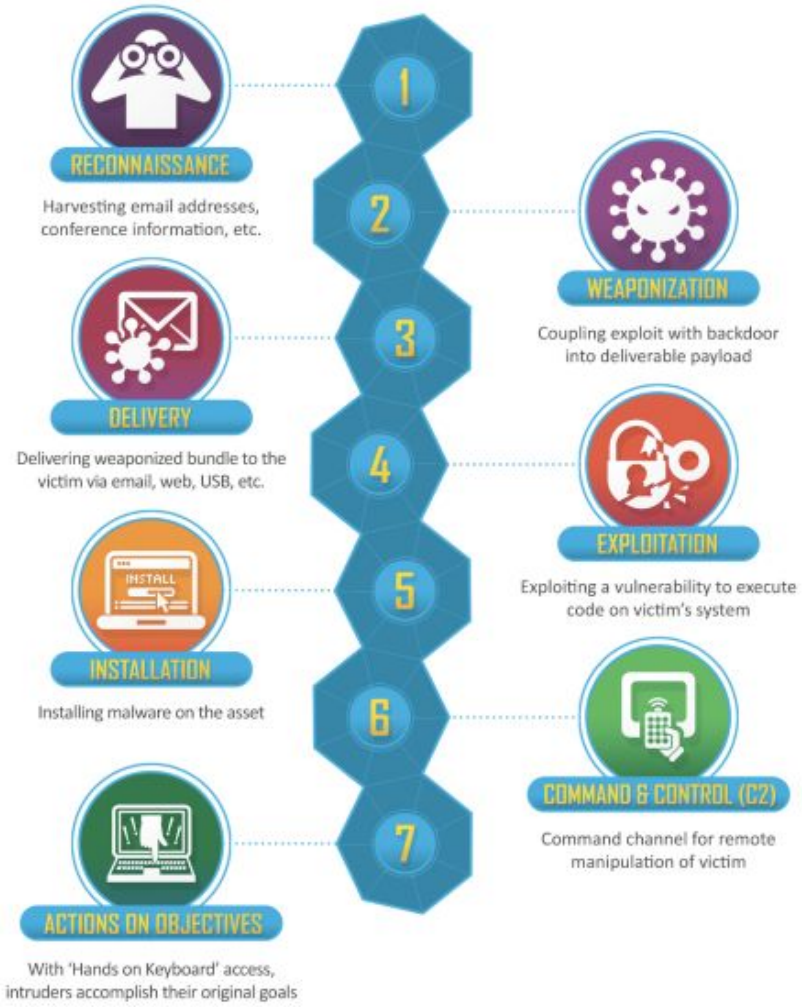
- Select up to 5
- Can be a combination of “implemented” and “should-have-implemented”

+

SCRAM
Secure Cyber Risk Aggregation and Measurement

Question: Kill chain approach?

- As you consider loss attribution for your losses, are frameworks such as the **kill chain** a good approach to think through failed / should-have-been-implemented controls?
- Would it still apply to insider events?



SCRAM
Secure Cyber Risk Aggregation and Measurement

Loss attribution: Weighting

Current approach:

Equal loss attribution

CIS 1.04:	20%
CIS 20.02:	20%
CIS 5.04:	20%
CIS 3.04:	20%
CIS 14.06:	20%

Potential future approach:

Variable loss attribution

CIS 1.04:	40%
CIS 20.02:	15%
CIS 5.04:	25%
CIS 3.04:	10%
CIS 14.06:	10%

SCRAM
Secure Cyber Risk Aggregation and Measurement

Loss attribution - Choosing the 5

Consistency in coding attributed losses

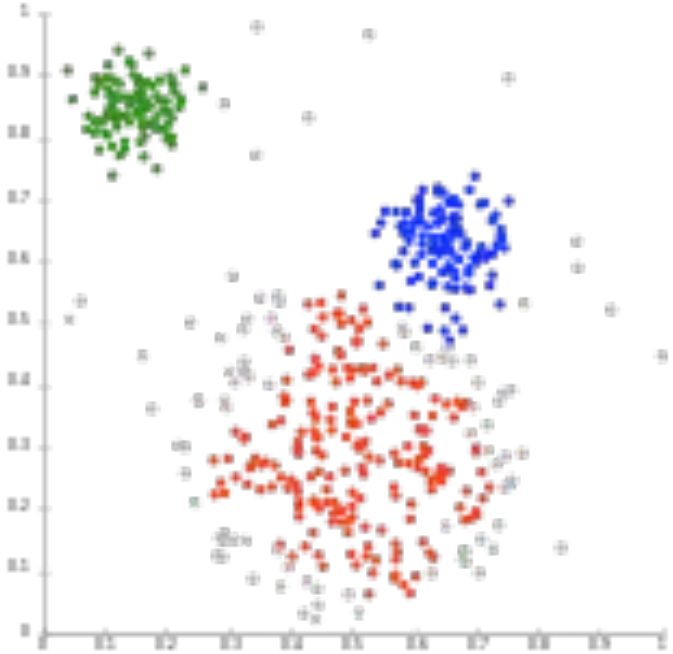
Some CIS subcontrols are similar so the same failure can be categorized by different people in different ways. Examples include:

- Asset inventories
  - 1.04 Maintain Detailed Asset Inventory
  - 1.05 Maintain Asset Inventory Information

- Logging
  - 6.03 Enable Detailed Logging
  - 6.04 Ensure adequate storage for logs
  - 6.05 Central Log Management

Attribution clustering - Post computation

- Look for clusters in the results and combine similar fields
- Take a higher-level view and examine the losses at the control (n=20) instead of subcontrol (n=171) level



SCRAM
Secure Cyber Risk Aggregation and Measurement

Loss attribution exercise

Two hypothetical incidents to code

Event 01: **Successful DDoS attack** (USD 100,000 loss)

- Select up to 5 controls that failed or would have stopped the loss if they were implemented)

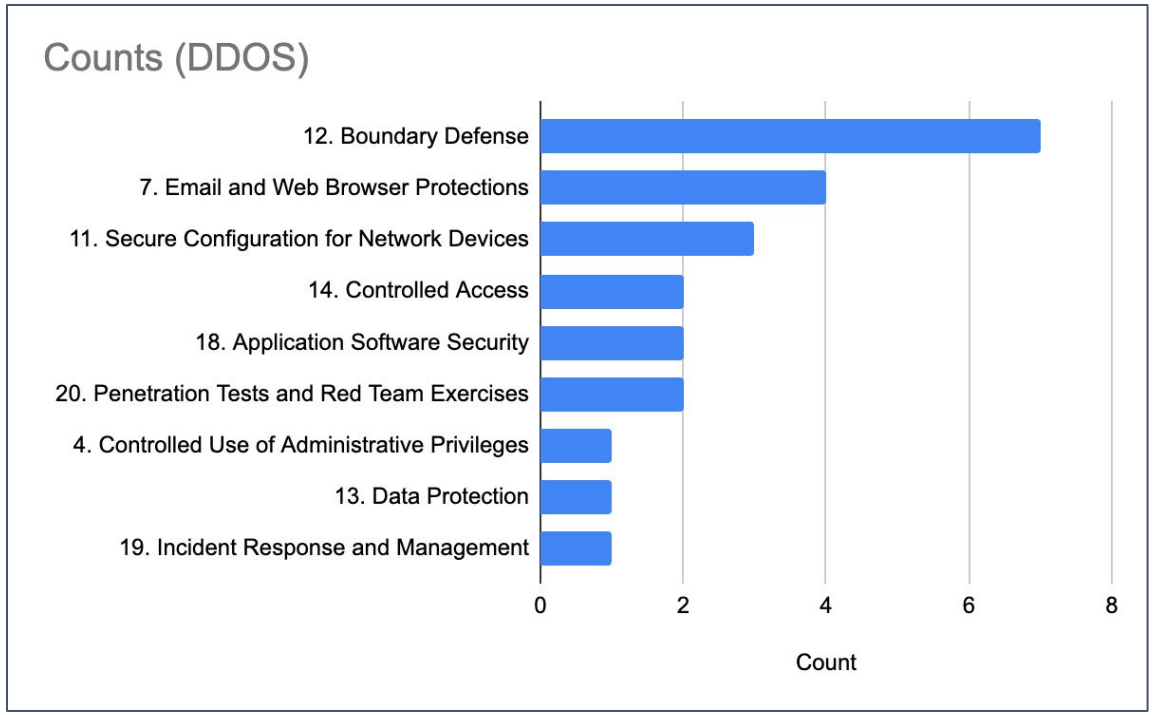
Event 02: **Successful Ransomware attack** (USD 150,000 loss)

- Select up to 5 controls that failed or would have stopped the loss if they were implemented)

SCRAM
Secure Cyber Risk Aggregation and Measurement

Results: Assigned responsibility - DDoS
(6 participants)

CISNum	CISName	DDoS (implications)
7.07	Use of DNS Filtering Services	3
12.03	Deny Communications with Known Malicious IP addresses	3
11.01	Maintain Standard Security Configurations for Network Devices	2
12.04	Deny Communication over Unauthorized Ports	2
14.02	Enable Firewall Filtering Between VLANs	2
18.1	Deploy Web Application Firewalls (WAFs)	2
4.07	Limit Access to Script Tools	1
7.06	Log all URL requests	1
11.02	Document Traffic Configuration Rules	1
12.07	Deploy Network-Based Intrusion Prevention Systems	1
12.1	Decrypt Network Traffic at Proxy	1
13.03	Monitor and Block Unauthorized Network Traffic	1
19.01	Document Incident Response Procedures	1
20.02	Conduct Regular External and Internal Penetration Tests	1
20.03	Perform Periodic Red Team Exercises	1

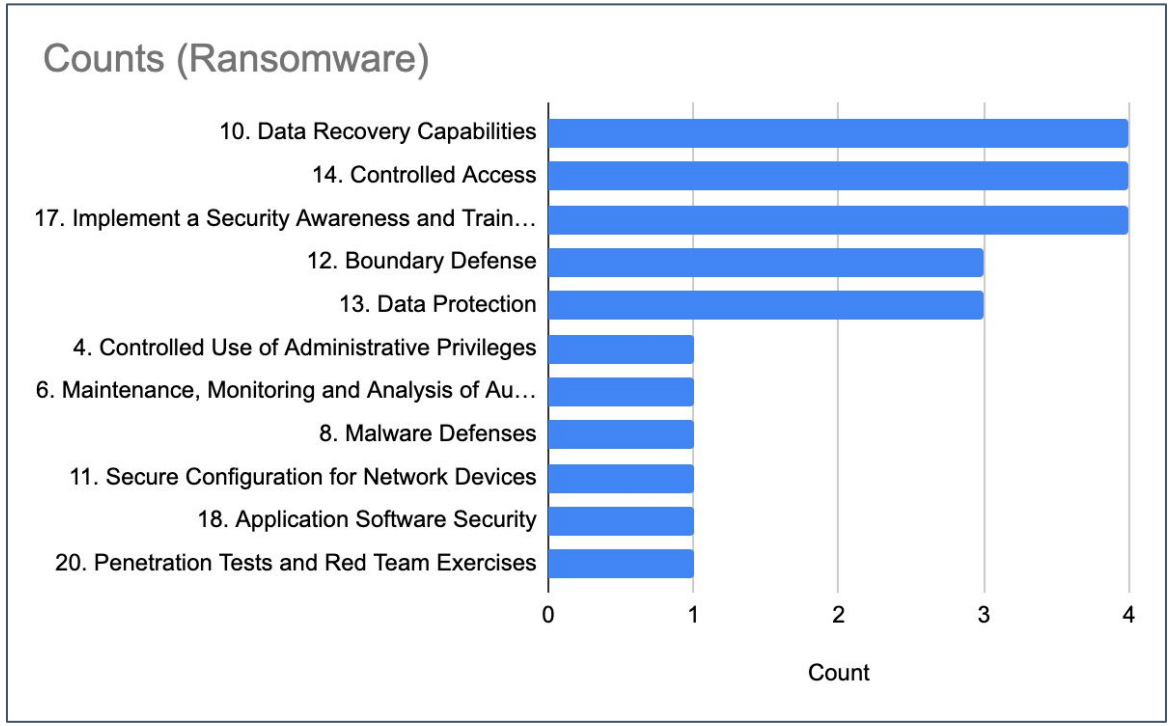


SCRAM
Secure Cyber Risk Aggregation and Measurement

Note: Two additional subcontrols seemed to be implicated, but had formatting errors in the data and couldn't be counted. They were:

- 4.09 - Log and Alert on Unsuccessful Administrative Account Login
- 2.01 - Maintain Inventory of Authorized Software

Results: Assigned responsibility - Ransomware
(6 participants)



CISNum	CISName	Ransomware
10.01	Ensure Regular Automated Back Ups	2
14.09	Enforce Detail Logging for Access or Changes to Sensitive Data	2
4.08	Log and Alert on Changes to Administrative Group Membership	1
6.06	Deploy SIEM or Log Analytic tool	1
8.01	Utilize Centrally Managed Anti-malware Software	1
10.02	Perform Complete System Backups	1
10.05	Ensure All Backups Have at Least One Offline Backup Destination	1
11.05	Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions	1
12.04	Deny Communication over Unauthorized Ports	1
12.11	Require All Remote Login to Use Multi-factor Authentication	1
12.12	Manage All Devices Remotely Logging into Internal Network	1
13.02	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	1
13.05	Monitor and Detect Any Unauthorized Use of Encryption	1
13.08	Manage System's External Removable Media's Read/write Configurations	1
14.05	Utilize an Active Discovery Tool to Identify Sensitive Data	1
14.07	Enforce Access Control to Data through Automated Tools	1
17.03	Implement a Security Awareness Program	1
17.04	Update Awareness Content Frequently	1
17.06	Train Workforce on Identifying Social Engineering Attacks	1
17.07	Train Workforce on Sensitive Data Handling	1
18.1	Deploy Web Application Firewalls (WAFs)	1
20.01	Establish a Penetration Testing Program	1

SCRAM
Secure Cyber Risk Aggregation and Measurement

Note: Two additional subcontrols seemed to be implicated, but had formatting errors in the data and couldn't be counted. They were:

- 4.09 - Log and Alert on Unsuccessful Administrative Account Login
- 2.01 - Maintain Inventory of Authorized Software

Thank you