MIDWEST RELIABILITY ORGANIZATION

Meeting Agenda

Security Advisory Council (SAC)

June 22, 2022
9:00 am to 3:30 pm central

MRO Corporate Offices, King Conference Center
St. Paul, MN 55102

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.**

AGENDA 1

Call to Order and Determination of Quorum

a. Roster

Clayton Whitacre, MRO SAC Chair

Name	Role	Company	Term
Clayton Whitacre	**Chair**	Great River Energy	12/31/22
Michael Meason	**Vice-Chair**	Western Farmers Electric Cooperative	12/31/23
Brett Lawler	Member	Xcel Energy	12/31/23
Chad Wasinger	Member	Sunflower Electric Power Cooperative	12/31/23
Daniel Graham	Member	Basin Electric Power Cooperative	12/31/24
Douglas Peterchuck	Member	Omaha Public Power District	12/31/24
Jamey Sample	Member	Xcel Energy	12/31/22
Jason Nations	Member	Oklahoma Gas and Electric	12/31/24
Justin Haar	Member	Minnkota Power Cooperative	12/31/23
Laura Liston	Member	Alliant Energy Corporation	12/31/22
Matthew Szyda	Member	Manitoba Hydro	12/31/23
Norma Browne	Member	Ameren	12/31/24
Sam Ellis	Member	Southwest Power Pool, Inc.	12/31/22
Tim Anderson	Member	Dairyland Power Cooperative	12/31/22
Tony Eddleman	Member	Nebraska Public Power District	12/31/22

AGENDA 1

Call to Order and Determination of Quorum

b. Robert's Rules of Order

Clayton Whitacre, 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.

MRO SECURITY ADVISORY COUNCIL Q2 MEETING AGENDA

Agenda Item

1 Call to Order and Determination of Quorum
Clayton Whitacre, MRO SAC Chair
a. Determination of Quorum and Roster
b. Robert's Rules of Order

2 Roll Call

3 Standards of Conduct and Anti-Trust Guidelines
Clayton Whitacre, MRO SAC Chair

4 Charter Review
Clayton Whitacre, MRO SAC Chair
a. SAC Charter
b. SACTF Charter

5 MRO Representatives on NERC Subgroups - Written Reports
Steen Fjalstad, Director of Security, MRO
a. NERC SupplyChain Working Group (SCWG) – Tony Eddleman, NERC SCWG Representative
b. NERC Security Integration and Technology Enablement Subcommittee (SITES) Alan Kloster, NERC SITES Representative

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

Break – 10:30 a.m. – 10:45 a.m.

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

8 SAC Work Plan Update
Clayton Whitacre, MRO SAC Chair

Lunch 12:00 p.m. – 1:00 p.m.

9 Joint Meeting with the OGOC
Clayton Whitacre, MRO SAC Chair
a. Outreach and Areas of Focus for Outreach
b. Enhanced Collaboration with Intelligence and Government Agencies
c. Regional Security Risk Assessment

Break – 2:00 p.m. – 2:15 p.m.

10 Regional Security Risk Assessment (RSRA)
Matt Szyda, MRO SAC Member

11 Action Item Review
Rebecca Schneider, Reliability Analysis Administrator

12 Other Business and Adjourn
Clayton Whitacre, MRO SAC Chair

AGENDA 3

Standards of Conduct and Antitrust Guidelines
Clayton Whitacre, MRO SAC Chair

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 4

Charter Review

a. SAC Charter

Clayton Whitacre, MRO SAC Chair

Action

Discussion

Report

Chair Clayton Whitacre will lead this discussion during the meeting.

AGENDA 4

Charter Review

b. SACTF Charter

Clayton Whitacre, MRO SAC Chair

Action

Discussion

Report

Chair Clayton Whitacre will lead this discussion during the meeting.

AGENDA 5

MRO Representative on NERC Subgroups – Written Reports

a. NERC Supply Chain Working Group (SCWG)

Tony Eddleman, NERC SCWG Representative

Action

Discussion

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 meets on the second Monday at 12:00 p.m. central time. The new Federal holiday Juneteenth required the June meeting to be rescheduled to Monday, June 27, 2022, at 11:00 a.m. (central time).

The SCWG completed work on the Supply Chain Effectiveness Survey. Survey results were presented at the March RSTC meeting and the May 12th NERC BOT meeting. Complete survey results were provided through an April 12th MRO SAC Webinar.

Much of the current work for SCWG is reviewing five Security Guidelines. Five small teams are performing the reviews.

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 developed eight Security Guidelines which are posted on the NERC SCWG website (Supply Chain Working Group (SCWG) (nerc.com)). A review of each guideline is required every three years. SCWG reviews are nearing completion of the first four listed below with the review of the Provenance getting started. Metrics are required in the updated Security Guidelines, and this has proved to be a challenge for the group.
    a. Supply Chain and Risk Considerations for Open Source Software
        Team Lead: George Masters, Schweitzer Engineering Laboratory, Inc.
    b. Secure Equipment Delivery
        Team Lead: Wally Magda, WallyDotBiz LLC
    c. The Supply Chain Cyber Security Risk Management Lifecycle
        Team Lead: Tom Alrich, Tom Alrich LLC
    d. The Vendor Risk Management Lifecycle

Team Lead: Tom Alrich, Tom Alrich LLC

e. Supply Chain Security Guidelines on Provenance
   Team Lead: David Steven Jacoby, Boston Strategies International

2. SCWG developed a Supply Chain Effectiveness Survey in 2021 and requested industry feedback. The survey closed on November 30, 2021, and SCWG analyzed the feedback from the survey. The results were presented at the March RSTC meeting and the May NERC Board of Trustees meeting on the survey.
3. SCWG discusses opportunities to partner with National Laboratories to identify vulnerabilities in legacy equipment and develop mitigation practices. An update from a National Laboratory is planned for the summer of 2022.

Challenges

1. Coordinating five review teams on Security Guidelines is a challenge.
2. Monitoring and staying current on Supply Chain developments in the federal government.

AGENDA 5

MRO Representative on NERC Subgroups – Written Reports

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

Alan Kloster, NERC SITES Representative

Action

Discussion

Report

The NERC SITES meeting on June 15, 2022 was canceled. There was no activity at last month's meeting. So there is nothing to report at this time.

AGENDA 6

Security Advisory Council Threat Forum (SACTF) Update

a. Threat Call Statistics

Brett Lawler, MRO SACTF Chair

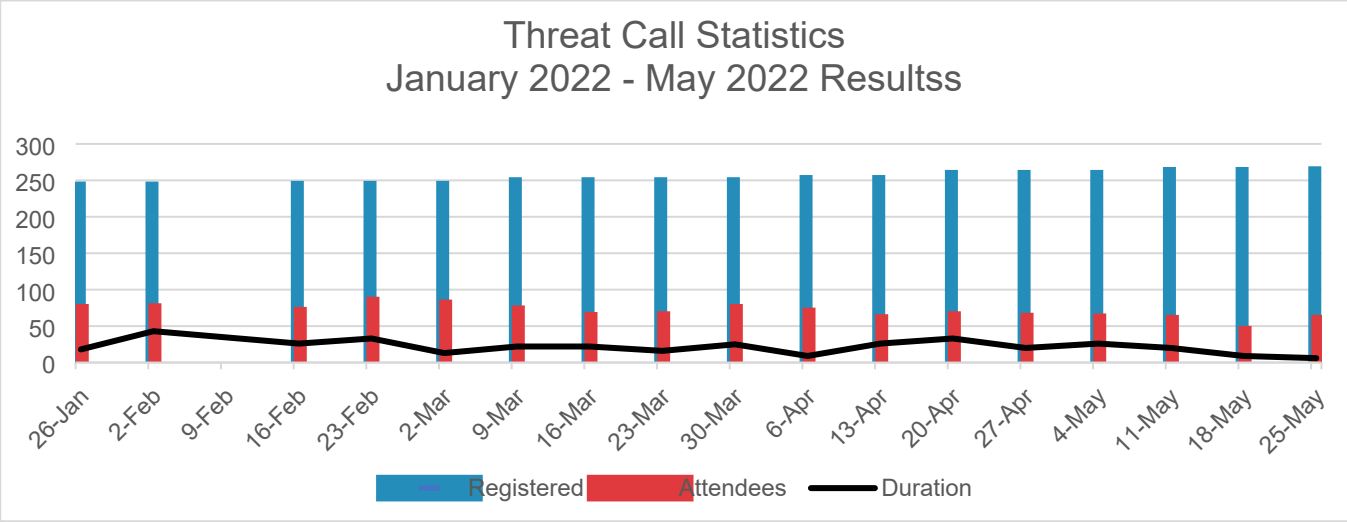
Action

Information

Report

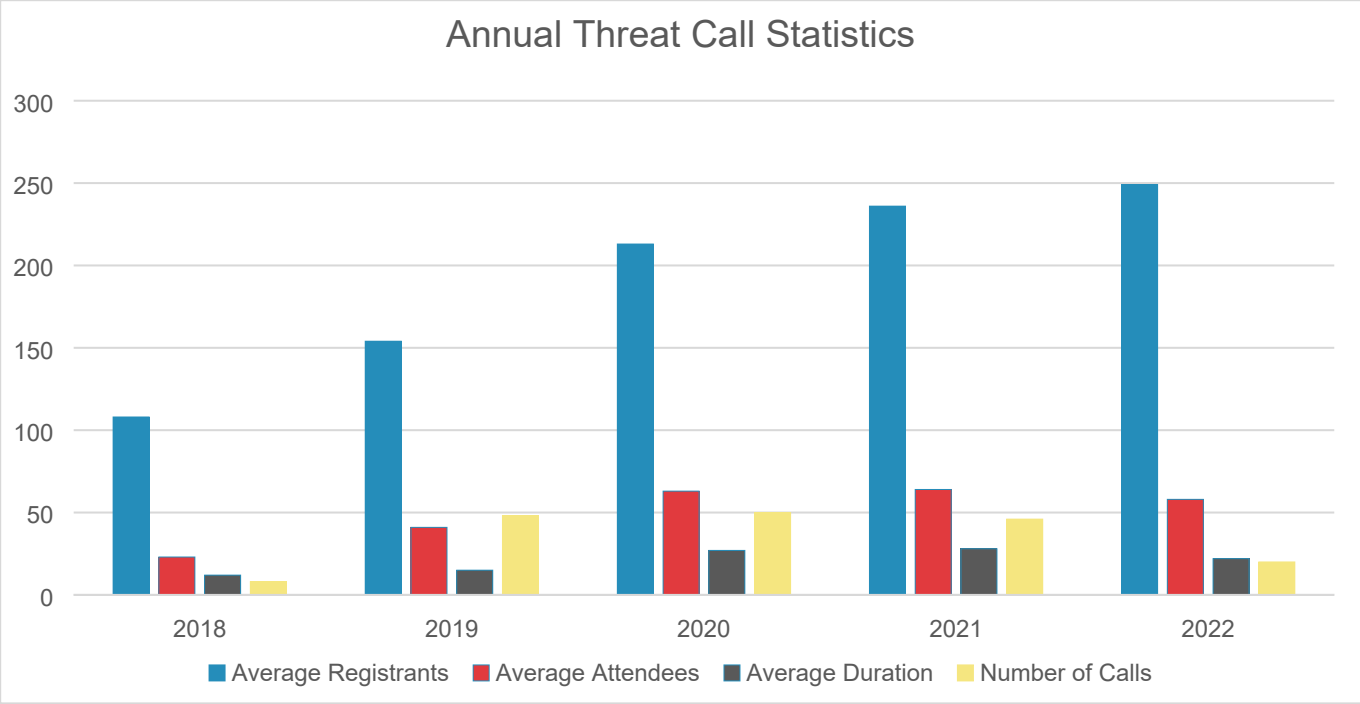
Threat Call

Date	Approved Registrants	Duration	Attendees
January 26, 2022	241	18 Minutes	73
February 2, 2022	241	43 Minutes	74
February 16, 2022	242	26 Minutes	69
February 23, 2022	242	33 Minutes	83
March 2, 2022	242	13 Minutes	79
March 9, 2022	247	22 Minutes	71
March 16, 2022	247	22 Minutes	62
March 23, 2022	247	16 Minutes	63
March 30, 2022	247	25 Minutes	73
April 6, 2022	250	9 Minutes	68
April 13, 2022	250	26 Minutes	59
April 20, 2022	257	33 Minutes	63
April 27, 2022	257	20 Minutes	61
May 4, 2022	257	26 Minutes	60
May 11, 2022	261	20 Minutes	58
May 18, 2022	261	9 Minutes	43
May 25, 2022	262	6 minutes	58
Averages	**254**	**20 Minutes**	**62**



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	249	58	22 Minutes	20 Calls



AGENDA 6

Security Advisory Council Threat Forum (SACTF) Update

b. WorkPlan

Brett Lawler, MRO SACTF Chair

Action

Discussion

Report

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

AGENDA 6

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 7

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.

MIDWEST RELIABILITY ORGANIZATION

NERC Reliability & Security Technical Committee (RSTC) Update

Marc Child

Great River Energy

CLARITY | ASSURANCE | RESULTS

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.

Sector Elected Members	
1. Investor-owned utility	Kayla Messamore (Evergy) – 2022-2024 Greg Stone (Duke Energy) – 2020-2023
2. State/municipal utility	Seat Converted to At-large – 2022-2024 Saul Rojas (NYPA) – 2020-2023
3. Cooperative utility	Gregory McAuley (Seminole Electric) – 2022-2024 Marc Child* (Great River Energy) – 2020-2023
4. Federal or provincial utility/Federal Power Marketing Administration	Robert Reinmuller* (Hydro One) – 2022-2024 Edison Elizeh** (Bonneville Power) – 2020-2023
5. Transmission dependent utility	Carter Manucy (Florida Municipal Power) – 2022-2024 John Stephens** (City Utilities of Springfield) – 2020-2023
6. Merchant electricity generator	Truong Le (CMS Energy)** – 2022-2024 Vacant
7. Electricity Marketer	Jodirah Green** (ACES Power) – 2022-2024 Seat Converted to At-large – 2020-2023
8. Large end-use electricity customer	Venona Greaff (Occidental Chemical) – 2022-2024 Travis Fisher (Electricity Consumers Resource Council) – 2020-2023
9. Small end-use electricity customer	Seat Converted to At-large – 2022-2024 Darryl Lawrence (PA Office of Consumer Advocate) – 2020-2023
10. Independent system operator/ regional transmission organization	Seat Converted to At-large – 2022-2024 CJ Brown (SPP) – 2020-2023
12. State Government	Cezar Panait (Minnesota Public Utilities Commission) – 2022-2024 Christine Ericson* (Illinois Commerce Commission) – 2020-2023
At-Large Members	
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
Jeff Harrison	AECI – 2022-2024
Monica Jain**	SCE – 2022-2024
Ian Grant	Tennessee Valley Authority – 2022-2023 (converted sector 7)
William Allen**	Exelon – 2022-2023 (vacant due to vice chair election)
Patrick Doyle**	Hydro Quebec – 2020-2023
David Jacobson	Manitoba Hydro – 2020-2023
Sandra Ellis**	Pacific Gas & Electric Company – 2020-2023
Todd Lucas*	Southern Company -2020-2023

*Denotes Executive Committee member
**Denotes Nominating Subcommittee member

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

Christine Ericson – Illinois Commerce

Todd Lucas – Southern Co

Robert Reinmuller – Hydro One

RSTC membership

- **Sector seats:**
  - Two per sector, 2-year terms
  - Sectors 2 (state/muni) & 9 (small end-use), no nominations. Converted to at-large for one cycle.
  - 18 members
- **At-large seats:**
  - Intended to balance: regions, interconnections, SME, org types, US/Can
  - 14 members, including converted sector seats
- **Chair and vice chair**
  - 2 members

Action & informational items – June 2022 meeting

- **Items of note to MRO SAC:**
  - 2022 NERC State of Reliability Report
  - All things DER and Inverters
  - RSTC & the SAR process
  - TOCC Field Test (CIP-002)
  - 6 GHz task force
  - SWG Whitepaper – Internal Network Security Monitoring

Action and informational items

Item	Type	Action
Energy Reliability Assessments Task Force (ERATF) Standard Authorization Requests (SARs)	SAR	Endorse
GMD Monitoring Reference Document	Document	Approve
Reliability Coordinator Reliability Plan Reference Document	Document	Approve
2022 State of Reliability Report	Report	Informational
GADS Section 1600 Data Request	Document	Post for 45-day comment
BPS Reliability Perspectives for Distributed Energy Resource Aggregators	Document	Approve
Recommendations for Simulation Improvement and Techniques Related to DER Planning	Document	Approve
DER Impacts to Under Voltage Load Shedding Program Design	Document	Req for review
Beyond Positive Sequence RMS Simulations for High DER Penetration Conditions	Document	Req for review
June-August 2021 CAISO Solar PV Disturbance Report	Report	Informational

Action and informational items

Item	Type	Action
EMT Models in NERC MOD, TPL, and FAC Standards (SAR)	SAR	Endorse
TOCC Field Test Update	Project	Informational
Strengthening Industry Action to Address Emerging Issues	Project	Informational
Inter-Area Short Circuit paper	Document	Req for review
Facility Ratings Task Force Update	Project report	Informational
Electric Vehicle (EV) Charging and Potential Reliability Risks	Report	Informational
6 GHz Task Force (6GHZTF)	Project report	Informational
SPCWG Cold Weather Report Recommendation #13	Proposal	Approve
EOP-004 Standard Authorization Request	SAR	Endorse
ERO and RSTC Strategic Plan Alignment	Project	Informational

Action and informational items

Item	Type	Action
RAS LTRA Preview and 2022 Assessment Plan	Document	Informational
WECC-NERC Joint Report: Assessment of High Penetration and Ramping of Variable Energy Resources	Report	Informational
FERC RM22-3: Internal Network Security Monitoring (SWG Whitepaper)	Document	Informational

Future meetings

2022-2023 Meeting Dates	Time	Location	Hotel
September 13, 2022 September 14, 2022	Please reserve entirety of both days	Atlanta	Grand Hyatt Buckhead
December 6, 2022 December 7, 2022	Please reserve entirety of both days	Virtual	Virtual
March 8, 2023 March 9, 2023	Please reserve entirety of both days	TBD	TBD
June 14 2023 June 15, 2023	Please reserve entirety of both days	TBD	TBD
September 13, 2023 September 14, 2023	Please reserve entirety of both days	TBD	TBD
December 6, 2023 December 7, 2023	Please reserve entirety of both days	TBD	TBD

Security Integration & Technology Enablement Subcommittee (SITES)

- **Forum to identify & eliminate barriers to adoption of emerging technologies**
- Brian Burnett Chair (NCEMCS), Thomas Peterson Vice-chair (GE)
- FERC filing: BES Operations in the cloud – Google ***'nerc.com RM20-8-000'***
- Larry Collier new staff liaison
- **Workplan**
  - BES Operations in the Cloud (Asset owner & CSP perspective)
  - The integration of security considerations into conventional grid planning, design, and operations
  - Zero-Trust Concept
  - Roadmap for Field Trials
  - IT/OT Convergence
  - Reliability/Resilience/Security Balance
  - Emerging Technologies
  - Identify risks and propose mitigations while also considering the potential risks and benefits of increasing system complexity (and attack surface) and decreasing diversity of equipment.
  - Security Implementation
- **Contact Stephanie Lawrence (Stephanie.Lawrence@nerc.net) to be added to the roster**

Security Working Group (SWG)

- **Current initiatives**
  - Working group -> promote to subcommittee
  - Cloud encryption guidance & BCSI tabletop
  - CIP evidence request tool review
  - CIP mapping project
  - FERC CIP-002 lessons learned whitepaper
- **Contact Tom Hofstetter (Tom.Hofstetter@nerc.net) to be added to the roster**

Supply Chain Working Group (SCWG)

- **Current initiatives**
  - Review of existing guidelines
  - Automated risk data library (joint project with Trades)
  - Supply chain effectiveness survey (complete)
  - Partner with national labs (ex. CyTRICS)
  - Track software-bill-of-materials (SBOM) efforts
- **Contact Tom Hofstetter (Tom.Hofstetter@nerc.net) to be added to the roster**

AGENDA 8

SAC Work Plan Update
Clayton Whitacre, MRO SAC Chair

Action
Discussion

Report
Chair Clayton Whitacre will lead this discussion during the meeting.

Joint Meeting with the OGOC

- Outreach and Areas of Focus for Outreach
- Enhanced Collaboration with Intelligence and Government Agencies
- Regional Security Risk Assessment

AGENDA 9

Joint Meeting with the OGOC

a. Outreach and Areas of Focus for Outreach

Clayton Whitacre, MRO SAC Chair

Action

Discussion

Report

Chair Clayton Whitacre will lead this discussion during the meeting.

AGENDA 9

Joint Meeting with the OGOC

b. Enhanced Collaboration with Intelligence and Government Agencies

Clayton Whitacre, MRO SAC Chair

Action

Discussion

Report

Chair Clayton Whitacre will lead this discussion during the meeting.

AGENDA 9

Joint Meeting with the OGOC

c. Regional Security Risk Assessment

Clayton Whitacre, MRO SAC Chair

Action

Discussion

Report

Chair Clayton Whitacre will lead this discussion during the meeting.

AGENDA 11

Regional Security Risk Assessment (RSRA)
Matt Szyda, MRO SAC Member

Action
Discussion

Report
Matt Szyda will lead this discussion during the meeting.

2022 MRO Regional Security Risk Assessment Survey Results

2022-06-22

Background

- Annual Risk Assessment Survey for physical, cyber & operational security SMEs
- Information provided helps:
  - Input into MRO Reginal Risk Assessment
  - MRO SAC workplan development
  - Future topics for webinars, presentation etc. from the MRO SAC

Background

- 2022 Risk Assessment Survey
  - Incorporated some lessons learned from prev. surveys
  - Only 1 Survey!
  - Always looking to improve – feedback welcome!

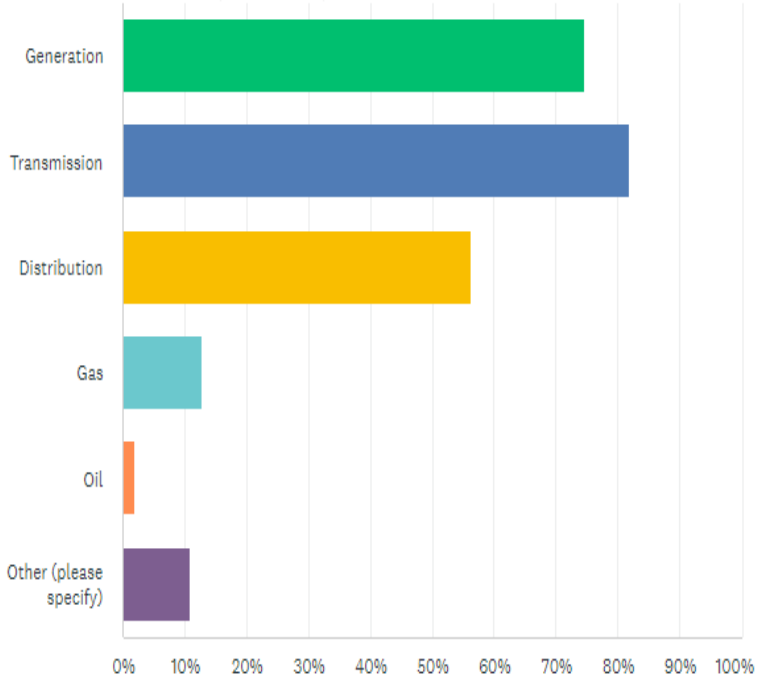
Background – Survey Method

- Rank ~ 20 threats on consequence X likelihood
- Consequences
    1. No impact
    2. Impact your organization only
    3. Impacts cause span beyond your organization, but do not impact region
    4. Impacts cause blackouts limited to the region
    5. Impacts cause nation-wide blackouts
- Likelihood
    1. <5% chance of happening
    2. 5-40% chance of happening
    3. 41-70% chance of happening
    4. 71-95% chance of happening
    5. >95% chance of happening

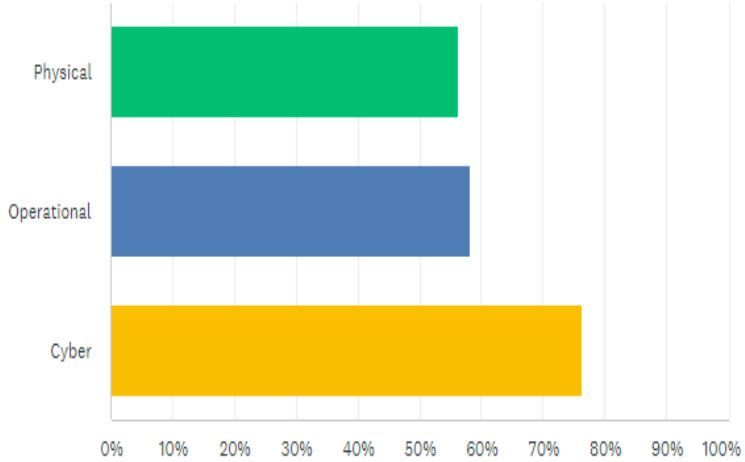
Discussion – Breakdown

Total of 55 responses (from last year)

Sector

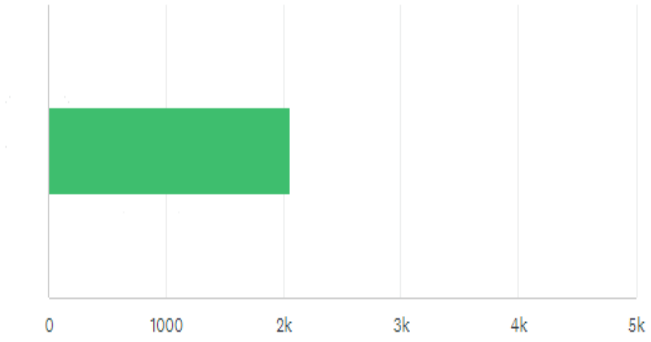


Security Domain



Discussion – Breakdown

Organization Size



ANSWER CHOICES	AVERAGE NUMBER	TOTAL NUMBER	RESPONSES
Responses	2,059	113,224	55

Response

- Lowest: 17
- Largest: 10,000

Discussion – Summary

2022 Top Results

- Exploit of known vulnerability on unpatched system
- Data dump exposing sensitive information
- Malware Attack
- Ransomware
- Supply chain compromise
- Initial access – Phishing
- An attack that corrupts backups integrity or makes backups unavailable
- Attack that Impairs process controls
- Inhibit response functions
- Initial access – exploitation of remote services
- Physical – Large equipment damage
- Insider Threat

2021 Top 10

- Accessing and applying threat intelligence
- Adequate security resources
- Asset inventory & management
- CIP compliance fatigue
- Insider threat
- Malware/Ransomware
- Network visibility & monitoring
- Physical perimeter security controls
- Security awareness and training
- Supply chain compromise
- Unsupported/Legacy devices

Discussion – Summary scores

Question #	Description	Impact	likelihood	Score
6	Exploit of known vulnerability on unpatched system	2or3	2	4 or 6
4	Data dump exposing sensitive information	3	2	6
19	Malware Attack	3	2	6
20	Ransomware	3	2	6
22	Supply chain compromise	3	2	6
13	Initial access - Phishing	2	2	4
5	An attack that corrupts backups integrity or makes backups unavailable	3	1	3
7	Attack that Impairs process controls	3	1	3
9	Inhibit response functions	3	1	3
11	Initial access – exploitation of remote services	3	1	3
17	Physical – Large equipment damage	3	1	3
21	Insider Threat	3	1	3

Discussion – Summary scores

Question #	Description	Impact	likelihood	Score
8	Attack that impairs safety instrument systems	2	1	2
10	Initial access – internet accessible devices	2	1	2
12	Initial access – wireless compromise	2	1	2
14	Initial access - Drive-by-compromise	2	1	2
15	Physical – Drones	2	1	2
16	Physical – Access controls (compromise to systems that would enable unauthorized access)	2	1	2
18	Physical – blockades (Unable to physically access facilities)	2	1	2

Discussion – Proposed top 10

1. **Q6: Exploit of known vulnerability on unpatched system**
2. **Q4: Data dump exposing sensitive information**
3. **Q19: Malware Attack**
4. **Q20: Ransomware**
5. **Q22: Supply chain compromise**
6. **Q13: Initial access – Phishing**
7. **Q7: Attack that Impairs process controls**
8. **Q9: Inhibit response functions**
9. **Q17: Physical – Large equipment damage**
10. **Q21: Insider Threat**

Discussion – Proposed top 10 Rationale

- More then 25% indicated higher impacts (impact level 4 or 5)
- Comments indicated perceived risk

In

- Q7: Attack that Impairs process controls
- Q9: Inhibit response functions
- Q17: Physical – Large equipment damage
- Q21: Insider Threat

Out

- Q5: An attack that corrupts backups integrity or makes backups unavailable
- Q11: Initial access – exploitation of remote services

Discussion – 2022 Vs. 2021

2022 Top 10

- Exploit of known vulnerability on unpatched system
- Data dump exposing sensitive information
- Malware Attack
- Ransomware
- Supply chain compromise
- Initial access – Phishing
- Attack that Impairs process controls
- Inhibit response functions
- Physical – Large equipment damage
- Insider Threat

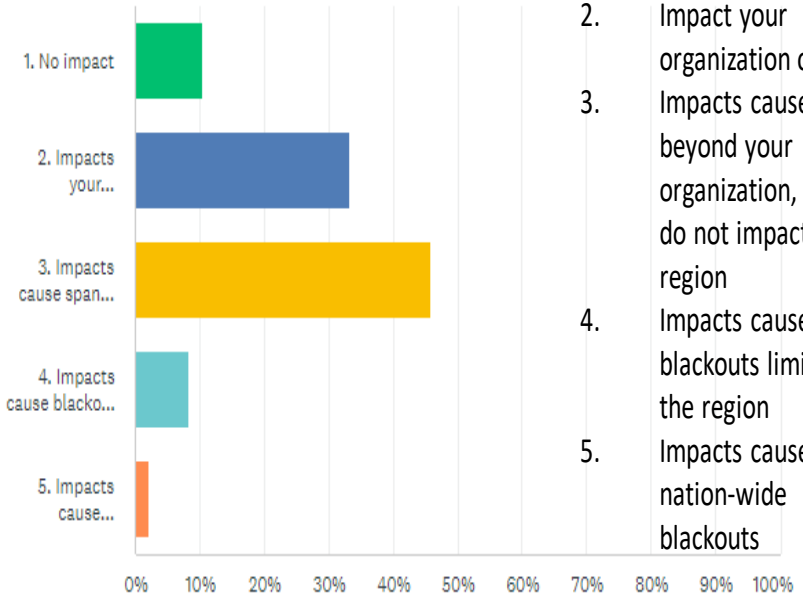
2021 Top 10

- Accessing and applying threat intelligence
- Adequate security resources
- Asset inventory & management
- CIP compliance fatigue
- Insider threat
- Malware/Ransomware
- Network visibility & monitoring
- Physical perimeter security controls
- Security awareness and training
- Supply chain compromise
- Unsupported/Legacy devices

Survey Results

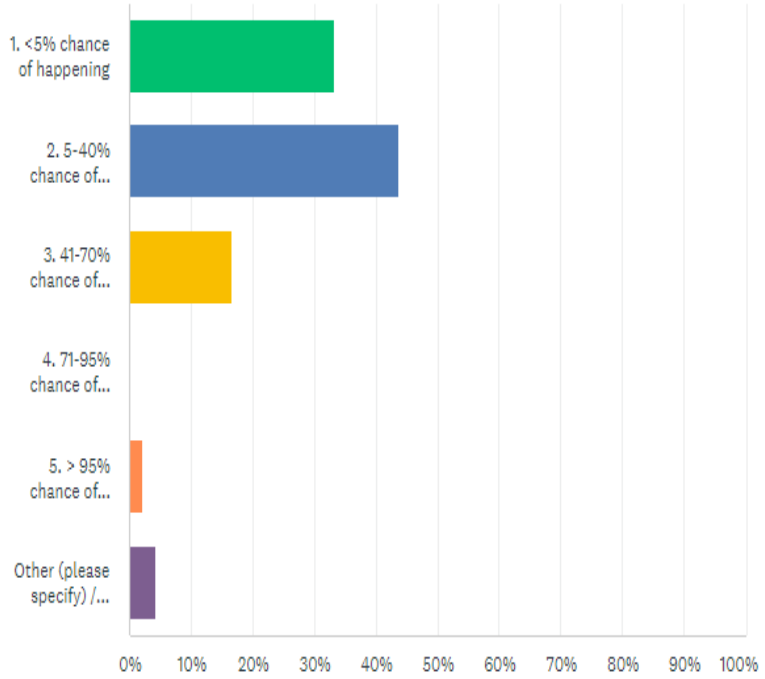
Discussion – Q4: Data dump exposing sensitive information

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

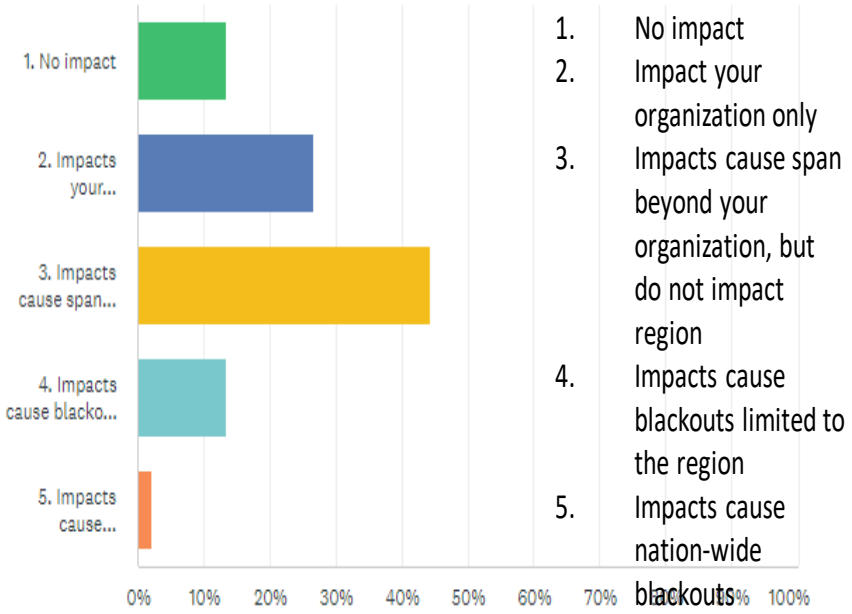


Comments:

- no impact to operations. Impact to reputation & regulatory
- Not sure this impacts the Grid/BES
- Only impacts the organization and very little sensitive information is held. Additionally, all sensitive information is encrypted at rest and in transit.
- really tough to assess since this is forward looking

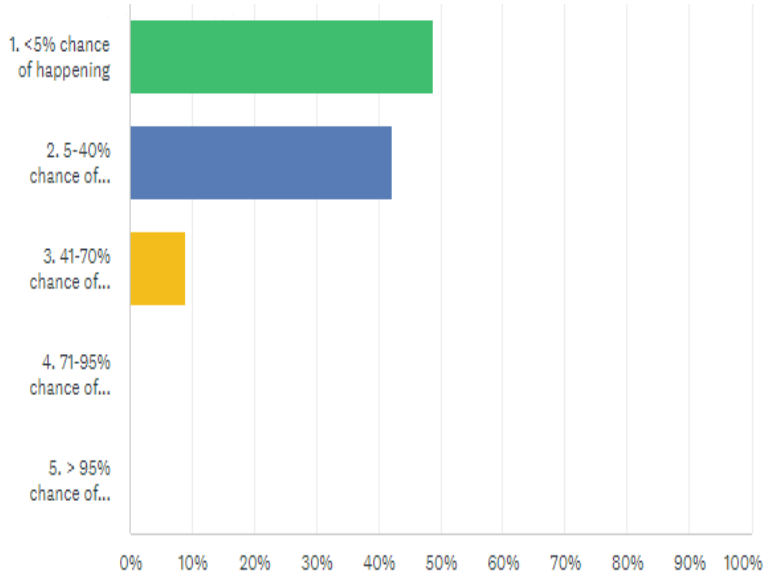
Discussion – Q5: An attack that corrupts backups integrity or makes backups unavailable

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

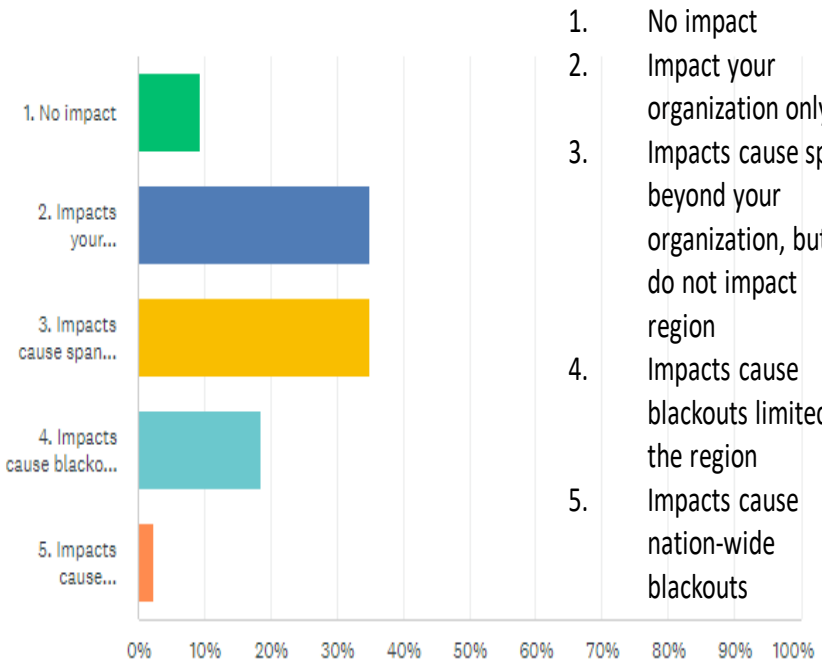


Comments:

- Loss of backup by itself would have very little impact. Coupled with another incident could multiply the impacts (increased outage duration)
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

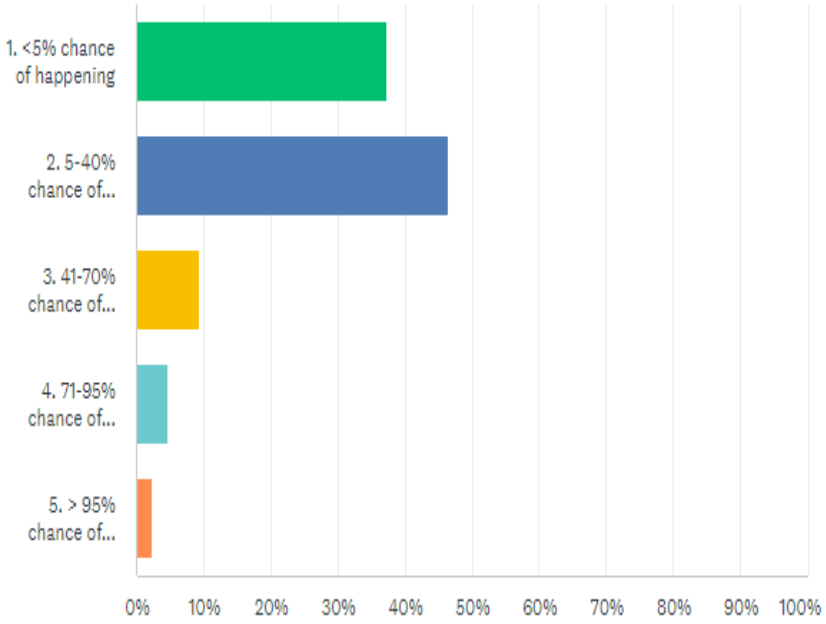
Discussion – Q6: Exploit of known vulnerability on unpatched system

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

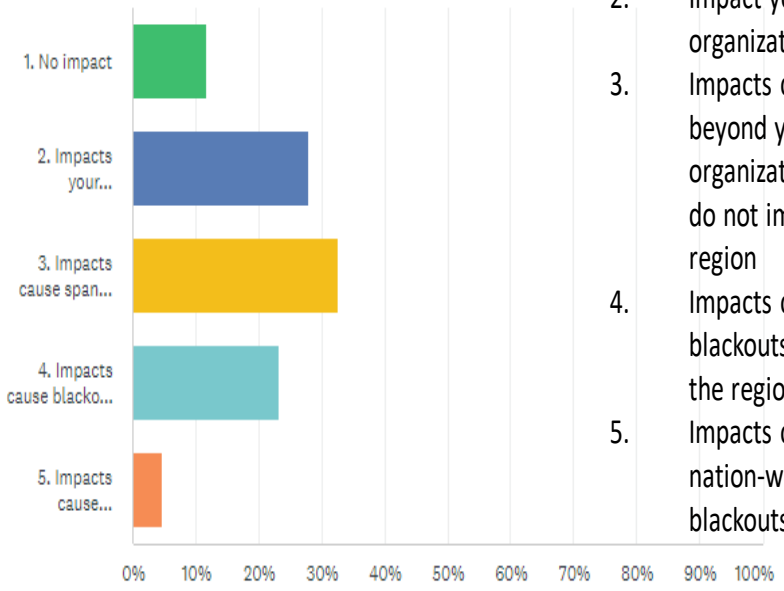


Comments:

- I assume worst case scenario.
- Not sure this impacts the Grid/BES
- Answering #2 although none of the choices really seem appropriate for this scenario. An exploit of a perimeter vulnerability is only the first step in a long sequence of events that have a multitude of possible consequences depending on the intent of the adversary. As cyber defenders we rarely concern ourselves with intent
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

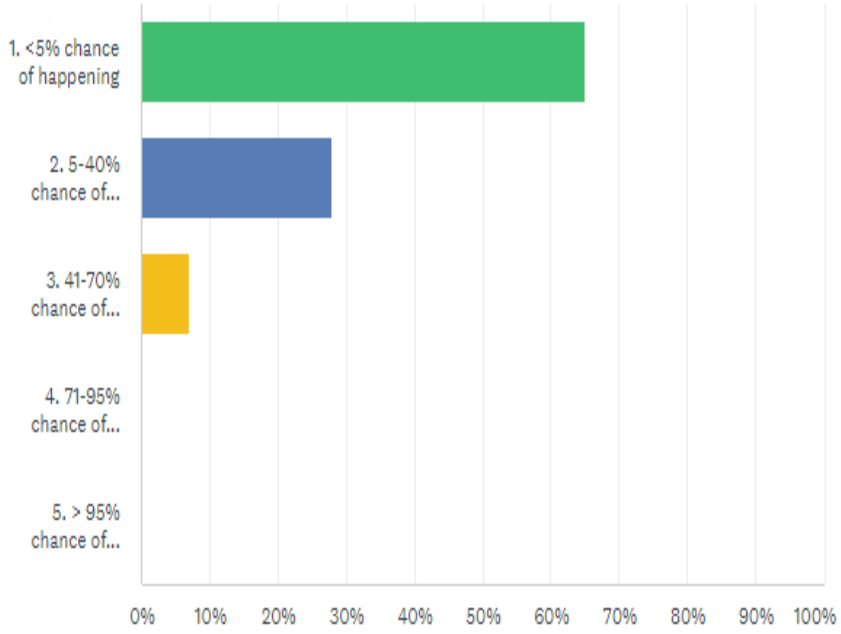
Discussion – Q7: Attack that impairs process controls

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

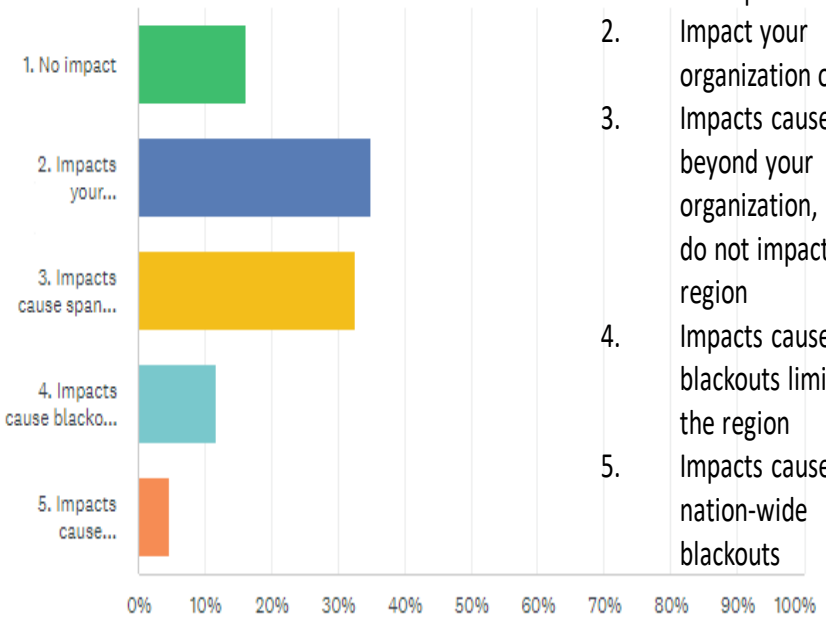


Comments:

- There are 3-4 interconnects in North America. No single event can cause a nationwide blackout.
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

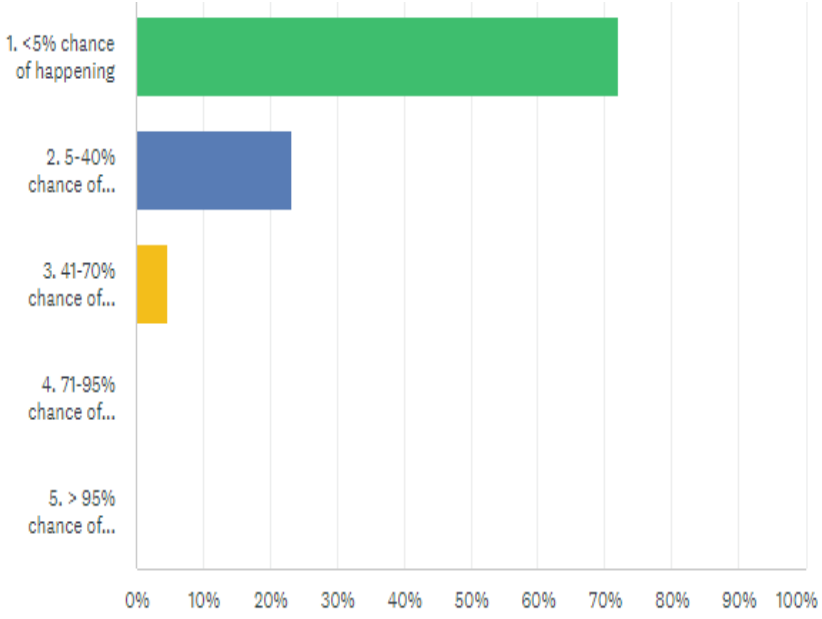
Discussion – Q8: Attack that impairs safety instrument systems

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

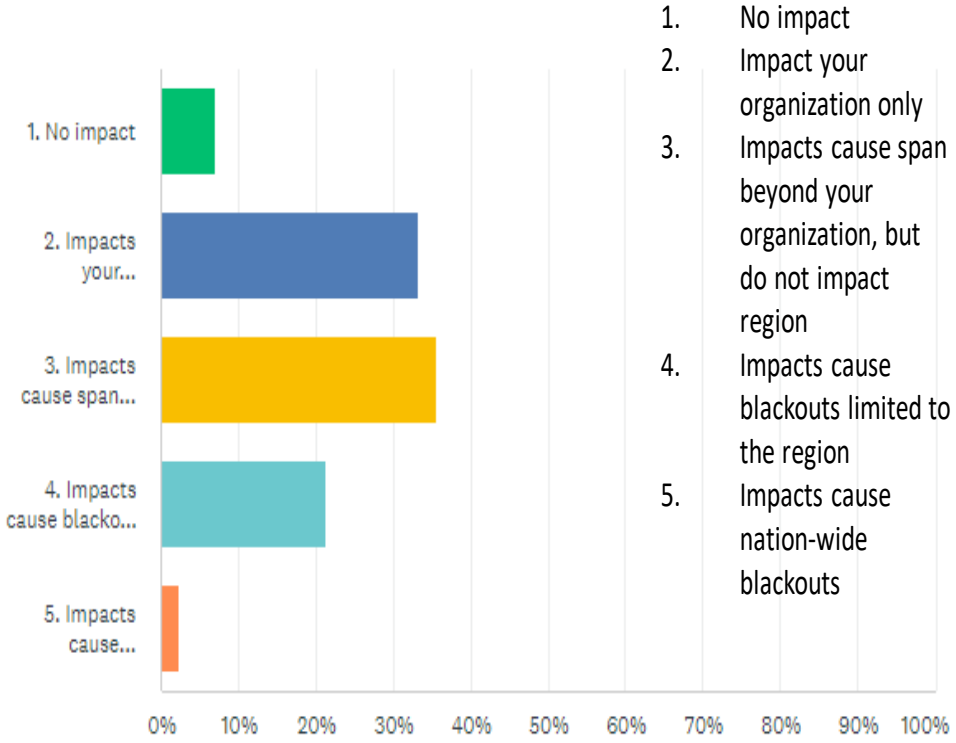


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

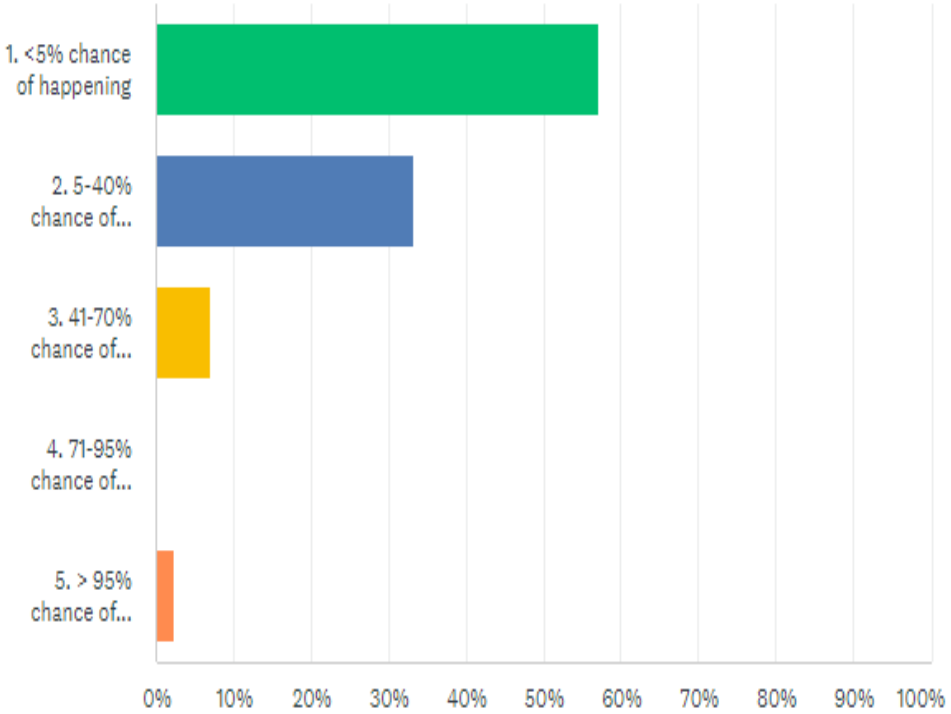
Discussion – Q9: Inhibit response functions e.g. – Denial Of Service, System firmware, Configuration Manipulation

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

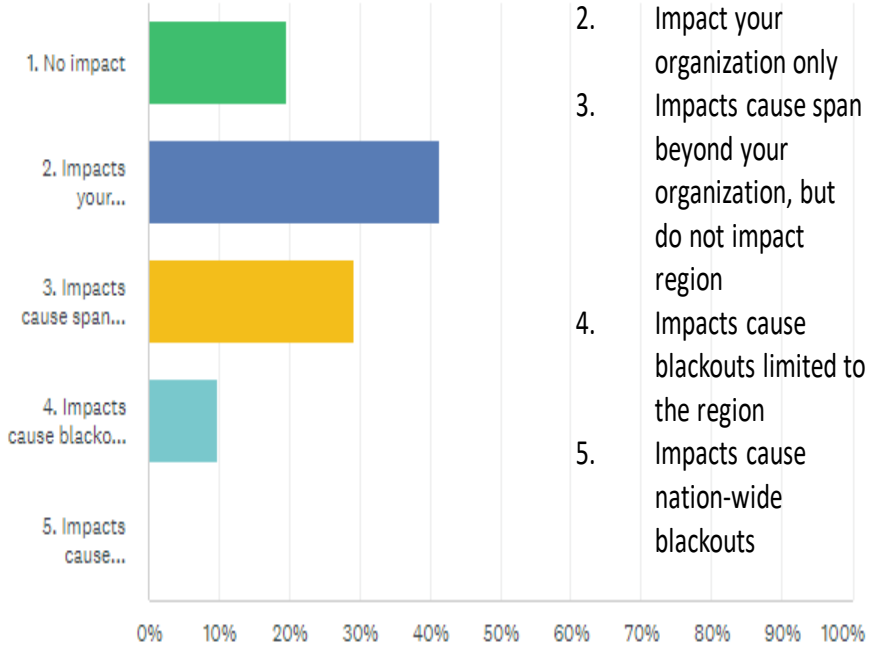


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

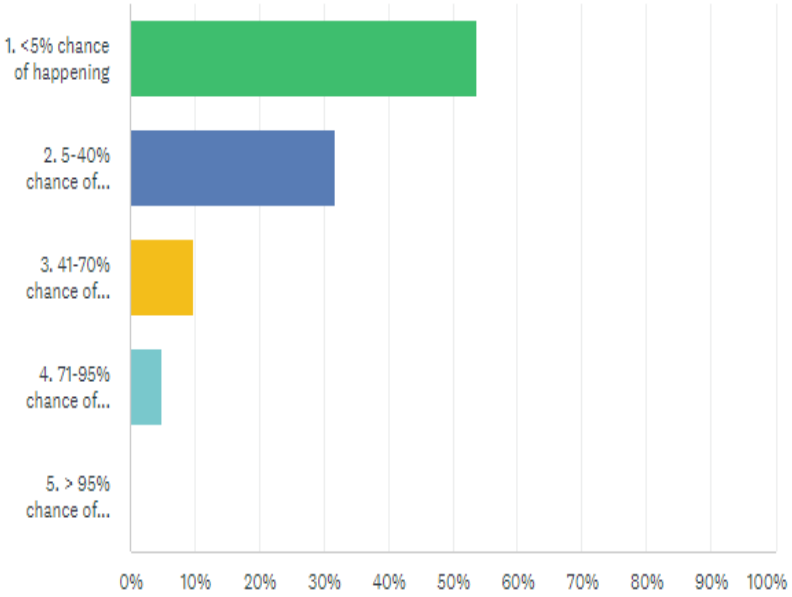
Discussion – Q10: Initial Access – internet accessible devices

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

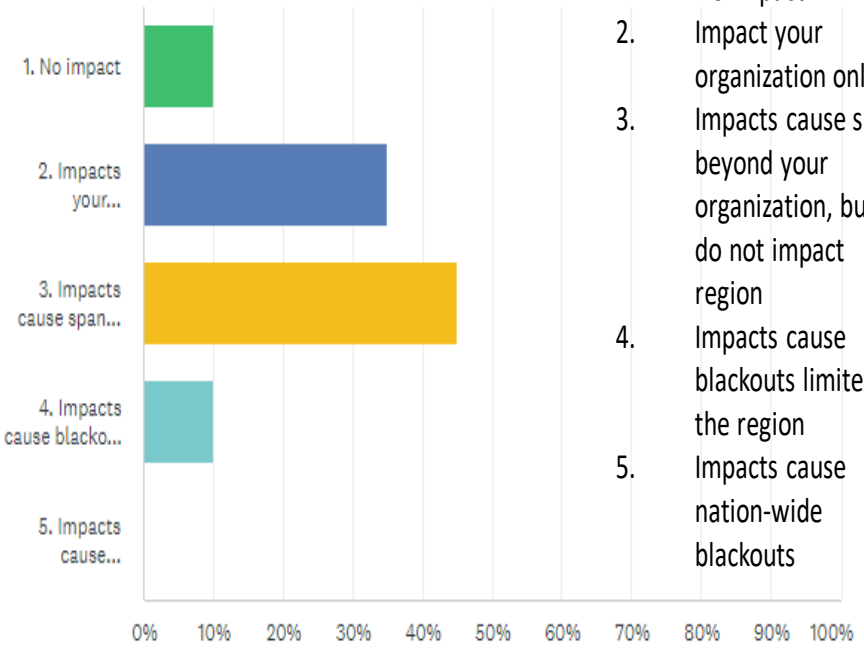


Comments:

- Not sure that this affects Grid/BES
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

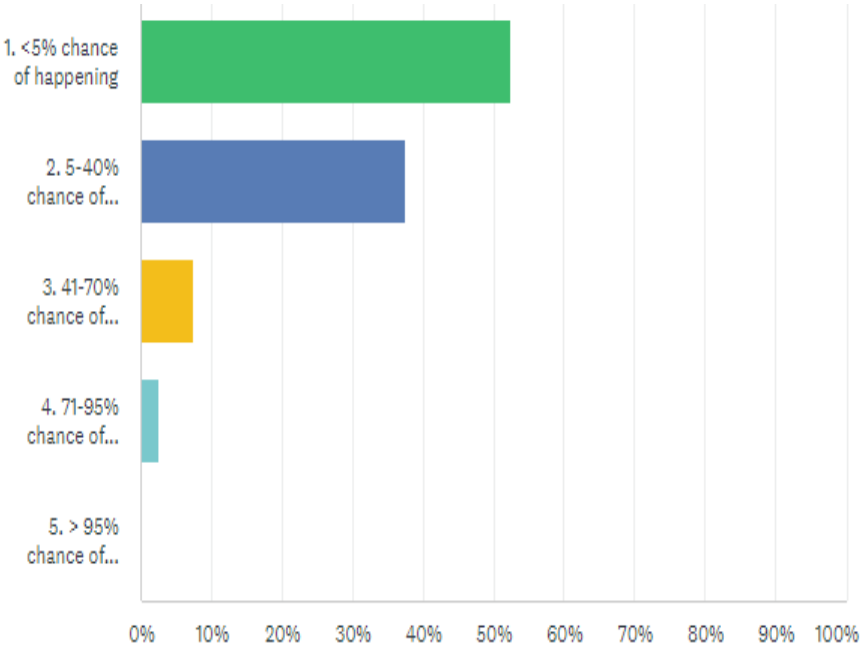
Discussion – Q11: Initial access – exploitation of remote services

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

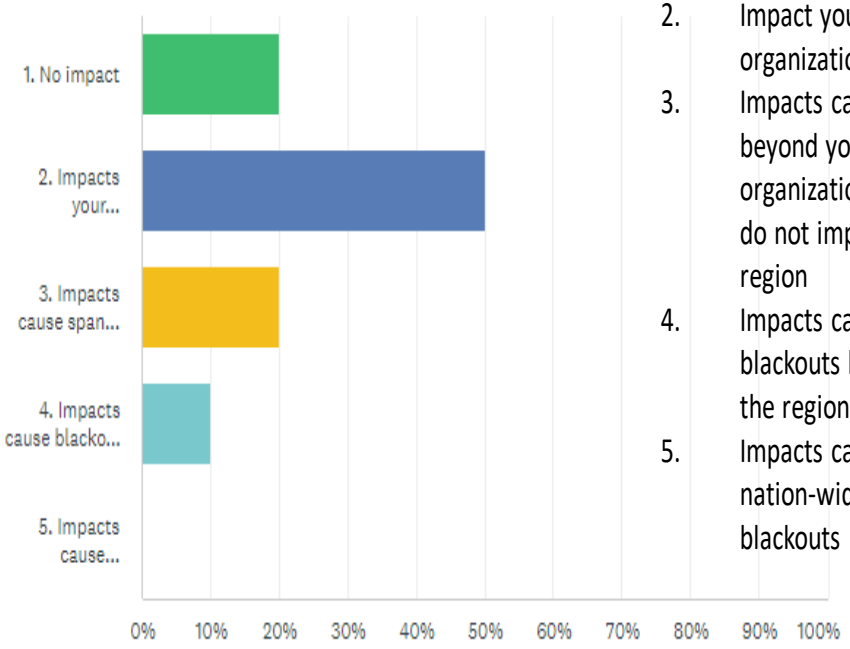


Comments:

- No remote access.

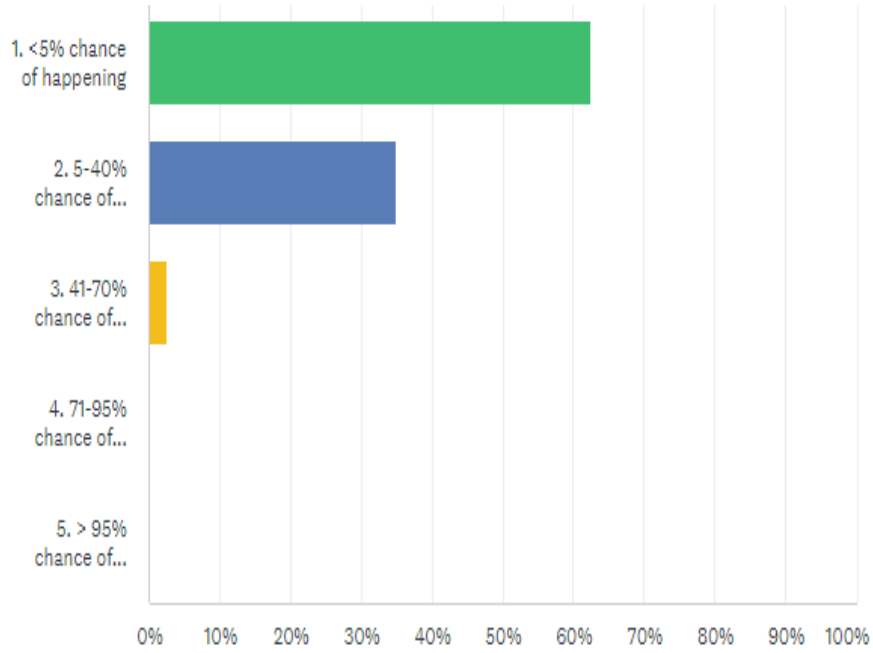
Discussion – Q12: Initial access – wireless compromise

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

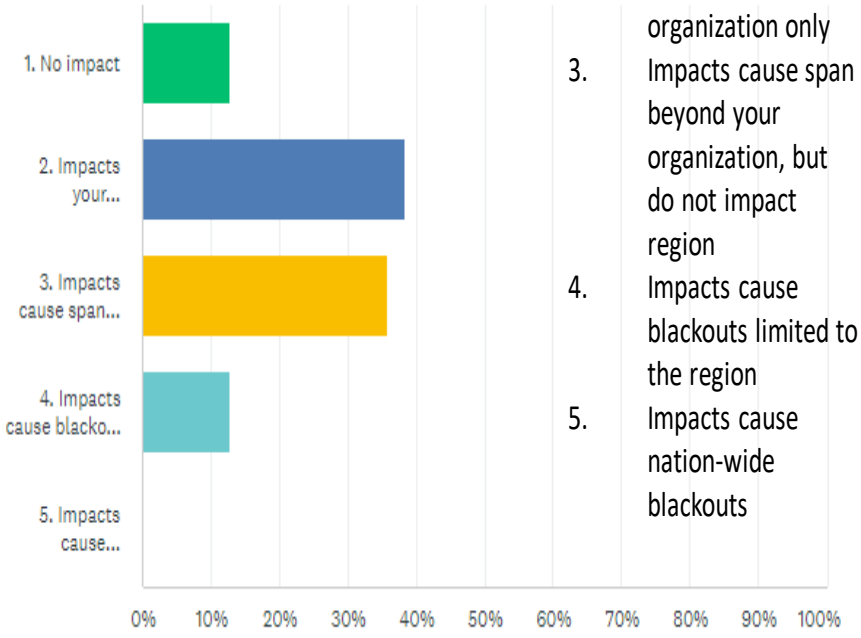


Comments:

- Not sure that this affects Grid/BES
- No wireless access
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

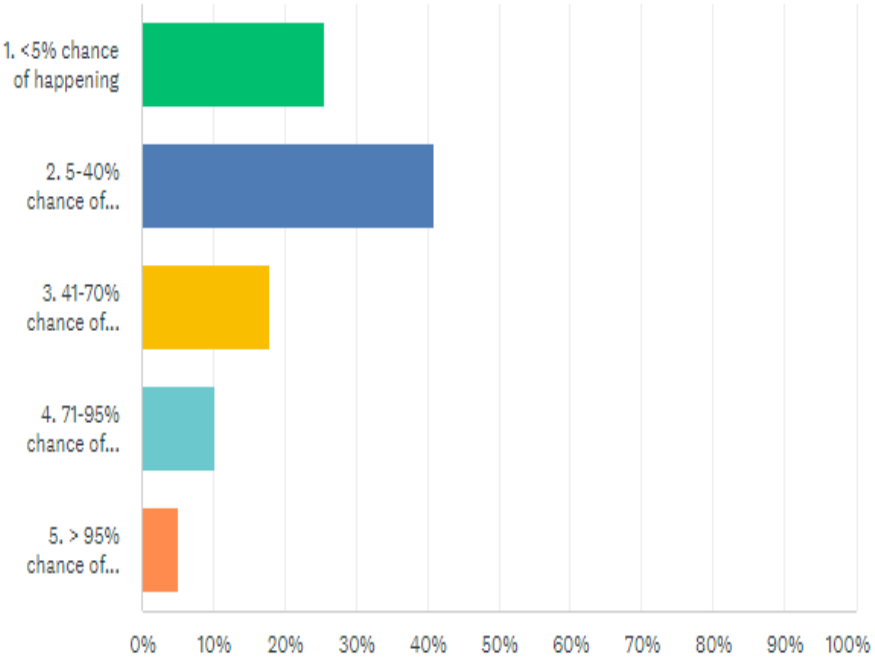
Discussion – Q13: Initial access – Phishing

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

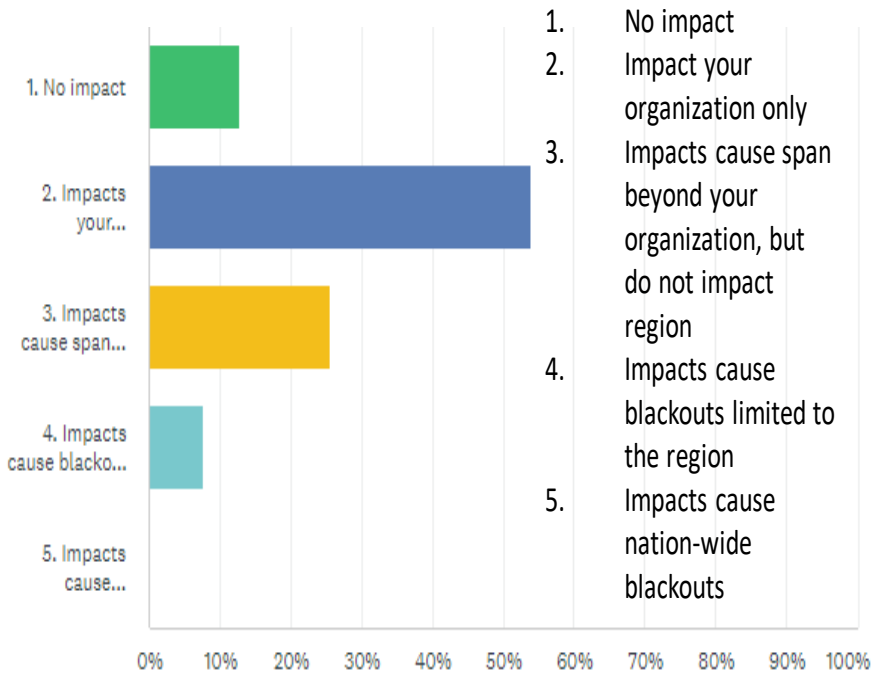


Comments:

- Email not connected to critical systems.
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

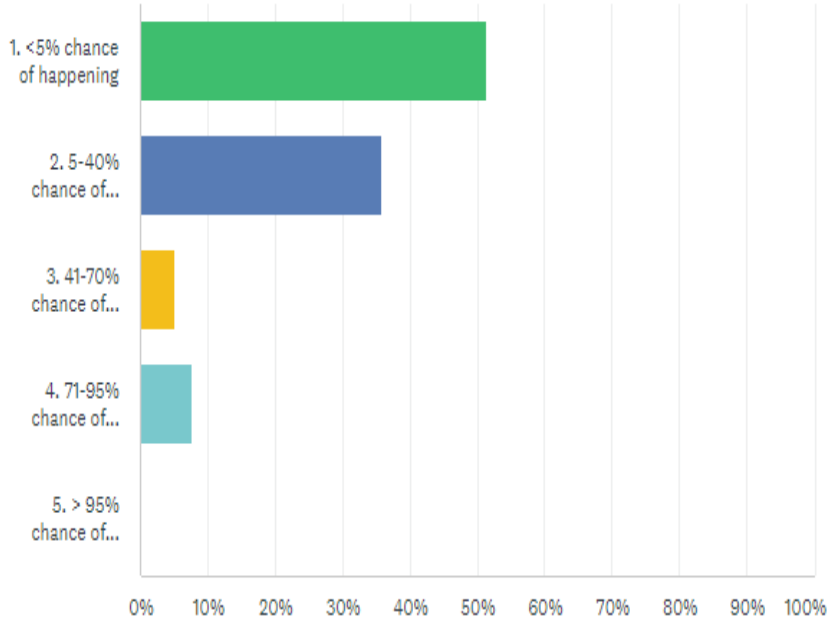
Discussion – Q14: Initial access - Drive-by-compromise

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

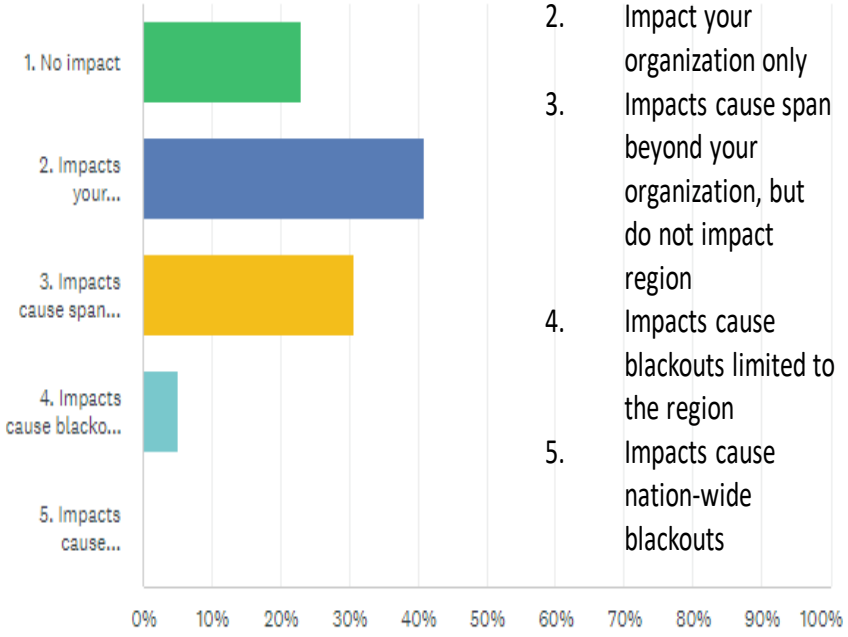


Comments:

- Not sure that this affects Grid/BES
- Not connected to web.
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

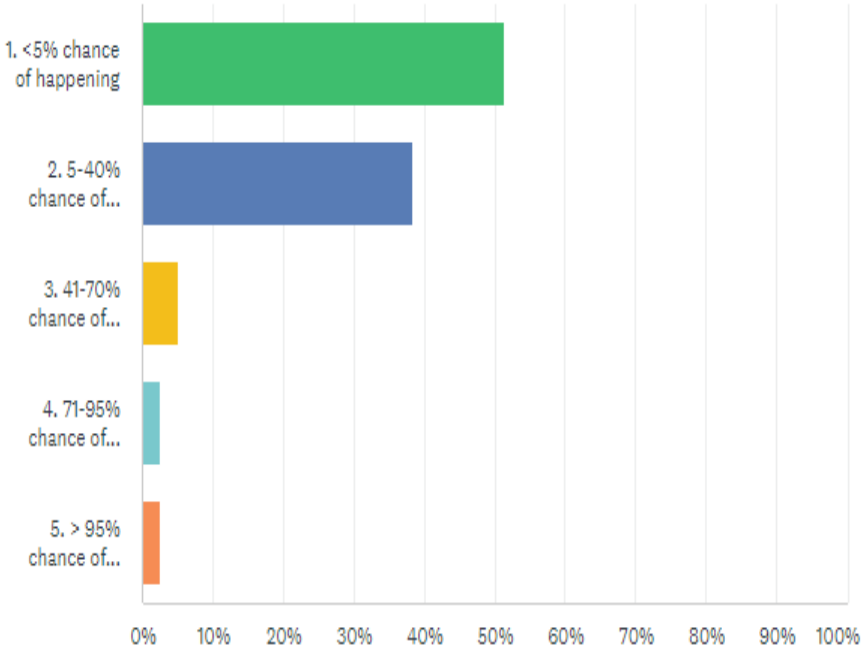
Discussion – Q15: Physical – Drones

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

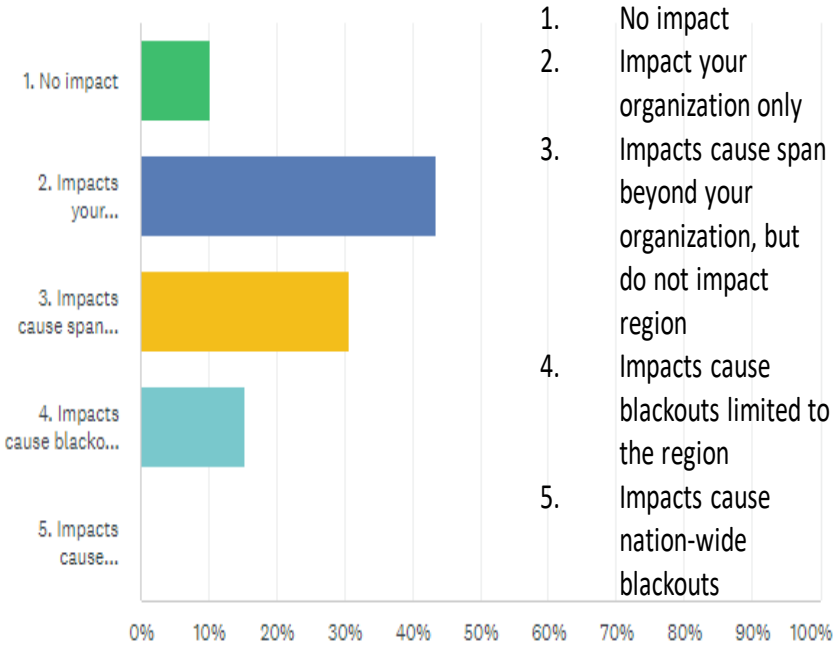


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

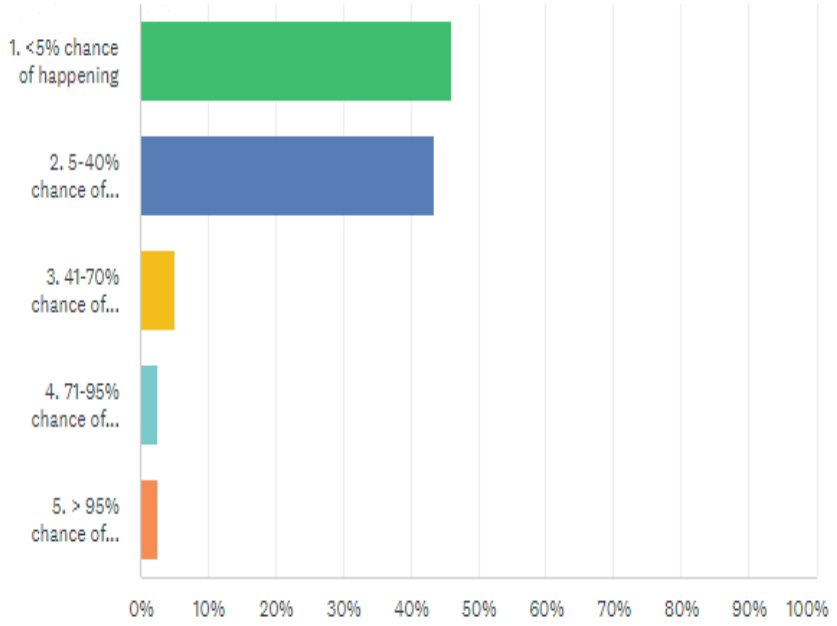
Discussion – Q16: Physical – Access controls (compromise to systems that would enable unauthorized access)

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

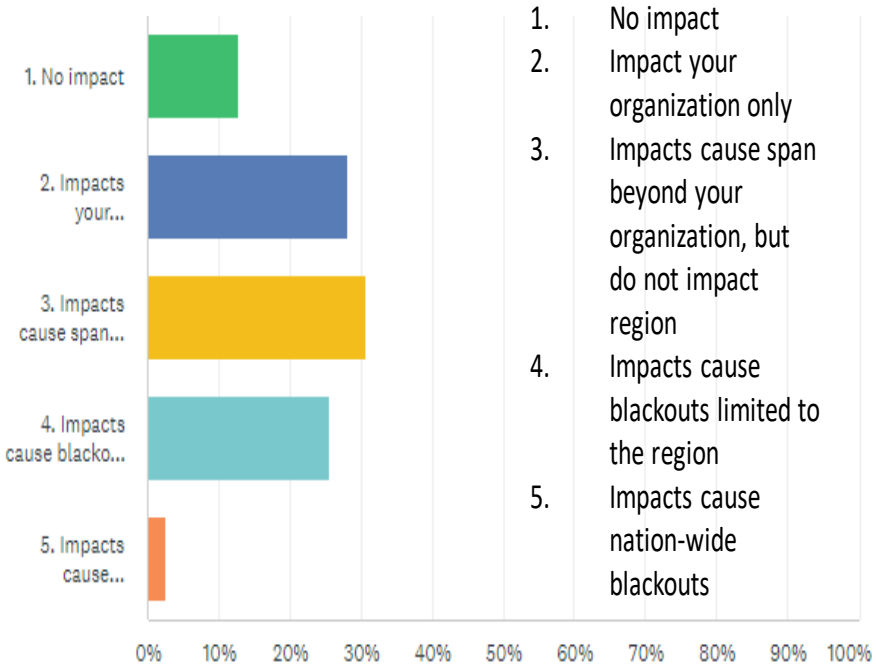


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

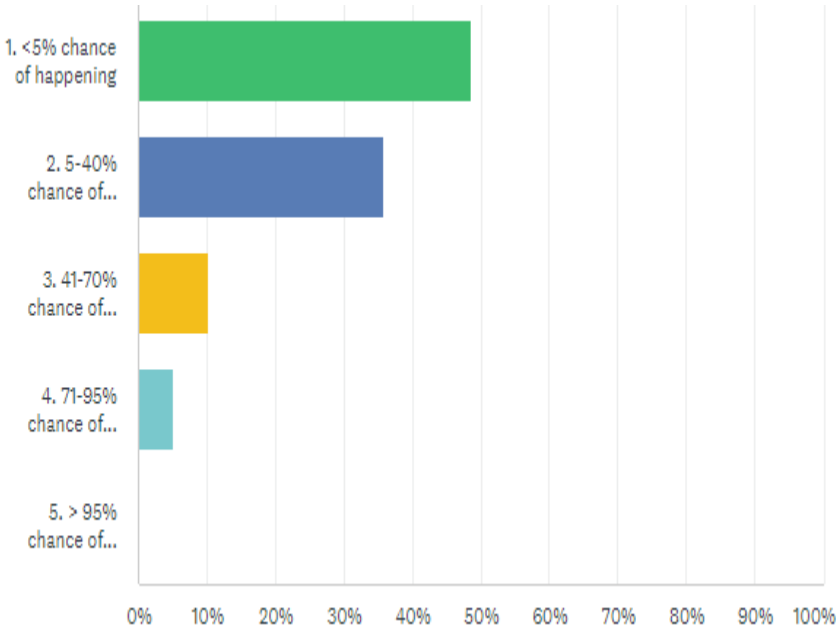
Discussion – Q17: Physical – Large equipment damage

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

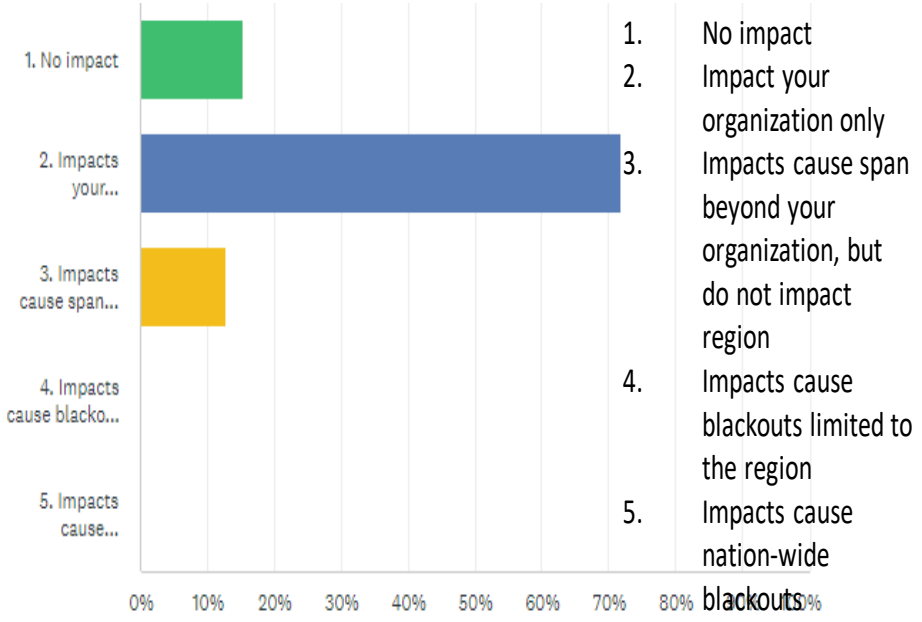


Comments:

- 0% as we own now such equipment
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

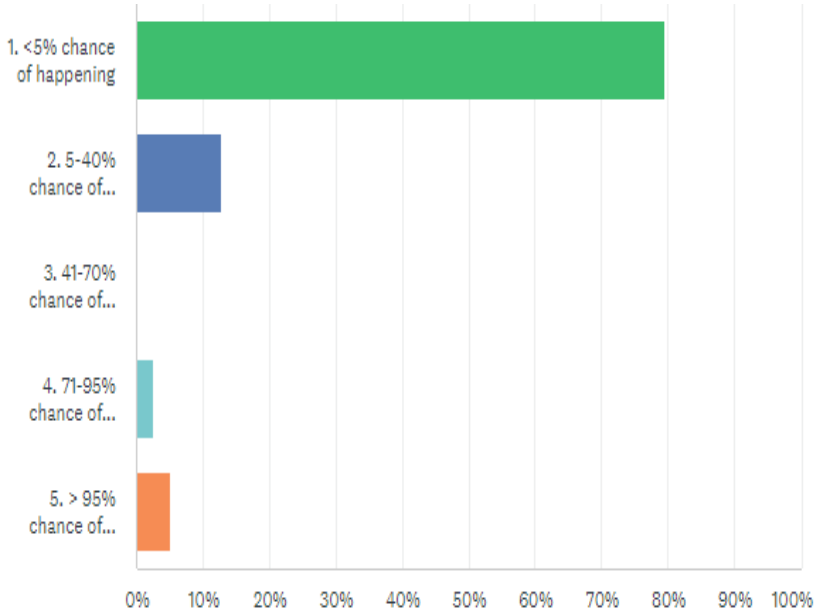
Discussion – Q18: Physical – blockades (Unable to physically access facilities)

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

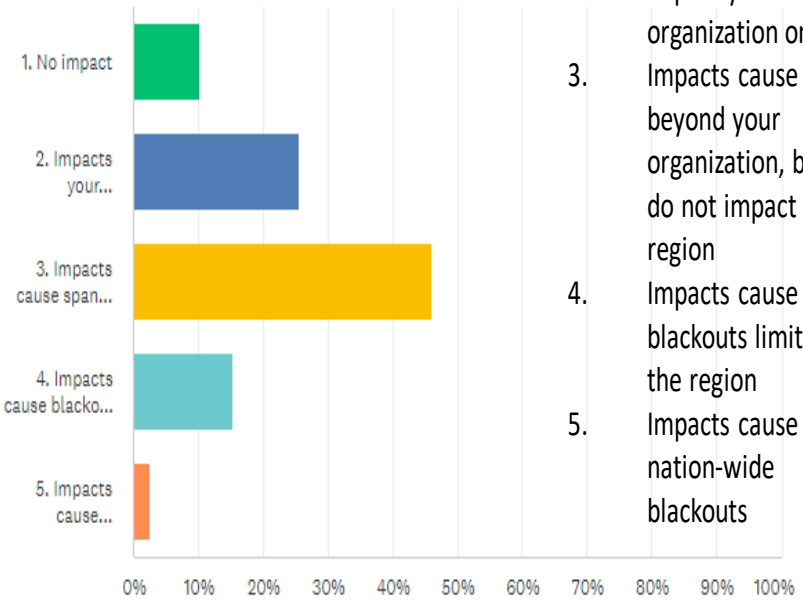


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

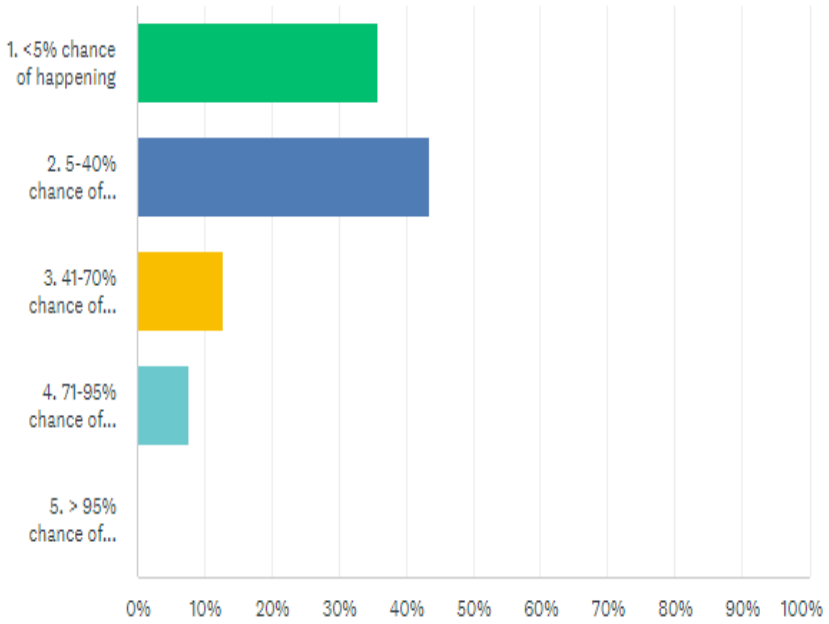
Discussion – Q19: Malware Attack

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

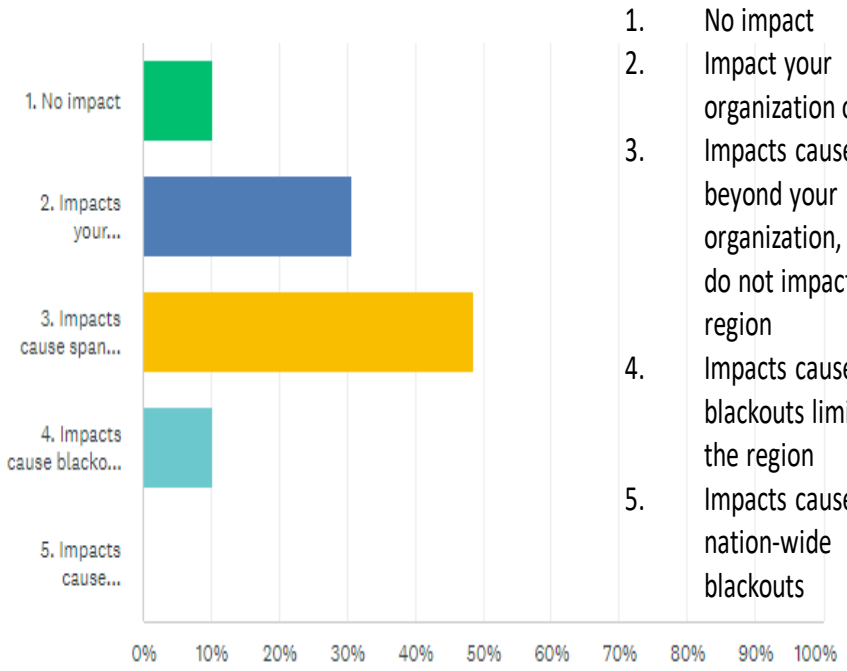


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

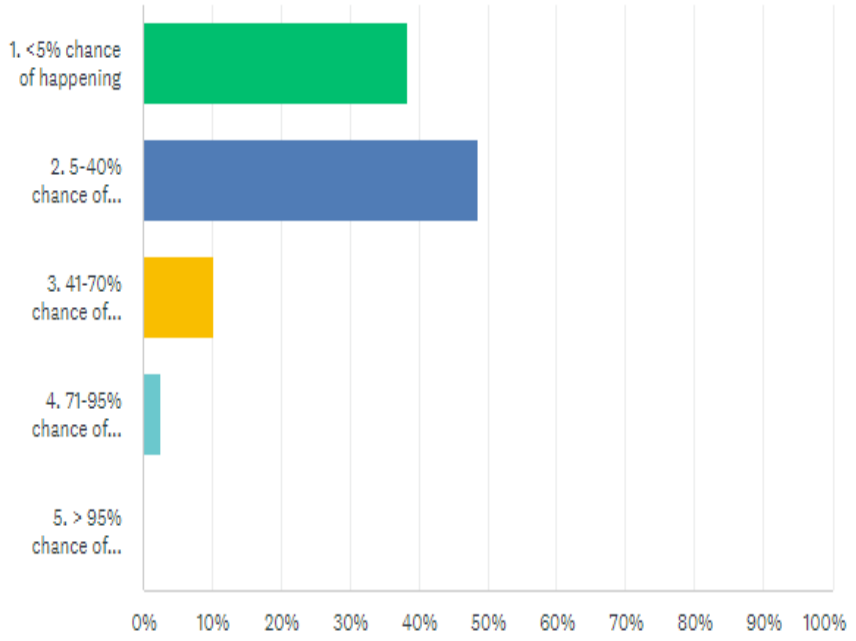
Discussion – Q20: Ransomware

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

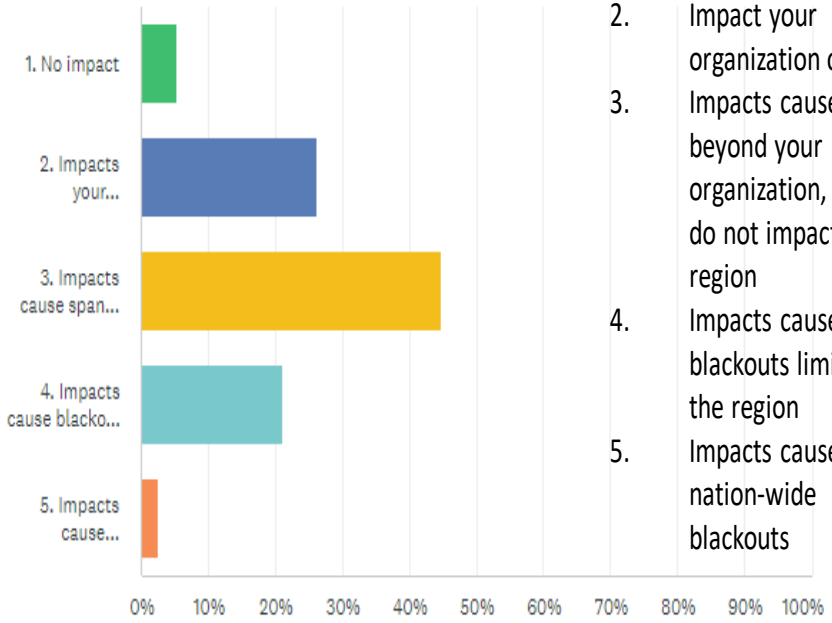


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

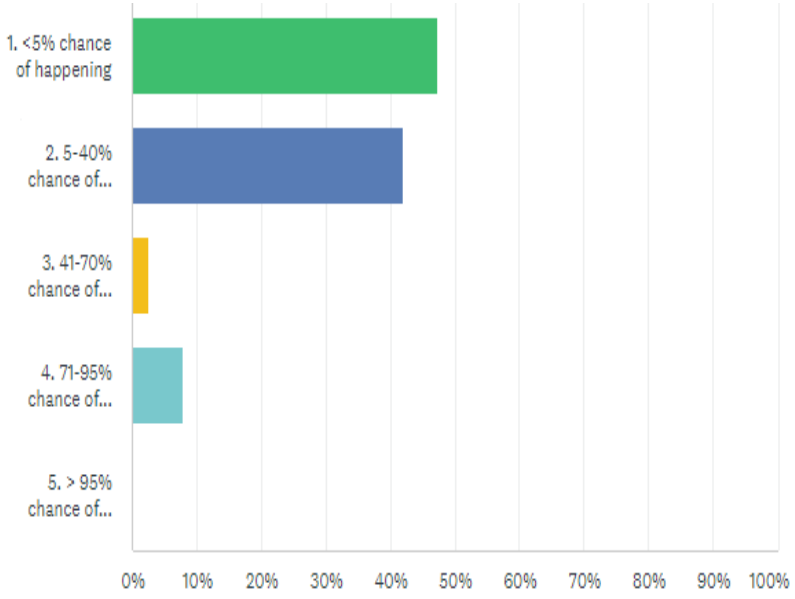
Discussion – Q21: Insider Threat

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood

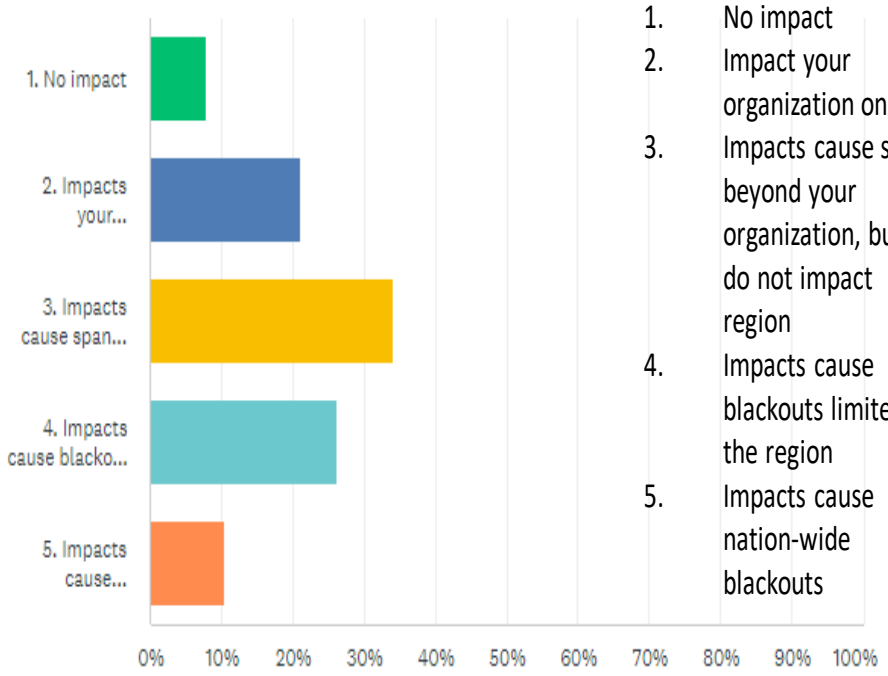


Comments:

- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

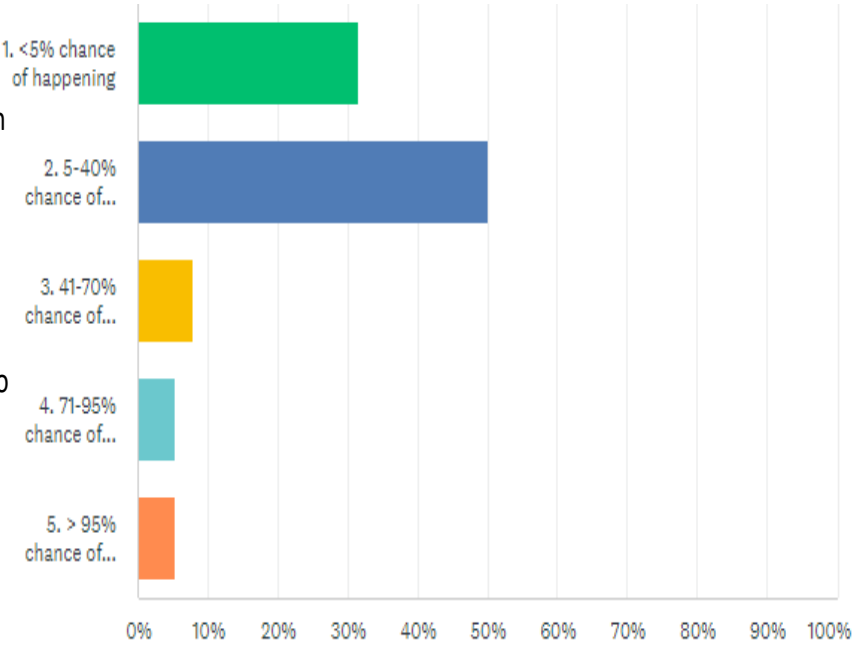
Discussion – Q22: Supply Chain Compromise

Consequences



1. No impact
2. Impact your organization only
3. Impacts cause span beyond your organization, but do not impact region
4. Impacts cause blackouts limited to the region
5. Impacts cause nation-wide blackouts

Likelihood



Comments:

- 5%
- No button for "Other" provided. Any of the above over next 5 years depending on posture of organization and industry.

Discussion – Q23: What keeps you up at night…

- Ransomware
- Cyber attack that compromises the DCS
- Nothing really keeps me up at night
- Ransomware and other implications of zero-day vulnerabilities
- Ransomware on the corporate IT network traveling to the control system networks. The corporate network is where email and internet access live. They are the two most likely attack pathways for us.
- Coordination between different sectors during a major incident.
- Employees
- Securing the human is continuously a challenge as 99% of the time actions taken that cause an event are not malicious nor intentional. Making sure our users are constantly choosing to Stop, Think, Observe, and Proceed (STOP) whether its considering a physical or cyber safety threat is something we continuously stress.
- Supply chain, insider

Discussion – Q23: What keeps you up at night…

- Drone-based attacks
- The volume of information and threats.
- Phishing, ransomware
- Supply chain risks and lack of complete visibility in OT areas.
- Lack of effective security due to industry churn both in cyber-security, standards, and transition to carbon free-neutral.
- For things we have control over I feel pretty confident in the overall security of our organization. I can patch quickly or institute a higher level of defense in reaction to threats or vulnerabilities, I can train my employees not to click, and I can buy best in class prevention, analysis and detection tools. Where I feel powerless is in supply chain vulnerabilities where "the intruder is already in the house". No CIP-013 plan or risk assessment would have stopped Solarwinds. What if it is Siemens or OSI next?
- Being Hacked
- Possible unknown malicious software on Cyber Assets, Physical Damage/Destruction at substations

Discussion – Q23: What keeps you up at night…

- Main threats - Cyberthreat, or manipulated personnel within. Physical - Sites are targets of opportunity. Offenders that do not understand the dangers of entering powered sites could cause short term mayhem to the power grid, *"My Company"* has sound protocols in place to divert power through other channels.
- No concerns. Our small system is not a target or would have any impact if indeed targeted.

Discussion – Q24: Additional threats that you would like to have assessed?

- Supply chain vulnerabilities
- We are considering a red team exercise in the next 18 months in order to gauge our defenses.
- No <*Note: There were a number of responses that said no – I have show just 1 to save some space)*
- Restructuring of industry without adequate security foresight - e.g. assets such as renewables controlled/montored via circuits over the internet.
- Increasing dependence on telco's is something we need to start talking about. Are utility communications networks as resilient as they could be? What would a combined cyber attack on utilities and their communications providers look like?
- Physical barriers

Discussion – Q25: Questions or suggestions regarding this survey or the online 2022 Risk Assessment meeting

- I thought the <5 being number one the number 2 going from 5 to 40 was to large of a jump.

AGENDA 12

Action Item Review

Rebecca Schneider, Reliability Analysis Administrator

Action

Discussion

Report

Rebecca Schneider will lead this discussion during the meeting.

AGENDA 13

Other Business and Adjourn
Clayton Whitacre, MRO SAC Chair

Action
Discussion

Report
Chair Clayton Whitacre will lead this discussion during the meeting.