

Montana State Information Security Advisory Council (MT-ISAC)

Minutes

April 12, 2017

1:00 PM

Cogswell Building, Room 151

Members Present:

Lynne Pizzini, CISO – Chair

Erika Billiet, City of Kalispell

Joe Chapman, Justice

Jesse Callender, Montana Analysis Technical
Information Center/Justice

General Brian Fox, Military Affairs – Alternate

Adrian Irish, University of Montana

Margaret Kauska, Revenue

Manuel Soto, Office of Public Instruction

Staff Present:

Joe Frohlich, Wendy Jackson, Sarah Mitchell

Guests Present: Dawn Temple, Lance Wetzel, Tom Murphy, Sean Rivera, Carroll Benjamin, Craig Stewart, Craig Marquardt, Dave Johnson

☞ **Real-time Communication:** Darren Mclean, Madison Iler, Rawlin Richardson, Channah Wells, Brian Jacobson, Maura Gruber, John Cross, Clynis Gibson, Bert Quick, Erin Stroop, Daniel Nelson, Cheryl Pesta, Brad Flath, Michael Barbere, Jerry Marks, Christi Mock, Tim Kosena, Edwina Morrison, Ed Silvis

Welcome

Lynne Pizzini welcomed the council to the April 12, 2017 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes

Motion: General Bryan Fox made a motion to approve the March 8, 2017 minutes. Margaret Kauska seconded the motion. Motion passed.

Business

Legislative Session

Ms. Pizzini provided a brief update regarding legislative session. The bill Representative Zolnikov presented to provide funding for cyber security was tabled in committee. Representative Zolnikov proposed an amendment to House Bill 2 that would disallow service providers from selling or sharing an individual's information.

MT-ISAC Council Members for Next Biennium

Mr. Frohlich stated individuals interested in participating in the MT-ISAC council should contact him at JFrohlich@mt.gov. Mr. Frohlich will submit a list of participants to the Governor's Office for approval.

Department of Homeland Security (DHS) Cyber Security Evaluations

Mr. Frohlich reviewed the free cyber security evaluations offered by the Department of Homeland Security (DHS). A complete list of the evaluations is included within the MT-ISAC Topics of Discussion located at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>.

The Cyber Resilience Review (CRR) is a one-day, onsite assessment that includes a pre-meeting call to prepare for the event. CRR implementation is scheduled to take place the week of August 7, 2017. Mr. Frohlich requested that CRR participants contact him to select their preferred day of review. At this time, the CRR is full. Mr. Frohlich noted openings are available for the Cyber Infrastructure Survey (C-IST). The C-IST entails a half day, onsite evaluation. C-IST differs from CRR in that participants will not receive a report. Participants can access a website that contains information similar to the report provided by CRR. C-IST is scheduled to take place the week before or after the August 7, 2017 CRR evaluations.

Cyber Hygiene (CH) entails penetration testing for public facing websites. CH is open to all agencies, including those participating in the CRR and C-IST evaluations. CH evaluations can be scheduled two weeks in advance.

Please contact Mr. Frohlich JFrohlich@mt.gov if your agency is interested in participating in these evaluations.

Data Loss Prevention (DLP)

Dave Johnson spoke to the council regarding the DLP process. In order to add individuals to review DLP reports, agencies will need to create a group within the system. Mr. Frohlich stated the purpose of DLP reports is to provide information regarding the source of DLP violations. This report will identify individuals who would benefit from receiving additional training with regards to securely sending sensitive information. As of April 10, 2017, 40 non-IT users outside of the Department of Administration (DOA) have participated in live DLP testing. Mr. Frohlich noted additional DLP testers within bureaus and agencies are needed. Mr. Frohlich shared DLP's testing is reviewed frequently to determine the feasibility of a July 1, 2017 launch date. Mr. Frohlich stated DOA is ready to implement DLP. Joe Chapman commented that, with the legislative session, the Department of Justice's (DOJ) ability to participate in live testing is limited. Mr. Chapman suggested the option of postponing the July 1, 2017 launch date to allow agencies more time to assign DLP testers.

Q: Ms. Krause: Can DLP be activated by each agency?

A: Ms. Pizzini: No.

Q: Dawn Temple: What is meant by "no changes for 6 months"?

A: Mr. Frohlich: "No changes for 6 months" refers to configuration changes. Confidence levels are adjusted as problems occur.

Ms. Temple noted that DOJ feedback from DLP testers has generated several questions and concerns. Ms. Temple proposed SITSD review the Add-In available for Windows 7.

Mr. Frohlich recommended that agencies with questions or concerns regarding DLP should submit a detailed list to Mr. Johnson Dave.Johnson@mt.gov or Mr. Frohlich JFrohlich@mt.gov.

Mr. Frohlich stated that agencies currently testing DLP will need to perform live tests regarding any forms utilized by staff or placed on their public site.

Mr. Frohlich reviewed the DLP's policy website located at <https://sitsd.mt.gov/Information-Security/Policy/DLP-Policy>. The website's purpose is to educate users regarding protecting sensitive information and preventing inadvertent disclosure of privileged information. Please contact Mr. Johnson Dave.Johnson@mt.gov or Mr. Frohlich JFrohlich@mt.gov with any suggestions regarding the information provided on the website.

Mr. Chapman recommended scheduling bi-weekly meetings for agencies to offer feedback regarding DLP.

Q: Mr. Frohlich: Can this be addressed during the Network Managers Group (NMG) meetings?

A: Mr. Chapman: Yes.

Action Item: Mr. Frohlich will add DLP Discussion as a standing agenda item for the weekly NMG meetings.

Workgroup Updates

Best Practices / Tools Workgroup Update

Ms. Pizzini noted the workgroup did not receive additional comments regarding the Acceptable Use - Rules of Behavior document located at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>. Ms. Pizzini stated that the Best Practices forms may be modified by agencies.

Motion: Ms. Kauska made a motion to approve the Acceptable Use – Rules of Behavior document as a Best Practice. Manuel Soto seconded the motion. Motion passed.

Ms. Pizzini noted that modifications to Appendix A of the Information Security Policy were proposed to achieve Best Practice standards. Mr. Frohlich discussed the changes to Appendix A, which can be found at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>. Mr. Frohlich reviewed that, per Internal Revenue Service (IRS) Publication 1075 requirements, an added change to Appendix A Section 5 will include a minimum age of 24 hours for a password. Mr. Frohlich shared an additional modification to Appendix A which will require passwords for elevated/privilege/administrative/su accounts to be 15 characters long and contain both lower and upper case letters and numbers. Mr. Frohlich also commented, per IRS Publication 1075, a final change to Appendix A will reduce the mandatory eight hour lock out period to a 15-minute lock out period.

after 6 unsuccessful login attempts.

Ms. Pizzini presented the changes to Appendix A to the committee for approval. Ms. Kauska commented that the Appendix should note these changes are IRS Publication 1075 requirements.

Motion: Ms. Kauska moved to accept changes to Appendix A. Mr. Chapman seconded the motion. Motion passed.

Mr. Frohlich reviewed the Identification and Authentication Best Practices document located at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>. This document educates users regarding how information is authenticated to the network. Mr. Soto suggested that a recommended frequency for resetting service accounts be added to this policy. Mr. Johnson stated current process requires resetting service accounts when staff changes occur.

Action Item: Mr. Frohlich will revise the Identification and Authentication Best Practices document to include the requirement of resetting service accounts when staff change occurs.

Motion: Mr. Soto moved to approve the Identification and Authentication Best Practices document with the proposed revision. General Fox seconded the motion. Motion passed.

Mr. Frohlich stated the Best Practices workgroup has selected SentinelOne as the chosen Antivirus (AV) augmentation for the state. Documentation for Proof of Concept (POC) has been signed. SentinelOne will be onsite to perform the POC within the next three weeks. Mr. Frohlich noted that the proposal to SentinelOne includes one console. Each agency will receive five licenses to install on workstations to enable product review. Ms. Pizzini mentioned, once POC is completed, a contract will be negotiated. With the completion of negotiations, agencies will have the capability to purchase the AV augmentation tool. Ms. Pizzini thanked the Best Practices team for their support and dedication to this project.

Situational Awareness / Outreach / Public Safety Workgroup Update

General Fox provided a brief update regarding the Situational Awareness/Outreach/Public Safety workgroup. Informational letters have been generated regarding the public education program. A link to the website was included in the letter. The workgroup will review proposed website content at their next meeting on April 26, 2017.

Current Threats

Sean Rivera gave a presentation regarding Current Threats. Due to the Freedom Hosting II hack performed by Anonymous in February 2017, the number of Dark Web services has decreased from 30,000 services in 2016 to 4,400 services in 2017. Mr. Rivera stated current phishing attacks involving air travel themed campaigns have experienced a 95% success rate. The current theme uses a variety of techniques to capture sensitive data from individuals and deploy Malware with attachments that are sent through e-mail. Mr. Rivera noted other forms of phishing attacks currently circulating contain tax themes.

Mr. Rivera shared information regarding the vulnerability residing in a WiFi chipset manufactured by Broadcom. Mr. Rivera noted a researcher at Google Project Zero compromised a phone by WiFi proximity alone without requiring user interaction. There is an Apple patch available to address this vulnerability. This vulnerability will not be addressed for Android devices until another update is available. Mr. Rivera mentioned that Microsoft released a patch on April 11, 2017 to resolve a zero-day vulnerability that compromises users' computers using the Dridex banking Trojan. Mr. Rivera shared this vulnerability was exploited by a massive campaign used by attackers on April 10, 2017 in Australia.

Mr. Rivera stated April, 2017 is the last month for Win Vista to receive updates. Due to Microsoft's changed approach to deploying security updates and patching, SITSD will no longer be providing a breakout of Microsoft Knowledge Base (KB) articles. The revised report will contain a table instructing clients to patch within 24 hours and servers to patch as soon as possible. Changes with the presentation of Microsoft Notifications may occur as needed. Please send any suggestions or comments regarding the presentation of Microsoft notifications to Mr. Rivera at SRivera@mt.gov.

Open Forum

None

Future Agenda Items

Mr. Frohlich stated that, per Kreh Germaine's request, a panel will meet in the May 10, 2017 to discuss SITSD's process with handling Ransomware in a shared environment.

Action Item: Mr. Frohlich will add the Meet the Threat discussion to the May 10, 2017 MT-ISAC agenda.

Public Comment

None

Next Meeting

May 10, 2017

1:00 PM to 3:00 PM

Cogswell Building, Room 151

Adjournment

The meeting adjourned at 1:51 PM.