Topic: Cybersecurity Readiness for Energy Industry

* Required

Name *

Your answer

Email

Your answer

Would others or you consider yourself a cyber security expert? *

◯ Yes

◯ No

Work Type *

◯ Academia

◯ Science or Government

◯ Industry or Commercial

Mission Resources *

○ Severely Constrained

○ Constrained

○ No Feasible Limit

Which sector of Energy IT do you mostly work in *

○ Industrial Control Systems (ICS)/National Grid

○ IoT/Smart Grid

○ Nuclear

*

Perspective importance to topic ca1: Technical vs Organizational

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Perspective importance to topic ca2: Professional vs Technical

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Perspective importance to topic ca3: Leadership vs Professional *

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Perspective importance to topic ca12: Professional vs Organizational

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Perspective importance to topic ca13: Leadership vs Technical

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Perspective importance to topic ca23: Leadership vs Organizational

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Organizational Perspective cb1: Cybersecurity Readiness Assessments vs
Presence of Implementation Oversight

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb2: Presence of legislative understanding vs
Cybersecurity Readiness Assessments

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb3: Computer users settings and permissions are known vs Presence of legislative understanding

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb4: Social impact of breaches is talked about in the company vs Computer users settings and permissions are known

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Organizational Perspective cb5: Documents are marked and protected vs Social impact of breaches is talked about in the company

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb6: There is an organizational common vocabulary for cybersecurity in the energy industry vs Documents are marked and protected

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Organizational Perspective cb12: Presence of legislative understanding vs Presence of Implementation Oversight

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb13: Computer users settings and permissions are known vs Cybersecurity Readiness Assessments

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb14: Social impact of breaches is talked about in the company vs Presence of legislative understanding

1 ⭘

2 ⭘

3 ⭘

4 ⭘

5 ⭘

6 ⭘

7 ⭘

8 ⭘

9 ⭘

10 ⭘

*

Organizational Perspective cb15: Documents are marked and protected vs
Computer users settings and permissions are known

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb16: There is an organizational common vocabulary for cybersecurity in the energy industry vs Social impact of breaches is talked about in the company

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb23: Computer users settings and permissions are known vs Presence of Implementation Oversight

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb24: Social impact of breaches is talked about in the company vs Cybersecurity Readiness Assessments

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb25: Documents are marked and protected vs
Presence of legislative understanding

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb26: There is an organizational common vocabulary for cybersecurity in the energy industry vs Computer users settings and permissions are known

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Organizational Perspective cb34: Social impact of breaches is talked about in the company vs Presence of Implementation Oversight

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb35: Documents are marked and protected vs
Cybersecurity Readiness Assessments

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb36: There is an organizational common vocabulary for cybersecurity in the energy industry vs Presence of legislative understanding

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb45: Documents are marked and protected vs Presence of Implementation Oversight

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb46: There is an organizational common vocabulary for cybersecurity in the energy industry vs Cybersecurity Readiness Assessments

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Organizational Perspective cb51: Presence of Implementation Oversight vs There is an organizational common vocabulary for cybersecurity in the energy industry
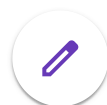
1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc1: Data loss prevention system is in place vs Logging is sufficient for security and forensics

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc2: Planning for forensic evidence collection vs Data loss prevention system is in place

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc3: Retention periods are in place and used for information and data vs Planning for forensic evidence collection

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc4: Network modeling for IoT is done vs Retention periods are in place and used for information and data

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc5: Standards are understood vs Network modeling for IoT is done

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc6: Energy system outages are planned for vs Standards are understood

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Technical Perspective cc7: Machine limitations are recorded vs Energy system outages are planned for

*

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc8: Network and System admin procedures documented vs Machine limitations are recorded

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc9: Outages are not required for security updates vs
Network and System admin procedures documented

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc10: Info Officer is in contact with Internet Service Provider vs Outages are not required for security updates

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc11: Logging is sufficient for security and forensics vs
Info Officer is in contact with Internet Service Provider

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc12: Planning for forensic evidence collection vs Logging is sufficient for security and forensics

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc13: Retention periods are in place and used for information and data vs Data loss prevention system is in place

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc14: Network modeling for IoT is done vs Planning for forensic evidence collection

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc15: Standards are understood vs Retention periods are in place and used for information and data

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc16: Energy system outages are planned for vs Network modeling for IoT is done

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc17: Machine limitations are recorded vs Standards are understood

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc18: Network and System admin procedures documented vs Energy system outages are planned for

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc19: Outages are not required for security updates vs
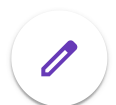Machine limitations are recorded

1   ○

2   ○

3   ○

4   ○

5   ○

6   ○

7   ○

8   ○

9   ○

10 ○

*

Technical Perspective cc20: Info Officer is in contact with Internet Service Provider vs Network and System admin procedures documented

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc21: Logging is sufficient for security and forensics vs
Outages are not required for security updates

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc22: Data loss prevention system is in place vs Info
Officer is in contact with Internet Service Provider

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc23: Retention periods are in place and used for information and data vs Logging is sufficient for security and forensics

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc24: Network modeling for IoT is done vs Data loss prevention system is in place

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc25: Standards are understood vs Planning for forensic evidence collection
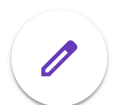
1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc26: Energy system outages are planned for vs Retention periods are in place and used for information and data

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc27: Machine limitations are recorded vs Network modeling for IoT is done

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc28: Network and System admin procedures documented vs Standards are understood

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc29: Outages are not required for security updates vs Energy system outages are planned for

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc30: Info Officer is in contact with Internet Service
Provider vs Machine limitations are recorded

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc31: Logging is sufficient for security and forensics vs
Network and System admin procedures documented

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc32: Data loss prevention system is in place vs Outages are not required for security updates

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc33: Planning for forensic evidence collection vs Info
Officer is in contact with Internet Service Provider

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc34: Network modeling for IoT is done vs Logging is sufficient for security and forensics

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc35: Standards are understood vs Data loss prevention system is in place
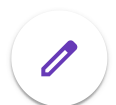
1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc36: Energy system outages are planned for vs Planning for forensic evidence collection

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc37: Machine limitations are recorded vs Retention periods are in place and used for information and data
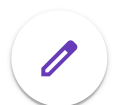
1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc38: Network and System admin procedures documented vs Network modeling for IoT is done

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc39: Outages are not required for security updates vs Standards are understood

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc40: Info Officer is in contact with Internet Service
Provider vs Energy system outages are planned for

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc41: Logging is sufficient for security and forensics vs
Machine limitations are recorded

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc42: Data loss prevention system is in place vs Network and System admin procedures documented

1   ◯

2   ◯

3   ◯

4   ◯

5   ◯

6   ◯

7   ◯

8   ◯

9   ◯

10 ◯

*

Technical Perspective cc43: Planning for forensic evidence collection vs Outages are not required for security updates

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc44: Retention periods are in place and used for information and data vs Info Officer is in contact with Internet Service Provider

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc45: Standards are understood vs Logging is sufficient for security and forensics

1 ◯
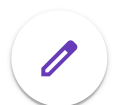
2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc46: Energy system outages are planned for vs Data loss prevention system is in place

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc47: Machine limitations are recorded vs Planning for forensic evidence collection

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc48: Network and System admin procedures documented vs Retention periods are in place and used for information and data

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc49: Outages are not required for security updates vs Network modeling for IoT is done
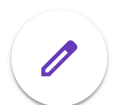
1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc50: Info Officer is in contact with Internet Service
Provider vs Standards are understood

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc51: Logging is sufficient for security and forensics vs Energy system outages are planned for
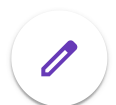
1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc52: Data loss prevention system is in place vs Machine
limitations are recorded

1   ◯

2   ◯

3   ◯

4   ◯

5   ◯

6   ◯

7   ◯

8   ◯

9   ◯

10 ◯

*

Technical Perspective cc53: Planning for forensic evidence collection vs Network and System admin procedures documented

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Technical Perspective cc54: Retention periods are in place and used for information and data vs Outages are not required for security updates

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Technical Perspective cc55: Network modeling for IoT is done vs Info Officer is in contact with Internet Service Provider

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Professional Perspective cd1: External vendor/supply coordination is done vs External reporting is done

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Professional Perspective cd2: Threats to organization are modeled vs External vendor/supply coordination is done
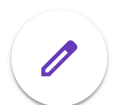
1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Professional Perspective cd3: Cyber awareness of all staff is checked vs Threats to organization are modeled

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Professional Perspective cd4: Change Management is considered vs Cyber awareness of all staff is checked

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Professional Perspective cd12: Threats to organization are modeled vs External
reporting is done

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Professional Perspective cd13: Cyber awareness of all staff is checked vs External vendor/supply coordination is done

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Professional Perspective cd14: Change Management is considered vs Threats to organization are modeled

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Professional Perspective cd23: Cyber awareness of all staff is checked vs
External reporting is done

1   ◯

2   ◯

3   ◯

4   ◯

5   ◯

6   ◯

7   ◯

8   ◯

9   ◯

10   ◯

*

Professional Perspective cd24: Change Management is considered vs External vendor/supply coordination is done

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Professional Perspective cd34: Change Management is considered vs External
reporting is done

1   ◯

2   ◯

3   ◯

4   ◯

5   ◯

6   ◯

7   ◯

8   ◯

9   ◯

10   ◯

*

Leadership Perspective ce1: Cybersecurity goals of energy organization are
identified vs Cybersecurity learning sources are available

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce2: Cybersecurity risk is considered priority by C-Suite vs Cybersecurity goals of energy organization are identified

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce3: Professionals with cyber certifications are in operations vs Cybersecurity risk is considered priority by C-Suite

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Leadership Perspective ce4: Policies are updated vs Professionals with cyber certifications are in operations

1   ◯

2   ◯

3   ◯

4   ◯

5   ◯

6   ◯

7   ◯

8   ◯

9   ◯

10 ◯

*

Leadership Perspective ce5: Supply chain cyber risk is considered during procurement vs Policies are updated

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce12: Cybersecurity risk is considered priority by C-Suite vs Cybersecurity learning sources are available

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce13: Professionals with cyber certifications are in operations vs Cybersecurity goals of energy organization are identified

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

*

Leadership Perspective ce14: Policies are updated vs Cybersecurity risk is considered priority by C-Suite

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce15: Supply chain cyber risk is considered during procurement vs Professionals with cyber certifications are in operations

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce23: Professionals with cyber certifications are in operations vs Cybersecurity learning sources are available

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce24: Policies are updated vs Cybersecurity goals of energy organization are identified

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce25: Supply chain cyber risk is considered during procurement vs Cybersecurity risk is considered priority by C-Suite

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce34: Policies are updated vs Cybersecurity learning sources are available

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce35: Supply chain cyber risk is considered during procurement vs Cybersecurity goals of energy organization are identified

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

*

Leadership Perspective ce45: Supply chain cyber risk is considered during procurement vs Cybersecurity learning sources are available

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Organizational Alternative cf1: Follower vs First Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Organizational Alternative cf2: Slow Mover vs Follower

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Organizational Alternative cf3: Do Nothing vs Slow Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Organizational Alternative cf12: Slow Mover vs First Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Organizational Alternative cf13: Do Nothing vs Follower

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Organizational Alternative cf23: Do Nothing vs First Mover

1   ○

2   ○

3   ○

4   ○

5   ○

6   ○

7   ○

8   ○

9   ○

10 ○

Technical Alternative cg1: Follower vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Technical Alternative cg2: Slow Mover vs Follower

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Technical Alternative cg3: Do Nothing vs Slow Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Technical Alternative cg12: Slow Mover vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Technical Alternative cg13: Do Nothing vs Follower

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Technical Alternative cg23: Do Nothing vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Professional Alternative ch1: Follower vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Professional Alternative ch2: Slow Mover vs Follower

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Professional Alternative ch3: Do Nothing vs Slow Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Professional Alternative ch12: Slow Mover vs First Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Professional Alternative ch13: Do Nothing vs Follower

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Professional Alternative ch23: Do Nothing vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Leadership Alternative ci1: Follower vs First Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Leadership Alternative ci2: Slow Mover vs Follower

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Leadership Alternative ci3: Do Nothing vs Slow Mover

1 ○

2 ○

3 ○

4 ○

5 ○

6 ○

7 ○

8 ○

9 ○

10 ○

Leadership Alternative ci12: Slow Mover vs First Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Leadership Alternative ci13: Do Nothing vs Follower

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Leadership Alternative ci23: Do Nothing vs First Mover

1 ◯

2 ◯

3 ◯

4 ◯

5 ◯

6 ◯

7 ◯

8 ◯

9 ◯

10 ◯

Page 1 of 1

Submit   Clear form

Never submit passwords through Google Forms.

This form was created inside of Portland State University. Report Abuse

Google Forms