Idaho Cyber Security
INTERDEPENDENCIES WORKSHOP

Event Summary

November 13, 2014
Hewlett-Packard Campus, Garden City, ID

IDAHO BUREAU OF HOMELAND SECURITY
PREVENT PROTECT RESPOND RECOVER

CRDR
Center for Regional Disaster Resilience

Contact:

Brandon Hardenbrook
Deputy Director
Pacific NorthWest Economic Region
206-443-7723
brandon.hardenbrook@pnwer.org

Megan Levy
Program Manager
Pacific NorthWest Economic Region
206-443-7723
megan.levy@pnwer.org

Executive Summary

Over 115 participants gathered at the Hewlett Packard Campus in Garden City, Idaho on November 13, 2014 for the Idaho Cyber Security Interdependencies Workshop hosted by the Idaho Bureau of Homeland Security (IBHS) with assistance from the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR).

The one day workshop provided excellent information on current Cyber threats, and best practices utilized to develop organizational Cyber Security plans. Guest speakers, panel discussions, and round table facilitated conversations contributed to a very successful workshop.

The event was developed over the course of four months through a series of conference calls and meetings. The planning team included local public and private sector organizations, including: Idaho National Laboratory (INL), MK Hamilton & Associates, Office of the Idaho State Controller, Office of the Idaho Chief Information Officer, Idaho Bureau of Homeland Security, Petso Financial Consultants LLC, University of Idaho, Hewlett Packard, Idaho State Police, Zions Bank, Idaho Transportation Department, and St. Luke's Health System.

Feedback from the event was strong, with every participant replying answering "excellent" or "very good" regarding the overall impression of the workshop. Some of the key takeaways for participants included the fact that information technology (IT) security teams were wearing too many hats and unable to focus on security, and that they better understood the resources available for response and information sharing. Many participants recognized the need to create or revise their incident response plans, and integrate physical and cyber security. Participants noted that they would have benefited from a checklist to bring back to their organizations to better utilize the information learned over the course of the day, and some indicated they needed a greater understanding of interdependencies.

Based on the presentations and group discussions, a few recommendations have emerged. A full list can be found on page 13. A key point that emerged throughout the day is the need for employees at all levels of an organization to understand the role cyber systems play in their business--how much and what kind of data is being stored, what they impact, and how they help the organization to complete mission critical tasks--as well as their role in keeping those systems Online. This means integrating cyber security with physical as part of a company-wide security integration, and knowing how to recognize when something is wrong--from training employees how to recognize phishing emails to increasing knowledge of how to recognize suspicious hardware and software, a whole organization approach can increase the awareness of employees to the importance of cyber issues, and provide greater security.

This workshop was the first in a three year initiative to develop a public/private sector partnership for resilience in the state of Idaho. In 2015 IBHS and PNWER CRDR will host a table top exercise to help identify interdependencies and gaps in existing partnerships. Following that, the team will develop a Action Plan for the development of an Idaho Public/Private Sector Resilience Partnership.

Background

Over 115 participants gathered November 13, 2014 at the Hewlett Packard Campus in Garden City, Idaho for the Idaho Cyber Security Interdependencies Workshop hosted by the Idaho Bureau of Homeland Security (IBHS) with assistance from the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR). This event was the first in a three year initiative to develop a public/private sector partnership for resilience in the state of Idaho.

Presentations

Welcome featuring Brigadier General Brad Richy, Director, Idaho Bureau of Homeland Security

Brigadier General Brad Richy explained what prompted him to bring this cyber security workshop to Idaho, and the goal for building better private and public sector collaboration in the state. He praised the Emerald Down III event in Seattle, Washington, and a expressed a desire to recreate such information sharing events in Idaho. He emphasized the excellent support from Lt. Governor Brad Little in pursuing this partnership.

Opening Remarks featuring Lt. Governor Brad Little, Idaho

Lt. Governor Brad Little began by discussing all the ways cyber security has evolved, but emphasized how often people override their security for ease and convenience.

Setting the stage for the event, Lt. Gov. Little explained that the state receives 2.3 million emails a month, half of which are spam. They experience over 400 malware critical insertions weekly. They experience hundreds of thousands of attacks each month. Every day as technology advances, so do our cyber vulnerabilities.

According to Lt. Gov Little, we are at the dawn of a technological arms race, between those who are using cyber systems for good, and those using it for ill, like drug cartels, nation states, and criminals. Cyber crime is a two trillion dollar business. He compared it to flood planning: investing in protection isn't an easy sell, but when the river floods, it's suddenly a top concern. He told participants that what they were doing at this event was building protection for their individual organizations and the state. He brought up Moore's law, Intel co-founder Gordon Moore's declaration that "The number of transistors incorporated in a chip will approximately double every 24 months." This, he said, applies to the high speed world of cyber security, but government statutory protections by comparison move like molasses.

He highlighted the downward pressure cyber crime has on the economy, impacting it negatively to the point of 1% GDP or 200,000 jobs. Cyber security is a growth industry; there will soon be 50 billion Internet connected devices in the world. The Internet of today is barely the size of a golf ball compared tomorrow's universe the size of the sun.

Idaho government agencies are faced with challenges in partnering with residents because of suspicion of the government; However, he said, Idaho is also a state with incredible resources, including INL and the Idaho Bureau of Homeland Security. Cyber attacks will continue, and everyone will have to continue to evolve: Change is inevitable; adaptation and survival is optional. This threat is one of the biggest to the economy of the state of Idaho.

Current Cyber Threat Landscape featuring Special Agent Clark Harshbarger, Boise RA, Salt Lake City Division, FBI

Mr. Harshbarger is the FBI agent for Idaho. He started by saying it is difficult for large organizations and especially government to evolve. IT staffs are often small with a big job to do. There is a lot of changing technology that presents challenges and opportunities--for example the rise of Bitcoin and alternate currencies, a trend that makes investigation of crimes difficult. If they are using a virtual currency, the paper trail disappears.

When it comes to cyber security, the best day is the one where nothing breaks. It's a very difficult position to uphold—If you only have a defensive position, you will always lose. In cyber security it is hard to go on the offensive. Buy-in for cyber security is a challenge: upper management in most organizations remembers a cyber attack for no more than six months. Security is falling off while we move quickly to adopt new technologies, like cloud-based storage, open software, and open hardware.

Turning to cloud-based storage he said a key question was who owns the data. If you don't own the data and you don't own the architecture, it is difficult to know how many people out there might have access to your information. Cloud storage makes it especially hard for them to do forensics. However, it is a useful tool for businesses because it is good for redundancies and reducing the costs of equipment and personnel.

THE COMPANY MAN

The FBI has created a series of movies based on real-life investigations to use as training videos for organizations and their own staff. The Company Man shows how much impact one employee turning on you can have on your organization.

View the trailer at: www.youtube.com/watch?v=_fT060aGnt4

Personal information is protected in different ways under the law. When it comes to medical data, the Health Insurance Portability and Accountability Act (HIPPA) laws protect your personal information at medical centers. The FBI cannot enter someone's home without a warrant. However, when you're talking about a private sector business, like a mom and pop pizza shop – there are some laws, but no constitutional protection of privacy for your personal information. These are protected only so far as case law reaches. Case law is greatly affected by what the average United States citizen considers private; the more we post Online publicly, the less expectation of privacy we can have in the eyes of the law.

The FBI's overall priorities are terrorism, counter-intelligence, and protection from cyber based attacks and high-technology crimes. There are real life impacts to cyber systems: for example, a Supervisory Control and Data Acquisition (SCADA) system attack that could affect the amount of chlorine in your water system. He added that economic espionage costs $500-700 billion annually. They have been taking some huge steps in this past year, including issuing formal letters to countries where cyber ex-filtration of intellectual property are occurring. It is hard to get a country to stick its neck out in a large economic market and be willing to come out and make an accusation against its citizens on behalf of the United States.

Mr. Harshbarger told participants the likely aim of attacks against their organization would to gain access to credentials or credentialing mechanisms. He recommended participants review their policies:

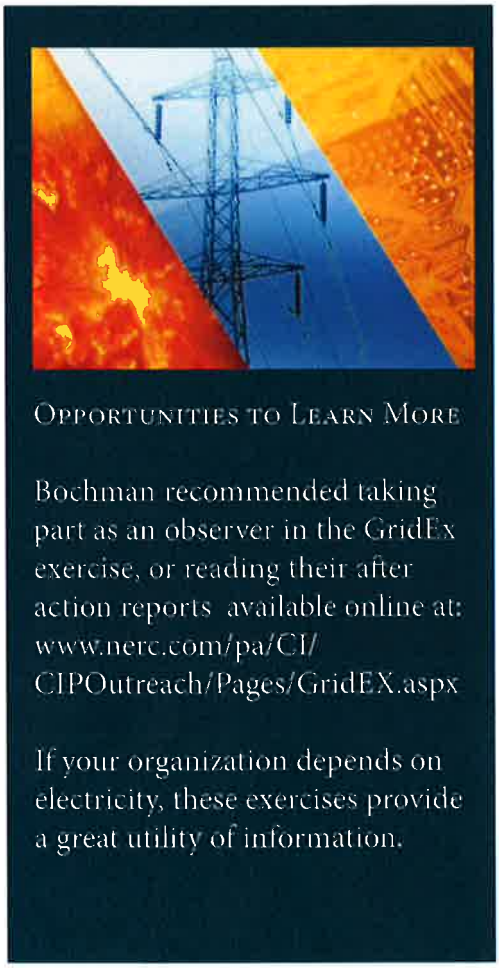
- What kind of non-disclosure do your employees sign?
- How often do you revise and have employees re-sign those?
- Do you have banners at log in or anything that gives specific information?
- Have you identified the most important information? Do you clearly mark and delineate that information?

He suggested organizations pursue policies and practices that help diminish their vulnerabilities. The best thing he has seen against spear phishing was marking every single email that comes in from an outside server as [EXTERNAL] which has decreased successful attacks through spear phishing by 95%.

He offered that the FBI can come to your company and talk about international espionage and cyber protection.

Cyber Interdependencies: Examining the Cascading Impacts of Cyber Incidents featuring Andy Bochman, Senior Cyber and Energy Security Strategist, National and Homeland Security Directorate, Idaho National Lab

Mr. Bochman began by explaining that dependencies and interdependencies can sometimes be challenging to recognize and tease out the differences. Everything has some aspect of cyber now; this is especially true in banking and energy. However, he noted, this didn't mean cyber has overtaken everything. He noted that there are still remote regions where things have not been fully automated, and Internet access is intermittent. This may be seen as backward, but it may also be an advantage against those of us who are fully dependent on cyber systems.



OPPORTUNITIES TO LEARN MORE

Bochman recommended taking part as an observer in the GridEx exercise, or reading their after action reports available online at: www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx

If your organization depends on electricity, these exercises provide a great utility of information.

He used the electric grid as an example of the way cyber technologies have changed how we do things. He said it used to be very static, but now there is new technology being put out at a rapid pace. There are unique threats to the grid as well. For example, the end users--utilities--are not the primary owners, but they are still plugged into the grid.

All our critical infrastructure depends on the electrical grid. However, you cannot have electricity without your cyber systems.

In individual organizations, dependencies include the people there today, everyone they work with, and everyone who is dependent on their organization. Each organization needs to recognize what key applications they couldn't do business without. For example, what befalls Windows often befalls your organization. On a larger scale, the military is very GPS dependent. He emphasized identifying the technology needed for business and exercising outages to improve preparedness and system restoration.

Mr. Bochman called cyber security a post-security world, meaning that we have come to accept that the systems cannot be protected completely, and have probably already been compromised whether it has been identified or not. Instead of devoting our efforts to all-around prevention, he emphasized the need to draft response plans, build systems that can withstand an attack, and segment data to prevent losses.

When it comes to the large energy utilities, security is well funded and staffed, and while there is always room for improvement, incident response is strong. They know their plans well, and their gaps and weaknesses. Energy is one of the only sectors with mandatory security requirements, which improves the ability to gain buy-in.

The same cannot be said for smaller utilities. There are many in Idaho, and throughout the country, which suffer from weak or non-existent security or cyber staffing. They outsource much of their IT. He emphasized the need to know cyber security basics even when outsourcing IT because it allows you to better understand your own risk and who is absorbing the liability.

Scenario Driven Table Discussion

Each table discussed cyber outage scenarios and the impact they would have on operations. This fast discussion was meant to spark ideas about interdependencies and prepare participants for the next year, when IBHS will host a cyber exercise.

Scenario 1: Internet is out for 4 days at all locations

After short discussions, each table shared the content of their conversations with the room. There were some questions about the scenario. Firstly, they wanted to know why the Internet was down and whether they could do anything to respond. They also noted that there may be options to reroute their traffic to other locations of providers. They emphasized the need to communicate with customers. It is important to identify what services were critical--reminding the audience that perception is important as well, so getting services back online that the customer sees as important is key. Communications were a significant concern for participants, as email is a large chunk of their business. Response needs included radios, portable logistic centers, or alternative locations. Non-essential personnel will be asked to work from home. If the outage affects a large area, or 911 services, police would increase patrols.

Scenario 2: Customer and employee personally identifiable information data lost/leaked and reported by the press.

Step one, according to the discussion: Stop it. Recognize the scope. Do the appropriate fix. Other concerns include the media, meaning businesses would need to engage their public information offices. Citizens will want to know whether their information has been compromised. Legal will also be key, as each organization will have to identify which of the customers and affected and notify them.

Scenario three: Loss of access to most of your data center servers and cloud provided services with 1/3 to 1/2 of your organizations desktops and laptops are made permanently nonoperational. Duration unknown.

Participants agreed that this was a scale issue--if you have a small business it will be way easier; if you're a huge organization then you have a serious problem. If you're small you may be able to start swapping systems around. In a large organization you hopefully have a scalable network and redundant network. The first steps are to identify, isolate, and figure out the scope. This might be a time to escalate up and call in others, like the FBI, to help. Participants thought this scenario was a "how prepared are you" kind of scenario. This tests whether the backups are current, where they are, and how much access you have. Organizations need to know what core things have to be back up quickly. Do you have alternate data centers and can they be brought Online quickly? Scenarios like this are why it is important not to abandon all offline processes--if your system still allows it, you can break out the paper forms. These backups should be part of your plans and exercises.

It's Not IF, It's WHEN, You Need to Know HOW - Protecting your organization featuring Russ McRee, Director, Threat Intelligence & Engineering, Online Services Security & Compliance, Microsoft

TEST YOUR OWN VULNERABILITIES

Shodanhq.com: Use to expose your online facing devices and identify what kind of information you're providing Online.

Sourceforge.net/projects/spiderfoot: SpiderFoot is an open source footprinting tool that obtains a wide range of information about a target, such as web servers, netblocks, e-mail addresses and more.

mimikatz: A process for identifying clear text passwords on Windows

Mr. McRee emphasized throughout his talk, the need to use the same tools hackers do on your own system in order to increase your ability to protect your systems and understand what information you're unwittingly making public. He said his organization now works under the assumption they have lost something. Without question, there are always evil people looking to exploit weaknesses.

Mr. McRee walked participants through what it would look like to pick a target and attempt to infiltrate them. Hackers look for a variety of vulnerabilities, and intentions vary from are trying to steal data to using your bandwidth.

There are many different kinds of hackers. This may include highly-trained people completing state sponsored projects; idealists acting on principals; professional mercenary; commercially motivated hacks for intellectual property, malicious employees, or any variety of other motivations.

The greatest tool for hackers continues to be social engineering. However, there are other methods for reconnaissance. You can learn a great deal through search engines and social networks. Through Facebook and Twitter alone you can build a profile that would give you a 70% greater likelihood of guessing the answers to an individual's security questions

There are also online tools for learning about a company and its network. He recommended use of www.shodanhq.com. This will allow you to see what sort of information you're leaving online. For instance, META data--if you're not scraping this off files before posting it online, you may be giving away information about your network, your contact information and other information that could be valuable for hackers. People make it optimal to attack them. For example, "LinkedIn" job descriptions often include detail that explain what kinds of systems and security you are running. Run these searches on your own organization and employees, and be aware of what kind of information you are leaving out there. Are your employees well trained? 50% of people are using the same passwords across multiple platforms.

"SpiderFoot" is a tool that goes through every exposed resource. This allows you to see what part of your network map is available online. Check your defenses. Map yourself. Regularly assess your exposures – are you running services unnecessarily? What system are you using for your website? For example, plug-ins for "Wordpress" sites are often created by third parties. Their lack of coding skill could leave your site vulnerable.

He showed how he would use the tools he had outlined to learn about a company, and then exploit that knowledge.

Asymmetric Resilient Cyber Security Initiative featuring David Manz, PhD, Senior Cyber Security Scientist, National Security Directorate/ Secure Cyber Systems, Pacific Northwest National Laboratory (PNNL)

PNNL's missions are national security, energy, science, and environment. National labs are kind of the bridge

between industry and academia. Cyber analytics provide a high level view of the network.

There are many challenges for cyber security. For example, the internet is anonymous, and that presents challenges tracking back to the culprit. This is primarily an issue for forensic evidence needed for pressing charges. A key problem is between the keyboard and the chair, i.e. people. However, it isn't as easy as saying the user is to blame. Perhaps the developer is to blame.

When it comes to cyber, you need to understand how it impacts your mission and operations. He noted that if the goal is keeping the lights on, that isn't really a cyber issue. You must understand your own domain. 80% of all attacks are simple, easy to address; the other 20% are major and hard to tackle. Do not let your adversaries know your domain better then you do. Learn your networks.

Even in your own simple environment, for example all the IP enabled devices in your own home, there can easily be nine devices. What are the cyber assets on your more complex network?

In cyber we are always hypothesizing about the future, which makes our predictive ability woefully inaccurate. Enhancing this ability is what PNNL is trying to so, as a means of moving the advantage from the attacker to the defender.

Bridges were built before science, but we now have science which allows us to build better bridges depending on their use. In Cyber, the bridge is built of many materials, users are using it in ways you could never understand, and there are holes. We have defend not against normal use cases, but the resources of attackers.

We must look at the entire system in context. This is how you build resilient and robust cyber network defense. Through asymmetric cyber security, you can enhance resilience and robustness, while disproportionately raising the cost for the attacker. In this way, they are developing a fundamental science behind cyber security to create better cyber technologies.

Practical Cyber Security and System Resilience featuring Bob Timpany, Chief, Idaho Operations, NCCIC-ICS-CERT, US Department of Homeland Security

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides resources for improving the cyber security of your organization, like lists of proactive steps, training and self-assessments. They also provide incident response, technical analysis, vulnerability coordination, and situational awareness once you've been hit. The majority of the incidents they respond to, they are the ones informing the victim.

Industrial Control Systems (ICS) are the link between the cyber and physical worlds, where you translate cyber ones and zeros into the actual execution of complex processes. In the past this was totally isolated, but this has become more and more integrated across networks. There are ways to limit the access into the environment; however it is more likely that we are working on ways to open it up, which increases risk. For instance, if you're opening up connections to mobile phones, that is not a best practice.

Mr. Timpany explained that there at millions of Internet facing devices. It is challenging to mitigate potential incidents because you can't track who the owners of all those devices are. A lot of this is Heating, Ventilating, and Air Conditioning (HVAC) systems.

There have been malware campaigns against control systems. This is possible sometimes because people leave the structure of their control systems available Online. Some systems are accessed through computers that also have outside access, and interface with the web servers, which can be a method for infection, ICS is complex and their reach is often outside of the IT world. In the data world you are scared to patch because of the possible effects on

the end process.

To strengthen your cyber systems, you should ensure an awareness of your environment, enhance network segmentation especially from ICS, harden remote access, control your users, reduce/eliminate internet connectivity and routing to the internet to/from the ICS. Try to do your remote access from a static IP, which can help identify whether the people remotely accessing the system are approved. He emphasized segmentation, saying that just because someone can get into your control environment doesn't mean they can affect your systems.

He recommended the development of an ICS cyber incident team. Their role would be to plan, prevent, detect, contain, manage, re-mediate, and recover. Do a training that is about the ICS systems and red blue exercises.

ICS-CERT has self-assessment tool kits they will send to your organization. These kits are free for critical asset owners. More information on ICS-CERT resources can be found at ics-cert.us-cert.gov

Lastly, he recommended you make connections to information sharing, join groups that have to do with you, sign up for public alerts and portal accounts. There are many online courses that are free and will help raise your awareness.

Panel: Cyber Security Across Sectors facilitated by Megan Levy, Program Manager, Pacific NorthWest Economic Region featuring Greg Zickau, Chief Technology Officer, State of Idaho; J.R. Tietsort, Chief Information Security Officer, Micron Technology; Reid Stephan, Director, IT Security, St. Luke's Health System and, Vince Skinner, AVP of Security, Dadco

What are the most important factors to take into consideration when building a cyber security policy for you organization?

Panelists each gave insight from their own organizations. The highlighted the need to share data with partners and suppliers. It is important to identify what other agencies and organizations you should partner with, and build closer ties with the government and private sector. Cyber security policy needs to be built with IT, policy leads, and operations. Policies must be continually reviewed and updated. One popular update, is the integration of the network as part of the overall security picture. As with physical security, it is important to understand your assets and prioritize them. It may be equipment, intellectual property, personal information, or other key data sets. They noted that businesses big and small are feasible targets.

They also highlighted the need to define compliance in cyber. There was an acknowledgment that sometimes policy was crafted to suit policy requirements, to pass the audit, but not used otherwise. This doesn't lead to the most realistic assessment or robust.

How do you get buy-in at all levels of your organization for cyber security?

Some people only get religion after a near death experience. Having a problem leads to some corrective measures; however, cultural change on security can be difficult. This leads to a lot of questions like "why can't we do things the way we have always done them?" To get organization buy-in, you must have executive level support. Over time you build trust which you can leverage for security. Now is a good time to be a cyber security

professional--stories come out every day in the news that highlight the importance of this field. Security and IT need to be brought together to help set the policies.

What mistakes did you make, or concerns you took into account that you would recommend other's consider when developing or revising their plans?

One of the greatest challenges is that people want to eliminate all risk, however you can't get any wins if you don't take any risks. Change can be seen as a threat or an accusation against employees; you have to start first on changing the culture, and highlighting how that change will positively impact the organization as a whole. This really comes down to being willing to listen to candid feedback. Once policy changes have been implemented, you must train your staff. You can't hold employees accountable if they don't know what the policies are. The change will take time to be adopted. The business functions need to be the ones accepting the risk—it is not yours to do for them. Explain the risks, and allow them to decide.

What are you doing to increase employee awareness?

Panelists suggested using a commercial service to look for phishing, the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. There is good information on the success of such efforts. Over 40% of all employees were captured the first time. Spear, or victim specific, phishing dropped to 20% the second time.

Participant Discussion: What keeps you up at night? What issues need to be explored for the resilience of Idaho? What issues or interdependencies should we discuss in the future?

Participants said it is a blessing and a curse, but they haven't experienced that many attacks. This proves to be a challenge, raising the question of how to build leadership on preparedness when they never practice response. There is a great fear of not being able to identify what it is you don't know. Institutional knowledge poses a threat. They expressed concern about the physical systems that support their cyber systems, like fiber optic cables. They expressed doubts that telecommuting after a disaster would be as easy as they were assuming.

Panel: Regional Capabilities, Tools and Resources facilitated by Eric Holdeman, Director, Center for Regional Disaster Resilience, Pacific NorthWest Economic Region featuring Dan Goicoechea, Chairman, Idaho Technology Authority; David Matthews, Chair, Cyber Incident Response Coalition and Analysis Sharing (CIRCAS); Bob Timpany, Chief, Idaho Operations, NCCIC-ICS-CERT, US Department of Homeland Security

Emergency management and physical security are growing together, and the same is happening with IT and physical security. How do you see these being integrated and working together, and what resources do they share?

There is a lot of discussion how to integrate cyber into the ICS physical security, however this creates a world where cyber has a physical consequence. It's very important that you know who has access to your facilities both cyber and physical, and run background checks. You can't just hope things will turn out okay, you have to build policy that encourages it. And yet we override those policies every day when we let a trusted vendor onto the network who hasn't been through a background check. There are opportunities here as well. Physical security can be allies--teach them what a rouge wireless router looks like, or where flash drives should not be in a computer.

This also requires buy-in from the organization. We need to identify what each of these elements is costing us, and from there the cost/benefit of each of these issues can be identified. Risk assessment/management should be first. Looking at all the different risks, threats, likelihood then identifying how much is it going to cost and how to prioritize with all other risks. Cyber security must be part of the risk management organization in the entire picture. It has to be a risk management decision. In any organization there will be competing priorities, budgets

and needs. In government this poses a different kind of challenge because if money isn't spent within the year, it's gone.

How can IT Security professionals and small businesses learn about emerging threats and share in a circle of trust?

We want to be able to share information, ideas and resources. However, you have to start by building a trust relationship. It is important to meet the people you want to work with in person; sit down and talk to find out what opportunities and hurdles you face. This is how you can establish ongoing partnerships. If you are on the IT side, make sure you sign up to the US-CERT portal, FBI, InfraGard or one of a number of private sector entities. There is a lot of stuff out there, but it's worth exploring and identifying who on your teams should be involved. We owe it to our community to share information, and not assume it is a one-time attacks or is an issue facing only our own organization. There is safety in numbers, but you don't want your organization to be the weakest link. However, you can't ask people to partner with you if it's going to compromise their mission; you must make it safe for people to share with you.

Next Steps – Developing a statewide public/private partnership facilitated by Brandon Hardenbrook, Deputy Director, Pacific NorthWest Economic Region

Resilience is built through relationships, trust, sharing information and understanding own your interdependencies. Resilience in cyber security is based not just on technological solutions. Our end goal is to share information, establish relationships, understand interdependencies, and build trust. This tautology to the left shows the way resilience is built. It can only exist with all four elements feeding one another.

This meeting is the first step in forming a public/private resilience partnership in Idaho. Over the next three years, the main objective to develop an action plan for this partnership. An example of a task on that action plan might be the development of a cyber security check list for small/medium size organizations. However, the focus of this project is everything across the board that relates to disaster resilience, not just cyber security. The chart on the right summarizes the three year project timeline and activities.

2014	2015	2016
Year 1 Workshop	Year 2 Exercise	Year 3 Action Plan
Hold a "kick-off" interactive workshop to raise awareness and facilitate networking	Enable key stakeholders to design and conduct an infrastructure interdependencies tabletop "exercise".	Based on the Exercise Report, work with stakeholders to develop a prioritized Action Plan of activities for inclusion in existing preparedness plans

Closing Remarks featuring Brigadier General Brad Richy, Idaho Bureau of Homeland Security

Idaho Bureau of Homeland Security needs to know the private sector better to learn their priorities and concerns, get to know their emergency managers, and identify how to help organization become more resilient. IBHS wants to know about emerging threats and concerns, and facilitate information sharing. By knowing one another, we all become stronger.

RECOMMENDATIONS

Based on the presentations and discussions, the following recommendations and findings were developed to help participants bring the lessons learned from the day back to their own organizations.

- Educate employees at all levels of an organization to understand the role cyber systems play in their business--how much and what kind of data is stored there, what they impact, and how they help them to complete mission critical tasks--as well as their role in keeping those systems secure and functioning.
- Integrate cyber security with physical security as part of a company-wide security integration.
- Utilize resources to check your policies and train your staff. The FBI is willing to provide briefings, and ICS-CERT has self-assessment tools
- Develop a cyber policy, train your employees in it, and develop performance measures around it.
- Identify your mission critical systems and simulate system outages and how to respond. Identify ways you could segment these systems from the remainder of your network.
- Use the same tools as hackers to test your system. This might mean incentivizing employees to find security gaps, or performing cursory research and hacks on your own systems.