

Montana State Information Security Advisory Council (MT-ISAC)

Minutes

May 10, 2017

1:00 PM

Cogswell Building, Room 151

Members Present:

Ron Baldwin, State CIO/SITSD – Chair
Erika Billiet, City of Kalispell
Joe Chapman, DOJ
Stuart Fuller, DPHHS
Adrian Irish, UM
Margaret Kauska, DOR

Manuel Soto, OPI
Jon Straughn, Corrections
Maura Gruber, DNRC – Alternate
Chief Craig Stewart, DMA – Alternate
☞ Kreh Germaine, DNRC

Staff Present: Joe Frohlich, Wendy Jackson, Sarah Mitchell

Guests Present: Matt Van Syckle, Maura Gruber, Chief Craig Stewart, Jerry Marks, Sean Rivera, Suzi Kruger, Michael Barbere, Jennifer Viets, Dawn Temple, Craig Marquardt, Rebecca Cooper, Lance Wetzell, Carroll Benjamin, Marieke Baughman, Cyndie Lockett, Dave Johnson, Tim Kosena

☞ **Real-time Communication:** Peder Cannon, Phillip English, Paul Kozlowitz, Alan Grover, Sky Foster, Angie Riley, Terry Meagher, Brian Jacobson, Chris Gleason, Dan Chelini, Christi Mock, Cheryl Pesta, Channah Wells, Dave Danicich, Irvin Vavruska, John Cross, Anne Kane, Judy Kelly, Darrin McLean, David Swenson, Edward Sivils, Glynis Gibson, Larry Krause, Michael Jares, Matt May

Welcome

Ron Baldwin welcomed the council to the May 10, 2017 Montana Information Security Advisory Council (MT-ISAC) meeting. All members and guests were introduced.

Minutes

Motion: Margaret Kauska made a motion to approve the April 12, 2017 minutes. Jon Straughn seconded the motion. Motion carried.

Business

Legislative Session

Ron Baldwin provided a brief update regarding the 2017 legislative session. House Bill 61, to modernize the 911 laws, and was signed by the Governor. This update is located at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>.

Protection Against Ransomware

Sean Rivera presented an overview of State Information Technology Division's (SITSD) Malware and Ransomware security and incident response. SITSD's Disaster Recovery (DR) response includes a virtual server platform and shared private cloud. Storage options include live storage on the Net App and archive storage on Isilon. All virtualizations, storage solutions, and services provided by SITSD include built in DR. Snapshots can be restored upon agency request. Replicas of live storage are taken and stored using similar practices. DR is also provided during Convergence to the host platform. Antivirus (AV) is included on all virtualizations as mandated by policy. Network security provided by SITSD includes traditional and Next-Generation Firewall and Web-content filtering. SITSD maintains an Internet Protocol (IP) Black list. The Network is architected to maximize network isolation to allow agencies to operate with as much autonomy as possible. If you have any questions regarding how this works in the virtual realm contact Dave Johnson at dave.johnson@mt.gov or Jerry Marks at jmarks@mt.gov.

Network Operations Security Center (NOSC) provides 24/7 monitoring from a Tier One perspective and escalates cases to the appropriate bureau as needed.

SITSD also has a third-party provider that conducts 24/7 monitoring of an Intrusion Detection System (IDS).

Recent changes to policy in the Exchange environment prevent most malicious attachments from getting through by utilizing a series of scans. Discussions are taking place to utilize an advanced protection program to increase state Malware and Ransomware protection.

MT-ISAC has developed a Device Hardening strategy, through development of Best Practices document, to address the growing rate of Ransomware. This document is located on the MT-ISAC website at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>. The strategy addresses issues relevant to end users including application whitelisting, patch management, concept of least privilege, 2-Factor Authentication, Microsoft's Enhanced Mitigation Experience Toolkit (EMET), Approved Software List (ASL), and BitLocker.

Each agency is responsible for developing and testing their own incident response plan. End user education and awareness is also mandated. Annual SANS training is a requirement for all state employees. SITSD has developed the Information Systems Incident Response Team (ISIRT) to address security incidents, service interruptions, as well as physical incidents that may occur regarding natural disasters. This plan is based upon the Federal Emergency Management Agency (FEMA) Incident Response model.

The State of Montana is further protected from Ransomware and Malware through a State Cybersecurity insurance policy that is managed through the Risk Management and Torte Division.

A variety of Best Practice documents have been developed to address both small and large incident handling. This information is located on the MT-ISAC website at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>.

Please contact Sean Rivera at SRivera@mt.gov or Joe Frohlich at JFrohlich@mt.gov with any questions.

Q: Manual Soto: Is there a standard practice regarding access to state services by individuals outside of the United States?

A: Mr. Rivera: There is no requirement that limits access to these services. Most state agency services are focused locally and can justify geographic restriction of services. Some agencies, such as the department of Commerce (DOC), may have a business requirement for global exposure. It is recommended that agencies defer to business requirements. Global access to agency services can be facilitated by contacting Mr. Rivera at SRivera@mt.gov. There is a risk for adversaries with resources to establish a cloud presence that appears to generate from within the United states. For this reason, the use of geographic IP Isolation strategies for Malware and Ransomware protection may not offer the same level of protection as it has in the past.

Data Loss Prevention (DLP)

Mr. Frohlich stated the DLP confidence level for SSN has been adjusted to address false positives. This has resulted in a decrease of false positives. Increasing confidence levels too much may lead to an elevated potential for sensitive information to be sent.

Mr. Johnson provided a demonstration on how to properly secure and share information using Microsoft OneDrive. Distribution lists that are mail enabled can be utilized with OneDrive. Users whose email are not enabled will still receive the document, but will not receive an e-mail notification signaling that the document was placed into OneDrive. To enable sharing with external entities, they must first set up a Microsoft account. This will facilitate a one-way sharing of sensitive information from state users to external entities via OneDrive. Mr. Johnson noted that mobile devices work the same as computers with regards to accessing documents through OneDrive. OneDrive is enabled across the Enterprise and can be can be enabled via the O365 Licensing attribute in Active Directory.

Mr. Marks commented that there are no written policy restrictions to prevent users from downloading the OneDrive for Business Microsoft App to a personal device. This capability is offered with SITSD's Enterprise Agreement. Future discussions will take place regarding SITSD's mobile device management solution and certificate based authentication. Restrictions may also be considered regarding the ability to access OneDrive for Business on devices that are enrolled in Multiple Device Management (MDM).

Action Item: Mr. Frohlich will post this presentation posted to the DLP policy website at

Action Item: Mr. Johnson will explore the possibility of delegating across logs for auditing purposes to discover what information is being shared.

Mr. Baldwin commented DLP is on track and the MT-ISAC has voted to move forward with the July 1, 2017 go live date.

Dawn Temple reviewed findings from the Department of Justice's (DOJ) testing of DLP. The majority of violations were due to SSNs. Ms. Temple stated that a five-second delay was experienced by DOJ test users. Due to this delay, it is possible to send the information quick enough to bypass the DLP response. The majority of information was blocked if the test user waited five seconds before sending. It was discovered that DLP was not catching a large amount of the sensitive information sent via email. DOJ test users also experienced some confusion regarding the ToolTips link to the DLP policy. There were several instances where users did not receive the ToolTip. These inconsistencies may be due to older versions of Office being used by DOJ. Test users also experienced inconsistencies with the File Transfer Service (FTS) Add-in. This option is not supported by the majority of DOJ users. Updates to DOJ Windows and Office programs may mitigate these issues. The implementation of DLP for DOJ will involve activities such as software upgrades, user education, and business process adjustments. This will require time and resources to complete.

Jennifer Viets provided feedback regarding the blockage of mission critical/extremely time sensitive emails for the DOJ. In emergency situations, e-mail is the preferred method for timely communication of information. There is a concern is that DLP may block incoming e-mails that contain time sensitive information needed for a critical situation.

Mr. Johnson verified that incoming e-mails are not blocked by DLP. DLP does, however, block malicious e-mails. If agencies feel information is being blocked in error, they should open a case with Service Desk.

Ms. Temple reviewed suggestions for the roll-out of DLP. DOJ does not feel ready for the July 1, 2017 DLP implementation date. DOJ would like to increase their test users from 80 to 100 individuals as this represents 10% of the DOJ users. DOJ suggested the following options: DLP customization at the agency level, exploration of the Override Option, or a delay implementation date to allow DOJ to more time to fully prepare for the roll out.

Mr. Johnson stated that with the override option will prevent the customized bounce back option.

Mr. Johnson stated that agency specific customization of DLP is possible, however this option will increase the level of complexity for DLP. SITSD will forego agency specific customization until DLP has been successfully rolled out and is running smoothly.

Margaret Kauska commented that Department of Revenue (DOR) is satisfied with the testing they have done. They are ready for the July 1, 2017 implementation date. Mr. Soto shared that all of Office of Public Instruction (OPI) is utilizing DLP. Mr. Fuller noted that the Department of Human and Health Services (DPHHS) is still in the testing phase.

Mr. Frohlich noted that SITSD is considering a DLP Awareness campaign in June, 2017 to disseminate DLP information to the Enterprise as a whole.

Action Item: The Service Desk will also send notifications to all state employees advising them of the upcoming implementation of DLP and helpful tips to prevent interruption of business functions.

Mr. Baldwin suggested the creation of a FAQ (Frequently Asked Questions) sheet to provide examples of the appropriate way in which to send sensitive information.

Joe Chapman suggested the formation of a smaller group to review agency's options.

Mr. Baldwin also recommended the creation of a workgroup to consider the results of DOJ test user findings

and provide an opportunity for other agencies to present their test results.

Mr. Frohlich stated that this topic could be addressed by the Best Practices workgroup which initiated DLP. This could be quickly addressed at the workgroup and discussions could take place whether to delay the DLP release date.

Action Item: Mr. Johnson will attend the Best Practices workgroup DLP discussions to gain a greater understanding of DLP issues and develop solutions.

Mr. Fuller from Personally Identifiable Information (PII) standpoint DLP helps agencies have compliance with HIPAA.

Ms. Temple stated employees sending sensitive information internally via Lync is an issue that should be addressed.

Action Item: Mr. Frohlich will post a link to DLP training to the MT-ISAC website at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>.

Action Item: Mr. Frohlich will scheduled a meeting with agencies to review DLP.

Workgroup Updates

Best Practices / Tools Workgroup Update

Mr. Frohlich presented documents under consideration by the Best Practices Workgroup. These documents include; enterprise methods on how to encrypt, media protection and vulnerability scanning.

The Best Practices workgroup has selected SentinelOne as the Enterprise Antivirus (AV) augmentation for the state. SentinelOne's technology is behavior-based threat detection. The AV technology compares suspicious malicious patterns against normal system patterns to determine if a threat exists. The 30-day Proof of Concept (POC) will begin May 11, 2017. The initial phase of the POC entails installation of the console on a server. Once installed, SentinelOne will be pushed out to SITSD servers and workstations. Phase Two involves each agencies choosing 10 licenses to push SentinelOne to servers and/or workstations within their environment. If POC is successfully completed, SITSD plans to purchase licenses for all state servers and all SITSD workstations. Mr. Frohlich noted a specialist with Gartner recommended installation of SentinelOne on all servers within the environment. Agencies are encouraged to purchase SentinelOne for their IT departments. SentinelOne will be a catalog item for agencies to purchase licensing for workstations. The cost per license for one year is \$31.24. SentinelOne has proposed a 3-year agreement at a cost of \$62.50 per user.

Action Item: Mr. Frohlich will post a SentinelOne demo link to the MT-ISAC website located at <https://sitsd.mt.gov/Governance/Boards-Councils/MT-ISAC>.

Situational Awareness / Outreach / Public Safety Workgroup Update

The workgroup has developed public outreach letters regarding information security that have been sent to key external entities. These letters reference the information security page located at <http://sitsd.mt.gov/Information-Security/Outreach>. This site contains website toolkits, resources, self-assessment kits and ways to report incidents within the private sector. Mr. Frohlich encouraged members to visit the page to review its contents for accuracy. Please e-mail Mr. Frohlich at jfrohlich@mt.gov with any suggestions through e-mail.

Enterprise security will follow-up with letters that were sent to recipients within 10 days to solicit feedback.

Current Threats

Mr. Rivera provided a brief update regarding current threats. In 2017, the Federal Bureau of Investigation (FBI) began tracking Business Email Compromises (BEC) as a unique crime. Since 2013, this activity is responsible for \$1.6B in United States (US) business loss and \$5.3B in business losses globally 2015. The BEC occurs when cyber criminals target senior level executives to gain access to or control over e-mail accounts or

impersonate with e-mail from a domain. The cybercriminal then instructs lower level employees to wire money or divulge sensitive data, such as W-2s. The records received are then sold on the Dark Web.

Critical security vulnerability in the Microsoft protection engine was released. Vulnerability included products such as Windows Defender and EndPoint Protections. This vulnerability could be exploited via email attachments. Version 1.1.13704.0 or less are susceptible to the bug. The bug fix was included in Microsoft's May, 2017 monthly rollup.

A sever vulnerability was discovered in certain Intel based business systems. Intel has released a downloadable tool to identify if machines contain this vulnerability. This vulnerability poses very little risk from the Enterprise level. SITSD can conduct vulnerability scans for agencies interested in checking for this vulnerability. To schedule this scan, please open a POB case with the SITSD Service Desk.

According to Google, fewer than 1/10 of a percentage of email users were actually affected by the recent Gmail Phishing campaign. Google was able to halt the phishing campaign within an hour and took measures to protect users by disabling accounts as well removing phony pages and malicious applications. Users were prompted to change passwords if they were identified.

Open Forum

Future Agenda Items

DLP workgroup will provide a review at the June 14, 2017 meeting.

General Quinn and Lynne Pizzini will provide an update on Meet the Threat at the June 14, 2017 meeting.

Review of the Biennium of the MT-ISAC council work plan, goals and objectives will be provided at the June 14, 2017 meeting. The list of nominees has been sent to the governor for signature. Agencies are encouraged to bring feedback with them to the June 14, 2017 meeting regarding MT-ISAC accomplishments and goals.

*****NOTE: June's MT-ISAC meeting has been changed to June 21st.**

Public Comment

Mr. Irish thanked everyone who attended the security conference. MT-ISAC is looking to move the conference to October during Cyber Security Awareness Month.

Jerry Marks requested volunteers from agencies to participate in SentinelOne's Proof of Concept (POC) within SITSD shared environment. There is a very short period of time for developing this POC. Interested individuals should contact Joe Frohlich at jfrohlich@mt.gov .

Next Meeting

June 21, 2017

1:00 PM to 3:00 PM

Cogswell Building, Room 151

Adjournment

The meeting adjourned at 2:56 PM.