Status Update:

Research Exploring Malware in Energy Delivery Systems
(REMEDYS)

DR. KERI PEARLSON
MIKE SAPIENZA

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Agenda

Status Report
• Orientation to REMEDYS
• Approach and Gap Analysis
• MIT’s Core Contributions to REMEDYS
  • Foundational Trust Modeling
  • Organizational Design Criteria
  • Evaluation Tool
  • Model Description for Stakeholder Engagement

Next Steps
• Transition
• Research Approach
• Tool for the EDS Ecosystem
First, let me set the stage...
Malware Attack on the Electricity Sector

• Extreme cold front descends on Northeast and Midwest United States, expected to last 3-4 days.
• Power goes out on day one. Over 100 million are left without heat.
• Nearly 200 utilities scramble to recover.
• Utilities identify malware as the culprit and initiate emergency response plans.

What Can the EDS Do to Prevent or Mitigate a Cyber Event?
Now Imagine...
EDS Cyber Event Response Organization

• Collaborative organization led by EDS stakeholders
• Reliable, possibly dedicated staff
• Collectively have the latest information and intelligence
• Ability to create and propagate a mitigation quickly
• Covers gaps between individual response plans
• Ability to coordinate EDS stakeholders response

REMEDYS: An Organizational Structure for Coordinated Cyber Event Response

REMEDYS's objective is to develop, evaluate, and refine organizational structures that could be used to coordinate the nation's multiple energy sector stakeholders in the rapid research, development, and distribution of mitigations to reduce the risk of an imminent or emerging cyber-attack that might otherwise disrupt energy delivery.

• Initiated by DoE in 2017
• Focused on electricity sub-sector but applicable to all EDS sub-sectors
• REMEDYS team included MIT, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory
The team created 5 candidate organizational structures to test with stakeholders

We are at a decision point about how to proceed

Today, we will summarize some of the work done to date and our proposal about next steps

**REMEDYS Approach**

- Evaluate current cyber threat landscape
- Profile EDS stakeholders and define potential roles in organization
- Analyze existing and forthcoming solutions to cyber threats in EDS ecosystem
- Explore sector-wide and other sector CIP best practices
- Identify relationships that can be leveraged to achieve sector-wide participation
- Define organizational requirements and test hypotheses
Gap Analysis Findings:

- No dominate model
- No centralized coordinating entity
- Opportunities for responses to get caught in the gaps between current solutions

Challenges in Current EDS Cyber Event Response

- **High Barriers to Establish Trust Among Stakeholders**
  - Cyber domain characterized by high barriers to trust between stakeholders
  - Difficult to determine sufficiency of measures and mitigations
  - High information saturation and relevancy unclear

- **Complicated Communication and Coordination**
  - Lack of well-defined approach to alerting and reporting
  - Difficulty communicating with vendors
  - Lack of coordination and prioritization of large-scale response efforts
  - Lag time between malware identification and mitigations

- **Limited In-House Expertise and Resources**
  - Limited in-house ability for utilities to identify malware vulnerabilities and attacks
  - Limited in-house ability to apply mitigations

- **Complex Regulatory and Legal Barriers**
  - Reporting could trigger regulatory punitive measures
  - Valuable information is classified
MIT’s Core Contributions to REMEDYS Organization Research

1. Created a trust model to inform organizational design
2. Used organizational design literature to study existing cyber resilience organizations
3. Developed criteria for designing REMEDYS organizational models
4. Developed tool to evaluate the models
5. Refined organization structure descriptions for stakeholder engagement

“The 4 Requirements of Trust”
Review of Trust Model Literature

<table>
<thead>
<tr>
<th>Requirements of Trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarity and agreement of objectives</td>
</tr>
<tr>
<td>Clarity about assignments and roles</td>
</tr>
<tr>
<td>Appropriate and clear safeguards</td>
</tr>
<tr>
<td>Appropriate confidentiality</td>
</tr>
</tbody>
</table>
Criteria for Organizational Design

- Incorporated organizational theory to establish baseline requirements for effective REMEDYS organization
- Integrated fundamental organizational theory concepts from literature on structural options and building blocks (criteria)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Definition</th>
<th>Organizations of Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chain of Command</td>
<td>Lines of authority for decision making, reporting and information flow</td>
<td>Who reports to whom between entities and how information will flow</td>
</tr>
<tr>
<td>Span of Control</td>
<td>Number of subordinates a superior can effectively manage</td>
<td>Number of entities 'reporting into' each other</td>
</tr>
<tr>
<td>Decision Authority</td>
<td>Decision making process or authority</td>
<td>Where decisions are made in the structure (centralized, decentralized)</td>
</tr>
<tr>
<td>Specialization</td>
<td>Division of labor or how activities in an organization are broken down and divided between entities</td>
<td>How activities are broken down between entities defining the work each will do</td>
</tr>
<tr>
<td>Departmentalization</td>
<td>Grouping activities in order to coordinate common activities</td>
<td>Groups of entities to coordinate common activities to be done</td>
</tr>
<tr>
<td>Formalization</td>
<td>Amount of rules, procedures and other mechanisms that govern how activities are done</td>
<td>Rules, procedures and other mechanisms that govern how entities work together</td>
</tr>
<tr>
<td>Culture</td>
<td>The unwritten rules of the organization</td>
<td>The unwritten rules necessary for the entities to work together (Trust, etc)</td>
</tr>
</tbody>
</table>

Studied Existing Cyber Resilience Organizations

- No organization is dedicated to coordinating EDS ecosystem malware response
- More criteria required to design REMEDYS organizational structures

**Existing Organization**

- ISA Security Compliance Institute (ISCI)
- Center for Ultra-Wide-Area Resilient Electric Energy Transmission Networks (UT CURENT)
- Edison Electric Institute Cyber Mutual Assistance (EEI CMA)
- US Nuclear Energy Community
- SPAREConnect
- Advanced Cyber Security Center (ASCS)
- Financial Systemic Analysis and Resilience Center (FSARC)
- Electricity Information Sharing and Analysis Center (EISAC)
- Wireless Industrial Networking Alliance (WINA)
## Refined Criteria for Designing/Describing REMEDYS Organization Models (14 Criteria)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Definition/explanation</th>
<th>Evaluation Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Overall goal of the organization. High level objective that all participants can agree on.</td>
<td>How well will this structure support the goal of REMEDYS to create and propagate mitigation? How well will this structure ensure that all participants are aligned and agree to this objective?</td>
</tr>
<tr>
<td>Members</td>
<td>Participating organizations, companies and/or groups. Characterization of the participants or groups of participants.</td>
<td>Membership Participating organizations, companies and/or groups. Characterization of the participants or groups of participants.</td>
</tr>
<tr>
<td>Structure</td>
<td>The formal reporting relationships of the organization such as committees, leadership positions, etc. Often depicted as an org chart.</td>
<td>Governance The activities, decisions, and control systems that support the organization and enable it to work.</td>
</tr>
<tr>
<td>Decision Processes</td>
<td>Steps and entities involved in making a decision.</td>
<td>How well does this structure identify critical assets? How well will this structure identify key risks to its ability to be successful? How well will this structure provision for protection from these risks?</td>
</tr>
<tr>
<td>Operational Processes</td>
<td>The day-to-day work to be done and how it’s done (steps necessary for the work to get done)</td>
<td>How well does this structure ensure that appropriate constitutes are participating?</td>
</tr>
<tr>
<td>Roles &amp; Responsibilities</td>
<td>Key roles for each of the entities in the organization</td>
<td>Organizational Structure The formal reporting relationships of the organization such as committees, leadership positions, etc. Often depicted as an org chart.</td>
</tr>
<tr>
<td>Basis of Trust</td>
<td>Activities/ org components specifically designed to provide a foundation for sharing and working together (objectives alignment, activities expectations, clear safeguards, appropriate confidentiality)</td>
<td>How well defined are the structure, reporting relationships and lines of communication in this model?</td>
</tr>
<tr>
<td>Key areas for Legal Arrangements</td>
<td>Areas necessary to include in the participation agreement to protect participants and provide guidance on actions and activities.</td>
<td></td>
</tr>
</tbody>
</table>
Develop 5 Candidate Models

- ORNL and PNNL developed and refined hypothetical models to:
  - Malware Coordinating Council (MCC)
  - Dedicated Malware Task Team (DMTT)
  - CMA Malware Subcommittee (CMS)
  - Volunteer Malware Task Team (VMTT)
  - Malware Mitigation Society (MMS)

Key Differentiating Attributes

Of 14 descriptive criteria, 5 criteria are the key ways to describe the differences in the candidate models.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Candidate 1</th>
<th>Candidate 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create New</td>
<td>Governance of Organization</td>
<td>Use Existing Org. Governance</td>
</tr>
<tr>
<td>Decentralized</td>
<td>Decision Making Authority</td>
<td>Centralized</td>
</tr>
<tr>
<td>Volunteers</td>
<td>Resource Availability</td>
<td>Dedicated, Resourced Team</td>
</tr>
<tr>
<td>Affected Entity Plus Vendor</td>
<td>Development of Malware Mitigation</td>
<td>Affected Entity Plus Vendor &amp; Others</td>
</tr>
<tr>
<td>Decentralized</td>
<td>Information Sharing and Flow</td>
<td>Centralized</td>
</tr>
</tbody>
</table>
Sample Key Attribute: Decision Making Authority

- **Continuum** – Captures where decision making authority lies
- **Centralized** – Authority lies in a single entity, often a board and/or a executive, which directs the organization. Participating entities are represented through delegates on the board or by choosing the executive
- **Decentralized** – Models are characterized by a high degree of voluntary participation. Decisions may require consensus of the entire organization or only affected members have decision authority

Candidate Model Summary Slide Example 1

**Dedicated Malware Task Team (DMTT)**

- **Distinguishing Characteristics**
  - Dedicated center with formal relationships across electric and other sectors.
  - Established coordination with government entities, i.e. DoD, FBI, and DHS
  - Structure emphasizes collaboration across industry and private sector boundaries to perform better analysis and malware mitigation

- **Description**
  - Address malware mitigation under multi-sector organization.
  - Fully staffed and funded
  - Analyses are used to pre-emptively develop malware mitigations when possible and ensure resources, playbooks, and critical processes are disseminated to members
  - Dedicated response teams rapidly respond to malware infections of its energy sector stakeholders and when asked by other industries for the purpose of mutual defense

- **Governance of Organization**
  - Create New
  - Use Existing Org Governance

- **Decision Making Authority**
  - Decentralized
  - Centralized

- **Resource Availability**
  - Volunteers
  - Dedicated, Resourced Team

- **Development of Malware Mitigation**
  - Affected Entity
  - Affected Entity Plus Vendor
  - Affected Entity Plus Vendor & Others

- **Information Sharing / Flow**
  - Decentralized
  - Centralized

https://veritusgroup.com
Today: 5 Candidate Organization Structures

Transition

- Leadership changed in research arm of DoE
- REMEDYS moved off the list of currently funded projects
- Originally identified problem has not gone away
- Still have gaps sector-wide malware mitigation response
Next Steps – Research Approach

Proposed revised project objective
- Not continue with REMEDYS as previously laid out
- New objective: Identify the optimal mechanism to coordinate a sector-wide response to a malware attack

Stakeholder outreach and engagement
- Coordination directly with E-ISAC, CREDC members, and other stakeholders

Leverage expertise at MIT
- Trust modeling
- Governance theory
- Economic game theory

Next Steps:
Tool for the EDS Ecosystem

1. Helps highlight the gap in sector-wide malware response
2. Builds consensus on how to close the gaps
3. Lays the foundation for a mechanism to rapidly respond to malware attack on the EDS ecosystem
Questions?

Mike Sapienza
• Research Assistant
• (504) 220-8465
• msapienz@mit.edu

Dr. Keri Pearlson
• Executive Director
• (512) 694-7768
• kerip@mit.edu

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.