Energy Industry Cybersecurity Desirability Questions Guide v1

This is a reference document (of the 29 criterion) for the creation ordinal and cardinal desirability questions for strategic decision makers to rank the importance (n their minds) towards cybersecurity at their organization based on their strategic goals.

In this ideological model each criteria would have inclusively implemented each element of a control to meet a threshold score (a percentage to weight the criterion by against the Technical SME's ranking from step 1).

Note: Phrases to use: expected level, degree of, required, amount of, extent, and complexity of

What is the expected level that change management will be considered?

1. Awareness of need for change management – 20%
2. Naming conventions, version control in place – 40%
3. There is a system, and document and storage retrieval system – 60%
4. Scope assessment against: quality, risk, schedule, cost, resources, and customer satisfaction is done - 80%
5. A repeatable and sustainable framework is in place - 90%

To what degree are computer user's settings and permissions known by line management?

1. Settings are unknown to the management and is thus a gap in security – 25
2. What each staff person needs to know is understood by the manager – 50
3. Overprivileged settings have a plan for remediation – 70
4. Users' computer settings for chances of breaches of data are low because user settings are audited by manager – 90

To what extent is cybersecurity awareness of working staff checked?

1. Phishing emails sent (and responses captured) – 20
2. Training courses provided (and data captured) – 40
3. Systems access and authorization is logged and reviewed -75
4. Scanning is done for rogue access points (aka hotspots) – 95

Are Cybersecurity goals at one of these expected levels?

1. Cybersecurity goals are updated periodically – 30
2. Cybersecurity scanning tools are used – 60
3. Dashboards are monitoring cybersecurity controls – 90

What is the amount of Cybersecurity learning sources available?

1. Threats to energy systems are trained on – 30
2. Internet crime is postered or communicated – 50
3. Credentials as the main source of penetration is discussed – 60
4. Cybersecurity personnel have working policies and formal procedures – 90

What is the expected level of Cybersecurity Readiness Assessments in the organization?

1. Self-assessments – 25
2. Internal auditing surveys and checklists are used – 45
3. Assessment results are integrated into Administrative and Strategic workers methodology (not only Technical workers) – 65
4. Quantitative ratings are done – 90

Cybersecurity Risk is a required topic by C-Suite

1. Security is considered important by C-Suite – 40
2. CIO is making strategic decisions at the board level or equivalent – 70
3. There is a plan for Cyber experts to be involved at the strategy level – 80
4. Is terrorism planned for? – 95

What is the complexity of Data Loss Prevention (DLP) systems that are in place?

1. Have Incident Response Plan - 10
2. Logging, threats, retention, reporting, and cloud are included in the thought process -30
3. Legal team checks on document retention - 40
4. Contracting includes DLP - 60
5. Have a forensic model - 80
6. Have a system for threat management covering all the topics above – 95

What is the level that documents are marked and protected?

1. Language to use for communication of high importance topics is circulated - 30
2. Sensitive information is stored on separate systems - 60
3. Inconsistent markings are mitigated – 90

To what degree are Energy System outages planned to?

1. There is a plan for power loss - 40
2. Maintenance outages are part of the planning process - 60
3. Long term outages contingency has been planned for - 75
4. Cascading grid failures are considered – 90

What is the required amount of external reporting?

1. Security reports are done - 30
2. Escalation plan for incidents is in place - 55
3. Electricity Information Sharing and Analysis Centers (E-ISAC) and Computer Security Incident Response Teams (CSIRT) are part of the process – 95

What is the degree of vendor and supply alignment on security?

1. Supply chain is monitored - 40
2. Sharing with vendors is done - 80
3. Periodic updates on cyber security are pushed to vendors and pulled from supply chain – 90

What is amount of communication sharing with Internet Service Provider?

1. Chief Information Office (CIO's) office has a line of communication – 50%
2. Cyber awareness activities are exchanged – 75%

Logging required is sufficient for Security and Forensics

1. Timestamps/log time of systems is maintained - 30
2. Logs are retrievable and accessible to specialists – 50
3. Backup storage restoration is tested - 75
4. Timestamps/log time is protected – 90

What is the degree that machine limitations are recorded?

1. Subnetting is done for ICS/IoT/Nuclear – 30
2. Industrial Control Systems (ICS and IoT/Nuclear) hardening limitations are known - 50
3. Required protocols are known and deny all others to these machines - 70
4. Intrusion detections systems are best in class based on budget – 90

What is the extent that Network and System Administration procedures are documented?

1. Procedures are vetted in the company - 40
2. Operational procedures are shared and include roles - 70
3. Interfaces that are routable are at least medium risk - 80
4. Third parties have validated the procedures – 95

What is the degree of network modeling for ICS/IoT/Nuclear done?

1. A network model that shows protocols and cloud connections exists - 50
2. Non-TCP/IP network communication is modeled - 75
3. Network diagrams are requirements in contracting language - 90

What is the expected level of outages required for applying security updates?

1. There is a work stoppage plan – 50
2. Spares enable continuous operation – 80
3. Assessments of machines is done regularly while keeping machines in operable state – 95

What is the degree of planning done for forensic evidence collection?

1. Internal requirements for evidence collection exist (including chain of custody) – 50
2. A legal attribution model exists in company - 80
3. A cloud provider forensic plan exists – 95

What is the expected level of policy updating?

1. Policies are updated regularly - 30
2. Data disclosure has a policy -50
3. Jurisdictional (Federal, State, Local) requirements are accounted for - 80
4. Monetary penalties for violations/non-conformance are known – 95

What is the degree of implementation oversight?

1. Implementation baselines are known and tested periodically - 50
2. Need to know (including users computer settings) is defined and discussed in the workplace - 75
3. Standards are used such as ISO, NIST, etc. for firewalling and operational procedures – 90

What is the degree of legal understanding?

1. Non-compliance and resultant forced oversight are mitigated - 60
2. Monetary penalties are possible to be reduced because legal is aware and reacting to new legislation – 95

What is the required level of certification in operations roles?

1. Development plans have been implemented that control for operations roles - 50
2. Staff is aware of industry governance landscape – 75

What is the degree of retention periods for data and information?

1. The organization has a retention plan - 40
2. Is attribution able to be evidenced within a reasonable time frame (e.g., 5 years per Sarbanes Oxley or 3 years or more for Federal Records “FOIA”)? - 50
3. Offline backups are kept for records - 60
4. Cloud assets retention plan exists – 90

What is the extent to which social impact of breaches are talked about?

1. Organization has some awareness campaigns - 50
2. Breach plans are clear in Incident Response Plan - 75
3. Social manipulation is discussed (con artistry tactics, slander) - 90

What is the expected level that standards are understood?

1. Models in organization are referenced to standards - 45
2. Discussion about standards meanings is encouraged and captured in notes - 65
3. Auditor assessments compare organizational requirements with standards – 75
4. Self-checklists are formed from standards – 95

Are complex Cyber supply chain risks considered in procurement?

1. Third party information sharing is done - 50
2. Controls are in place with suppliers (and vendors) – 80

What is the expected level of Cybersecurity vocabulary awareness?

1. Vocabulary specific to attacks is created - 60
2. A comprehensive vocabulary dictionary exists that can be referenced for any discussion – 90

What is the expected level that threats to the organization are modeled?

1. Threat models are created for new implementations - 50
2. Lessons learned are used for threat modeling - 60
3. Threat models go through a validation process before being accepted – 65
4. Threat models are shared with trusted partners - 95