Review of MT-ISAC

- First Official Meeting August 2015
- Policy Approved
  - Information Security Policy
    - Appendix A, B, C and D
  - Rescinded 28 Enterprise Security Policies
  - Data Classification Policy
- Standards Approved
  - 7 Enterprise Standards
  - 3 Forms
  - 3 Guidelines
  - NCSR for compliance
- Mission and Goals and Objectives approved Sept 2015

Workgroups of MT-ISAC

- Started with 10 Different workgroups
  - 1. Best Practices
  - 2. Assessment
  - 3. Tools
  - 4. Awareness & Training
  - 5. Resources
  - 6. Situational Awareness
  - 7. Outreach
  - 8. Public Safety
  - 9. Fostering Future Security Professionals
  - 10. Legislative
- 2 Regular meeting workgroups
  - Best Practices
  - Situational Awareness

Topics Discussed at MT-ISAC

- DLP
- Cyber Security Awareness Month
- Fraud and Identity Theft – DOR Task Force
- Data Classification
- MT-ISAC Communications – SharePoint, Website, MOM
- Phishing
- Security Conferences and Summits (IT Conference, TechJunction)
- University Security Incidents
- Antivirus
- OneDrive
- MT Drive
- EMET
- Various Cybersecurity Training (Professional and End User)
- Cyber Security Insurance
- Tabletop exercises
- 20 plus various Current Threats –Sean Rivera
- Several Day/Time ISAC meeting changes
- Several special guest speakers from MS-ISAC, NW Energy, DHS, RMTD, Governor

37 Total Goals and Objectives

Assessment

MT-ISAC Goals and Objectives

1.2 Develop and implement a statewide standardized information security program **assessment** and measures for Departments and the State

1.2.1 Provide a yearly State information security assessment to the Governor showing program successes and a plan to address shortcomings

1.2.2 Develop a Governor's information security dashboard

Awareness & Training

MT-ISAC Goals and Objectives

2.1 Implement a comprehensive information security awareness and training program

2.1.1 For managers, users, contracted support, and IT staff

2.1.2 Develop a campaign to deliver the message of information security in a positive and informational manner that engages the listener and encourages them to integrate information security into their daily activities

2.9.0 Provide information on best practices for information security **insurance**, recommendations, (training) options, awareness, coverage, cost, and other considerations

Best Practices

MT-ISAC Goals and Objectives

1.1 Update State of Montana information security policies and documents to align with the **NIST** Cybersecurity Framework

1.2 Implement a statewide standardized system risk management template (measures, authority to operate, etc) based on best practices

2.3 Collaborate with other States and organizations and utilize/leverage industry **best practices**.

2.3.1 Evaluate national best practices and training of the cyber units of the National Guard and apply similar practices in Montana where applicable (DOA, DOJ, National Guard, etc.).

2.4 Develop and implement process(es) for comprehensive patch management

2.5 Develop limited user rights strategy for state information systems.

2.8 Recommend security requirements for solicitation of and inclusion in state **contracts** involving information technology. Address breach language in contracts.

Fostering Future Security Professionals

MT-ISAC Goals and Objectives

1.7 Encourage development of a trained and educated information security workforce in Montana through the **University** System with private sector input.

1.8 Assess an **apprenticeship** or internship program to develop hands-on information security skills

MT-ISAC Goals and Objectives

Legislative

1.5 Recommend new **legislation** or update current statutes, administrative and criminal, to address the present-day information security environment

Outreach

MT-ISAC Goals and Objectives

1.4 Share risk management guidance and recommendations with local governments and the private sector

1.9 Identify **key players** within industry sectors and provide a forum for developing guidance and communicating with industry sectors

1.10 Collaborate with private industry to understand the information security posture of **critical infrastructure**

2.1.3 Support and participate in statewide information security groups and help to facilitate and leverage the existing communications channels

Public Safety

MT-ISAC Goals and Objectives

4.2 Enhance State information security **law enforcement** capability

4.2.1 Improve the State of Montana's investigative expertise in the information security area

4.2.2 Explore additional resources in DOJ/DCI for Network Cyber Investigations

4.2.3 Research and recommend criminal investigative response in coordination with HSA, DOA, DOJ, and FBI

4.2.4 Develop a plan to increase the education of Montana's law enforcement group regarding information security

Resources

MT-ISAC Goals and Objectives

1.6 Recommend **resources** (funding, people, etc.) and methods, such as Security Assistance Teams (SAT), to assist agencies in performing work in order to enhance the agency, and thereby the State, information security posture

2.6 Identify **legacy systems** which exist on the State of Montana network and create a plan for securing or removing those systems

2.11 Identify location of **sensitive data** and methods to protect it

Situational Awareness

MT-ISAC Goals and Objectives

2.2 Enhance **situational awareness**

2.2.1 Document standing threat/vulnerability needs/sources and determine fast, efficient, and secure sharing methods

2.2.2 Foster better communication in information security between federal, state, local, and tribal governments

Tools

MT-ISAC Goals and Objectives

2.7 Recommend software, hardware, services, processes, and resources to increase **protection capabilities**

2.10 Recommend methods and/or tools to inventory authorized and/or **unauthorized software**

3.1 Recommend software, hardware, services, processes, resources, etc. to increase **detection capabilities**

4.1 Recommend software, hardware, services, processes, and resources to enhance agency and State **incident response** - tools, procedures, checklists, lessons learned, and guidelines

5.1 Recommend software, hardware, services, processes, and resources to enhance agency and State system **recovery** - tools, procedures, checklists, lessons learned, and guidelines

Review of MT-ISAC

Questions?

Comments?

Recommendations?