SCRAM

Secure Cyber Risk Aggregation and Measurement

Internet Policy Research Initiative
Massachusetts Institute of Technology

Backgrounder:
Overview and multi-party computation

SCRAM Data partners

What you will receive

- Benchmarks of firm defenses
- Data: Loss event frequencies for specific controls
- Data: Loss magnitudes for specific controls
- Standards: Templates for calculating cyber losses
- Guidance: How firms can take action on results

What it will take

We estimate that the total time required for a company who decides to participate in the computation is between **9-18 hours of an FTE** to prepare for and run the computation with us:

- Virtual information meeting: 1 hour
- Security control benchmarking prep: 2 hours
- Internal loss calculations and attribution: (2-10 hours)
- Calls every two weeks with MIT team (4 x 1 hour calls = 4 hours)
- Computation (1 hour)

SCRAM
Secure Cyber Risk Aggregation and Measurement

Process

Data collection (2 parts)

Benchmark

- ✓ 12.01 Maintain an Inventory of Network Boundaries
- ✓ 12.03 Deny Communications with Known Malicious IP addresses
- ✓ 12.04 Deny Communication over Unauthorized Ports
- ✓ 12.09 Deploy Application Layer Filtering Proxy Server
- ✗ 12.10 Decrypt Network Traffic at Proxy

(…)

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

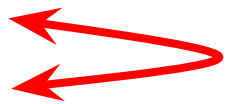
(…)

SCRAM
Secure Cyber Risk Aggregation and Measurement

MPC: Data cleaning done all BEFORE submission

- Typical data analysis
  - 1. Gather data
  - 2. Clean data
  - 3. Run analysis

- Multi-party computation analysis (SCRAM)
  - 2. Clean data
  - 1. Gather data
  - 3. Run analysis



SCRAM
Secure Cyber Risk Aggregation and Measurement

SCRAM data entry

Part 1: Benchmarking

Part 2: Losses

	B	C	D	E	F	G	H	I	J
1	**Status:**	**Not Ready**	CIS-Num	Variable	**EXAMPLE:Calc1**	Calc1:ImplementedControls(y=1, no = blank or 0)	**EXAMPLE:Calc2**	Calc2:Event01	Calc2:Event02
2	**Errors/Missing:**	2	0.01	LOSS (in USD, e.g. 1m = 1,000,000)			145,000		
3	CISControl	CIS-SensorCategory	CIS-Num	Variable					
4	Inventory and Co	Active Device Discovery	1.01	Utilize an Active Discovery Tool	1				
5	Inventory and Co	Passive Device Discover	1.02	Use a Passive Asset Discovery Tool	1				
6	Inventory and Co	Log Management Syste	1.03	Use DHCP Logging to Update Asset Inventory					
7	Controlled Use o	Log Management Syste	4.08	Log and Alert on Changes to Administrative Group Membership					
8	Controlled Use o	Log Management Syste	4.09	Log and Alert on Unsuccessful Administrative Account Login	1		1		
9	Maintenance, M	Log Management Syste	6.02	Activate audit logging	1				
10	Maintenance, M	Log Management Syste	6.03	Enable Detailed Logging					
11	Maintenance, M	Log Management Syste	6.04	Ensure adequate storage for logs	1				
12	Maintenance, M	Log Management Syste	6.05	Central Log Management	1				
13	Maintenance, M	Log Management Syste	6.06	Deploy SIEM or Log Analytic tool					
14	Maintenance, M	Log Management Syste	6.07	Regularly Review Logs	1				
15	Maintenance, M	Log Management Syste	6.08	Regularly Tune SIEM					
16	Email and Web E	Log Management Syste	7.06	Log all URL requests					
17	Malware Defens	Log Management Syste	8.08	Enable Command-line Audit Logging					
18	Controlled Acces	Log Management Syste	14.09	Enforce Detail Logging for Access or Changes to Sensitive Data	1				
19	Account Monito	Log Management Syste	16.12	Monitor Attempts to Access Deactivated Accounts	1				
20	Account Monito	Log Management Syste	16.13	Alert on Account Login Behavior Deviation	1				
21	Inventory and Co	Asset Inventory System	1.04	Maintain Detailed Asset Inventory					
22	Inventory and Co	Asset Inventory System	1.05	Maintain Asset Inventory Information	1				
23	Inventory and Co	Asset Inventory System	1.06	Address Unauthorized Assets	1				
24	Inventory and Co	Network Level Authent	1.07	Deploy Port Level Access Control					
25	Inventory and Co	Public Key Infrastructur	1.08	Utilize Client Certificates to Authenticate Hardware Assets					
26	Inventory and Co	Software Application Ir	2.01	Maintain Inventory of Authorized Software	1		1		
27	Inventory and Co	Software Application Ir	2.02	Ensure Software is Supported by Vendor					
28	Inventory and Co	Software Application Ir	2.03	Utilize Software Inventory Tools					
29	Inventory and Co	Software Application Ir	2.04	Track Software Inventory Information					
30	Inventory and Co	Software Application Ir	2.05	Integrate Software and Hardware Asset Inventories	1				
31	Inventory and Co	Software Application Ir	2.06	Address unapproved software	1				

SCRAM-CyberRisk-Template-2021 | CalcLosses | CalcLoss^2 | Checks | Output | +

SCRAM
Secure Cyber Risk Aggregation and Measurement

Current version at: https://scram.mit.edu/participate/

Computation steps

Step 1:
Key generation
(Key holders only)

Step 2:
Data entry and computation
(All participants)

Step 3:
Decryption
(Key holders only)

Local

1. Each participant generates a public/private key pair
2. Each participant sends in the public key

Server

3. All keys are used to generate a shared meta-public key
4. New meta-public key is distributed to all participants

Local

5. Everyone encrypts their data using the meta-public key and sends it to the server

Server

6. Computation over encrypted data
7. Encrypted result is sent back to each participant

Local

8. Each keyholder decrypts a share of the result using their private key that only they know
9. Keyholders send their partial decryption shares back to the server

Server

10. The combined received decryption shares unlock just the result - not the inputs

SCRAM
Secure Cyber Risk Aggregation and Measurement

Computation steps - Simplified

Step 1: Key generation (Key holders only)	Local	1. Each participant generates a public/private key pair 2. Each participant sends in the public key
	Server	3. All keys are used to generate a shared meta-public key 4. New meta-public key is distributed to all participants
Step 2: Data entry and computation (All participants)	Local	5. Everyone encrypts their data using the meta-public key and sends it to the server
	Server	6. Computation over encrypted data 7. Encrypted result is sent back to each participant
Step 3: Decryption (Key holders only)	Local	8. Each keyholder decrypts a share of the result using their private key that only they know 9. Keyholders send their partial decryption shares back to the server
	Server	10. The combined received decryption shares unlock just the result - not the inputs

Step 1:
Key holders meet to create the keys

Step 2:
All participants **upload their Excel sheet** into their browser where the data is extracted and encrypted before being sent to the server

Step 3:
Key holders meet again to help decrypt the result

SCRAM
Secure Cyber Risk Aggregation and Measurement

Thank you