Idaho Cyber Security Interdependencies Workshop

Event Summary

October 8, 2015
St. Alphonsus Regional
Medical Center
Boise, Idaho

Idaho Bureau of Homeland Security
PREVENT PROTECT RESPOND RECOVER

CRDR
Center for Regional Disaster Resilience

Contact:

Brandon Hardenbrook
Deputy Director
Pacific NorthWest Economic Region (PNWER)
206-443-7723
Brandon.Hardenbrook@pnwer.org

Megan Levy
Program Manager
Pacific NorthWest Economic Region (PNWER)
206-443-7723
Megan.Levy@pnwer.org

Executive Summary

The Idaho Cyber Security Interdependencies Workshop was held October 8, 2015 in Boise Idaho at the St. Alphonsus Regional Medical Center. More than 130 participants from both public and private sectors, and from across the Pacific Northwest, took part in the exercise that focused on current cyber threats, common challenges for securing data and continuing operations despite cyber disruptions.

Idaho Lieutenant Governor Brad Little and Brigadier General Brad Richy, Chief of the Idaho Bureau of Homeland Security, spoke at the event along with other experts on cyber security preparedness, response, supervisory control and data acquisition systems.

Through this event, participants sought to improve their own cyber plans by challenging their planning assumptions, gained a greater understanding of their interdependencies and built relationships with others across the state and region.

Background

This workshop was the second event in a three year initiative to develop a public/private sector partnership for resilience in the state of Idaho. In 2016, Idaho Bureau of Homeland Security (IBHS) and the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR) will develop an Action Plan for the development of an Idaho Public/Private Sector Resilience Partnership.

Development

The event was developed over the course of seven months through a series of conference calls and meetings. In addition to Idaho Bureau of Homeland Security and PNWER CRDR, planning team participants included Zions Bank, Bonner County, Idaho National Lab, HP, Blaine County, Idaho Department of Transportation, Office of the State Controller, University of Idaho, Office of the Chief Information Officer, Infragard, ICS-CERT, the City of Boise, Micron, and United Water.

Meeting Themes and Key Takeaways

Over the course of the day, a few themes and key takeaways emerged from the discussions, panels and speakers.

One of the most prevalent topics of the day was around the need for holistic cyber security—calling on organizations to move cyber security planning beyond the Information Technology departments and involve executive leadership, legal, and human resources. There is a strong need to train all staff members. According to IBM's 2014 Cyber Security Intelligence Index, 95 percent of all security incidents involve human error. This can take many forms, from clicking on links, giving away passwords, or failing to follow security protocols.

Every company has cyber security risk and should have a cyber security plan. From small businesses to sectors that are not typically seen as cyber focused, like agriculture, there are cyber security risks. There are also many great tools in the State of Idaho for getting assistance in building cyber security plans and responding to cyber security incidents that need to be shared and made more easily accessible to all organizations.

For all organizations, it is essential to have governance and policies around cyber security in place before having to respond to an incident. These would include policies around protecting data and procedure for response, including structure (the incident command system was recommended) and involvement of law enforcement. With these policies in place, organizations can test their systems through exercises and help build a security culture in an organization.

A common theme was the acceptance of breach. Not all information within an organization is equally sensitive and critical. By accepting that some cyber attacks will be successful, and focusing extra levels of security on the most important data, organizations can use their limited resources more effectively.

Identifying key information is a vital part of assessing the risk in each organization. The risk assessment also includes security protocols, equipment, software, public presence, business type, and all other aspects of a business that might make it an easy or desirable target for cyber attackers. Risk will never be fully eliminated as long as computers, automation and the internet are needed to complete business tasks, an organization will have cyber risk. All parts of a cyber plan should attempt to mitigate that risk, while helping identify procedures for protection of critical data and detecting access to or loss of that data. Too often companies don't know they have been breached until they are informed by an outside agency.

Recommendations

Based on participant feedback, planning team input, discussion outcomes, and common themes from the day's speakers, the following recommendations were developed:

- Develop training materials and regular webinars and other training opportunities to help organizations grow cyber security plans and facilitate information sharing.
- Provide training for executive leadership, legal departments, human resources, and other key departments to encourage organization-wide cyber security.
- Grow state-wide knowledge of the Idaho cyber security annex through training and outreach.
- Provide resources specific to small businesses and sectors where cyber security may not be prioritized (example: agriculture).
- Develop a single repository for cyber security preparedness information
- Develop formal partnership for information sharing around cyber security and other critical infrastructure concerns

Event Summary

Idaho Lt. Governor Brad Little kicked off the day with a call for proactive defense in cybersecurity

Brigadier General Brad Richy, Idaho Bureau of Homeland Security, noted the importance of training to cybersecurity

Opening and Introduction

An introduction for Lt. Gov. Little was provided by Sen. Chuck Winder, Idaho.

Lt. Governor Brad Little, Idaho

Lt. Governor Brad Little provided opening remarks for the day, emphasizing the importance of strong cyber security for the state of Idaho. From technology companies to agriculture, we are all at risk from cyber attacks. With an average of 200 days between cyber breach and when a breach is discovered, companies are really divided between those that know they have been hacked and those that don't know it yet.

To help improve preparedness in the state of Idaho, Governor C.L. "Butch" Otter appointed a cabinet level task force. The state recognizes the need to protect itself—risks include consumer privacy data, health information, tax returns, and critical safety concerns. Cyber security will affect the velocity of the economy going forward. It can be a hard sell, because you are taking a defensive position and the benefits won't show up on an income statement. You don't see the effects on the bottom line until something goes wrong. Lt. Governor Little pointed to the recent cyber breach in the state of South Carolina where tax data was stolen; the costs are estimated at $100 million dollars. He called that experience reason enough for the State of Idaho to be proactive and offensive more than defensive. The state is lucky enough to have the Idaho National Lab to provide expertise.

Government, however, moves slowly. The speed of technology outpaces government significantly. In order to take an effective stance against cyber threats, the way government reacts will have to evolve.

Brigadier General Brad Richy, Idaho Bureau of Homeland Security

Brig. Gen. Richy began by thanking Lt. Gov. Little for his opening remarks, noting that the Lt. Governor truly understood and embraced the complexity of this issue, and was positioning the entire team to address that complexity. Drawing on the feedback from the 2014 event in developing this agenda, people wanted to focus on interdependencies and self-preparedness. By exploring these two factors, we can work to improve the culture around cyber security.

If you told a business owner that through employee training they could boost sales by 20%, they would do it. Well, you can prevent 20% of data attacks through employee training. He noted that when he began in his current position, he was shown his computer and how to connect to the network. There was no additional training on how to keep that network safe. This has only become a more complex challenge as new technology becomes available—cell phones and tablets connect to the networks as well; our personal devices may be exposing the network.

The people in attendance—he noted that in 2016 he would like to see twice as many—already know and understand this issue. It is time to implement these lessons in our communities, to understand our interdepencies and implement the changes that protect us all.

Panel: Information Sharing, Resources, and Support

U.S. Attorney Wendy Olson and Ken Dunham, CEO of 4D5A Security Inc., Infraguard, addressed cybercrime and security

Panel participants included (from left) Derek Meyer, Kevin Maloney, Wendy Olson and Ken Dunham

Panel: Information Sharing, Resources, and Support

Moderator Eric Holdeman introduced the panel. The panelists make up some of the team of resources available in the state of Idaho for information sharing, resources and support.

Members of the panel included:

- Derek Meyer, Vulnerability Coordination Lead, DHS ICS/CERT
- United States Attorney Wendy Olson, District of Idaho, U.S. Department of Justice
- Kevin Maloney, Assistant U.S. Attorney, District of Idaho, U.S. Department of Justice
- Ken Dunham, CEO, 4D5A Security Inc., Infragard

Who do you call to report a cybercrime? Would 911 be a place to call to direct that to appropriate agency?

Mr. Dunham explained that if you call local police station, you are going to want to ask for a fraud investigator. However, he recommended organizations reach out to their local FBI and ask for the cyber lead. In the Boise area, this call would go to Clark Harshbarger. Any person in an organization can make this call and get the process moving.

Mr. Meyer explained that response is complex. An organization will look first to its internal team to identify the problem and fixes. This can be at odds with preserving evidence and information you may need when reaching out to law enforcement.

Ms. Olsen explained that there are steps to take within an organization before bringing in law enforcement. Information technology, corporate and executive leadership, legal and human resources departments need to have formulated a plan together. This will ensure everyone is on the same page when you make the call for help, and prevent a situation where the process has begun, just to have the legal team come and put a stop to it. Your legal counsel needs to be involved so they know what steps they need to take. Entities need to work together on what to do during cyber intrusions because it delays things on the backend if all parties are not involved. She added that the authorities know how to treat your organization as a victim and respectful of information.

Mr. Meyer added that reporting a cyber breech is useful, even if an organization isn't planning to bring in outside agencies to help. This is because they track breeches, as do other government agencies, to help identify trends and recognize if a single attack is part of a larger campaign. Reporting helps to track incidents and get the necessary help. Response help may not even have to happen on site-through images and logs from the hard drives; a lot of the analysis can be done off-site. These logs provide more help and information then a phone call ever will, because they build a technical view of the situation.

Question: When did you start to notice cyber security was really relevant to criminal aspects and not just an IT issue?

Ms. Olsen answered that it was really in the last ten years. With 9/11 there was a focus on national security issues but cyber intrusions didn't get a lot of attention until 10 years ago; this means everyone is behind in this game.

Panel continued...

Mr. Maloney added that a large proportion of attacks came in 2003-2004. This was when cyber security concerns moved from single attacks to large scale automation. This was followed by maturation of targeted attacks and espionage. Additionally, there was a growing understanding of cyber security as an interdependencies issue. There is no such thing as a border.

Mr. Meyer added that the growing number of SCADA systems has also led to a greater focus on cyber security. These systems are used for running and maintaining key systems including the electrical grid and water treatment. They are used because they make the system easy to control, but they are also easy to hack.

Question: What is Infraguard? Do you have advice for small organizations?

Mr. Dunham explained that Infraguard was founded in the late ‘90s as an effort to bridge the gap between corporate America and the FBI/federal sources. The goal was to put together all these people so we have resources to enhance the ability to respond to any situation. Small organizations face the same kind of governance issues that large organizations face but they don’t have budget or people. Small organizations need to make it a goal to get involved with local organizations that are free. Make it a priority to learn something every single day and don’t just fight foes.

Eric Holdeman asked the panel to explain what SCADA is and the interdependences come from that.

Question: What is the difference between USCERT and ISC-CERT?

Mr. Meyer explained that USCERT focuses more on corporate networks and the financial sector. ICS-CERT has more options for small businesses and more localized work. There are training classes offered through ICS-CERT that can help improve the level of cyber security knowledge across your organization.

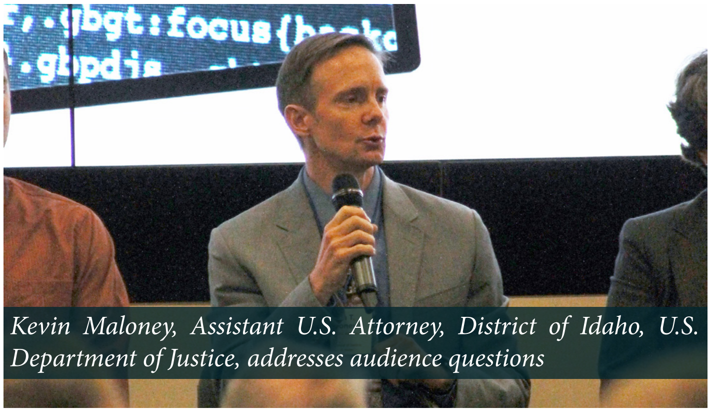
Question: How do we balance restoring operations with preserving evidence?

Mr. Maloney explained that in the initial stage, the organization should collect everything possible. Then as incidence response moves forward, decisions can be made on what is pertinent and how to preserve the chain of evidence. It is essential to have governance in place ahead of time, so you can prioritize either removing the threat to the detriment of data collection or working with the authorities to capture the data. For each option, the policy should be known and followed by all in an organization.

Participant Sean Malone noted that there is still a lot of difference of opinion on when or if to disclose when a breach occurs. There are many reasons for this. The first is embarrassment. Organizations don’t want to look irresponsible with information because it hurts its public image and can affect consumer confidence and stock prices. Secondly, organizations tend to want to maintain control of data involved with an investigation; there are concerns that once you send information offsite, you lose control over it. He noted that the people in the room represented people with a desire to cooperate across organizations, but others in their own organizations may not have the confidence or desire to share. This needs to be discussed in organizations, and each individual must decide what assurances they need to participate.

Mr. Maloney remarked that the criminal process is fairly secretive and confidential. We don’t confirm or deny until an indictment is filed. That takes 6 to 18 months. There are breeches every day, but very few get prosecuted. In a hypothetical situation, even if you have a breech that we can attribute to specific actor that we can apprehend, file indictment and bring to the trial, your company will have a long time to decide how to respond. Additionally, indictments are not meant to make a company look bad—they wouldn’t, for example, include in the indictment that the organization had inefficient security. Bringing it to trial should not cause trouble for an organization, either. This is thanks in part to the Economic Espionage Act, which ensures there are provisions to protect trade secrets, such as not discussing company details in open court. Mr. Maloney emphasized that it did them no good to embarrass an organization that comes to them for help, or to release sensitive data that hurt its competitiveness—if they did that, the next company to be breached would never come to them for help.

Mr. Meyer explained that with the ICS-CERT work, they first discuss with an organization which information is sensitive and identify who will have access to that data.



Kevin Maloney, Assistant U.S. Attorney, District of Idaho, U.S. Department of Justice, addresses audience questions

Panel continued...

Mr. Maloney added that whenever possible, organizations should share data about breaches with others. Even with identifying information scrubbed, this data can be hugely helpful in identifying patterns. This is useful in identifying whether a coordinated, wide-spread attack is occurring and new patterns and methods for breaching organizations.

Question: What is Infraguard? Do you have advice for small organizations?

Mr. Dunham explained that Infraguard was founded in the late '90s as an effort to bridge the gap between corporate America and the FBI/federal sources. The goal was to put together all these people so we have resources to enhance the ability to respond to any situation. Small organizations face the same kind of governance issues that large organizations face but they don't have budget or people. Small organizations need to make it a goal to get involved with local organizations that are free. Make it a priority to learn something every single day and don't just fight foes.

Eric Holdeman asked the panel to explain what SCADA is and the interdependences come from that.

Question: What is the difference between USCERT and ISC-CERT?

Mr. Meyer explained that USCERT focuses more on corporate networks and the financial sector. ICS-CERT has more options for small businesses and more localized work. There are training classes offered through ICS-CERT that can help improve the level of cyber security knowledge across your organization.

Question: How do we balance restoring operations with preserving evidence?

Mr. Maloney explained that in the initial stage, the organization should collect everything possible. Then as incidence response moves forward, decisions can be made on what is pertinent and how to preserve the chain of evidence. It is essential to have governance in place ahead of time, so you can prioritize either removing the threat to the detriment of data collection or working with the authorities to capture the data. For each option, the policy should be known and followed by all in an organization.

Participant Sean Malone noted that there is still a lot of difference of opinion on when or if to disclose when a breach occurs. There are many reasons for this. The first is embarrassment. Organizations don't want to look irresponsible with information because it hurts its public image and can affect consumer confidence and stock prices. Secondly, organizations tend to want to maintain control of data involved with an investigation; there are concerns that once you send information offsite, you lose control over it. He noted that the people in the room represented people with a desire to cooperate across organizations, but others in their own organizations may not have the confidence or desire to share. This needs to be discussed in organizations, and each individual must decide what assurances they need to participate.

Mr. Maloney remarked that the criminal process is fairly secretive and confidential. We don't confirm or deny until an indictment is filed. That takes 6 to 18 months. There are breeches every day, but very few get prosecuted. In a hypothetical situation, even if you have a breech that we can attribute to specific actor that we can apprehend, file indictment and bring to the trial, your company will have a long time to decide how to respond. Additionally, indictments are not meant to make a company look bad—they wouldn't, for example, include in the indictment that the organization had inefficient security. Bringing it to trial should not cause trouble for an organization, either. This is thanks in part to the Economic Espionage Act, which ensures there are provisions to protect trade secrets, such as not discussing company details in open court. Mr. Maloney emphasized that it did them no good to embarrass an organization that comes to them for help, or to release sensitive data that hurt its competitiveness—if they did that, the next company to be breached would never come to them for help.

Mr. Meyer explained that with the ICS-CERT work, they first discuss with an organization which information is sensitive and identify who will have access to that data. Mr. Maloney added that whenever possible, organizations should share data about breaches with others. Even with identifying information scrubbed, this data can be hugely helpful in identifying patterns.

Panel continued...

This is useful in identifying whether a coordinated, wide-spread attack is occurring and new patterns and methods for breaching organizations.

Question: What is Infraguard? Do you have advice for small organizations?

Mr. Dunham explained that Infraguard was founded in the late '90s as an effort to bridge the gap between corporate America and the FBI/federal sources. The goal was to put together all these people so we have resources to enhance the ability to respond to any situation. Small organizations face the same kind of governance issues that large organizations face but they don't have budget or people. Small organizations need to make it a goal to get involved with local organizations that are free. Make it a priority to learn something every single day and don't just fight foes.

Eric Holdeman asked the panel to explain what SCADA is and the interdependences come from that.

Question: What is the difference between USCERT and ISC-CERT?

Mr. Meyer explained that USCERT focuses more on corporate networks and the financial sector. ICS-CERT has more options for small businesses and more localized work. There are training classes offered through ICS-CERT that can help improve the level of cyber security knowledge across your organization.

Question: How do we balance restoring operations with preserving evidence?

Mr. Maloney explained that in the initial stage, the organization should collect everything possible. Then as incidence response moves forward, decisions can be made on what is pertinent and how to preserve the chain of evidence. It is essential to have governance in place ahead of time, so you can prioritize either removing the threat to the detriment of data collection or working with the authorities to capture the data. For each option, the policy should be known and followed by all in an organization.

Participant Sean Malone noted that there is still a lot of difference of opinion on when or if to disclose when a breach occurs. There are many reasons for this. The first is embarrassment. Organizations don't want to look irresponsible with information because it hurts its public image and can affect consumer confidence and stock prices. Secondly, organizations tend to want to maintain control of data involved with an investigation; there are concerns that once you send information offsite, you lose control over it. He noted that the people in the room represented people with a desire to cooperate across organizations, but others in their own organizations may not have the confidence or desire to share. This needs to be discussed in organizations, and each individual must decide what assurances they need to participate.

Mr. Maloney remarked that the criminal process is fairly secretive and confidential. We don't confirm or deny until an indictment is filed. That takes 6 to 18 months. There are breeches every day, but very few get prosecuted. In a hypothetical situation, even if you have a breech that we can attribute to specific actor that we can apprehend, file indictment and bring to the trial, your company will have a long time to decide how to respond. Additionally, indictments are not meant to make a company look bad—they wouldn't, for example, include in the indictment that the organization had inefficient security. Bringing it to trial should not cause trouble for an organization, either. This is thanks in part to the Economic Espionage Act, which ensures there are provisions to protect trade secrets, such as not discussing company details in open court. Mr. Maloney emphasized that it did them no good to embarrass an organization that comes to them for help, or to release sensitive data that hurt its competitiveness—if they did that, the next company to be breached would never come to them for help.

Mr. Meyer explained that with the ICS-CERT work, they first discuss with an organization which information is sensitive and identify who will have access to that data.

Mr. Maloney added that whenever possible, organizations should share data about breaches with others. Even with identifying information scrubbed, this data can be hugely helpful in identifying patterns. This is useful in identifying whether a coordinated, wide-spread attack is occurring and new patterns and methods for breaching organizations.

Question: How much do services cost?

Ms. Olsen explained that as their work is funded by taxpayers there is no additional cost for service.

Idaho Cyber Interdependencies Scenario and Exercise

Andrew Bochman, Strategic Planner, Idaho National Laboratory

Participants describe cyber systems within their own organizations and address how they would respond to a cyber attack scenario

Introduction to scenario and exercise format by Andrew Bochman, Strategic Planner, Idaho National Laboratory

The Idaho Cyber Interdependencies Exercise is a discussion-based scenario designed to help organizations identify ways to improve cyber resilience in both the public and private sectors. Through this process it is hoped that gaps and potential opportunities to improve cyber security in Idaho and region will emerge.

The objectives of the discussion are to increase awareness of interdependencies in coordinating public/private response to a cyber based incident; create an understanding of the need for cyber response plans; allow organizations to evaluate existing cyber response plans and identify improvements; identify gaps in planning, resources, policy, and response thresholds; evaluate communications and information sharing between critical service providers and public and private organizations in a crisis; understand the impact, both regionally and for separate organizations, of a loss of infrastructure; and identify opportunities for public/private resilience collaboration and information sharing.

The scope of the exercise covers the State of Idaho and cross-jurisdiction and cross-national border where key interdependencies extend.

Mr. Bochman said that we are coming at these questions from a cyber perspective because it is the purpose of the work should, but in real life, you might not know right away that you were facing a cyber incident. In the real world you won't know. When it is found out, you will address it as so. But it is unlikely to be the first thing on your mind.

It used to be that cyber security was thought of as a perimeter issue—however, that fell apart the minute perimeter was breached, because someone inside your network had access to everything. We are learning to separate data, and build layers of security to protect the most pertinent data, while leaving the less important data more vulnerable.

Our biggest vulnerability, when it comes to cyber, is our dependency. If we didn't rely on automation the way we do, an attack wouldn't matter. The purpose of this exercise in part, to help you think about how you would do your job without automation. The biggest obstacle is the complexity of our systems.

Table Discussion 1:

Exploring how cyber systems impact your organization and your ability to do business, the types of plans you have in place, and methods for gathering and sharing information

Scenario:

There are complaints of computer lock outs and others report loss of internet connectivity at some work stations. Employees online can only access local files and applications will not load.

Questions to consider:

- What actions does your organization take to improve cyber preparedness?
- What is your current plan for training staff?

Participants address specific questions on how they would respond to a cyber attack on their companies' systems.

Scenario and exercise continued...

- How would you engage your current response plan in this scenario?
- Where would you go for more information?
- Who would you need to inform, and how would you inform them, about service and communications disruptions?
- How do you detect malicious activity?
- What special considerations do you have to take for your sector?
- For example, are there records you must be able to access to continue business?
- What would be the expectation of employees if computers and connectivity were inaccessible?
- What organizations might you coordinate with for more information?
- If there are increases in complaints about IT issues, is there a chain for informing within the organization?
- Is there a means for sharing the information with the fusion center or with other organizations?
- Do you have a template or method for collecting information you would need to send to report issues?
- Would you share information with other organizations?
- How would you get approval to share information with other organizations?

Feedback from table discussions

After the discussion, each table reported on the discussion and key takeaways from their tables.
The tables agreed that the scenario would initially be seen as an IT issue, similar to what they deal with each day. The recognized the need to have a plan for transitioning from IT to a cyber security breach response, which should involve many different agency departments, not just IT.

At one table, participants recommended using the Incident Command System model typically used in emergency response and business continuity. Incident command can help with assigning the decision makers and protocol for providing briefings and information before an event. In adapting for cyber, protocols can be established around how to collect data and when to consider engaging law enforcement or outside help. This was just one example of a proven and established procedures that could be pulled off the shelf and adapted for cyber security.

In developing plans, participants said they would like to know the existing security standards. Recognizing that these standards will change all the time, they felt that if they were not meeting the most recent standards, they were not protected and there was no way for them to keep up. Many organizations have security systems installed, but there were concerns that patches and software were not always up to date. Updating this software should be a part of the security culture at an organization.

Participants highlighted the need for redundant communications capability. For example, with some phone systems, service is provided over the internet so when computers lack connectivity, so do phones. Having secondary phone systems or radios, or even plans for using personal or company cell phones are all examples of redundancies to the communications system. Decisions on how employees should contact one another without email and phones can be made well before an event, cyber or otherwise.

Luncheon keynote: Sean T. Malone

Director of Strategic Development, Fusion X

Sean T. Malone, Director of Strategic Development, Fusion X, provided a keynote speech focused on cybersecurity priorities

Luncheon keynote: Sean T. Malone, Director of Strategic Development, Fusion X

Mr. Malone started with an example of physical security and how it could affect cyber security, by acting out a phone conversation between an employee and a hacker posing as a helpful IT person. Cyber security protocols are more than just what you do online. They should apply to security decisions across an organization. With one five minute phone call, someone could gain access to wire transfer information and it wouldn't matter how well an organization's firewall or software worked. Buying expensive equipment often gives the feeling of security. This is really only as good as the people, processes, and infrastructure interacting with that equipment.

In the past, cyber security has been focused on keeping everyone out. However, this has to change. It is easy to say "every system will be breached" but much harder for organizations to internalize and use as a guide in planning for security. Accepting breach as a reality allows for a better security system. Not all data in an organization is critical. The key is avoiding major cyber breaches—the kind that lose personal information or cause major material damage to an organization.

The security model should be like an onion—layered with the most critical assets in the center so that adversaries must bypass layers of security controls that are not interdependent. This is a technical issue, but anyone in an organization can and should ask whether data is tied to security zones. Everything that is not essential data behind multiple layers of security staff should be assumed that it can and will be breached.

Workstations should be treated like the internet, when it comes to level of security—anything you save may get away from you.

Building security systems that protect key data and are understood and maintained by staff are essential to your full cyber security picture. Part of this is in how you set up your security infrastructure; part is in training. Everyone in an organization should understand how to minimize security risks, like giving out passwords over the phone or completing tasks for someone without verifying the caller. Decision making processes and classifications should be developed in an organization long before its first breach.

Once plans and systems are in place, exercises and drills are essential. The ideal drill is both zero knowledge and zero notice. This way it will be treated like a real event allowing the opportunity to see how plans and processes are used in the moment. With an exercise like this, responders wouldn't be told it was an exercise until the end, unless it got to the point of reaching out to law enforcement or a decision would negatively affect business. This is an excellent way to identify whether an organization's systems are working and how quickly issues are detected. Mr. Malone shared that in 80% of the attacks they perform at business' requests, the attack is never detected. One missed attack is all that it takes.

It is better that organizations are checking and testing their own systems. Mr. Malone acknowledged that financial and talent shortages made this difficult. However, but taking these action, organizations can better prioritize investments and make small changes without having to buy new hardware and software. This is contrary to beliefs that the process is too expensive and difficult. If funds are not there to bring in an outside agency, checklists and best practices are a good fall back. Due diligence can raise the bar, and make your organization less attractive to hackers. This will take more than ticking off the check boxes of a list; checklists should be used in conjunction with an assessment of key data and risk

Cyber Security, State Government, and Foreign Threats

Thomas MacLellan, Director of National Homeland Security Policy & Government Affairs, FireEye

Cyber Security
Interdependencies Workshop
Cyber Security, State Government, and Foreign Threats

Thomas MacLellan, Director of National Homeland Security Policy & Government Affairs at FireEye, covered cyber warfare chllenges

Thomas MacLellan, Director of National Homeland Security Policy & Government Affairs at FireEye spoke to State Government, and Foreign Threats

Mr. MacLellan explained that cyber security presents a different challenge then the warfare of the past. In the past, oceans provided protection to our nation. Now we don't have that option. For the first time, states are dealing directly with attacks from nation-states. This is all happening on the internet, an infrastructure that was not built with security in mind. The way the internet is used today would be unimaginable to those who developed it. The internet was built layer upon layer, like an onion. Security was an afterthought. Going back and making it secure is nearly impossible.

Because the risk cannot be eliminated, we have to identify organization specific concerns and build security. In the private sector, this is a major economic issue—from product data to job loss; the private sector takes huge hits from cyber-attacks. Government faces additional challenges because they have a tremendous duty to protect the information citizens are required to send. These governments are facing more specific and sophisticated attacks. For these reasons, a whole organization strategic approach is essential. Cyber security cannot be left to IT or Chief Information Officers/Chief Information Security Officers alone. A comprehensive approach will include accounting and finance, legal, human resources and executive leadership. The agencies with a stake in this are widespread, including homeland security, emergency management, National Guard, law enforcement, tax officials, education, courts, health care, and critical infrastructure and key resources (CIKR) owners and operators.

This kind of comprehensive approach is necessary because threats are more sophisticated. What used to be concerns about worms and spyware have become targeted and persistent attacks, and it is more than any one organization can be expected to manage on their own. In part, this is because of who is facilitating the attacks. The breaches that get an organization in the news and cost hundreds of thousands of dollars are coming from nation states and large scale criminal organizations; organizations are facing highly skilled people. These adversaries are using a combination of methods to gain access to key information. Besides computers and the internet, they use phone calls, information gathered from social media sites (for example LinkedIn), and familiarity with employees to gather information through social engineering. Not only are the methods more varied, the information and targets are evolving. Mr. MacLellan said that the personal information of students in K-12 has been of growing interest to foreign nation-states as they gather as much information on U.S. citizens as possible.

New technologies increase our insecurity. In addition to traditional servers and computer networks, mobile phones and other smart devices and cloud storage services create additional entrances to networks and personal information.

Prevention is essential, but so is detection and response. It is becoming more difficult to perform forensics as criminals learn to cover their tracks better. It is essential to an organization to know what information has been accessed, removed, or even changed. Mr. MacLellan gave an example of hacked court documents, asking what could be done if records were being changed with no way of discovering the hack.

Detection, however, is lacking. Mr. MacLellan shared that, in his experience, outside entities are on a network an average of 205 days before being detected. He once saw a system that had been breached 2982 days. Even with this long time on the network, 70% of victims are notified from outside their organization. One of the most important things an organization can do in the event of a system breach is to control the story—share pertinent details with the public and stakeholders as soon as possible. When an organization fails to detect its own breach, the ability to control the narrative is taken from them as well.

State Government, and Foreign Threats continued...

There are resources available to organizations, but it is a mistake to believe the cavalry will swoop in to help. Often law enforcement and forensic agencies don't have the capacity to provide the resources that will be needed it something really big happens. Every organization needs to be in the position to address its own needs. This begins with a comprehensive understanding of risk. This is a place many state and local governments are at risk. Organizations need to enhance intrinsic capabilities, allowing for the identification and response to adversaries. In order to support these efforts, effective governance and real-time threat monitoring should be in place. Mr. MacLellan suggested a new approach as well, recommending that organizations—specifically government—change the overall security posture. Instead of fighting off attackers who come to you, he recommended security professionals go out and hunt their adversaries.

These efforts will help increase the resilience of an organization's systems. It can be a hard sell—it will cost money and resources. However, the downside of risk is significant, especially when liability is taken into consideration.

He recommended seven questions to ask in each organization:

1. Who has already been in your network?
2. Do you know your risk profile?
3. How are you reducing your liability? (Example, do you have cyber insurance?)
4. How are you changing people's behaviors?
5. Are you using intelligence and information effectively?
6. Can your most critical systems defend against those top tier attacks?
7. Are you ready to respond? Who are you going to call?

Table 2 discussion:

Exploring methods for employee training, integration of business continuity teams, and information sharing around cyber breaches.

Scenario:

The local Water Treatment Plant fears they are under attack as their control operation system that provides SCADA capabilities has been unresponsive. They are unable to manage the majority of the PLC's and have been rapidly checking on them manually to ensure normal operations.

After further investigation, citizens in the area have been warned not to drink tap water as the engineers at the Water Treatment Plant found that excessive amounts of the disinfectant chemicals (eg. Ozone and Chlorine) have been added to the water. The plant has taken manual control of the systems but it isn't known how long the excess amounts of chemicals were being added. In addition, it seems possible that the water may have been diverted to other pipelines that interconnect the treatment plants in the area. Other citizens in the surrounding area may be at risk. The Water Treatment Plant is doing everything they can to take control over their control operation system.

Waste water plants operated and controlled by municipalities have begun to experience issues with their treatment process. Due to many municipalities operating on a flat network, it's possible that the intrusion/malware infection could have spread and attackers are now targeting these waste water plants in addition to water treatment/distribution plants. No more specifics have been given thus far as to the condition of the plants.

Questions to consider:

- What are your water dependencies and requirements?
- What other infrastructure interdependencies do you rely on and what alternatives do you have in place?
- How would cyber response and physical response teams coordinate?
- What are communication protocols and procedures?
- What would be the impacts on your employees in the office?
- And on employees outside of the office?
- How do you prepare employee families?

While many groups said their companies' cybersecurity systems were installed, not all knew if their systems were up-to-date.

Table 2 discussion continued...

Feedback from table discussions

After the discussion, each table reported on the discussion and key takeaways from their tables. Participants explained that the initial reaction to the scenario would be to switch to manual operations and disconnect until there was a better idea of what was going on. Switching to manual may be difficult in some areas because those who know how to continue operations in that manner are entering retirement. In some places, staff is running shifts with only six months experience. They are familiar with procedures but lacking operational knowledge. It would be beneficial to train and exercise staff in manual operations.

In addition to manual operations, staff should be trained to recognize an attack. IT staff needs to know how to track egress of information to ensure they know what data is leaving the network. A participant recommended that staff also review who is accessing the website and systems using analytics, which may give a heads up about possible adversaries that may be interested in your networks.

Communication would be essential in this event, both to inform the public of the risk and to identify who needs water immediately.

This scenario is based in part on the Stuxnet attack: https://vimeo.com/25118844

Table discussion 3:

Exploring infrastructure interdependencies that impact your ability to do business and the cyber security concerns that may cause economic and life-safety risks.

Scenario:

MSISAC releases a report that warns that there have been reports of malware (Who would this go to and how would that information be redistributed?) Malware has taken credit card processing offline for many local businesses, including local grocery stores.

A 911 center is reporting systems are down for receiving calls and dispatch, and calls are being rerouted to other call centers. A newspaper has noticed that employees are tweeting about not being able to work due to internet disruptions and has called asking for a statement. Credit card processing is down across the region. ATMs are unable to process requests. Grocery stores and gas stations are cash only. Outages at one 911 center are backing up calls and causing troubles with dispatch

Questions to consider:

- Where would you go for information and guidance about removing malware?
- Would you have received the report?
- How would you investigate malware problems, and how would you go about eliminating them?
- How would an apparent insider threat change our response and communication procedures?
- What are your reporting procedures (legal and regulatory considerations) about data breach?
- What crisis communications measures (internal and external) would you implement?
- How would you integrate your security or business continuity teams with your response?
- What are the policies around releasing information to the media or on social media?
- How well trained are your staff members in this policy?
- Do you have a plan in place for social media hacks or unauthorized messaging on behalf of the organization?

After the discussion, each table reported on the discussion and key takeaways from their tables. A participant from law enforcement reported out first, explaining that more of their notifications take place via email. He knew that an alternative option would be to call another agency out of the area, and ask them to send essential messages, however this is not something they have practiced and he couldn't be assured that other agencies would have the right distribution list. He recommended an annual test of this process.

Table 3 discussion continued...

Cyber security is very much about dependency—the need for automation to run our systems, the reliance on automation for our contacts, and the reliance on service providers to get companies back to full operation. It is essential that business and government work with internet service providers to understand security measures and, if possible, have secondary service providers. This was a key recommendation when it came to phones as internet based phone systems grow in popularity.

Participants had questions about the ability to activate the Emergency Operations Center (EOC) for a cyber security event, and whether any agencies did or could offer that service to IT. After discussion, it was determined that while the EOC could be activated, the request would have to go through the Emergency Manager.

Gen. Richy explained that the state now has a cyber annex to its emergency response plans. Participants were not familiar with the annex, and discussed the need for a presentation on the annex itself.

Scenario Hotwash and Key Takeaways

To close the day, participants shared their key takeaways and recommendations for cyber security in the state. Based on their input, and the input provided through feedback forms, several key takeaways were identified. Participants considered the conference very good overall. Many participants felt that those in the room understood the threat, or were at least willing to explore how it would impact their organizations, but that training for executive leadership was needed. Participants also expressed a desire for more frequent training, suggesting webinars and online materials would be useful in between opportunities to gather in-person.

Many participants identified additional organizations from throughout the state that should be involved in meetings, recommending that holding events outside of Boise might help with engagement. Those with small businesses or outside the technology world felt the event was above their level of understanding at times, and suggested training specific for small businesses and beginners' cyber security checklists and other guideline information.

Based on participant feedback, planning team input, discussion outcomes, and common themes from the day's speakers, the following recommendations were developed:

- Develop training materials and regular webinars and other training opportunities to help organizations grow cyber security plans and facilitate information sharing.
- Provide training for executive leadership, legal departments, human resources, and other key departments to encourage organization-wide cyber security.
- Grow state-wide knowledge of the Idaho cyber security annex through training and outreach.
- Provide resources specific to small businesses and sectors where cyber security may not be prioritized (example: agriculture).
- Develop a single repository for cyber security preparedness information
- Develop formal partnership for information sharing around cyber security and other critical infrastructure concerns