MIDWEST RELIABILITY ORGANIZATION

Meeting Agenda

Security Advisory Council (SAC)

May 24, 2023
9:00 am to 3:00 pm central

MRO Corporate Offices, King Conference Center
St. Paul, MN & Webex

Classification: Public

VIDEO AND AUDIO RECORDING

Please note that Midwest Reliability Organization (MRO) may make a video and/or an audio recording of this organizational group meeting for the purposes of making this information available to board members, members, stakeholders and the general public who are unable to attend the meeting in person.

By attending this meeting, I grant MRO:

1. **Permission to video and/or audio record the meeting including me; and**
2. **The right to edit, use, and publish the video and/or audio recording.**
3. **I understand that neither I nor my employer has any right to be compensated in connection with the video and/or audio recording or the granting of this consent.**

MRO ORGANIZATIONAL GROUP GUIDING PRINCIPLES

These MRO Organizational Group Guiding Principles complement charters. When the Principles are employed by members, they will support the overall purpose of the organizational groups.

Organizational Group Members should:

1. **Make every attempt to attend all meetings in person or via webinar.**

2. **Be responsive to requests, action items, and deadlines.**

3. **Be active and involved in all organizational group meetings by reviewing all pre-meeting materials and being focused and engaged during the meeting.**

4. **Be self-motivating, focusing on outcomes during meetings and implementing work plans to benefit MRO and MRO's registered entities.**

5. **Ensure that the organizational group supports MRO strategic initiatives in current and planned tasks.**

6. **Be supportive of Highly Effective Reliability Organization (HEROTM) principles.**

7. **Be supportive of proactive initiatives that improve effectiveness and efficiency for MRO and MRO's registered entities.**

MEETING AGENDA – Security Advisory Council (SAC) – May 24, 2023

Agenda Item

1 **Call to Order and Determination of Quorum**
Ian Anderson, MRO Security Advisory Council Chair
a. Determination of Quorum and Introductions
b. Robert's Rules of Order

2 **Standards of Conduct and Anti-Trust Guidelines**
Steen Fjalstad, Director of Security, MRO

3 **MRO Regional Risk Assessment (RRA)**
Mark Tiemeier, Principal Technical Advisor, MRO

4 **Regional Security Risk Assessment (RSRA) Survey Update**
Lee Felter, Principal Security Engineer, MRO

5 **Security Advisory Council Threat Forum (SACTF) Update**
Brett Lawler, MRO Security Advisory Council Threat Forum Chair
a. Threat Call Statistics
b. Threat Call Feedback
c. Threat Forum Open Source Information Sharing

Break – 10:30 a.m. – 10:45 a.m.

6 **SAC Member Discussions: Common Themes**
Steen Fjalstad, Director of Security, MRO

7 **Charter Updates**
Ian Anderson, MRO Security Advisory Council Chair
a. SAC Charter
b. SACTF Charter

Lunch 12:00 p.m. – 1:00 p.m.

8 **2023 Security Conference Planning Update**
Cris Zimmerman, Manager of Outreach and Stakeholder Engagement, MRO

9 **MRO Representatives on NERC Subgroups - Written Reports**
Steen Fjalstad, Director of Security, MRO
a. NERC SupplyChain Working Group (SCWG) (provided by MRO Representative)
b. NERC Security Integration and Technology Enablement Subcommittee (SITES) (provided by MRO Representative)
c. NERC Reliability and Security Technical Committee (RSTC)

Break – 2:00 p.m. – 2:15 p.m.

10 **Work Plan Updates**
Ian Anderson, MRO Security Advisory Council Chair
a. SAC Workplan
b. SACTF Workplan

11 **Action Item Review**
Margaret Eastman, Security Administrator, MRO

12 **Other Business and Adjourn**
Ian Anderson, MRO Security Advisory Council Chair

Classification: Public

AGENDA

Call to Order and Determination of Quorum

a. Determination of Quorum and Roster

Ian Anderson, MRO SAC Chair

Name	Role	Company	Term
Brett Lawler	**Vice Chair**	Xcel Energy	12/31/23
Chad Wasinger	Member	Sunflower Electric Power Corporation	12/31/23
Clayton Whitacre	Member	Great River Energy	12/31/25
Daniel Graham	Member	Basin Electric Power Cooperative	12/31/24
Douglas Peterchuck	Member	Omaha Public Power District	12/31/24
Ian Anderson	**Chair**	OGE Energy Corp.	12/31/25
Jason Nations	Member	Oklahoma Gas and Electric	12/31/24
Justin Haar	Member	Minnkota Power Cooperative	12/31/23
Matthew Szyda	Member	Manitoba Hydro	12/31/23
Michael Meason	Member	Western Farmers Electric Cooperative	12/31/23
Norma Browne	Member	Ameren	12/31/24
Patrick Glunz	Member	Nebraska Public Power District	12/31/25
Peter Grandgeorge	Member	MidAmerican Energy Company	12/31/25
Rocky Tolentino	Member	Southwest Power Pool	12/31/25
Tim Anderson	Member	Dairyland Power Cooperative	12/31/24

AGENDA

Call to Order and Determination of Quorum

b. Robert's Rules of Order

Ian Anderson, MRO SAC Chair

Parliamentary Procedures. Based on Robert's Rules of Order, Newly Revised, Tenth Edition

Establishing a Quorum. In order to make efficient use of time at MRO organizational group meetings, once a quorum is established, the meeting will continue, however, no votes will be taken unless a quorum is present at the time any vote is taken.

Motions. Unless noted otherwise, all procedures require a "second" to enable discussion.

When you want to…	Procedure	Debatable	Comments
Raise an issue for discussion	Move	Yes	The main action that begins a debate.
Revise a Motion currently under discussion	Amend	Yes	Takes precedence over discussion of main motion. Motions to amend an amendment are allowed, but not any further. The amendment must be germane to the main motion, and cannot reverse the intent of the main motion.
Reconsider a Motion already resolved	Reconsider	Yes	Allowed only by member who voted on the prevailing side of the original motion. Second by anyone.
End debate	Call for the Question *or* End Debate	No	If the Chair senses that the committee is ready to vote, he may say "if there are no objections, we will now vote on the Motion." Otherwise, this motion is not debatable and subject to majority approval.
Record each member's vote on a Motion	Request a Roll Call Vote	No	Takes precedence over main motion. No debate allowed, but the members must approve by majority.
Postpone discussion until later in the meeting	Lay on the Table	Yes	Takes precedence over main motion. Used only to postpone discussion until later in the meeting.
Postpone discussion until a future date	Postpone until	Yes	Takes precedence over main motion. Debatable only regarding the date (and time) at which to bring the Motion back for further discussion.

Remove the motion for any further consideration	Postpone indefinitely	Yes	Takes precedence over main motion. Debate can extend to the discussion of the main motion. If approved, it effectively "kills" the motion. Useful for disposing of a badly chosen motion that cannot be adopted or rejected without undesirable consequences.
Request a review of procedure	Point of order	No	Second not required. The Chair or secretary shall review the parliamentary procedure used during the discussion of the Motion.

Notes on Motions

Seconds. A Motion must have a second to ensure that at least two members wish to discuss the issue. The "seconder" is not required to be recorded in the minutes. Neither are motions that do not receive a second.

Announcement by the Chair. The chair should announce the Motion before debate begins. This ensures that the wording is understood by the membership. Once the Motion is announced and seconded, the Committee "owns" the motion, and must deal with it according to parliamentary procedure.

Voting

Voting Method	When Used	How Recorded in Minutes
	When the Chair senses that the Committee is substantially in agreement, and the Motion needed little or no debate. No actual vote is taken.	The minutes show "by unanimous consent."
Vote by Voice	The standard practice.	The minutes show Approved or Not Approved (or Failed).
Vote by Show of Hands (tally)	To record the number of votes on each side when an issue has engendered substantial debate or appears to be divisive. Also used when a Voice Vote is inconclusive. (The Chair should ask for a Vote by Show of Hands when requested by a member).	The minutes show both vote totals, and then Approved or Not Approved (or Failed).
Vote by Roll Call	To record each member's vote. Each member is called upon by the Secretary, and the member indicates either "Yes," "No," or "Present" if abstaining.	The minutes will include the list of members, how each voted or abstained, and the vote totals. Those members for which a "Yes," "No," or "Present" is not shown are considered absent for the vote.

Notes on Voting.

Abstentions. When a member abstains, he/she is not voting on the Motion, and his/her abstention is not counted in determining the results of the vote. The Chair should not ask for a tally of those who abstained.

Determining the results. A simple majority of the votes cast is required to approve an organizational group recommendations or decision.

"Unanimous Approval." Can only be determined by a Roll Call vote because the other methods do not determine whether every member attending the meeting was actually present when the vote was taken, or whether there were abstentions.

Electronic Votes – For an e-mail vote to pass, the requirement is a simple majority of the votes cast during the time-period of the vote as established by the Committee Chair.

Majorities. Per Robert's Rules, as well as MRO Policy and Procedure 3, a simple majority (one more than half) is required to pass motions

AGENDA

Standards of Conduct and Antitrust Guidelines
Steen Fjalstad, Director of Security, MRO

Standards of Conduct Reminder:

Standards of Conduct prohibit MRO staff, committee, subcommittee, and task force members from sharing non-public transmission sensitive information with anyone who is either an affiliate merchant or could be a conduit of information to an affiliate merchant.

Antitrust Reminder:

Participants in Midwest Reliability Organization meeting activities must refrain from the following when acting in their capacity as participants in Midwest Reliability Organization activities (i.e. meetings, conference calls, and informal discussions):

- Discussions involving pricing information; and
- Discussions of a participants marketing strategies; and
- Discussions regarding how customers and geographical areas are to be divided among competitors; and
- Discussions concerning the exclusion of competitors from markets; and
- Discussions concerning boycotting or group refusals to deal with competitors, vendors, or suppliers.

AGENDA

MRO Regional Risk Assessment (RRA) Report

Mark Tiemeier, Principal Technical Advisor, MRO

Action

Information

Report

Mark Tiemeier will provide an oral report during the meeting.

Classification: Public

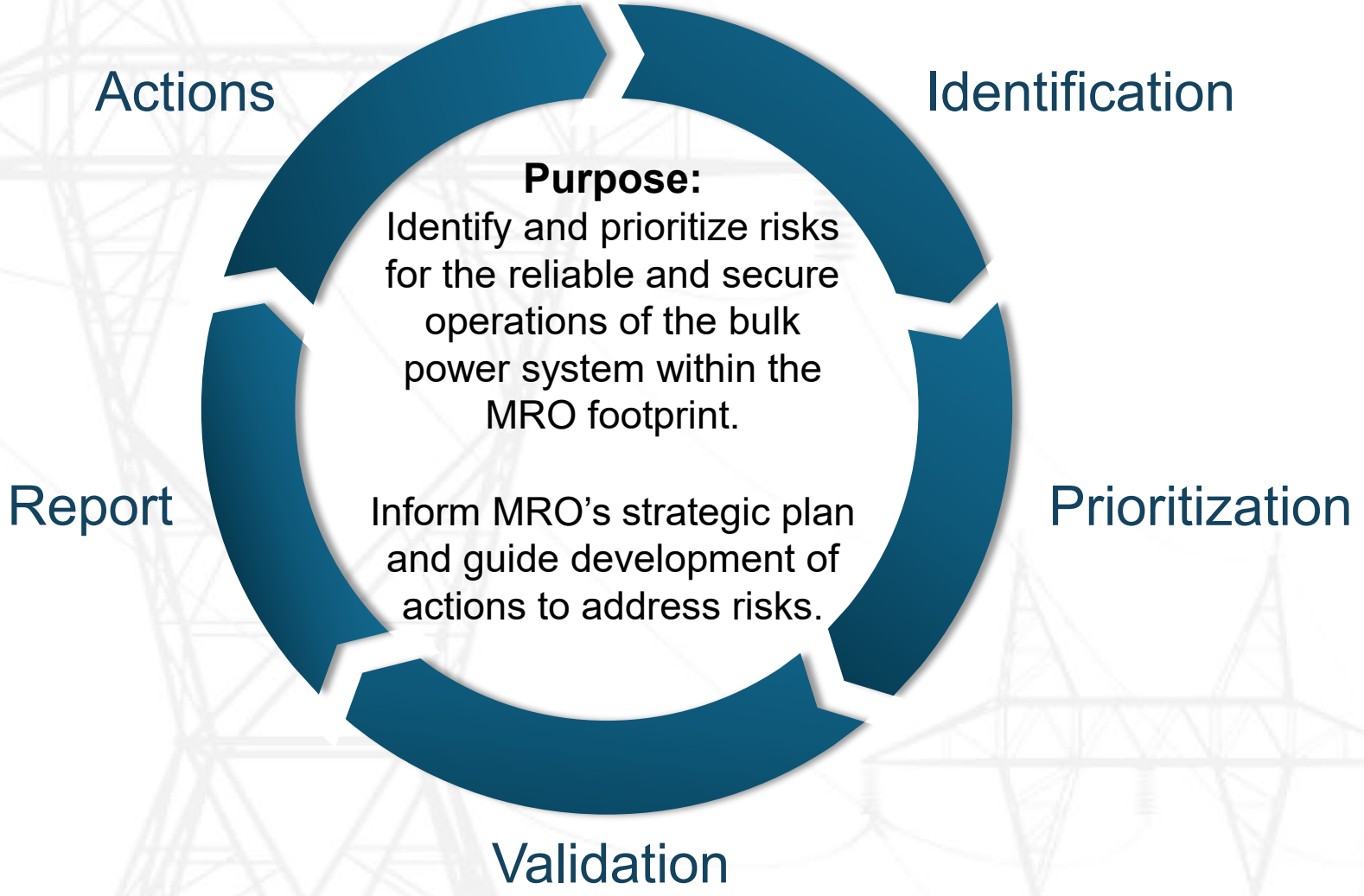
MIDWEST RELIABILITY ORGANIZATION

MRO 2023 Regional Risk Assessment Feedback

Mark Tiemeier

Principal Technical Advisor

Regional Risk Assessment Process

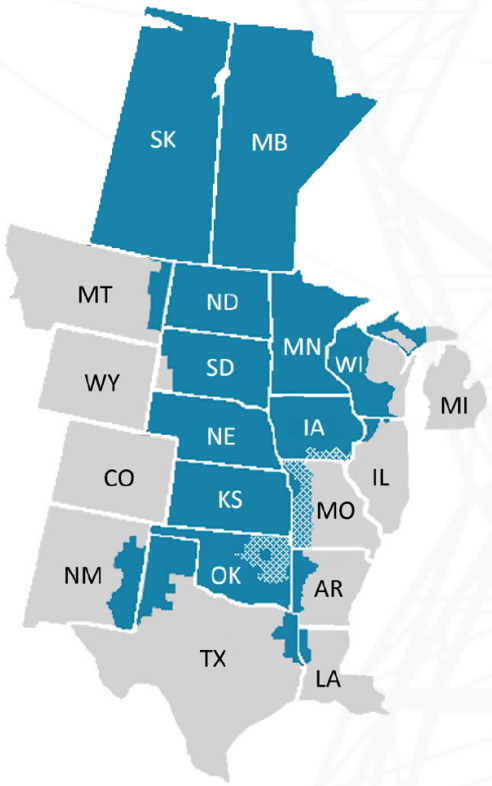


MRO 2023 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

MIDWEST RELIABILITY ORGANIZATION

Territory



About Us

As part of the ERO Enterprise, MRO is committed to a shared mission to identify, prioritize and assure effective and efficient mitigation of risks to the reliability and security of the North American bulk power system in its regional footprint.

Read more at www.MRO.net

MRO Reliability Risk Matrix: Risk Rankings

Consequence / Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major				4,5,6,16	
C3	Moderate		2	9,12,13	1	
C2	Minor			3,7,8,10,14,17	15	
C1	Negligible			11		

LOW
MEDIUM
HIGH
EXTREME

Top risks are reflected in orange above and described below. A full list of risks assessed can be found in the final report.

Assessment Overview

- Extreme weather, consumer demand, and changes in technology and generation resources continue to present a rapidly increasing number of challenges to grid planners and operators. Physical and cyber security risks also continue to evolve at an unprecedented pace.
- MRO's annual *Regional Risk Assessment* considers continent-wide risks to reliability and security of the North American bulk power system and determines which are more likely to occur and would have a higher impact in MRO's region.
- This report is focused on risk identification, prioritization and mitigation and highlights for industry the priorities needed to collaboratively address these challenges. It also serves to inform key decision makers of challenges the industry faces and the policies and regulations that will help define a variety of proposed solutions.
- **READ MRO'S 2023 REGIONAL RISK ASSESSMENT**

Applicable Reliability and Security Risks

High Regional Risks — HIGH

1. Bulk Power Model Assumption Accuracy
4. Conservative Practices to Calculate PRM
5. Energy Reliability Planning
6. Generation Unavailability During Extreme Cold Weather
9. Insider Threat
12. Overhead Transmission Line Ratings
13. Phishing/Malware/Ransomware
16. Supply Chain Compromise

Medium Regional Risks — MEDIUM

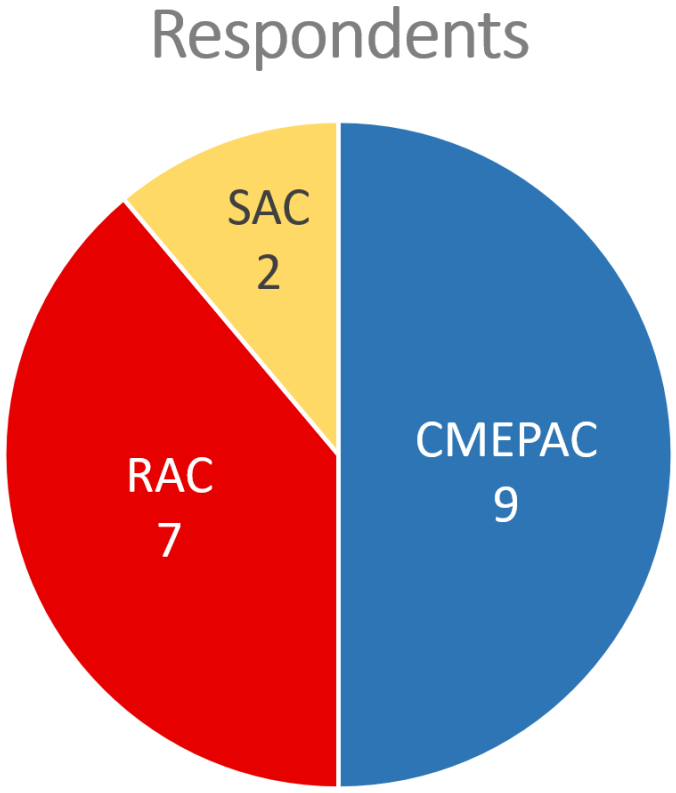
2. Changing Sources of Reactive Power
3. Compromise of Sensitive Information (NEW)
7. Inadequate IBR Ride-Through Capabililty
8. Increased Penetration of Internet-Connected Devices (NEW)
10. Material and Equipment Availability (NEW)
14. Physical Security Protections from Incidents
15. Tightening Supply of Expert Labor
17. Vulnerabilities of Unpatched Systems

Low Regional Risks — LOW

11. Misoperations Due to Human Errors

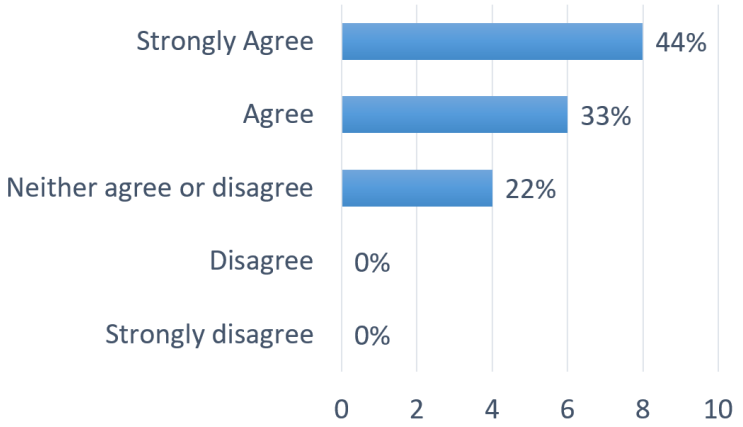
RRA Feedback Survey

- Gather council feedback on 2023 RRA results
- Understand how RRA is used by council member companies
- Seek enhancements for RRA process and 2024 RRA



2023 RRA High Risk Survey Results

Energy Reliability Planning

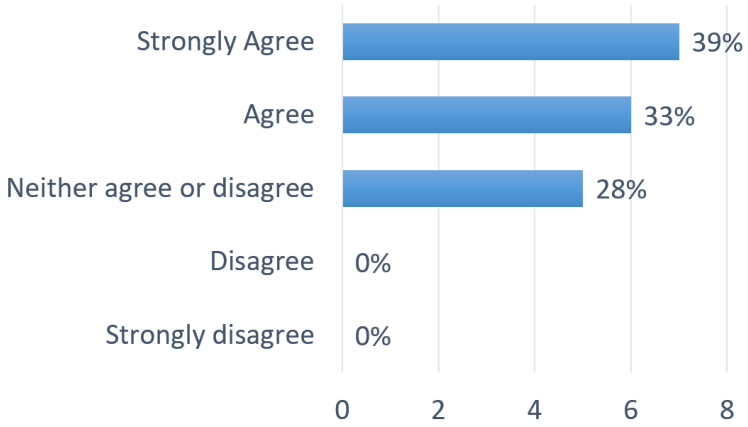


Comments

This identified risk appears to be an impact from the root causes of “Changing Sources of Reactive Power” & “Generation Unavailability During Extreme Cold Weather”

Concerned about velocity of changes and aggregation affects

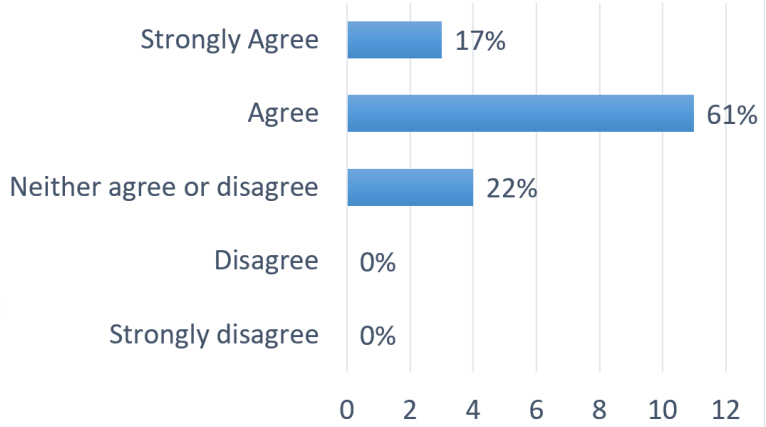
Conservative Practices to Calculate PRM



Comments

This identified risk appears to be an impact from the root causes of “Changing Sources of Reactive Power” & “Generation Unavailability During Extreme Cold Weather”

Bulk Power Model Assumption Accuracy



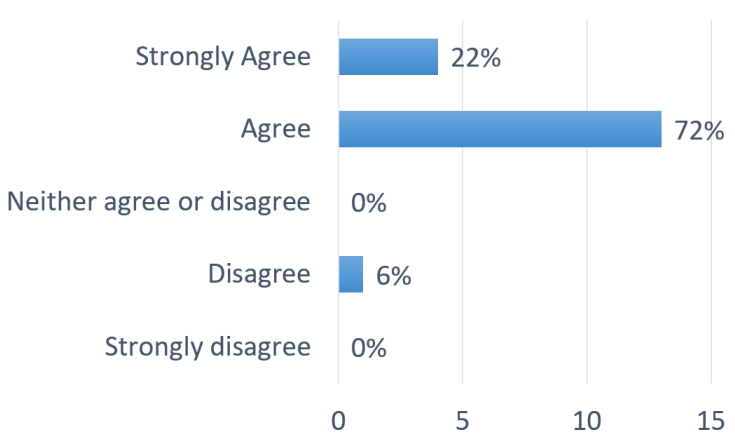
Comments

This identified risk appears to be an impact from the root cause of “Changing Sources of Reactive Power”

Concerned about velocity of changes and aggregation affects

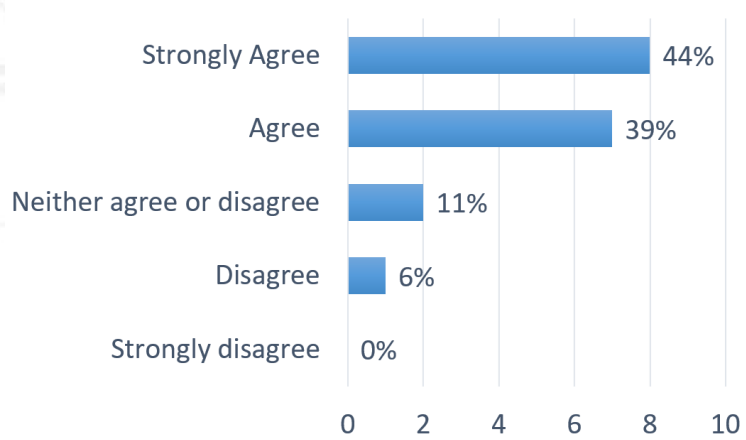
2023 RRA High Risk Survey Results

Supply Chain Compromise



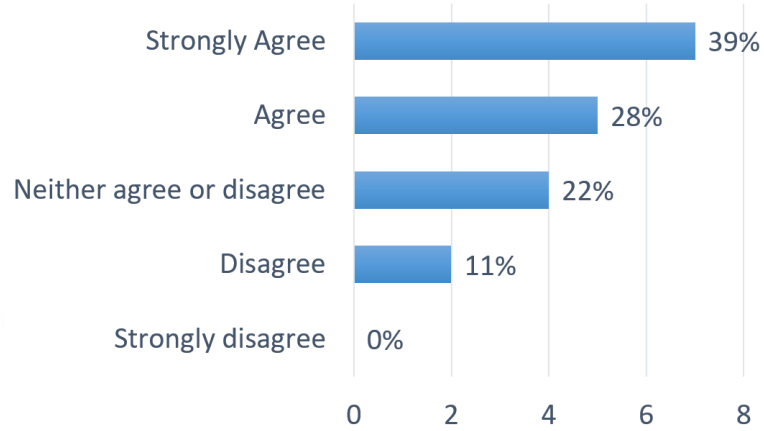
Comments

Phishing / Malware / Ransomware



Comments

Insider Threat



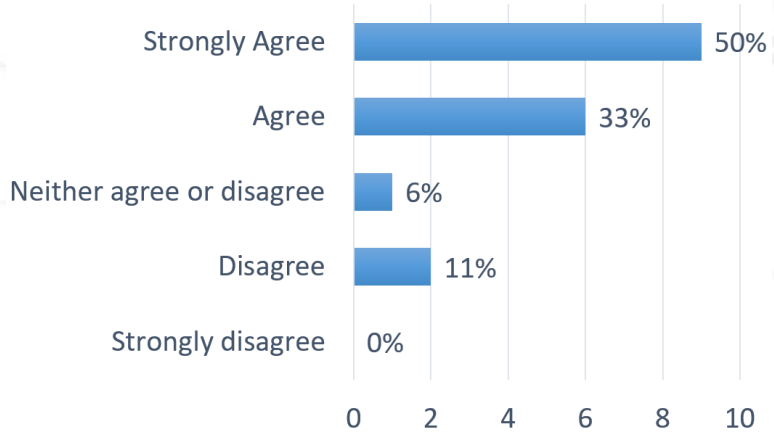
Comments

This also potentially exists with physical security as evidenced by recent events.

I haven’t heard about very many breaches or events related to Insider Threat. Although that has occurred on the rare occasion it doesn't rise to the level of High Priority. There simply aren't enough events to justify this ranking.

2023 RRA High Risk Survey Results

Generation Unavailability During Extreme Cold Weather



Comments

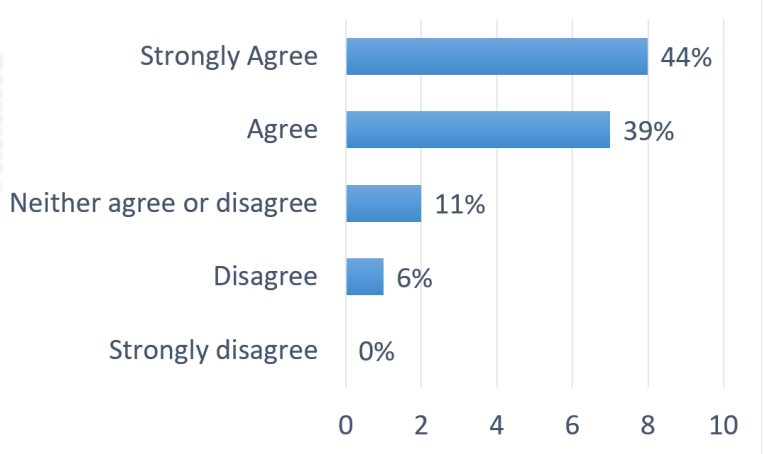
Winter is nothing new in the north. Maybe more of an issue for resources in the southern part of the system and then dealing with transmission constraints.

Also a considerable risk during shoulder seasons when units are down for maintenance.

NERC Standards are being developed to help mitigate this risk.

Is somewhat dependent on location of the resource

Overhead Transmission Line Ratings



Comments

Concerned about velocity of changes and aggregation affects

How are facility ratings a high risk when most of the recent FAC-008 violations are being processed as low risk?

I agree with this being a problem, and ambient adjusted ratings being overly complicated. I do not know how large of a risk it is. Has this been or is it expected to be the critical element? Is generation capability more of the concern?

2023 RRA High Risk Survey Results

Should any of the Low or Medium risks been categorized as High in the 2023 RRA?

- This is difficult to assess since the RRA does not provide a distinct listing of high, medium, or low risks.
- Supply Chain - material and equipment availability
- Material and Equipment Availability is becoming critical to maintain reliability. Recovery from a major storm will take much longer with the lack of availability of major material items.
- Changes sources of reactive power is a high risk given the generation transformation underway.
- If "Changing Sources of Reactive Power" was changed to "Changing Mix of Power Sources", this would cover more of the risks and should be high impact.

2023 RRA Risk Descriptions Survey Results

Are there risk descriptions in the 2023 RRA that are inaccurate or unclear?

- If "Changing Sources of Reactive Power" was changed to "Changing Mix of Power Sources", this would cover more of the risks and should be high impact.

2023 RRA Risk Descriptions Survey Results

Any unnecessary overlap in identified risks within the 2023 RRA?

- If "Changing Sources of Reactive Power" was changed to "Changing Mix of Power Sources", this would cover more of the risks and should be high impact.
- Not sure there is unnecessary overlap; however, these risks impact one another such that aggregated might result in different results.

- No unnecessary overlaps in the identified risks
- None identified
- None come to mind.

Potential 2024 RRA Risks Survey Results

Are there any risks not identified in the 2023 RRA that should be considered for the 2024 RRA?

- I think we should retain the risk "Bulk Power Model Assumption Accuracy" for next year and stress the need to have requirements in the interconnection process to have accurate models which include EMT models to support simulation studies. There are a number of NERC standard developments in progress to address the need for EMT studies and to support PCs and TPs having EMT models from GOs and developers (especially for IBR interconnections).
- The pace of electrification coupled with the retirement of conventional generation resources .
- I believe we have a great list.
- Interdependencies of critical infrastructure (i.e. electricity's dependency on pipelines for natural gas)
- Loss of Major Transmission Equipment with Extended Lead Times - Some correlation with Material and Equipment Availability...

Organizational Use of RRA Survey Results

How does your organization use the MRO RRA?

Compliance Use

- Standard/requirement data is considered when determining what high-risk standards/requirements will be annually reviewed (internally) by our compliance department to close possible compliance gaps and improve our internal processes and procedures.
- We use the MRO RRA as an input to our NERC Risk Assessment.
- We review the RRA with our companies NERC oversight committee. We discuss whether any policy change internal should be incorporated to address these risks or if we feel additional items could be added.
- The NERC Compliance group uses the RRA as an input to the NERC risk assessment.
- It is used in our annual compliance assessment to identify priority for focusing controls and monitoring compliance and identifying areas for internal audits to verify compliance.

Organizational Use of RRA Survey Results

How does your organization use the MRO RRA?

Used to inform needed operational and planning changes

- Our organization reviews the RRA, taking note of any risks that could impact or be impacted by our system, then we discuss preparations and operational adjustments that we may need to make.
- Not all regional reliability risks identified in the current RRA are applicable to our organization. Currently, we are more focused on Overhead Transmission Line Ratings and integrating DERs into our long-term planning assessments. However, security risks are very common in the region and applicable to most entities.
- The T&D group use the RRA as a reference/input when conducting their risk assessment

Organizational Use of RRA Survey Results

How does your organization use the MRO RRA?

Shared with Executives

- Reviewed at the Executive Level.
- The RRA is socialized with Operations at the Executive level.
- We brief the MRO RRA to the C-Suite and strategy team. The teams assign resources and include the RRA in decision making.

Other

- The MRO RRA is used as reference document
- Communicated to various audiences.
- This year, it was distributed around our organization more than in the past. I'm not sure who other than Compliance actually uses it.

RRA Process Improvements Survey Results

What suggestions do you have to improve either the RRA process, report, or results?

Compliance Use

- Continue to build off current process. Would like CMEPAC to have bigger role with identifying areas of risks that are not covered by Reliability Standards. Consider broader industry surveyor risk assessment and review results broadly.
- The CSI has been moved from this report to the CMEP Summary Report. Although I see the value in this, consolidating this type of information into a single report would be preferable. There are already so many different sources/reports and it easy to overlook important statistics/publications.

RRA Process Improvements Survey Results

What suggestions do you have to improve either the RRA process, report, or results?

Risk identification and ranking improvements

- As someone who participated in the RRA process for the first time, I had absolutely no idea what the process was until I was involved in it. Being a part of the process gave the process a lot more credibility to me. I think it would be nice if the process was documented and available to the MRO members so they understand how the risks are ranked. I still have no idea how the risks are initially identified!
- The voting followed by revoting process and having people with vote scores deviating from the average explain rationale process lead to groupthink and centralized scoring. The intent behind both of the process is good. The intent is for a more educated vote and stimulating discussion. Unfortunately, the process of having people with vote scores deviating from the average incentivizes voters to select a centralized score, so they will not be asked to explain. Voting followed by revoting incentivizes the group to revote like each other.

Other

- More focus on the reporting of the report with key stakeholders including policy makers .

RRA Process Improvements Survey Results

What suggestions do you have to improve either the RRA process, report, or results?

Increase involvement with key stakeholders and reporting to policy makers

- More focus on the reporting of the report with key stakeholders including policy makers.
- Not quite sure how well MRO reached out to the regional entities during the development process of the annual RRA other than working with selected individuals from MRO advisory councils. Hope this approach is consistent with the ERO Enterprise general industry practice.

Other

- None. It is currently valuable to our organization.

2024 RRA Risk Ranking Workshop

- **Two volunteers from each MRO Advisory Council**
- **Seeking input on two format options**

- **Option #1**
  Two-day Workshop
  - Monday 10/23 8am-3pm
  - Tuesday 10/24 8am-3pm

- **Option #2**
  Meeting Series

  Risk Information Sessions
  - Tuesday 10/17 2-4:30pm
  - Thursday 10/19 2-4:30pm

  Risk Ranking Workshop
  - Tuesday 10/24 8am-3pm

AGENDA

MRO Regional Security Risk Assessment (RSRA) Survey Update

Lee Felter, Principal Security Engineer, MRO

Action

Information

Report

Lee Felter will provide an oral report during the meeting.

MIDWEST RELIABILITY ORGANIZATION

2023 Regional Security Risk Assessment

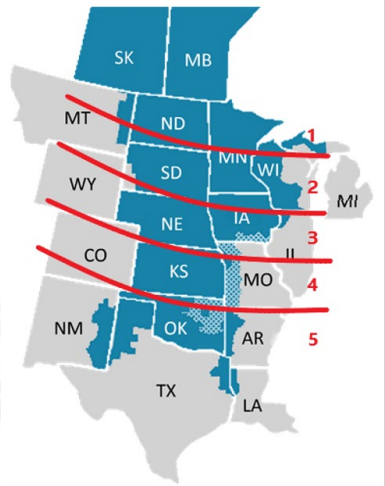
Survey Results

Lee Felter

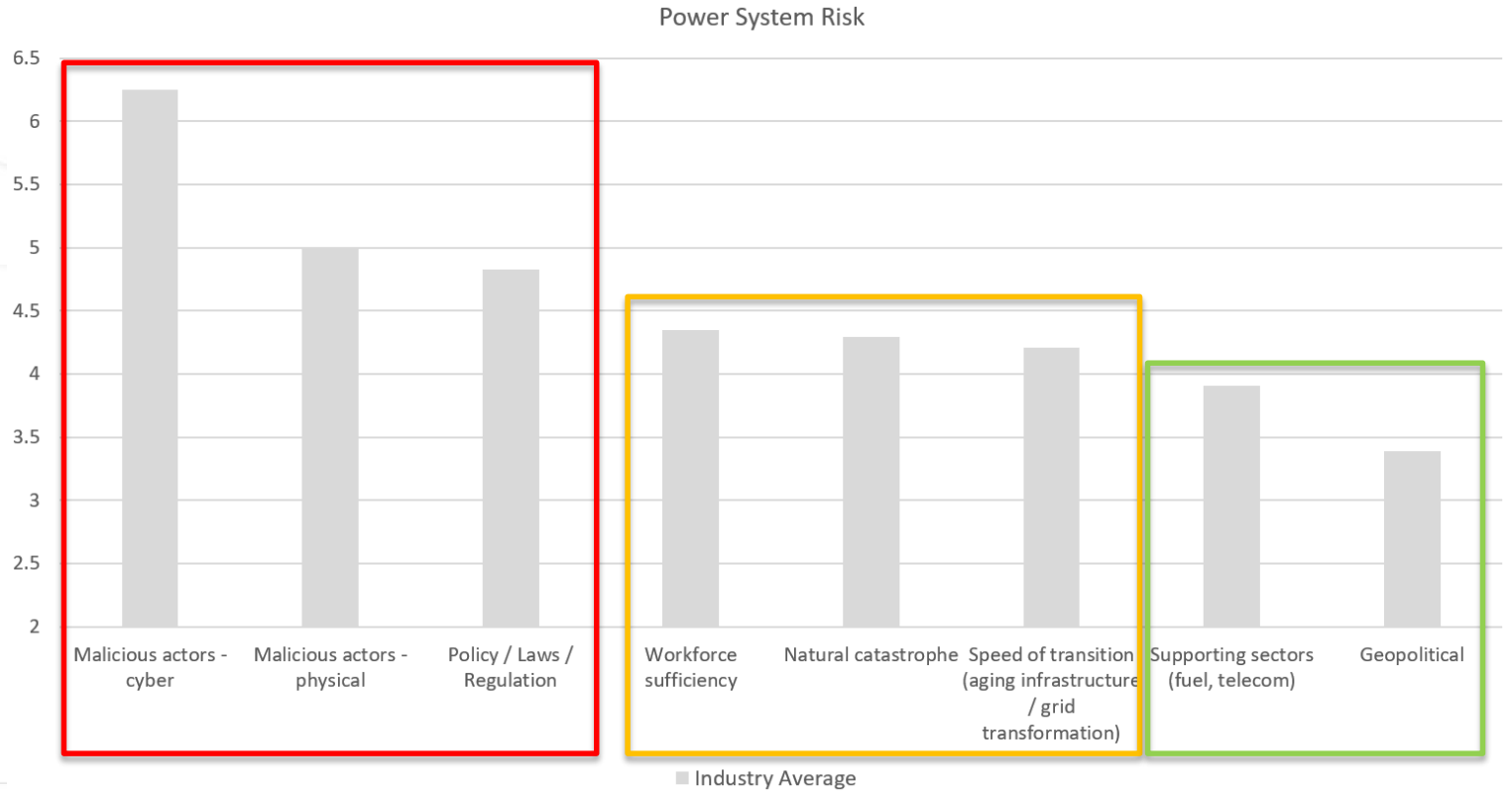
Principal Security Engineer

Responses

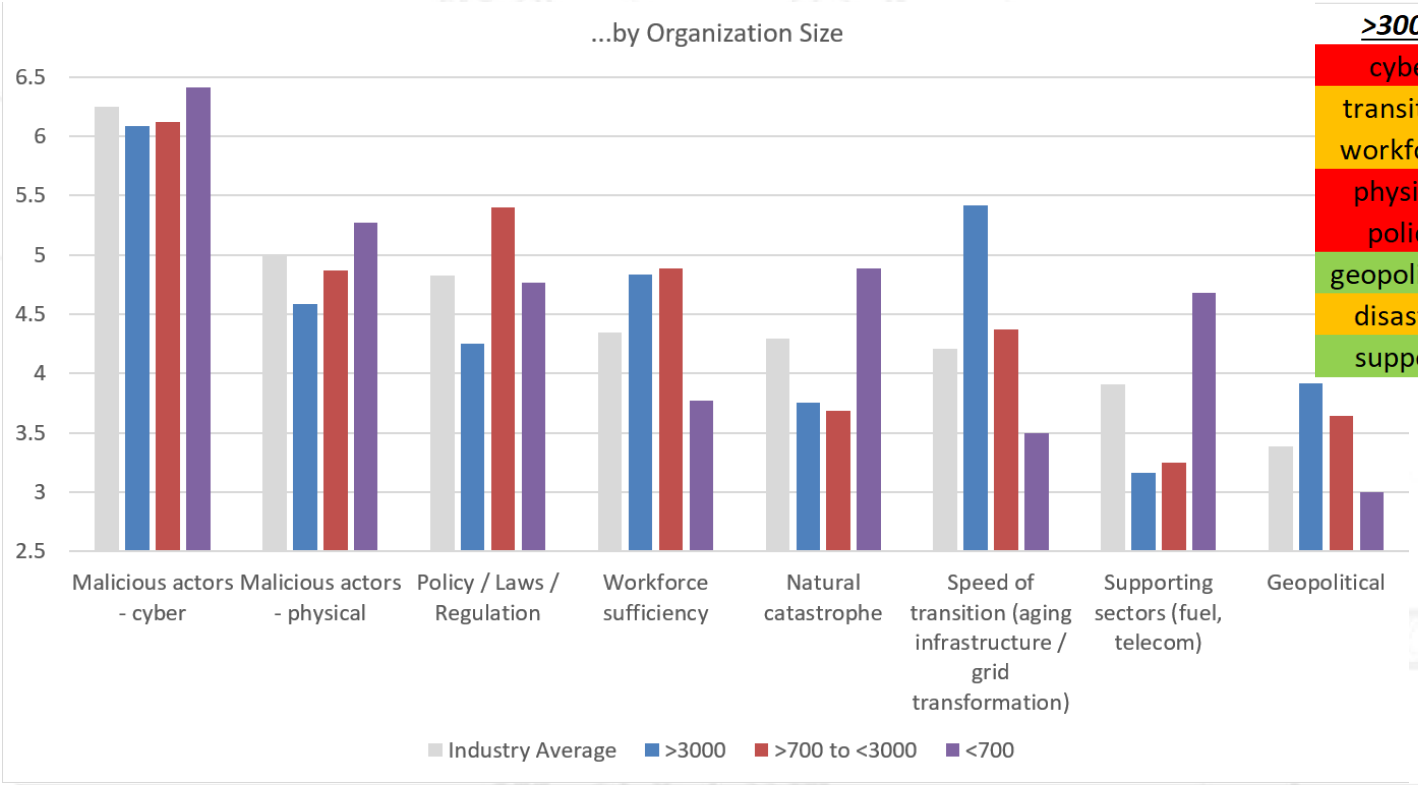
- 59 responses
- 14 minutes average
- Eliminated invalid answers
- Applied weights to responses
- Cross section of industry
- Even latitudinal representation



Ranking of Broad Topics

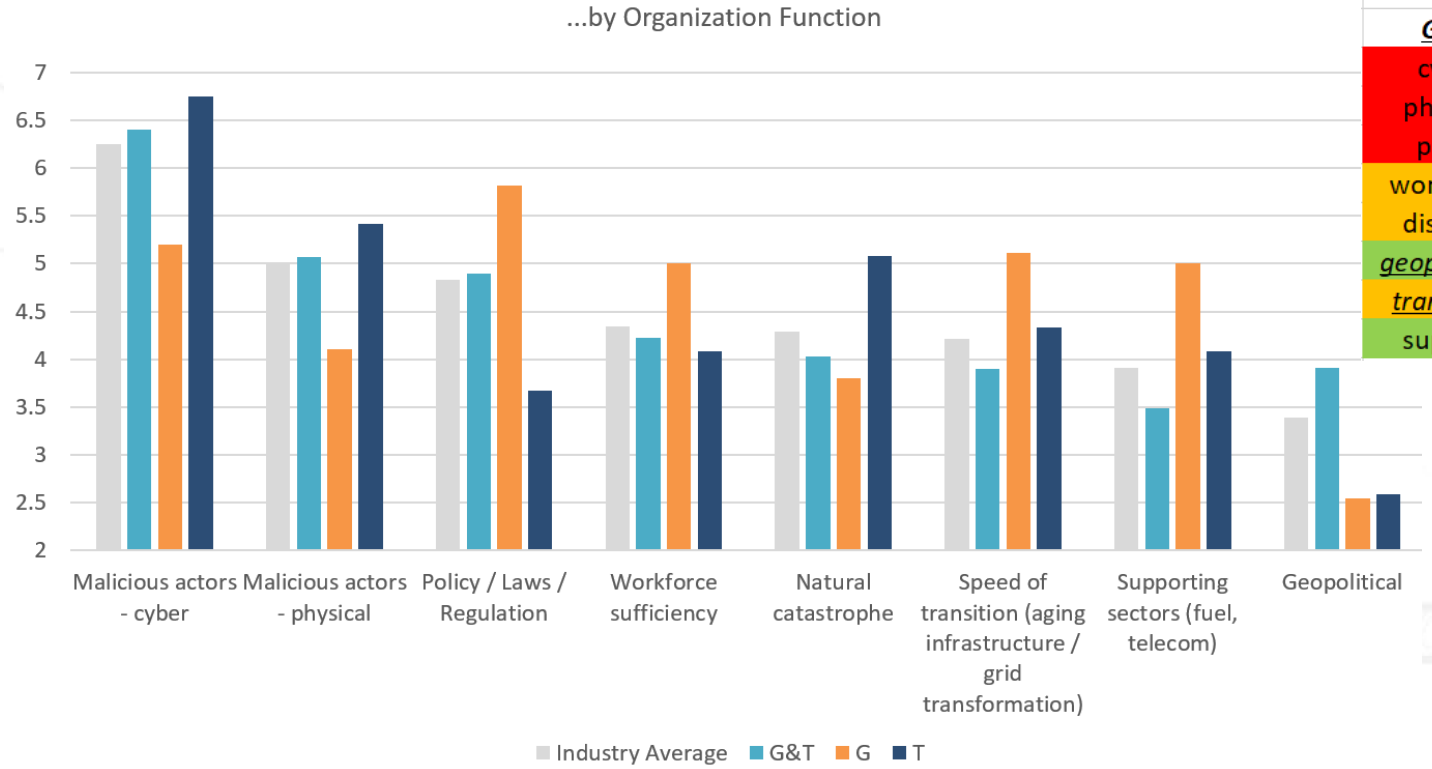


Ranking of Broad Topics



	Size	
>3000	**3k … 0.7k**	**<700**
cyber	cyber	cyber
transition	policy	physical
workforce	*workforce*	disaster
physical	*physical*	policy
policy	transition	support
geopolitical	*disaster*	workforce
disaster	*geopolitical*	transition
support	support	geopolitical

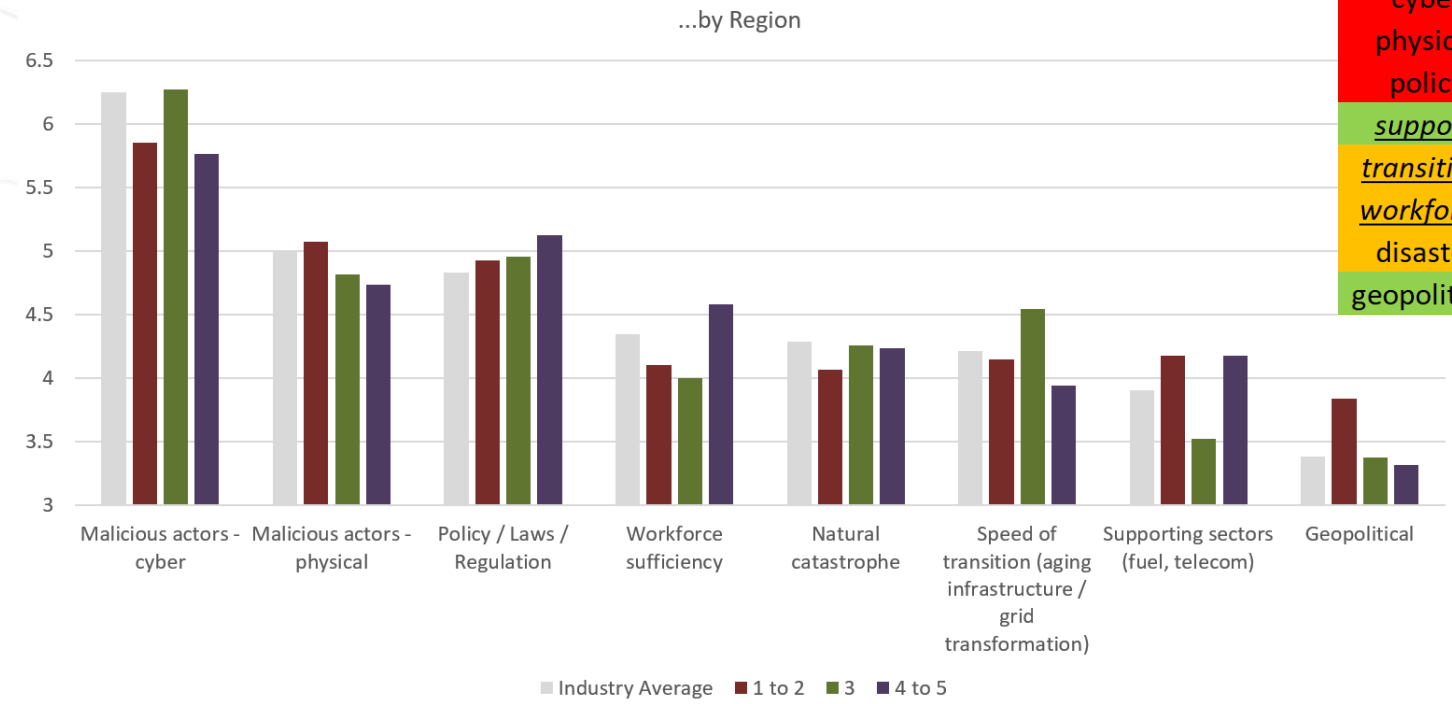
Ranking of Broad Topics

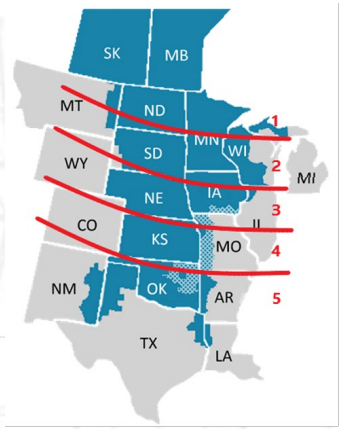


Function		
G&T	***G***	***T***
cyber	policy	cyber
physical	cyber	physical
policy	transition	disaster
workforce	*workforce*	transition
disaster	*support*	*support*
geopolitical	physical	*workforce*
transition	disaster	policy
support	geopolitical	geopolitical

Ranking of Broad Topics

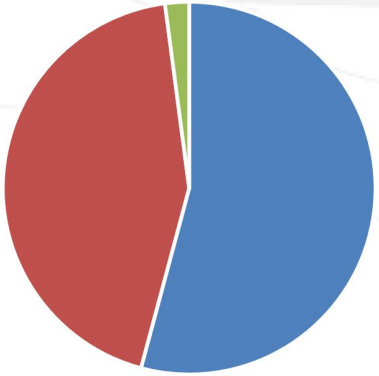
Region		
1-2	3	4-5
cyber	cyber	cyber
physical	policy	policy
policy	physical	physical
support	transition	workforce
transition	disaster	*disaster*
workforce	workforce	*support*
disaster	support	transition
geopolitical	geopolitical	geopolitical





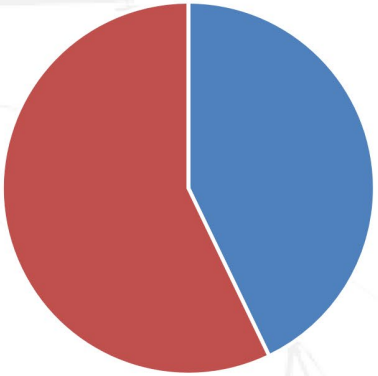
IT/OT Dependency

Overall

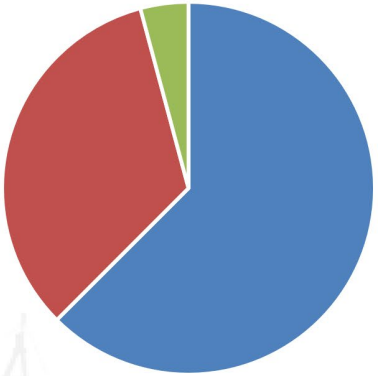


>3000

<3000 & >700

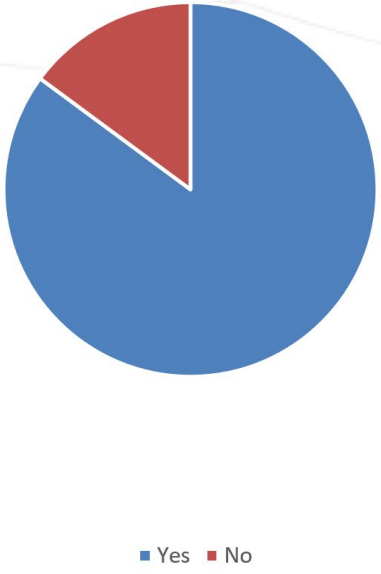


<700

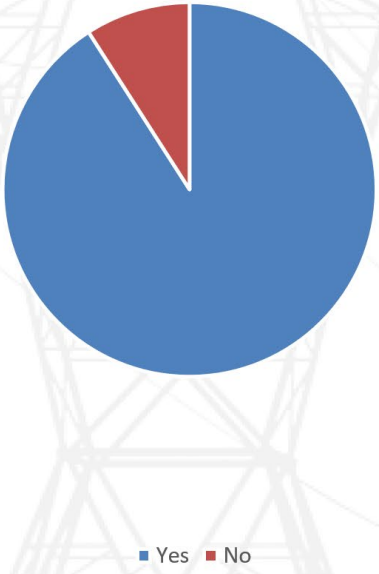


IT/OT Isolation Testing

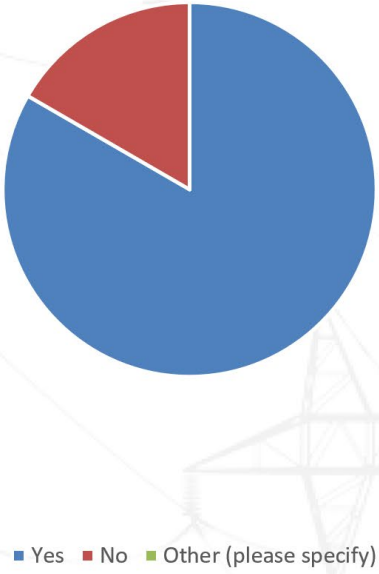
Overall



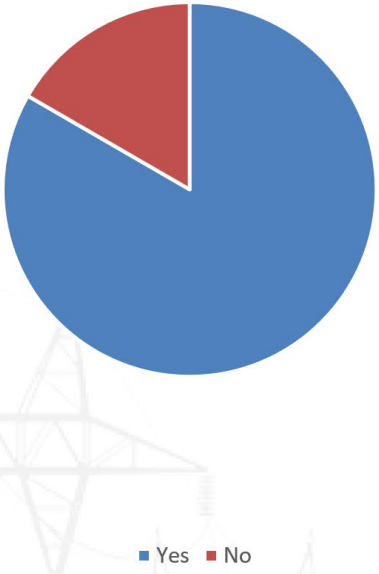
>3000



<3000 & >700 -

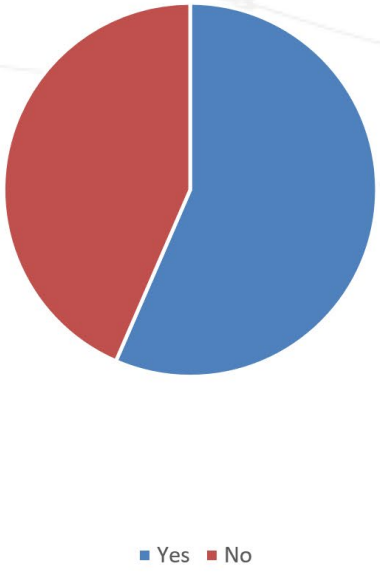


<700

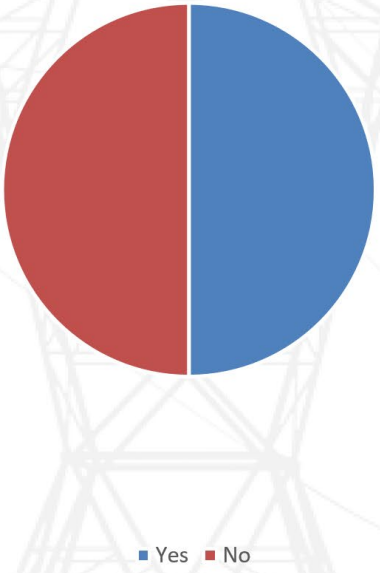


IT Impact OT?

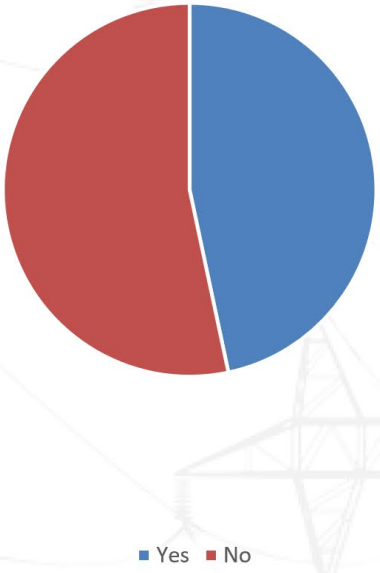
Overall



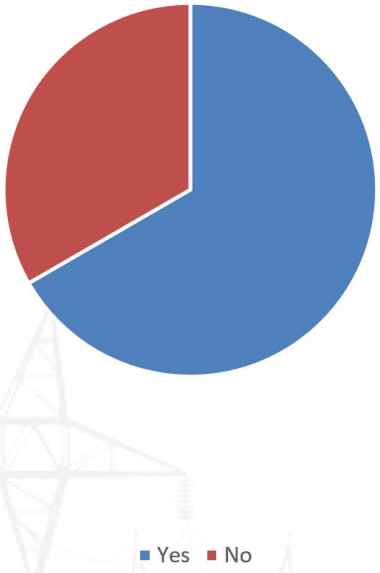
>3000



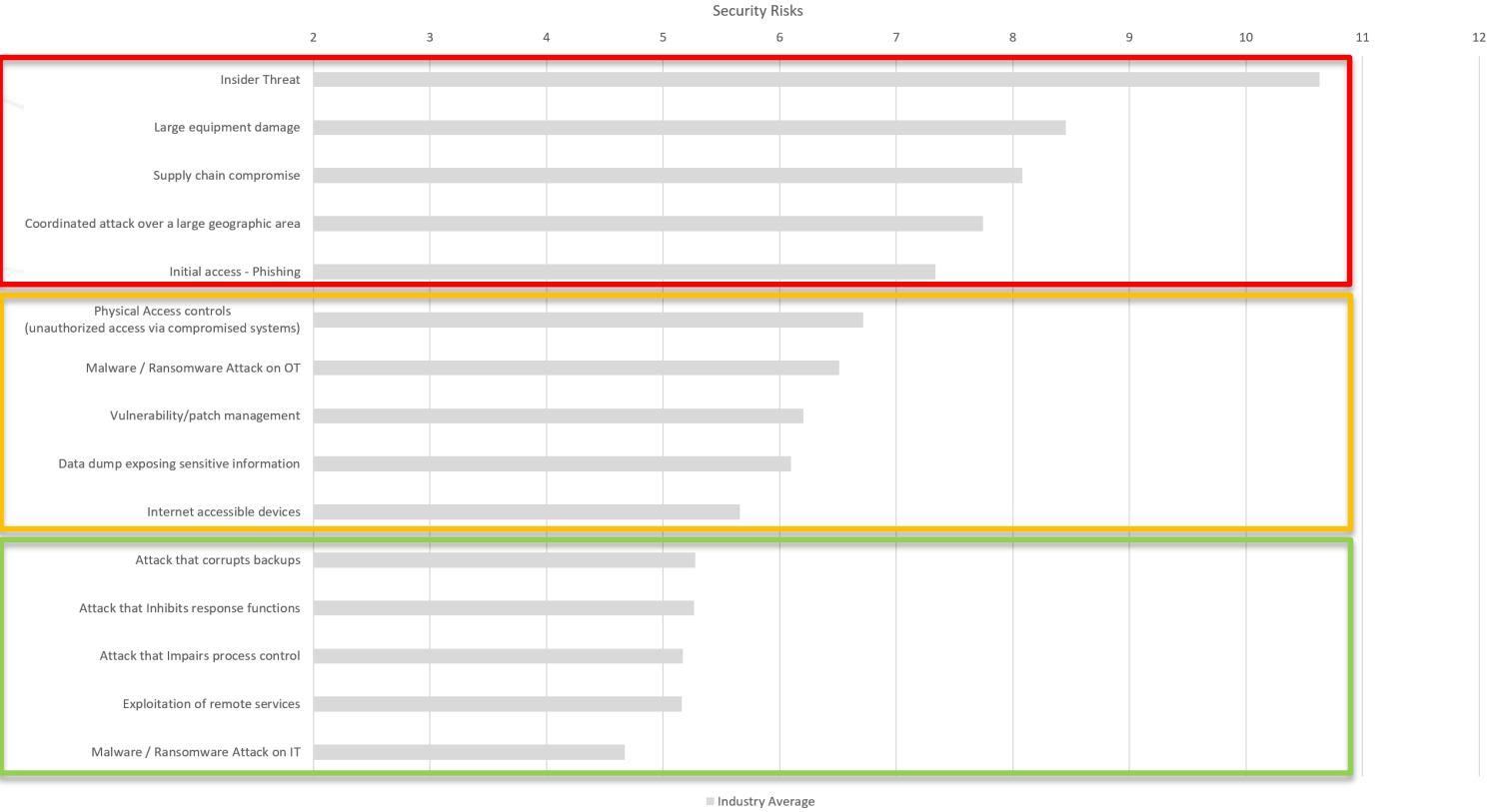
<3000 & >700



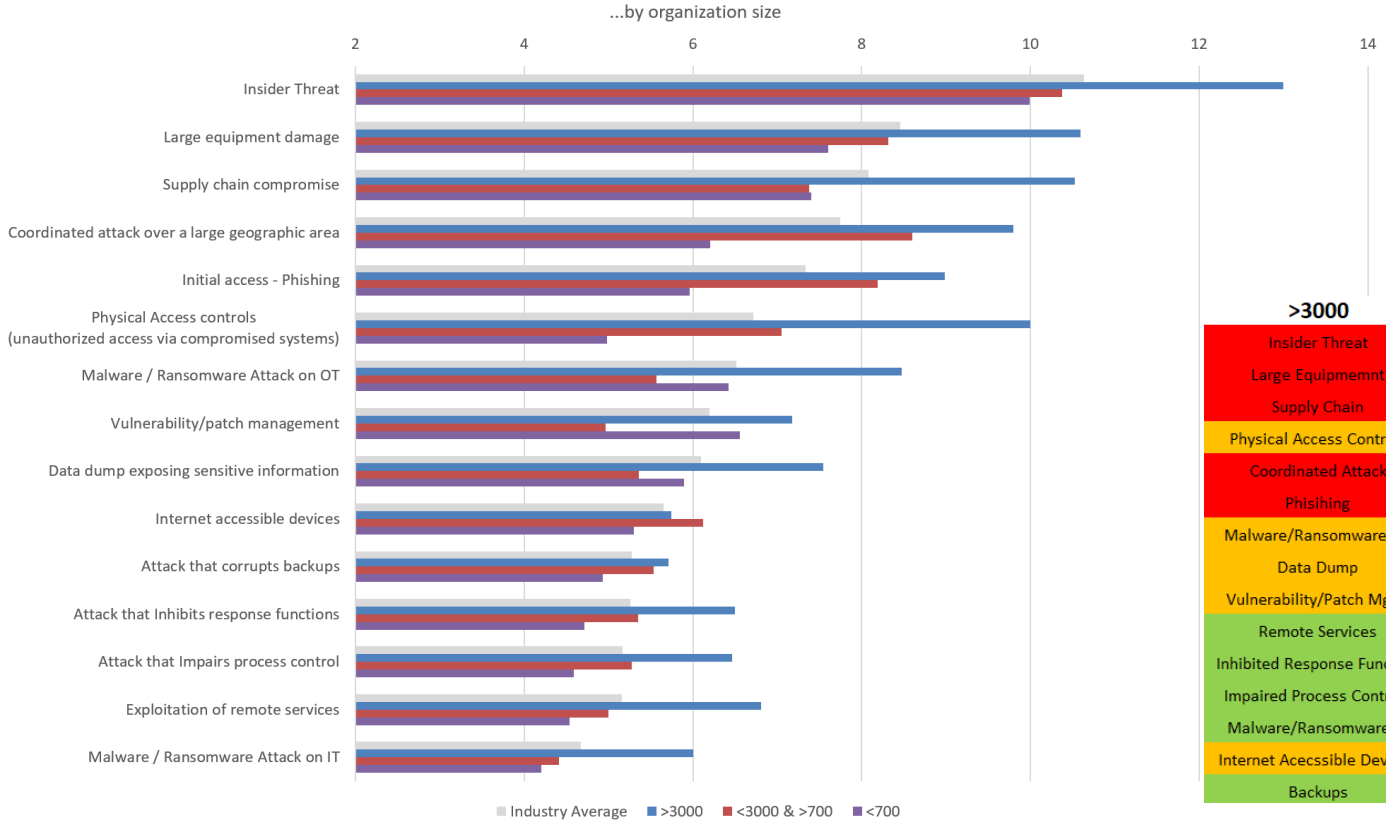
<700



Security Risk Ranking

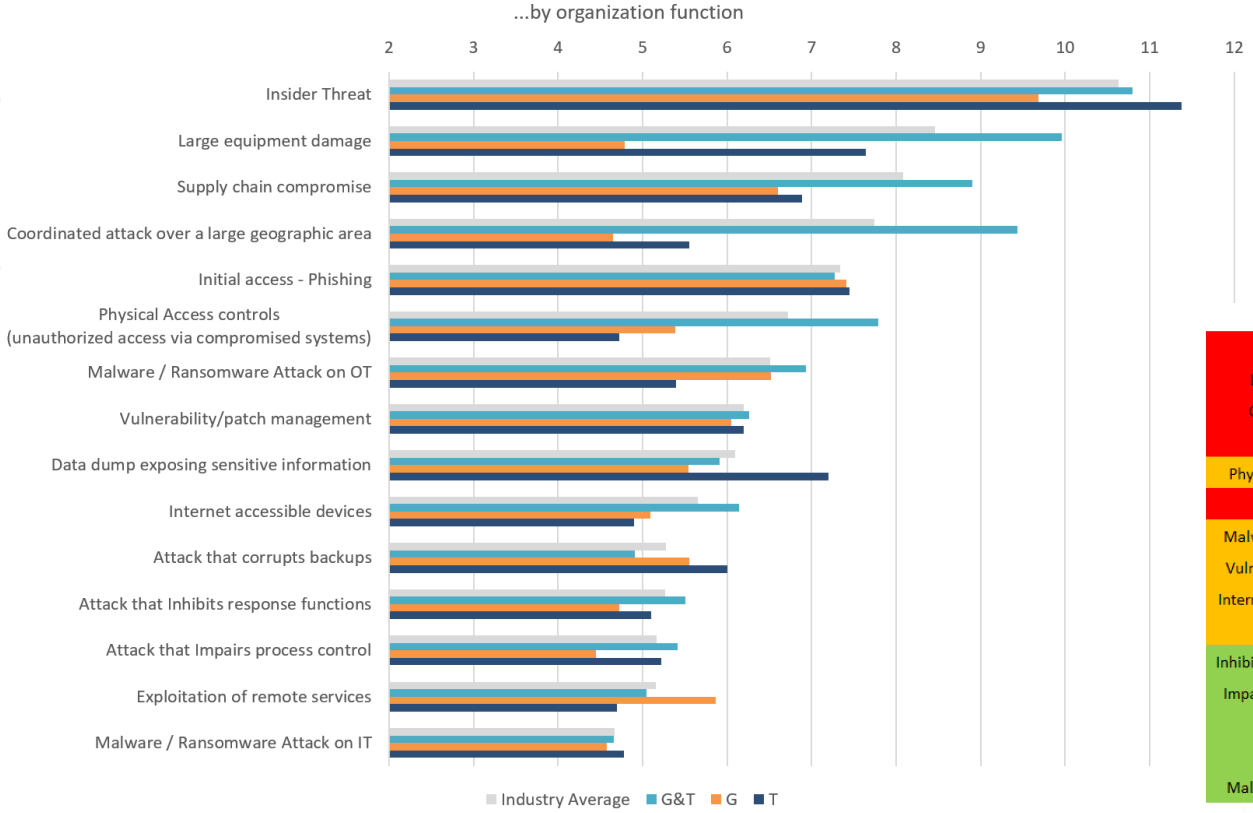


Security Risk Ranking



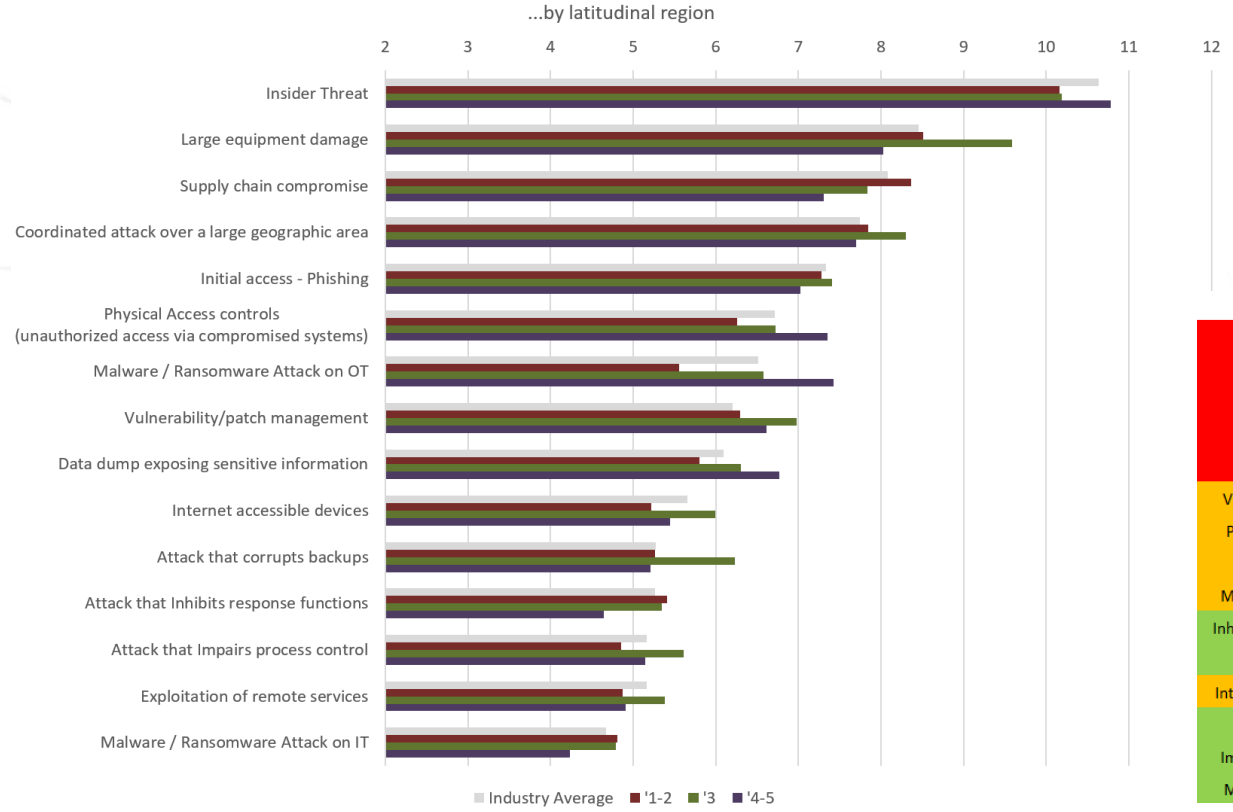
>3000	<3000 & >700	<700
Insider Threat	Insider Threat	Insider Threat
Large Equipmemnt	Coordinated Attack	Large Equipmemnt
Supply Chain	Large Equipmemnt	Supply Chain
Physical Access Controls	Phisihing	Vulnerability/Patch Mgmt
Coordinated Attack	Supply Chain	Malware/Ransomware OT
Phisihing	Physical Access Controls	Coordinated Attack
Malware/Ransomware OT	Internet Acecssible Devices	Phisihing
Data Dump	Malware/Ransomware OT	Data Dump
Vulnerability/Patch Mgmt	Backups	Internet Acecssible Devices
Remote Services	Data Dump	Physical Access Controls
Inhibited Response Function	Inhibited Response Function	Backups
Impaired Process Controls	Impaired Process Controls	Inhibited Response Function
Malware/Ransomware IT	Remote Services	Impaired Process Controls
Internet Acecssible Devices	Vulnerability/Patch Mgmt	Remote Services
Backups	Malware/Ransomware IT	Malware/Ransomware IT

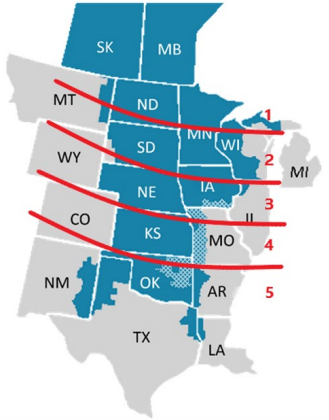
Security Risk Ranking



G&T	G	T
Insider Threat	Insider Threat	Insider Threat
Large Equipmemnt	Phisihing	Large Equipmemnt
Coordinated Attack	Supply Chain	Phisihing
Supply Chain	Malware/Ransomware OT	Data Dump
Physical Access Controls	Vulnerability/Patch Mgmt	Supply Chain
Phisihing	Remote Services	Vulnerability/Patch Mgmt
Malware/Ransomware OT	Backups	Backups
Vulnerability/Patch Mgmt	Data Dump	Coordinated Attack
Internet Acecssible Devices	Physical Access Controls	Malware/Ransomware OT
Data Dump	Internet Acecssible Devices	Impaired Process Controls
Inhibited Response Function	Large Equipmemnt	Inhibited Response Function
Impaired Process Controls	Inhibited Response Function	Internet Acecssible Devices
Remote Services	Coordinated Attack	Malware/Ransomware IT
Backups	Malware/Ransomware IT	Physical Access Controls
Malware/Ransomware IT	Impaired Process Controls	Remote Services

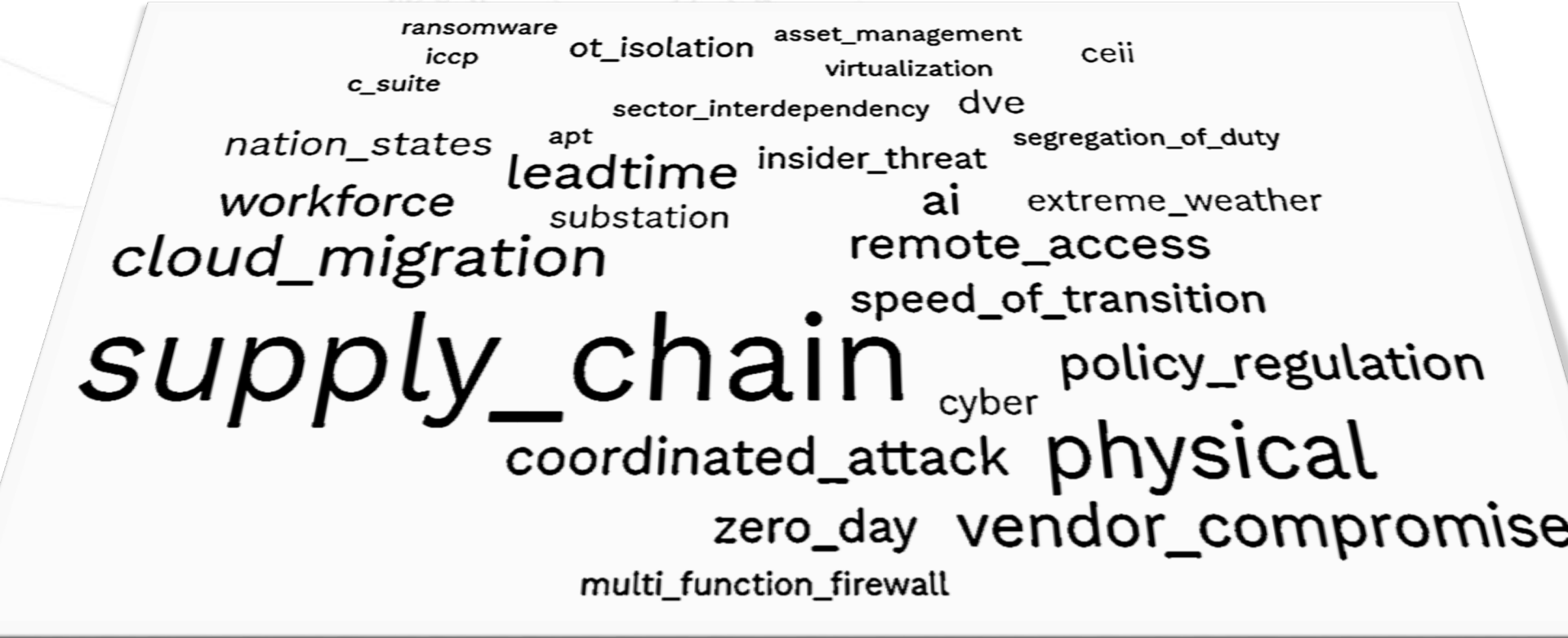
Security Risk Ranking





1-2	3	4-5
Insider Threat	Insider Threat	Insider Threat
Large Equipmemnt	Large Equipmemnt	Large Equipmemnt
Supply Chain	Coordinated Attack	Coordinated Attack
Coordinated Attack	Supply Chain	Malware/Ransomware OT
Phisihing	Phisihing	Physical Access Controls
Vulnerability/Patch Mgmt	Vulnerability/Patch Mgmt	Supply Chain
Physical Access Controls	Physical Access Controls	Phisihing
Data Dump	Malware/Ransomware OT	Data Dump
Malware/Ransomware OT	Data Dump	Vulnerability/Patch Mgmt
Inhibited Response Function	Backups	Internet Acecssible Devices
Backups	Internet Acecssible Devices	Backups
Internet Acecssible Devices	Impaired Process Controls	Impaired Process Controls
Remote Services	Remote Services	Remote Services
Impaired Process Controls	Inhibited Response Function	Inhibited Response Function
Malware/Ransomware IT	Malware/Ransomware IT	Malware/Ransomware IT

What keeps us up at night?



MEETING AGENDA – Security Advisory Council – May 24, 2023

AGENDA

Security Advisory Council Threat Forum (SACTF) Update

a. Threat Call Statistics

Brett Lawler, MRO SACTF Chair

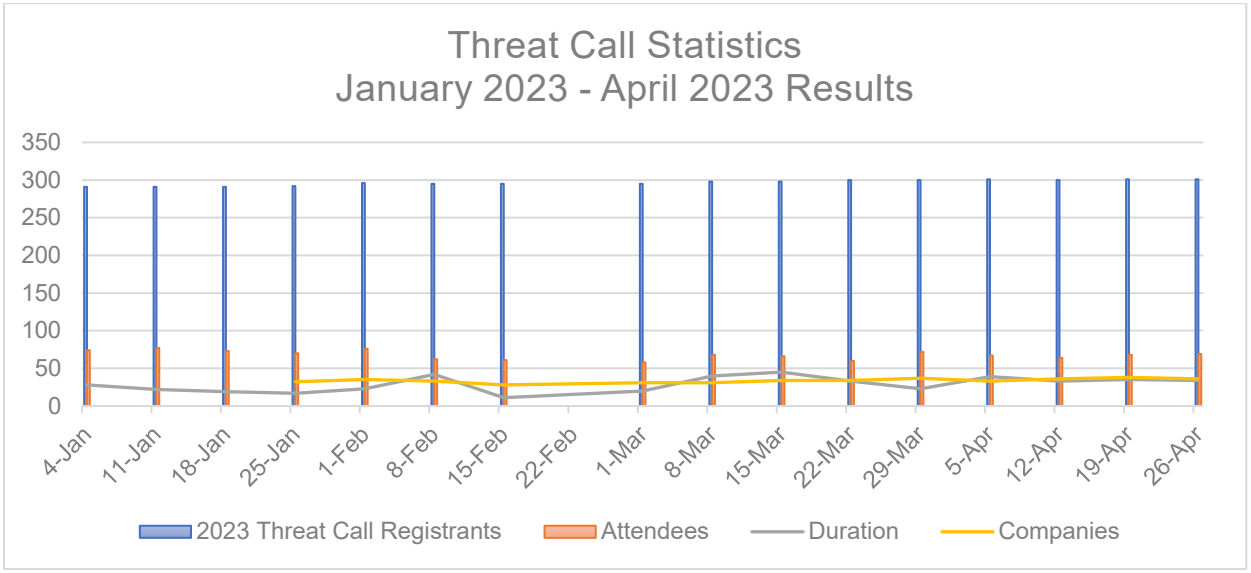
Action

Information

Report

Threat Call

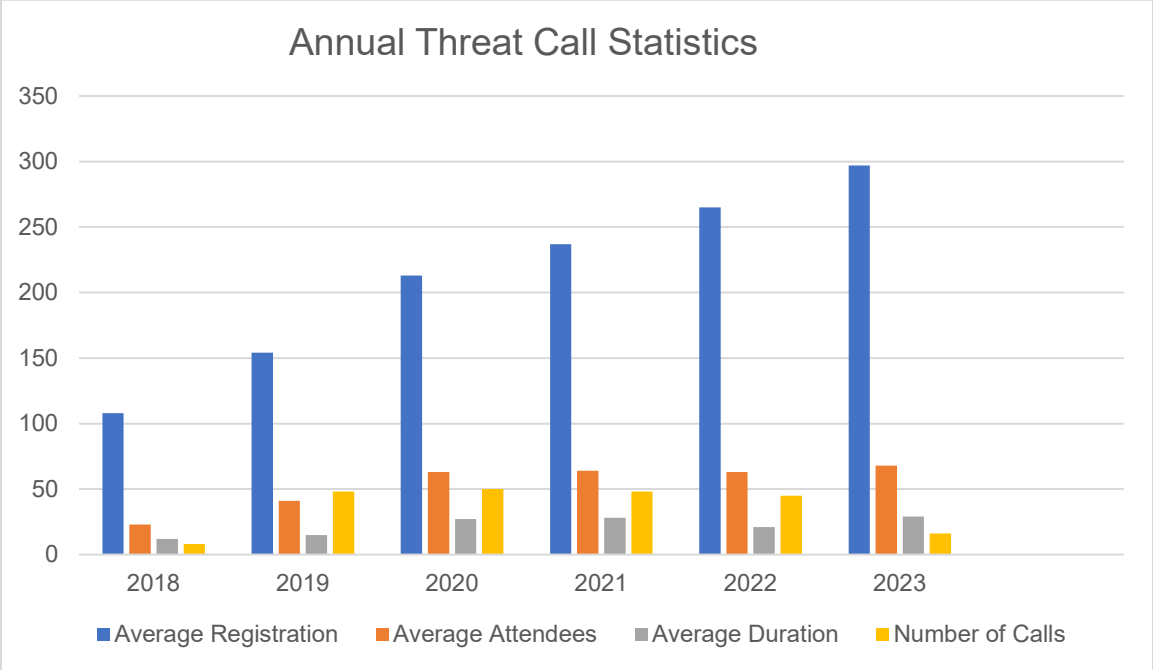
Date	Approved Registrants	Duration	Attendees	Unique Companes
January 4, 2023	291	28 Minutes	74	
January 11, 2023	291	22 Minutes	77	
January 18, 2023	291	19 Minutes	73	
January 25, 2023	292	17 Minutes	70	32
February 1, 2023	296	23 Minutes	76	35
February 8, 2023	295	42 Minutes	62	33
February 15, 2023	295	11 Minutes	61	28
March 1, 2023	295	20 Minutes	58	31
March 8, 2023	298	40 Minutes	68	31
March 15, 2023	298	45 Minutes	66	34
March 22, 2023	300	33 Minutes	60	34
March 29, 2023	300	23 Minutes	72	37
April 5, 2023	301	39 Minutes	33	33
April 12, 2023	300	33 Minutes	64	36
April 19, 2023	301	35 Minutes	68	38
April 26, 2023	301	34 Minutes	69	36
Averages	**297**	**29 Minutes**	**68**	**34**



Classification: Public

Annual Threat Call Statistics

Year	Average Registrants	Average Attendees	Average Duration	Number of Calls
2018	108	23	12 Minutes	8 Calls
2019	154	41	15 Minutes	48 Calls
2020	213	63	27 Minutes	50 Calls
2021	237	64	28 Minutes	48 Calls
2022	265	63	21 Minutes	45 Calls
2023	297	68	29 Minutes	16 Calls



Classification: Public

AGENDA

Security Advisory Council Threat Forum (SACTF) Update

b. Threat Call Feedback

Brett Lawler, MRO SACTF Chair

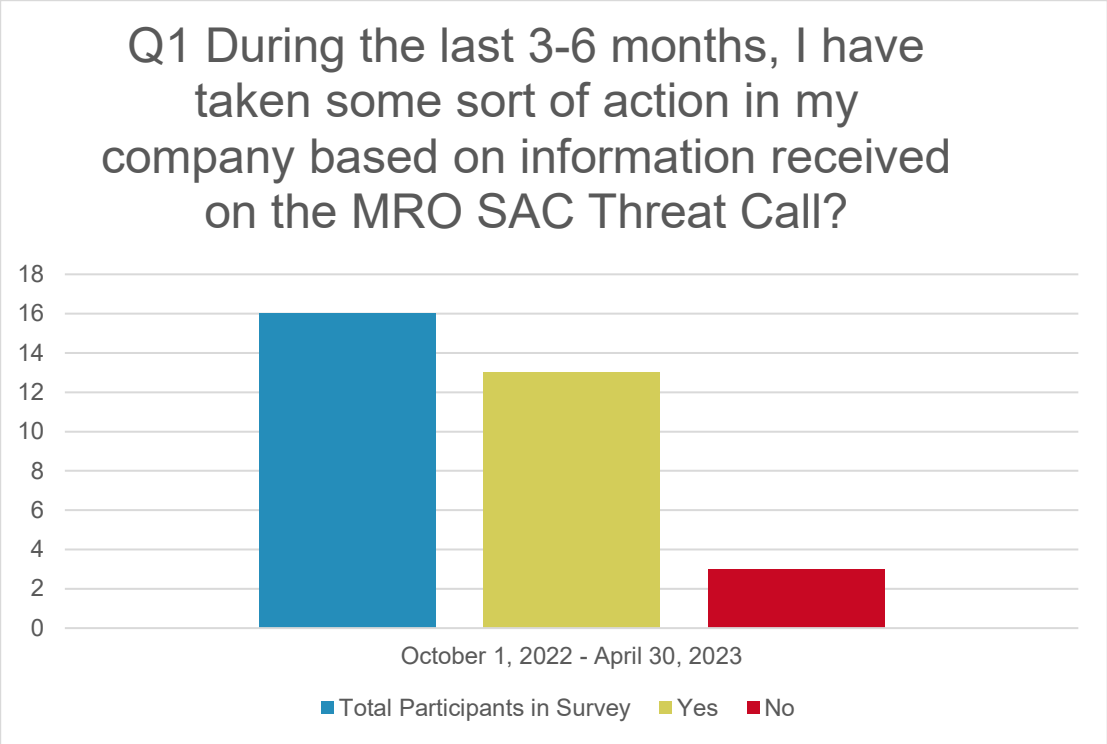
Action

Discussion

Report

SACTF Chair Brett Lawler will lead this discussion during the meeting.

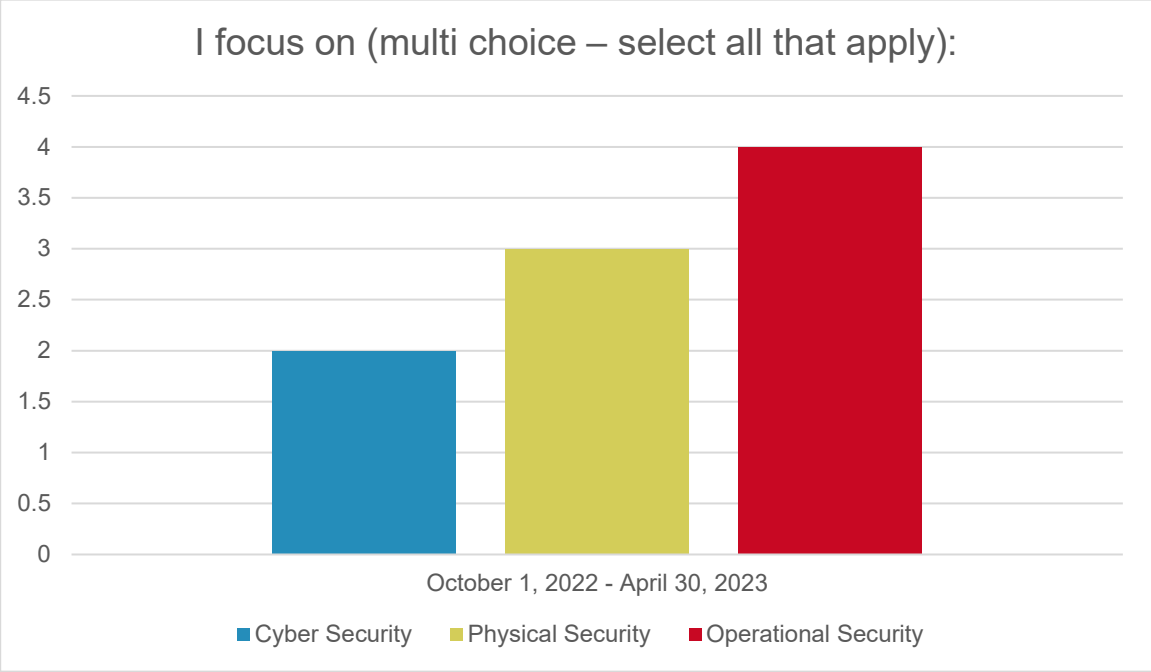
Question A:



- We need to focus on threats relevant to the electric industry that have a likelihood of actually happening. I understand there isn't that many new threats on a weekly basis. A lot of conversations would seem better suited to FBI agents investigating domestic terrorism.
- Good call and thanks for seed topics
- Information is shared with need-to-know staff.
- The E-ISAC loves participating in this regional threat briefing!
- This is an excellent forum.
- My role is one of compliance, so I have taken information from this meeting a shared with teams and they may have acted on the information
- Always a very useful conversation with a great diversity in terms of operational roles and knowledge. Thank you for organizing!

Classification: Public

Question B:

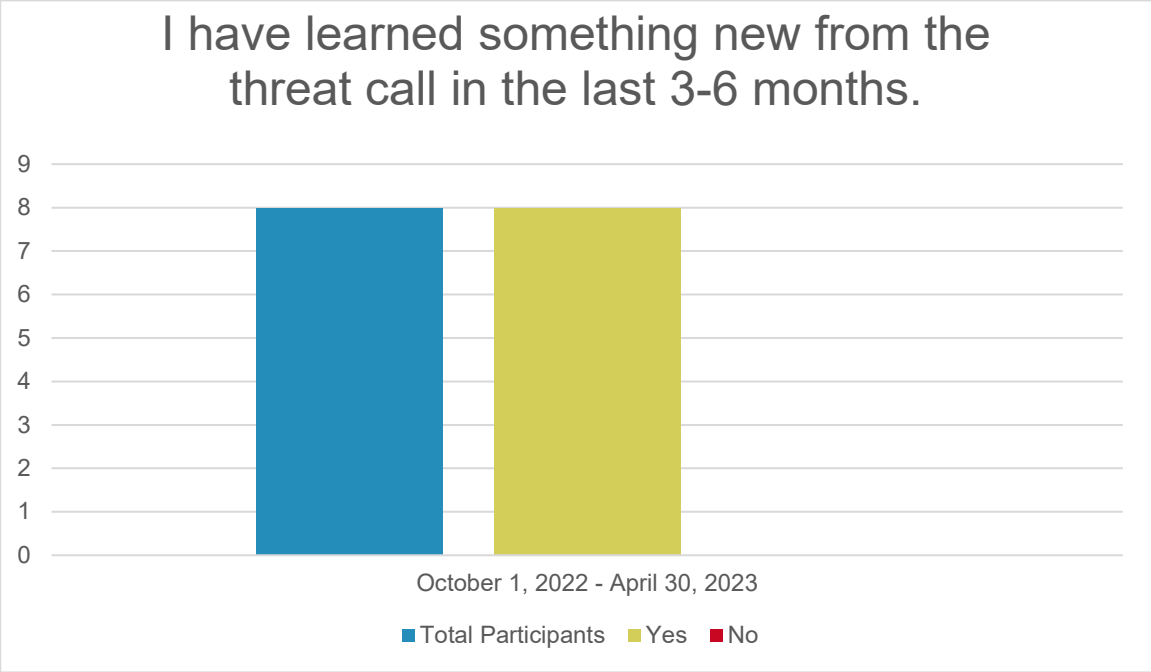


- Information from the SACTF is shared with need-to-staff.
- Great meeting, lots of good discussion as always.

Question C:

- I try to get on these as often as I can. We have other members in the company that act more as a official channel for communication so I usually defer to them for active participation. Iknow that this call is intended to be open and I do occasionally comment but I hope that any lack of participation is not viewed as a sign that I do not get value from this call.
- While we have not directly contributed, the discussions, tips and insight are invaluable toengaging our own team.12/14/2022 8:31 AM

Question D:



- Information is shared with need-to-know staff.
- This information is shared with need-to-know staff.
- This was the best call I have been on in a while. I appreciate the links everyone shares and the wide range of knowledge and solutions.

AGENDA

Security Advisory Council Threat Forum (SACTF) Update

c. Threat Forum Open Source Information Sharing

Brett Lawler, MRO SACTF Chair

Action

Discussion

Report

SACTF Chair Brett Lawler will lead this discussion during the meeting.

AGENDA

SAC Member Discussions
Steen Fjalstad, MRO Director of Security

Action
Discussion

Report
Steen Fjalstad will lead this discussion during the meeting.

Classification: Public

AGENDA

Charter Review

a. SAC Charter

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public

AGENDA

Charter Review

b. SACTF Charter

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

Classification: Public

AGENDA

2023 Security Conference Planning Update

Cris Zimmerman, Manager of Outreach and Stakeholder Engagement, MRO

Action

Information

Report

Cris Zimmerman will provide a report during the meeting.

Classification: Public

MIDWEST RELIABILITY ORGANIZATION

MRO Q2 SAC Outreach Update

Cris Zimmerman

Manager, Outreach & Stakeholder Engagement

New Outreach Coordinator

- **Shawn Keller Started on May 1st - Outreach Coordinator**
  - Conference & Event planning
  - Webinar support
  - Council support
  - Video development

MRO Upcoming Events

- **June 8th 10-11 a.m. Webinar – Network Exposure Analysis**
  - Daniel Graham – Basin Electric Power Cooperative
- **June 12th 10-11 a.m. CMEP Webinar Good Catch Program**
  - Carl Stelly – Southwest Power Pool
- **July 12th 1-4 p.m. Virtual RSRA**
  - Lee Felter & SAC members
- **July 25th & 26th CMEP Hybrid Conference MRO Offices St. Paul, MN**

- **Aug 29th Webinar IT/OT Convergence**
  - Doug Peterchuck

MRO & Security Upcoming Events

- **September 26th – 28th MRO Hybrid Security Conference**
  - Sheraton Downtown Hotel in OKC
- **Tuesday Sept 26th**
  - Security Training 11am – 4pm – Need to determine topics & presenters
  - Social Hour & Networking 5-7pm
  - Idaho National Labs (INL) ICS Cyber Escape Room Tuesday & Wednesday
- **Wednesday Sept 27th**
  - MRO Security Hybrid Conference 8am - 4:30pm
    - Rob Lee (Dragos)
    - Patrick Tatro- Army Ranger & Cyber Security Expert
    - Tentative - Executive presentations from OG&E, Western Farmers, GRDA
    - Need to fill 2 -3 slots – topics & presenters

MRO & Security Upcoming Events

- **September 26th – 28th MRO Hybrid Security Conference**
- **Thursday Sept 28th 8 a.m. – Noon TBD**
  - Tentative Security Debrief
  - Possible Local Tours

Planning, Action Items & Due Dates

May 22-25 send out save the date notice with high level agenda

June 30th finalize agenda and speakers

Week of July 10th send out announcement and open registration


QUESTIONS

AGENDA

MRO Representative on NERC Subgroups – Written Reports

a. NERC Supply Chain Working Group (SCWG)

Tony Eddleman, NERC SCWG Representative

Action

Information

Report

The SCWG reports to the NERC Reliability and Security Technical Committee (RSTC). SCWG meets monthly on the third Monday of each month at 12:00 p.m. (central time), except for the months of January, February, and June. Due to holidays in January and February, SCWG met on the second Monday of each month. The March 2023 SCWG meeting was a hybrid meeting (virtual and an in-person option at the Sheraton Sand Key Resort, Clearwater, Florida). The June 2023 meeting will be rescheduled to June 26th due to the Juneteenth holiday.

1. NERC issued a Call for Volunteers on March 28th to request a volunteer to fill the role of SCWG Chair. Christopher Strain of Florida Power & Light Company (FPL) volunteered and was approved by the RSTC Chair. Christopher is the IT Technology Director, and his team oversees NextEra Energy's CIP-013 process. Wally Magda was the SCWG Vice Chair, but due to increased work requirements, Wally requested to step aside. Dr. Thomas Duffey, ITegrity volunteered and was approved to fill the SCWG Vice Chair position.
2. SCWG presented two Security Guidelines at the March 2023 NERC RSTC meeting for approval and these Security Guidelines were approved:

    1) Supply Chain Security Guidelines on Provenance

    a) Team Lead: David Steven Jacoby, Boston Strategies International

    2) Vendor Risk Management Lifecycle

    a) Team Lead: Tom Alrich, Tom Alrich LLC

    These Security Guidelines are available on the NERC RSTC website: Reliability Guidelines, Security Guidelines, Technical Reference Documents, and White Papers (nerc.com)

3. SCWG is preparing four Security Guidelines for posting and public comments:

    1) Vendor Identified Incident Response Measures

    a) Team Lead: Mike Prescher, Black & Veatch

    b) Substantive content complete and ready for SCWG review

    2) Supply Chain Risks Related to Cloud Service Providers

    a) Team Lead: Matt Szyda, Manitoba Hydro

b) Request to RSTC to withdraw current guideline will be on the June agenda; team is developing a new guideline that will complement a new SITES guideline on cloud computing

3) Procurement Language

a) Team Lead: Shari Gribbin, CNK Solutions

b) The team plans to distribute to SCWG prior to the June SCWG meeting for review

4) Sourcing Issues with Supply Chain Procurements

a) Team Lead: Tobias Whitney, Fortress Information Security

b) The team is making good progress in developing a draft

4. The RSTC assigned a Whitepaper on NERC Reliability Standards Gap Assessment to the SCWG. A team will be appointed, and work will begin. The gap assessment will determine if there are gaps on supply chain security. A possible SAR will be developed to fix any gaps. If a gap is determined to be a bare minimum, then a SAR will be issued. If a gap is not a bare minimum, then a guideline may be developed.

Areas of Focus

1. Maintain a roster of technical cyber and operations security experts.
2. Identify known supply chain risks and address though guidance documentation or other appropriate vehicles including input to NERC Alerts or the E-ISAC advisories.
3. Partner with National Laboratories to identify vulnerabilities in legacy equipment and develop mitigation practices.
4. Assist NERC staff by providing input and feedback associated with the development and execution of supply chain documents.
5. Coordinate with the North American Transmission Forum (NATF) and other industry groups as appropriate to ensure bulk power system (BPS) asset owner supply chain security requirements are clearly articulated.

Accomplishments

1. SCWG received NERC RSTC approval for two Security Guidelines, and these have been posted.
2. SCWG has multiple review teams working concurrently.

Challenges

1. Continuing to review and post for comments Security Guidelines
2. New assignment from the RSTC to develop a Whitepaper on a NERC Reliability Standards Gap Assessment
3. Monitoring and staying current on Supply Chain developments in the federal government and industry

AGENDA

MRO Representative on NERC Subgroups – Written Reports

b. NERC Security Integration and Technology Enablement Subcommittee (SITES)

Alan Kloster, NERC SITES Representative

Action

Discussion

Report

Classification: Public

MIDWEST RELIABILITY ORGANIZATION

MRO NERC SITES Update

Alan Kloster
Regulatory Affairs Manager
Evergy, Inc.

CLARITY | ASSURANCE | RESULTS

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO SAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.

NERC Security Integration and Technology Enablement Subcommittee Update

- The NERC SITES has moved to a quarterly meeting cadence with the last meeting held in-person in Clearwater, Florida on March 21, 2023.
- NERC SITES, the Security Working Group and Supply Chain Working Groups also held a joint meeting for the RSTC to discuss work plans on March 23, 2023 in Clearwater.
- Since then, SITES sub-team working sessions have been held to finalize white papers that SITES has been developing.
- White papers are likely to be submitted to the RSTC for their June or September meetings for endorsement.

NERC SITES BES Ops in the Cloud White Paper

- The white paper suggests that using cloud computing services could be expanded for purposes other than BES Cyber System Information (BCSI) storage, including the nine BES reliability operating services (BROS) so long as the risks associated with these technologies are carefully addressed. It is currently slated to go before the RSTC in September.

NERC SITES BES Ops in the Cloud White Paper (cont.)

- **It currently contains the following recommendations:**
  - Industry should submit a SAR to develop a new NERC CIP standard dedicated to cloud security
  - SITES perform an analysis to determine specific CIP standards and requirements and control objectives necessary in a new CIP standard to go with the SAR.
  - Revise NERC Rules of Procedure to accept 3rd party cloud assessments.
  - Initiate an effort to map NERC CIP standards against cloud-based security frameworks.
  - Cloud vendors should pro-actively seek accredited 3rd party certification (FedRamp, SOC2, etc)
  - Industry to perform CIP audit tabletops covering cloud-hosted BCS use cases to identify compliance and security risks to inform CMEP Practice Guides
  - ERO Enterprise develop compliance implementation guidance for registered entities to evidence shared responsibility models for cloud-hosted BCS.
  - Industry develop and standardize use of a CIP-tailored cloud risk assessment framework for independent use by registered entities during evaluation and selection of CSPs for cloud hosted BCS.

NERC SITES Zero Trust Security for Electric OT White Paper

- The purpose of this white paper is to inform the electricity sector about zero trust (ZT) concepts and to provide considerations and recommendations regarding the adoption of ZT controls in operational technology (OT) and industrial control system (ICS) environments. It is currently slated to go before the RSTC in June for endorsement.

NERC SITES Zero Trust Security for Electric OT White Paper (cont.)

- **It currently expands on the following topics:**
  - A discussion of what Zero Trust means and gives the basic tenets of a zero trust system
  - A discussion of the CISA Zero Trust Maturity Model
  - Using zero trust in an OT or ICS environment and how that is different from current models
  - Benefits, challenges and recommendations for using zero trust for OT/ICS
  - Compliance considerations
  - Zero trust controls guidance
  - Network segmentation, application layer deep packet inspection gateways and other security controls

NERC SITES & SPIDERWG Joint Whitepaper

Privacy and Security Impacts of DER and DER Aggregator Cybersecurity

- This paper explores the technical facets of security controls available to DER and DER Aggregators and provide an example of potential attacks that can be mitigated through the implementation of those security controls. It also provides an overview on the security posture of distribution landscape (particularly for DER and DER Aggregators) and provide correlations to NERC Standards, should any exist. They are currently asking for review and input through June 9th by the SITES/SPIDERWG/RSTC membership.

NERC SITES & SPIDERWG Joint Whitepaper

Privacy and Security Impacts of DER and DER Aggregator Cybersecurity (cont.)

- **This paper will also provide high-level recommendations to DER and/or DER Aggregators on security controls or other risk mitigation measures. Those include:**
  - ISO/RTOs making sure that market rules do not inhibit cybersecurity and consider rules that encourage cybersecurity hygiene best practices.
  - DER Aggregators and U-DERs should implement strong access, perimeter and endpoint security controls.
  - DER owners should wipe personal information from old hardware and implement data management and access controls.

SITES New Technology Enablement White Paper

- This white paper is intended to explore and attempt to solve challenges around new technology enablement for entities that are interested in being early adopters and that constantly run into challenges with early adoption
- The paper is still in its early stages with an outline having been developed and the team is working from that outline.

SITES New Technology Enablement White Paper (cont.)

- **Some of the issues they are trying to tackle are:**
  - Utility business models are evolving faster than NERC Standards
  - Regulatory climate that require leading technology and innovation
  - Leading technology is outpacing NERC Standards
  - Utilities are driving innovation due to local and emerging environmental goals
  - Utilities struggle balancing innovation, technology and compliance
  - Utilities are delaying adoption due to compliance concerns
  - Retention and attraction of talent with the requisite skill sets

A Look SITES Look at the Work Plan

- **These are items on the SITES work plan that will be focused on as the previous issues roll off:**
  - White paper on reviewing cybersecurity maturity metrics. Getting compliance data is a challenging task and they are taking a look at that from a cybersecurity perspective.
  - SITES Industry Workshop (topics to be determined)
  - A State of Technology Report focused on a broad spectrum of technology. They are evaluating whether that should become a regular report SITES produces.

AGENDA

NERC Reliability and Security Technical Committee (RSTC) Update
Marc Child, NERC RSTC Representative

Action
Discussion

Report
NERC RSTC Representative Marc Child will provide a report during the meeting.

Classification: Public

MIDWEST RELIABILITY ORGANIZATION

NERC Reliability & Security Technical Committee (RSTC) Update

Marc Child

Great River Energy

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC)(or CMEPAC or RAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO SAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.

NERC RSTC Roster

*Chair – Greg Ford (GSOC)

*Vice Chair – Rich Hydzik (Avista)

Secretary – Stephen Crutchfield

Exec Sponsor – Mark Lauby

Executive Committee

Marc Child – Great River Energy

Robert Reinmuller – Hydro One

Christine Ericson – IL Commerce Commission

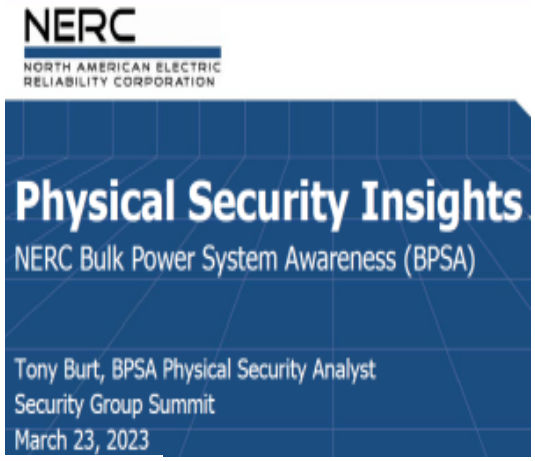
Todd Lucas – Southern Co

(*Elections currently underway for Chair & vice Chair that expire 6/2023)

Sector Elected Members	
1. Investor-owned utility	Greg Stone (Duke Energy) – 2023-2025 Kayla Messamore (Evergy) – 2022-2024
2. State/municipal utility	Saul Rojas (NYPA) – 2023-2025 Seat Converted to At-large – 2022-2024
3. Cooperative utility	Marc Child* (Great River Energy) – 2023-2025 Gregory McAuley (Seminole Electric) – 2022-2024
4. Federal or provincial utility/Federal Power Marketing Administration	Edison Elizeh (Bonneville Power) – 2023-2025 Robert Reinmuller* (Hydro One) – 2022-2024
5. Transmission dependent utility	John Stephens** (City Utilities of Springfield) – 2023-2025 Vacant – 2022-2024
6. Merchant electricity generator	Mark Spencer (LS Power) 2023-2025 Truong Le (CMS Energy)** – 2022-2024
7. Electricity Marketer	Seat converted to At-large – 2023-2025 Jodirah Green (ACES Power) – 2022-2024
8. Large end-use electricity customer	Seat converted to At-large – 2023-2025 Venona Greaff (Occidental Chemical) – 2022-2024
9. Small end-use electricity customer	Darryl Lawrence (PA Office of Consumer Advocate) – 2023-2025 Seat Converted to At-large – 2022-2024
10. Independent system operator/ regional transmission organization	Eric Miller (MISO) – 2023-2025 Seat Converted to At-large – 2022-2024
12. State Government	Christine Ericson* (Illinois Commerce Commission) – 2023-2025 Cezar Panait (Minnesota Public Utilities Commission) – 2022-2024
At-large Members	
Ian Grant**	Tennessee Valley Authority – 2022-2023 (converted sector 7 seat)
Marc-Antoine Roy	Hydro Quebec – 2023-2025 (converted Sector 8 seat)
William Allen**	Exelon – 2023-2025
Thomas Burns	PacifiCorp – 2023-2025
David Jacobson	Manitoba Hydro – 2023-2025
Srinivas Kapagantula**	Arevon Energy – 2023-2025
Todd Lucas*	Southern Company -2023-2025
Brett Kruse	Calpine – 2023-2024 (filled vacancy)
David Grubbs	City of Garland, Texas – 2022-2024 (converted Sector 2)
Wayne Guttormson**	SaskPower – 2022-2024 (converted Sector 9)
Dede Subakti	California ISO – 2022-2024 (converted Sector 10)
David Mulcahy	Illuminate Power Analytics, LLC – 2022-2024
Peter Brandien	ISO New England– 2022-2024
Monica Jain	SCE – 2022-2024
Chad Thompson	ERCOT - 2022-2024

Annual(?) Security Summit - Agenda

- **Intro speakers**
  - Rich Hydzik, RSTC vice Chair
  - David Ortiz, Director, FERC
- **National Lab updates**
- **NERC Updates**
- **Roundtable**
  - ChatGPT / AI use at utilities
  - Non-security supply chain issues



Action Items - Security

- **RSTC Info Session**
  - RSTC Work Plan Priorities
    - Energy Assurance
    - Inverter-based Resources
    - Distributed Energy Resources
    - Supply Chain Security

- SITES
  - Work Plan item #4: Collaboration Whitepaper: Privacy & Security Risks of DER Aggregators

- SCWG
  - Work Plan item #4: Provide input and feedback to NERC staff on Supply Chain security topics
  - Work Plan item #7: Physical Security Risks pertinent to the supply chain
- SWG
  - Work Plan item #7: Planning to Reduce Critical Facilities
- SITES (also included in DER Risk Priority)
  - Work Plan item #4: Collaboration Whitepaper: Privacy & Security Risks of DER Aggregators

Action Items - Security

- **Supply Chain Working Group (SCWG)**
  - Interim Chair Wally Magda, Sponsor Christine Ericson
  - Approved revised Security Guidelines:
    - Provenance
    - Vendor Risk Management

- **Security Working Group (SWG)**
  - Co-chairs Brent Sessions & Katherine Street, Sponsor Monica Jain
  - Approved: BCSI in the Cloud Tabletop Exercise (Technical Reference)
  - Approved: FERC Lessons Learned (Technical Reference)

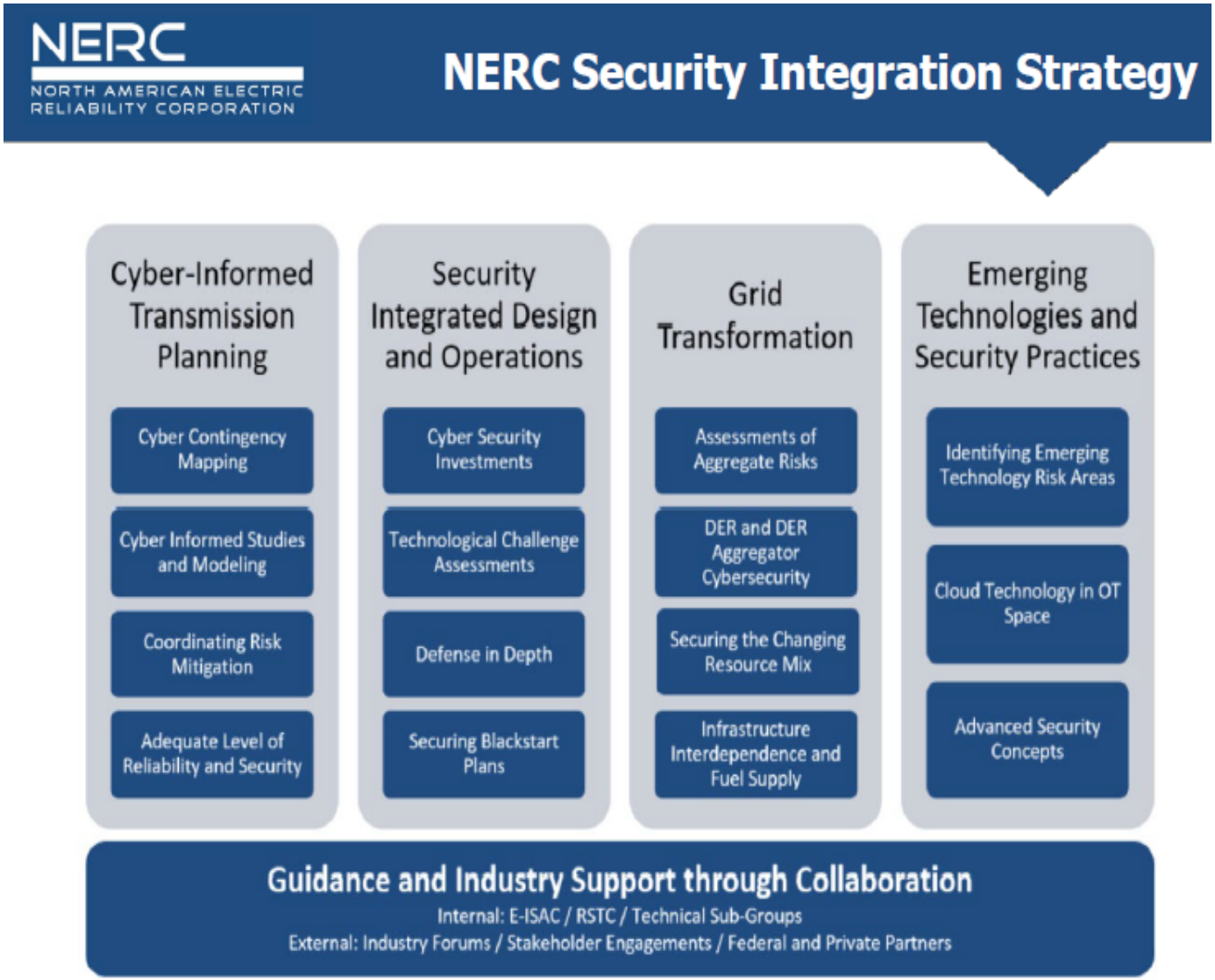
Informational Items - Security

Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

Action
Information

Summary
The risk posed by cyber and physical security threats to the electric grid is growing. Rapid digitalization and decarbonization of the electricity sector are some of the predominant drivers to grid transformation today and into the future. Large-scale changes to the generation resource mix, how and where they are connected, increased remote command and control capabilities, and the myriad technologies and communications networks that facilitate these changes pose significant challenges to reliability, resilience, and security of critical infrastructure such as the bulk power system which enables modern society. Historically, security has not played a strong role in traditional engineering practices such as transmission planning, power system design, and even power system operations. This report provides a foundation for establishing the concept of "security integration," which attempts to begin addressing these issues through a more integrated approach for cyber and physical security into the planning, design, and operational phases of the bulk power system. This report was created under the direction and guidance of a joint task force of IEEE members and the North American Electric Reliability Corporation (NERC).

Informational Items - Security



Subgroup workplans

Working Group	Current Projects
Supply Chain WG	Cloud Service Providers
	Contract Language
	Procurement Sourcing
	Vendor Incident Response
Security Working Group	Harmonizing Design Basis Threats (DBTs)
	Cloud Encryption
	CIP Evidence Request Tool updates
	CIP mapping (OLIR Team)
SITES	BES Ops in the Cloud
	Zero Trust
	DER Aggregator Security
	New Tech Enablement Field Testing

2023 schedule

2023-2024 Meeting Dates	Time	Location	Hotel
June 20, 2023* June 21 2023 June 22, 2023	3:00 – 5:00 PM 8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Hybrid	MRO – St. Paul, MN
September 19, 2023* September 20, 2023 September 21, 2023	3:00 – 5:00 PM 8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Hybrid	WECC – Salt Lake City, UT
December 6, 2023 December 7, 2023	11:00 a.m. – 4:00 p.m. 11:00 a.m. – 4:00 p.m.	Virtual	N/A
Annual Work Plan Summit January 30, 2024 January 31, 2024 February 1, 2021	1 p.m. – 5 p.m. 8:30 a.m. – 4:00 p.m. 8:30 a.m. – 12:30 p.m.	Hybrid	NERC Office in Atlanta

**This will be an informational session to review the RSTC work plan including specific high interest groups with a detailed review of their work plan. May also have some information items presented, mostly geared toward forward looking topics.*

AGENDA

SAC Work Plan Update

a. SAC Work Plan

b. SACTF Work Plan

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.

AGENDA

Action Item Review
Margaret Eastman, Security Administrator

Action
Discussion

Report
Margaret Eastman will lead this discussion during the meeting.

AGENDA

Other Business and Adjourn

Ian Anderson, MRO SAC Chair

Action

Discussion

Report

Chair Ian Anderson will lead this discussion during the meeting.