APPENDIX 3:
EPRI CYBER SECURITY METRICS

Appendix to **Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators**

Project Title: Europe and Eurasia Cybersecurity Partnership

Sponsoring USAID Office: USAID Bureau for Europe and Eurasia

Cooperative Agreement #: AID – OAA-A-16-00049

Recipient: National Association of Regulatory Utility Commissioners (NARUC)

Date of Publication: May 2020

Author: CNR-IRCrES, The National Research Council of Italy, Research Institute on Sustainable Economic Growth[1]

[1] The present document has been prepared by Elena Ragazzi (project leader), Ugo Finardi, and Alberto Stefanini.

1 DATA POINTS FOR EPRI CYBER SECURITY METRICS

EPRI CS metrics is based on 120 data points. These provide operational statistics collected from various points in utility operations. The data points that provide the metrics foundations are all measurable quantities. These simple indicators are the bases for the calculation of scores.

The source of the list presented in this section and in the following one is the EPRI report: Suh-Lee, C. (2017). Cyber Security Metrics for the Electric Sector: Volume 3. Palo Alto, CA: EPRI. The report is freely available from https://www.epri.com/#/pages/product/3002010426/?lang=en-US

Data Point ID	Data Point	Collection Scope
A01	Number of internal IPs reachable	Per asset
A02	Outbound connection to internet	Per asset
A03	Inbound connection from the internet	Per asset
A04	Distance from the internet	Per asset
A05	Outbound connection to non-secure network (applicable to a protected network without internet connection)	Per asset
A06	Inbound connection from non-secure network (applicable to a protected network without internet connection)	Per asset
A07	Distance from the non-secure network (applicable to a protected network without internet connection)	Per asset
A08	Asset criticality rating	Per asset
A09	Number of active default account/password	Per asset
A10	Number of active system-privileged accounts	Per asset
A11	Number of active shared accounts (shared password or no password)	Per asset
A12	Number of active shared system-privileged accounts	Per asset

Data Point ID	Data Point	Collection Scope
A13	Number of active user accounts with no password expiry	Per asset
A14	Number of active user accounts with expired password	Per asset
A15	Number of total users who can login to the system	Per asset
A16	Number of total users who are authorized to login to the system	Per asset
A17	Physical: Number of people who are authorized to access the asset (can touch)	Per asset
A18	Physical: Number of people who can access the asset without force	Per asset
A19	Physical: Number of physical barriers to the asset from the closest public location	Per asset
A20	Asset ID	Per asset
B01	Total number of personnel	Per business unit
B02	Number of personnel who participated in social engineering test	Per business unit
B03 B03	Failure rate on last email phishing test	Per business unit
B04	Number of organizations directly providing threat intelligence under contract/agreement	Per business unit
B05	Number of organizations directly providing threat intelligence informally	Per business unit
T06	Threat hunting practice	Per business unit
T07	Number of employees trained for threat hunting	Per business unit
T08	Number of threat hunting investigation per month	Per business unit
T09	Business unit ID	Per business unit
D01	Data criticality rating	Per database
D02	Encryption at rest	Per database
D03	Encryption in transit	Per database
D04	Mean network access control score of hosting assets	Per database
D05	Mean network vulnerability control score of hosting assets	Per database
D06	Data redundancy	Per database

Data Point ID	Data Point	Collection Scope
D07	Backup frequency	Per database
D08	Native audit trail enabled	Per database
D09	Audit trail review	Per database
D10	Segregation of duties enforced	Per database
D11	Asset ID of hosting server	Per database
E01	Device ID of event generating system	Per event
E02	Severity	Per event
E03	Date opened	Per event
E04	Date closed	Per event
E05	Confirmed security incidents	Per event
I01	Date first noticed	Per incident
I02	Date of first occurrence	Per incident
I03	Date first actioned	Per incident
I04	Date contained	Per incident
I05	Date completed recovery	Per incident
I06	Network penetration involved	Per incident
I07	Data leak/loss involved	Per incident
I08	Social engineering involved	Per incident
I09	Malware involved	Per incident
I10	Mobile end-point involved	Per incident
I11	Malicious email involved	Per incident
I12	Malicious URL involved	Per incident
I13	Physical access violation involved	Per incident
I14	Stationary end-point involved	Per incident
I15	Severity rating	Per incident
I16	Cost of response in man-hour (existing resources)	Per incident
I17	Cost of response in dollar amount (extra resources)	Per incident
I18	First noticed by category	Per incident
I19	Asset IDs of affected devices	Per incident
M01	Email: number of total inbound emails per day	Per email server/filter
M02	Email: number of total outbound emails per day	Per email server/filter
M03	Email: number of filtered emails per day	Per email server/filter
M04	Email: number of spams detected per week	Per email server/filter

Data Point ID	Data Point	Collection Scope
M05	Email: number of phishing attempts detected per week	Per email server/filter
M06	Email: number of malware detected per week	Per email server/filter
M07	Email: number of spams reported by the user per week	Per email server/filter
M08	Email: number of phishing attempts reported by the user per week	Per email server/filter
M09	Email: number of malware reported by the user per week	Per email server/filter
M10	Email: number of outbound email with sensitive data - detected per week	Per email server/filter
M11	Asset ID	Per email server/filter
M12	Date	Per email server/filter
N01	Number of inbound connections per day	Per network access Point
N02	Number of outbound connections per day	Per network access Point
N03	Number of dropped inbound connections per day	Per network access Point
N04	Number of all alerts per day	Per network access Point
N05	Number of security alerts per day	Per network access Point
N06	Number of probes per day	Per network access Point
N07	Number of confirmed DOS attempts per month	Per network access Point
N08	Number of confirmed intrusion attempts per month	Per network access Point
N09	Number of confirmed cyber incidents that required human intervention per month	Per network access Point
N10	Wireless communication allowed	Per network access Point
N11	Wireless: protocol	Per network access Point
N12	Wireless: signal strength in dBm	Per network access Point
N13	Wireless: encryption	Per network Access Point
N14	Wireless: antenna type	Per network access Point
N15	Wireless: frequency-hopping	Per network access Point
N16	Network access control enabled	Per network access Point
N17	Asset ID	Per network access Point
N18	Date	Per network access Point
P01	Last security awareness training	Per personnel
P02	System-privileged access to at least one system	Per personnel
P03	Physical access to at least one cyber asset	Per personnel
P04	Read-access to at least one type of high criticality rating data	Per personnel
P05	Write-access to at least one type of high criticality rating data	Per personnel
P06	Business unit ID	Per personnel

Data Point ID	Data Point	Collection Scope
T01	Intelligence received from	Per threat warning/alert
T02	Date threat warning/alert received	Per threat warning/alert
T03	Date threat warning/alert response action started	Per threat warning/alert
T04	Date threat warning/alert response completed	Per threat warning/alert
T05	Intelligence led to confirmed security incident	Per threat warning/alert
T06	Triggered by internal threat hunting	Per threat warning/alert
U01	Malware protection: anti-virus signature update frequency	Per end-user device
U02	Malware protection: anti-virus scan frequency	Per end-user device
U03	Malware protection: proportion of applications that are exempt from anti-virus scan	Per end-user device
U04	Malware protection: proportion of files/folders/drives that are exempt from anti-virus scan	Per end-user device
U05	Mobile device: encryption	Per end-user device
U06	Mobile device: central management of device security policy	Per end-user device
U07	Mobile device: theft/lost device control	Per end-user device
U08	HIDS management	Per end-user device
U09	Number of connections to critical data/asset/application allowed from this device	Per end-user device
U10	Asset ID	Per end-user device
V01	Vulnerability ID	Per vulnerability
V02	Vulnerability CVSS	Per vulnerability
V03	Asset ID	Per vulnerability
W01	Web Proxy: % of end-point going through proxy	Per web proxy
W02	Web Proxy: general social network sites allowed for all users	Per web proxy
W03	Web Proxy: private email access allowed for all users	Per web proxy
W04	Web Proxy: private cloud storage allowed for all users	Per web proxy

2 EPRI CYBER SECURITY METRICS

The listed data points are used to calculate operational metrics and some composite indicators, called scores. There is a hierarchy in the calculation of the metrics:

- Data points are used to calculate operational metrics (14-60)
- Operational metrics are summarized in tactical scores (4-13)
- Tactical scores are further summarized in three strategic scores (1-3)

Ref #	Metric ID	Metric	Description
1.	S-PS	Protection Score	A numerical value between 0 and 10, indicating the effectiveness of the overall protective controls in a target system.
2.	S-DS	Detection Score	A numerical value between 0 and 10, indicating the effectiveness of the overall detective controls in a target system.
3.	S-RS	Response Score	A numerical value between 0 and 10, indicating the effectiveness of the overall security incident response and recovery capability.
4.	T-NPPS	Network Perimeter Protection Score	A numerical value indicating the effectiveness of network perimeter protection controls. The security controls in place for perimeter protection are measured and balanced with the risk level associated with the control. These are controls on network access points (wired or wireless), and for internet traffics through the perimeter (e.g. http proxy, email filter, etc.)
5.	T-EPS	End-point Protection Score	A numerical value indicating the effectiveness of end-point device protection controls. The security controls in place for end-point protection for both stationary and mobile end-points are measured and balanced with the risk level associated with the controls. These include anti-malware software configuration, mobile device management, and host-based firewall management.

Ref #	Metric ID	Metric	Description
6.	T-PAS	Physical Access Control Score	A numerical value indicating the effectiveness of physical access controls. The security controls in place for physical access control are measured and balanced with the risk level associated with the controls. Number of people with physical access, authorization of access, and controls in place to prevent unauthorized access are among the considerations in measuring the effectiveness.
7.	T-HSS	Human Security Score	A numerical value indicating the effectiveness of human security components. The frequency and completeness of security awareness training, phishing test performance, number of incidents involving social engineering, and number of incidents first detected by employee or other personnel.
8.	T-NVS	Core Network Vulnerability Control Score	A numerical value indicating the vulnerability control in a network. The risk of a vulnerability is calculated with the respect to the network connectivity and proximity, capturing the controls in place through network design as well as patching.
9.	T-NAS	Core Network Access Control Score	A numerical value indicating the effectiveness of the access control in a network. The status of access control is calculated with the respect to the network connectivity and proximity, capturing the control in place through network design as well as access control to a device itself.
10.	T-DPS	Data Protection Score	A numerical value indicating the effectiveness of data protection in a network. This is a mean value of confidentiality score, availability score, and integrity score of all databases in the network.
11.	T-TAS	Threat Awareness Score	A numerical value indicating the level of situational awareness and effectiveness of threat intelligence management.
12.	T-TDS	Threat Detection Score	A numerical value indicating the effectiveness of threat detection in both technical and procedural perspectives. This score relies heavily on the accurate incident response/tracking data.

Ref #	Metric ID	Metric	Description
13.	T-IRS	Incident Response Score	A numerical value indicating the effectiveness of the incident response program. This score relies heavily on the accurate incident response/tracking data.
14.	O-A-MAC	Mean Asset Connectivity	An average asset connectivity of all assets in a target network. Asset connectivity represents the degree of connectivity within a network. Generally higher asset connectivity is associated with higher risk.
15.	O-A-MAP	Mean Asset Proximity to Hostile Network	An average asset proximity of all assets in a target network. Asset proximity represents how close an asset is logically located to a hostile network. A lower proximity indicates higher risk.
16.	O-A-MVRS	Mean Asset Vulnerability Risk Score	An average asset vulnerability risk score of all assets in a target network. The asset vulnerability risk score is the sum of the common vulnerability scoring system (CVSS) of all vulnerabilities discovered in the asset. A high asset vulnerability risk score indicates high risk to the asset.
Ref #	Metric ID	Metric	Description
17.	O-A-MNVRS	Mean Network Vulnerability Risk Score	An average asset vulnerability risk score of all assets in a target network. The asset vulnerability risk score is the sum of the common vulnerability scoring system (CVSS) of all vulnerabilities discovered in the asset. A high asset vulnerability risk score indicates high risk to the asset.
18.	O-A-MACS	Mean Asset Access Control Score	An average access control score of all assets in a target network. The access control score is higher where there is a higher degree of controls preventing possible unauthorized access.
19.	O-A-MNACS	Mean Network Access Control Score	An average network access control score of all assets in a target network. This value represents the asset access control score augmented by the asset connectivity and asset proximity to hostile network. A higher network access control score indicates a higher degree of control and lower risk.

Ref #	Metric ID	Metric	Description
20.	O-A-MPACS	Mean Physical Access Control Score	An average physical access control score of all assets in a network. The physical access control score represents the effectiveness of physical access controls for the asset.
21.	O-D-MDAS	Mean Data Availability Score	An average data availability score for all databases in a target network. The aata availability score represents the effectiveness of controls against data loss or unavailability for the database.
22.	O-D-MDCS	Mean Data Confidentiality Score	An average data confidentiality score for all databases in a target network. The data confidentiality score represents the effectiveness of controls against the unauthorized disclosure of data stored in the database.
23.	O-D-MDIS	Mean Data Integrity Score	An average data integrity score for all databases in a target network. The data integrity score represents the extent of controls against unauthorized or accidental modification of the data stored in the database.
24.	O-N-MAPS	Mean Access Point Protection Score	An average access point protection score of all access points in a target network. The access protection score must be calculated first for each access point from the numerical value representing security controls and risk associated with the access point.
25.	O-N-MWAPS	Mean Wireless Access Point Protection Score	An average wireless access point protection score of all wireless access points in a target network. The wireless access protection score must be calculated first for each wireless access point from the numerical value representing security controls and risk associated with the wireless access point.
Ref #	Metric ID	Metric	Description
26.	O-N-MIPS	Mean Internet Traffic Protection Score	An average internet traffic protection score of all internet traffic filtering devices in a target network. The score represents the extent of internet traffic controls in place such as DNS filtering, email filtering, and web proxies.

Ref #	Metric ID	Metric	Description
27.	O-H-MHSS	Mean Human Security Score	A numeric value indicating the effectiveness of security control involving human agents. Security awareness of individuals handling cyber assets and the security test results are considered in calculating this score.
28.	O-U-MSDPS	Mean Stationary End- Point Protection Score	A numerical value representing the effectiveness of security controls on the stationary end-point.
29.	O-U-MMDPS	Mean Mobile End-Point Protection Score	A numerical value representing the effectiveness of security controls on the mobile end-point.
30.	O-I-MCT	Monthly Incident Count - Total	An average time in days from the discovery of an incident to the complete recovery from the incident.
31.	O-I-MCH	Monthly Incident Count - High Severity	An average monthly count of high severity security incidents for a calendar year.
32.	O-I-MCM	Monthly Incident Count - Medium Severity	An average monthly count of medium severity security incidents for a calendar year.
33.	O-I-MCMSI	Monthly Count - Missed Security Incidents	An average monthly count of missed security incidents for a calendar year. Missed security incidents include the incidents first noticed by malfunction of device, non-security staff report, compromise notification, adversary notification, or public disclosure.
34.	O-I-MCDL	Monthly Incident Count - Data Leak/Loss	An average monthly count of security incidents involving data leak or loss for a calendar year.
35.	O-I-MCME	Monthly Incident Count - Malicious Email	An average monthly count of security incidents involving malicious email for a calendar year.

Ref #	Metric ID	Metric	Description
36.	O-I-MCMU	Monthly Incident Count - Malicious URL	An average monthly count of security incidents involving malicious URL for a calendar year.
37.	O-I-MCMW	Monthly Incident Count - Malware	An average monthly count of security incidents involving malware infection for a calendar year.
38.	O-I-MCNP	Monthly Incident Count - Network Penetration	An average monthly count of security incidents involving network penetration for a calendar year.
39.	O-I-MCMD	Monthly Incident Count - Mobile End-Point	An average monthly count of security incidents involving mobile end-point for a calendar year.
40.	O-I-MCSD	Monthly Incident Count - Stationary End-Point	An average monthly count of security incidents involving stationary end-point for a calendar year.
41.	O-I-MCSE	Monthly Incident Count - Social Engineering	An average monthly count of security incidents involving social engineering for a calendar year.
42.	O-I-MPAV	Monthly Incident Count - Physical Access Violation	An average monthly count of security incidents involving physical access violation for a calendar year.
43.	O-I-MTTD	Mean Time to Discovery	An average time in days from the first occurrence of an incident to the first discovery of the incident. The day of first occurrence is usually found after the discovery through investigation.
44.	O-I-MTBI	Mean Time between Incidents	The average time in days from the first occurrence of an incident to the first occurrence of incident in that month.

Ref #	Metric ID	Metric	Description
45.	O-I-MTTA	Mean Time to First Action	An average time in days from the discovery of an incident to the first action taken.
46.	O-I-MTTC	Mean Time to Containment	An average time in days from the discovery of an incident to the containment of the incident.
47.	O-I-MTR	Mean Time to Recovery	An average time in days from the discovery of an incident to the complete recovery from the incident.
48.	O-I-MCRM	Mean Cost of Response in Man-Hour (existing resource)	An average cost of response in man-hours for existing resources normally engaged in incident response activities.
49.	O-I-MCRX	Mean Cost of Response in Dollar Amount (extra resource)	An average cost of response in dollar amount for extra resources engaged in resolving a security incident.
50.	O-I-MCHR	Monthly Incident Count - Non-Security Staff Reporting	An average monthly count of incidents, first detected by non-security staff reporting.
51.	O-E-METP	Mean Security Event True Positive Rate	An average value of true positive rate for all security event generating devices in a target network. The true positive rate is the number of security events that are confirmed as genuine security incidents over the number of all events generated by the device. A higher true positive rate indicates higher accuracy.
52.	O-E-MC	Monthly Count - Security Events	An average monthly count of all security events generated in a target network for a calendar year.

Ref #	Metric ID	Metric	Description
53.	O-T-IES	Threat Intelligence Effectiveness Score	A numerical value representing the threat/situational awareness of an organization. A high score indicates high awareness of security threats/risks.
54.	O-T-MITP	Threat Intelligence True Positive Rate	An average value of true positive rate for all threat intelligence sources for an organization. The true positive rate is the number of threat intelligence warnings that are confirmed to lead to security incidents over the number of all threat intelligences generated by the source.
55.	O-T-MCI	Monthly Count - Threat Intelligence	An average monthly count of threat intelligence received by an organization for a calendar year.
56.	O-T-MTIA	Mean Time from Intelligence to Action	An average time in days from the day threat intelligence warning is received to the day the first action was taken by the receiving organization.
57.	O-T-MTIP	Mean Time from Intelligence to Protection	An average time in days from the day threat intelligence warning is received to the day the organization completed the protective action.
58.	O-T-THES	Threat Hunting Effectiveness Score	A numerical value indicating the effectiveness of threat hunting practices. A high score indicates a high degree of effectiveness.
59.	O-T-THTP	Mean Threat Hunting True Positive Rate	An average value of true positive rate for all threat hunting investigations occurring in a given period. The true positive rate is the number of threat hunting that lead to the discovery of security incidents over the number of all threat hunting investigations launched in the period.
60.	O-T-MCH	Monthly Incident Count - Threat Hunting Investigation	An average monthly count of threat hunting investigations for a calendar year.