Emerald Down IV

Puget Sound Cyber Security Workshop

March 5, 2015 | The Event Center at Emerald Downs | Auburn, Washington

After Action Report and Improvement Plan
May 1, 2015

CRDR
Center for Regional Disaster Resilience

King County

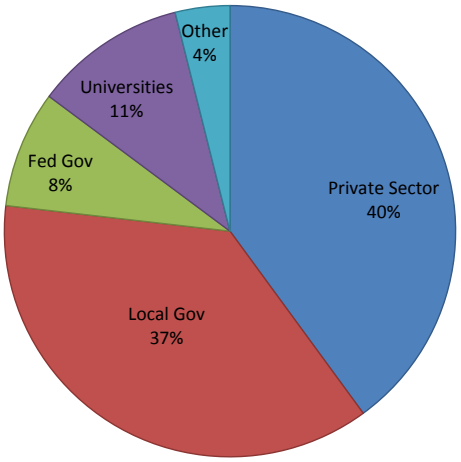
Contact:

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 260 participants gathered at the Event Center at Emerald Downs in Auburn, Washington on March 5, 2015, for the Emerald Down IV: Puget Sound Cyber Security Workshop hosted by King County Office of Emergency Management, with assistance from the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR).



Participants came from a variety of organizations as shown in this breakdown of registration

The one day workshop provided an excellent platform to engage the public and private sectors in learning more about current cyber threats and mechanisms to integrate information technology and physical security. Guest speakers, panel discussions and a scenario based discussion contributed to a very successful workshop.

The event was developed over the course of six months through a series of conference calls and meetings. The planning team included local public and private sector organizations, including: MK Hamilton Associates, Pierce County, the City of Bellevue, Microsoft, Puget Sound Energy, the City of Seattle, the University of Washington, the City of Kent, King County Office of Emergency Management, Seattle City Light, Seattle Department of Transportation, Kent Emergency Management, Seattle Emergency Management, SnoPUD, the Port of Seattle, and the Washington State Military Department Emergency Management Division.

Participant feedback was overwhelmingly positive with 89% of respondents rating the event as very good to excellent. Some of the key takeaways for participants included the importance of collaboration and partnership between all players in dealing with cyber issues. Also noted was the necessity of adaptive management theory to address the complexity in cyber threats, where a diverse group of interests are at play. Many participants emphasized the need to improve their incident response plans, and to integrate physical and cyber security. Participants also noted the importance of bridging the gap between company policy and best practices, recognizing that adherence to the minimum standard of cyber protection is accepting too large a risk. Many participants also recognized the need to better understand where their organizations stood in terms of restoration policy, and how their existing emergency controls operate.

A number of recommendations for the region came out of the discussion. It was clear from the discussions that there was need for greater access to resources throughout Puget Sound. Many organizations are now sharing information, but don't know the full breadth of their options for gathering or disseminating information, or building better plans within their organization. There were a number of examples of how to test plans and systems, but participants haven't had many opportunities, thus a exercise was suggested to help test plans and partnerships. Lastly, the importance of cyber to other systems has increased the recognized need to integrate cyber concerns into non-cyber exercises and planning.

This event was the fourth in a series of workshops designed to engage the public and private sectors in learning more about cyber security issues, creating new methods of collaboration in dealing with cyber threats, and discussing ways to integrate information technology and physical security.

Background

Over 260 participants gathered March 5, 2015 at the Event Center at Emerald Downs in Auburn, Washington for the Emerald Down IV: Puget Sound Cyber Security Workshop hosted by King County Office of Emergency Management with assistance from the Pacific NorthWest Economic Region (PNWER) Center for Regional Disaster Resilience (CRDR). The event was the fourth in a series of workshops meant to engage the public and private sectors in learning more about cyber security issues and ways to integrate information technology and physical security.

Over 260 participants from throughout the state of Washington took part in the full day workshop that included scenario driven discussion and presentations from Cyber security experts.

Presentations

Welcome featuring the honorable Nancy Backus, Mayor of Auburn

The Mayor provided welcoming remarks and thanked the audience for attending. As the internet evolves, more devices are connected which increases threats. It is critical to make sure we are taking good care of information entrusted to us. She thanked all the participants for taking part in this event, encouraging them to stay awake, stay alert, and be secure.

Opening Remarks featuring Eric Holdeman, Chair, Region 6 CIP Committee

Following a safety briefing, Holdeman explained the agenda for the day. Funding for this event came through King County. There is increasing activity around cyber security, including more education programs, and a greater focus on the issue from State emergency management, especially with new staff.

The Importance of Partnerships featuring Linda Gerull, IT Director, Pierce County

"It's not about data anymore; it's about influence and power."

In a natural disaster, when law enforcement, fire, and emergency management provide a response, they get together afterwards to learn about what they could do better. Linda Gerull expressed the importance of doing just that for cyber events for the attendees, emphasizing the role partnerships can play in increasing cyber resilience.

Pierce County has a fairly complex system. She explained that five years ago, they experienced a dedicated denial of services (DDOS) attack that took the system down for an hour but was easily fixed. Last month, a law enforcement incident in Pasco, Washington provoked an attack by Anonymous which affected Pierce County because they share the same server. Their government jobs listing website experienced problems indicating a DDOS. A minor amount of data was mishandled but it wasn't lost. She used these examples to emphasize that data access was not the only aim of cyber attacks. It's not about data anymore; it's about

influence and power. The concern used to be protecting information online; now the concern is that people who are upset about a government policy or court cases are using cyber means to protest and can cause havoc on infrastructure remotely.

This makes it all the more important to build partnerships and work together. She recommended building communities of interest, noting that Pierce County has partnered with a number of organizations in the room. She encouraged participants to participate in the day's conversations and use the dialogue to drive recommendations for improving their own systems, and direct assessments and milestones. She added that conferences like this one are a huge help in identifying partners and bringing them all together so we can collectively stay ahead of the hackers.

In cyber, the stakes are high--attacks can be a matter of life and death, not just an issue of a website being taken down. We are hearing more and more about cyber security attacks and concerns of an increasingly hackable world known as the "internet of things." She asked: Could somebody hack your pacemaker? What are new models for delivery like software as service? Are engineers trained and ready? Who has templates for recovery after event? Who has templates even to analyze that you are under an attack? She expressed her enthusiasm for meeting everyone in the room and hearing about their experiences.

The Intersection of Cyber Systems and Physical Infrastructure, featuring Alisha Griswold, Training and Exercise Program Manager, King County Office of Emergency Management

"Cyber security and information security are only as good as operational security."

Griswold began with a ground rule: Hackers are not your enemy. It's not about the act, but the intentions. She explained that parts of the presentation were based on research from Poneman Institute on operational penetration testing. They were extremely successful: Just by wearing a badge, their team could get access to sensitive information. They were not questioned by peers, were able to rummage around other's desks, look into open laptops, review open event calendars, and gain access to mobile devices, USB drives, and keys that were unsecured. We emphasize firewall, but cyber security and information security only as good as operational security. We have to balance security and access.

She shared the Kaspersky cyber security map showing cyber attacks in real time. The U.S. is third most attacked country during the day, and number one at night when the other side of the world is awake, where the majority of our attacks come from.

Griswold explained that there are a lot of legacy systems in fields like transportation and utilities that are being brought online for convenience, though they are old systems not designed for the internet. She referenced Gerull's mention of the "internet of things," the networking of physical objects, such as refrigerators, meant to increase efficiency through accessibility on the existing internet system. This can increase our vulnerability--for example hacking into things like doggy cams, which are meant to let people check on their dogs when they are away from home. Anything on the internet is accessible if not secured.

Griswold played a video of the Aurora Generator Test showing the real world physical impacts that can come from cyber attacks--in this case the complete destruction of a generator cause by a malware directive to overload itself. For this test they destroyed the generator, but Griswold emphasized that impacts need not be as extreme. If a cyber attack caused a machine to corrupt in increments or at a slow rate, the machine may be functionally unusable without damaging it enough to flag its owners that they were under attack.

Resources and Links

Kaspersky realtime cyber security map:
https://cybermap.kaspersky.com/

Aurora Generator Test (Video):
https://youtu.be/fJyWngDco3g

Shodan Search Engine
https://ics-radar.shodan.io/

As a tool for participants, Griswold shared the Shodan search engine. She explained that the displayed map of the globe on the Shodan front page showed industrial control systems that were accessible online. This kind of tool is useful when working with executives because it quickly displays information without a wall of text.

With more and more of our systems becoming accessible on the internet, critical infrastructure can now be attacked physically or electronically. Griswold emphasized useful tools available through the Department of Homeland Security for assessing your organization's risk. Self-testing of systems is essential for protecting assets.

Griswold explained that the threat isn't only to our our infrastructure systems. During the Carlton Complex fire, the largest fire in Washington state, network security measures were an essential part of response. When disasters occur, people can try to take advantage of the distracted staff to gain access, redirect folks who are trying to get key information, or prevent mission critical traffic.

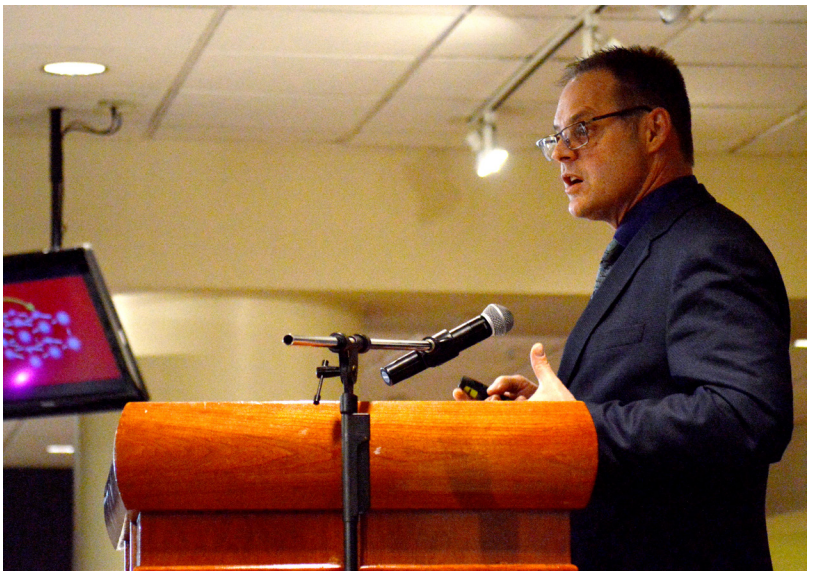
Cyber threats are not cyber alone--they can also be used to access physical systems or create real world consequences. These threats are real, and are already happening to businesses across the world. Every stakeholder in a business has a role to play, not just the IT staff. In fact, Griswold said, holistic approaches are the most impactful. Now is the time to train all staff in what to look for, when to raise red flags, and how to make good decisions.

James Rollins, Managing Partner, Takouba

"The best way to approach complexity is through adaptive management."

James Rollins spoke on the possibilities for using simulation to better understand the intersections between cyber and physical infrastructure. He began by highlighting the complexity, not only of this task, but of our every day lives: The information industry promises us everything from instant access to our data, to a three-minute response to a 911 call, to any entertainment we desire such as games and movies – on demand! The systems that deliver these services are complex. And complexity grows exponentially when overlaid on terrain, political and infrastructure topologies and interface with dynamics created by human populations.

Rollins said he believed people were happiest when they can problem solve. Through models we can do this, without relying on intuition, making decisions in an environment without the real world consequences. Cyber security is a complex issue and we are barely scratching the surface. Success is dependent on effective collaboration. So how do we develop that? How do you build effective partnerships? You need working knowledge.
Moving back to the concept of complexity, Rollins introduced the Complex Adaptive Environment, or the model ecosystem where participants can engage in decision making. This ecosystem helps people understand the complexities of their systems, how to adapt, and how to deal with surprises.



James Rollins explained to participants how to use modeling to learn how decisions made about complex systems like cyber will result in real-world consequences, prompting participants to include the need for greater regional exercises in their recommendations

Complexity can be thought of as layers, each interacting inside and in between each other all at once. Different non-linear relationships create complex environments. On the first level you might have roads, the second level up is the people using those roads that have decision making capability. They move through and interact with layers on lines of gender, ethnicity, and need. It's difficult to predict individuals, but these interactions can be used as the basis of crowd modeling.

He then explained adaptive management theory in relation to rational management process. Adaptive management is more collaborative with people coming together for decision making that don't have habitual relationships. There is great diversity in the group. It depends on communication. This planning style is necessary, because of the diverse group of interests, authorities and resources that are drawn to a single purpose – problem solving. This is a "just in time" planning strategy. The whole thing relies on experimentation and operational cycles and the trust factor. Why do we partner? So we know the people we are working with, so we know they have integrity, and so we know they can be relied on and have the support of their agency. We create this trust through using an effective decision space. A decision space is basically a safe place where people can come together.

There can be a disincentive to collaborate: a selfishness, where people don't want to have to share their resources with others. We need to know that our investment in collaboration is going to provide a benefit. If an organization can plug into a model and see some futures, it is more apt to make the investment having seen the outcomes. This play is essential to greater understanding of our partnerships.

We need to be like kids playing with blocks. Through play, kids are learning how to adapt to their environment but also learning about collaboration.

For collaboration and partnerships, each of us needs to do it over and over and over. We don't practice enough. Even tabletops are challenging to get on everyone's schedule to coordinate. In a simulation we can push a system to the breaking point, but without bringing people together, we can't really explore responses to a confluence of events. The best way to approach complexity is through adaptive management. We need to get in habit to do it more often. We need to learn how to play with blocks and practice putting stuff together again in an effective manner.

Panel: Physical Infrastructure, Cyber Systems, and our Region's Resilience, and John D. Schelling, Earthquake, Tsunami, and Volcano Programs Moderated by David Matthews, Chair, Cyber Incident Response and Analysis Sharing (CIRCAS)

Each of the panelists began by explaining their position and how they work with cyber and physical infrastructure.

David Holcomb, Protective Security Advisor, Seattle District, Office of Infrastructure Protection, U.S. Department of Homeland Security

David Holcomb explained that he is mostly focused on physical security. In the last couple of years, transportation, communications, water, energy have been defined as the lifeline sectors. These critical infrastructures all have a level of security to protect physical and cyber assets inside.

He noted that through thinking about cyber in the same way as physical security assets, he has come to realize the importance of protecting cyber assessments. The data needed for physical security is being analyzed and transmitted in the communications system.

There are 76 protective security advisors across the country, and ten regional directors. It is a pretty incredible information network. He recommended the audience look to partner with groups like ICS-CERT that have training tools, and are willing to come in to help. He noted that one of the benefits is that they don't take your information with them.

All security systems run on a backbone of communications. It's a symbiotic relationship. When talking to IT professionals during assessments, we ask about both physical and cyber security plans. Often these are weak areas or low hanging fruit that can be fixed by providing standards and guidance. He emphasize that it's not just having a response plan, but they look to see if there are training and exercise plans. He said he sees many facilities without security plans of any type.

From left: John D. Schelling, WA State EMD, John Adams Roach, Global Business Analysis, Lawrence Eichorn, Seattle Department of Transportation and David Holcomb, DHS address the interdependencies between cyber and physical security.

Lawrence Eichorn, Seattle Department of Transportation

Eichorn explained that with cyber security, there have been some vulnerabilities that are worth checking and keeping in mind, because they are easy fixes that can increase protection. He said one of the top vulnerabilities he sees is when a vendor installs equipment like routers but they don't change the factory installed password.

The City of Seattle has 1,070 traffic signals. If they were infiltrated and damaged, he said, it is hard to fathom the gridlock that would happen in Seattle. It would take 18 days to fix. That's billions of dollars lost. That's some real incentive for a bad actor to get in and do bad things."

Eichorn stressed the importance of infrastructure and fiber optic cables and how to go about fixing it when it breaks. It is not as easy as just fixing the cables, he explained. After the helicopter crashed in Seattle last year, fuel spilled into a communications vault. However, there was no certainty as to who owned and managed the infrastructure. He had to call five service providers to finally get someone to come and open the vault. There are hundreds and hundreds of communications vaults in Seattle. That is why it is important to have an understanding of cyber infrastructure, transportation infrastructure, hard infrastructure and how these impact the whole system.

John Adams Roach, Corporate Counsel, Director of Cybersecurity, Global Business Analysis

Roach explained that while cyber security is an emerging issue, it is one of incredible importance to the aviation industry. In aircraft cyber security, all the areas of security are also areas of vulnerability. On airplanes, cyber disruption is physical disruption. Airplanes have several layers of complexity; Complexity is an enemy of security. There are lots of threat vectors--for example, the computer chips used for managing the computer. In the past the discussion has been about how to secure hard infrastructure to protect cyber systems; Now we are trying to secure our cyber to protect hard infrastructure.

Disruptions to air traffic infrastructure mean delays, lost productivity, and lost dollars. In Istanbul, a passport verification system went down and planes were grounded for hours.
There are also threats to intellectual property. From a windmill maker in Massachusetts who had his business stolen to reports that China stole plans for the U.S. F-35, cyber espionage and terrorism is a growing threat.

The hardest then to accept about cyber security is that there are no solutions, no silver bullets. We will never have 100 percent security because it's impossible It's too expensive. Even if we could, no one could get any

work done. Instead we need to work together. We are working on sharing intelligence but there are lots of hurdles to get through. We are not where we want to be yet. So what are the options?. We have to allocate smartly to do the best we can with the resources we have--everyone is struggling with this, from the federal government to the private sector. We must know who is in charge and how to escalate issues ahead of time, not just as a plan, but as a clearly mapped flow. Normally the teams working together will have never met before, but with events like today's we can bridge that gap.

John D. Schelling, Earthquake, Tsunami, and Volcano Programs Manager, Washington State Military Department Emergency Management Division

Over many years, partnerships have been built in the Northwest to address response and recovery from a major earthquake. There are a lot of similarities between geologic matters like earthquakes and cyber security. Both can happen without notice or warning and can be devastating with long lasting consequences to business, environment, and infrastructure. Small cyber breaches and small to moderate earthquakes can be precursors to something bigger, but we only learn this after the fact.

It's clear that there are significant interdependencies between critical infrastructures, no matter if the disturbance is man made or natural. It is important to consider these cross-connections, and exercise the existence of these vulnerabilities.

The Washington State Emergency Management Division has begun to schedule regular exercises around nuclear issues, using injects as a way to strengthen our understanding of reality to our world. We should be integrating cyber injects into all exercises. When we do have significant earthquake, there are going to be cyber attacks.

Questions from the audience:

Q: What are your recommendations on background checks for people already checked once?
A Set time frame like 3 years or 5 years. or some other requirement when you see fit. It is an option to do periodic reviews for only those people operating critical systems.

Q: What is a good standard time line for audits?
A: This will be different for every organization. Through audits we are able to mitigate the easy items. A key thing to remember with audits is that they are not effective if your organization is only doing it to check a box--that makes you compliant, not secure. Instead, they are a chance to review your governance and assess risks.

Q: What is the biggest risk in unintentional insider threats?
A: Background checks are the first layer of protection. Avoiding unintentional information breaches means training people in how to manage data and emphasizing how sensitive data is. We often think about threats as an outside thing trying to get in, but we need to remember good standards and practices within our organizations.

Q: How do you communicate these issues to the executive c-suite and elected officials?
A: You have to frame it in terms of what is most important to them, and that's money and cost. If you can prevent lost revenue which costs money, audits, and staff time, that would be valued. It's key to show what the savings look like, and why it is important to be able to quickly mitigate issues and restore service. If every outage costs 1.8 billion dollars a day, and you can reduce down time from 18 days to 9 days that cost avoidance is income made for the organization.

With recent media attention, there has been more emphasis on cyber security in organizations. However, there isn't enough public pressure to make an organization pursue cyber security programs--people are still shopping at retailers that have experienced major hacks.

How these hacks translate into lawsuits will be another key issue to explore that will be of interest to the c-suite.

Scenario based discussion moderated by David Matthews, Chair, CIRCAS. Exploring the cross-section of cyber and physical security, dependence on fiber optics for connectivity, and the integration of business continuity with cyber response.

"Working in our silos, and agreeing with ourselves is dangerous"

Participants discussed two scenarios with their table groups, and then shared key takeaways to the room as a whole.

Scenario 1: Every day operations, attacks and outages.

Participants emphasized the need to know, train and improve plans, and understand where their organizations stood in terms of restoration priority. It was noted that there is a difference between a company policy and best practices, and that adherence to the minimum standard is a trap.

One organization explained that their network infrastructure is supplied by headquarters, which represented a point of failure in the case of severed communications lines. Knowing these vulnerabilities is the best way to find solutions for working around them.

Scenario 2: Cyber outage due to loss of fiber optic cables

Participants stressed the importance of redundancy in capabilities, including staff. For example, there is redundant cable running across the Ship Canal Bridge, but if only one person from the city knows that, and that person isn't available, we won't be able to utilize it.

During Oso, the cable was cut and commercial companies were wonderful in stringing an usable communications system together. So we can rely on commercial operators.

Participants used scenario questions to help discuss their internal planning and possible gaps in understanding regarding their partners and pathways for gaining information in cyber security events.

Dave Holcomb suggested the creation of a lifeline infrastructure coordination council, creating buy in at every level from the state, similar to a project in Utah. Initially, they did regional resiliency assessment in Salt Lake focused on public health. The goal was to look into life critical areas and report back what information is being shared and common knowledge gaps in the state and local jurisdictions. As part of that, they already started reaching out to the counties and identified what they thought critical infrastructure was. State transportation staff laid out geospatial routes. As they got the data from counties they started seeing gaps. They reached out to communication sectors, for an assessment of where their infrastructure was placed. Once the maps were created, they found that 80 percent of critical infrastructure was along state routes. This made it clear to the state where they should focus efforts after a disaster. Often the commercial operators just want the roads clear so they can make repairs--this will give a better idea about what roads need to be cleared.

Luncheon Keynote, featuring Matt DeVost, President & CEO, FusionX

"Cyber security is not about eliminating all risks but managing them in context."

How can you sleep with all the nightmare scenarios? You manage them. Devost explained that Fusion X does planning at the tactical level, doing red team consulting. This encourages thinking about the threats in terms of your adversaries: what are their objectives and goals, what are their incentives, what data and systems would they target to meet these goals, and what will be the impact that their current tactics, techniques and procedures have on your system. Be prepared to secure yourself from those within your organization, as well as attacks from the outside. To understand your adversary requires a deep understanding of your own organization. To plan, you must know what would be catastrophic for your own organization, as well as your vulnerabilities. This will help you find focus: are you trying to protect everything, or are you focusing your efforts to protect only your most sensitive systems and data. If you're trying to protect everything, all information becomes equally vulnerable. Thinking about cyber security as a perimeter around your systems is a thing of the past. Instead, we must operate on the assumption of breach. Security should focus on pools of aggregate risk.

Cyber security is not about eliminating all risks but managing them in context. There are no silver bullets or magic tech that will prevent cyber breach, but there are silver concepts.

Firstly, it is important to establish metrics. This means collecting data that will frame your understanding of your security stance, like how many incidents are reported, how much time it takes to detect an attack, and how efficient is your response.

Secondly, have a plan and exercise it--don't just punch the punching bag; practice in the ring. Following the metaphor he noted that you won't be able to decide who your opponent will be in the cyber realm. For this reason, it is important to practice cross-silos and test your plans.

Historical lessons are important to capture and learn from in helping us make predictions, giving the ability to manage from future not just the past. Post-stuxnet, we now see that critical infrastructures are fair game. We haven't had any real cases of impacts to critical infrastructure (CI), but that doesn't mean they aren't being targeted It only means those that are comprising CI systems don't have intent. We can prepare now for CI attacks that might still be 5 to 10 years down the road. Our adversaries are innovative and defense technology is not keeping pace. Destructive attacks will continue to happen. We must examine the future intent that might exists in the attacks of today. He gave the example of the attempted attack on the World Trade Center in New York in 1993 The plan was to detonate a radiological device at surface level with the target of taking financial services offline. Lessons from that failed attacked drove resilience and planning for the September 11 attacks in 2001.

He explained that the information we make available changes our security. Hackers can use information on sites such as LinkedIn to collect the information they need to impersonate a person or become friendly with them. This can be used in a range of ways -- from impersonating a person to gain access to finances, to trying to lure people into dangerous situations. Security is only as strong as a well trained staff that understands the best practices for protecting data.

The Evolving Geopolitical Threat Landscape, featuring Dr. Amelia Phillips, Highline College

"There are more devices on the internet than there are people in the world"

Internet was not meant to be secure, but was built as a platform for open information sharing. The way we've chosen to use it has driven the need for security in a system not meant for these measures. For protection, you need to frame the problem: create solutions and look at monitoring. Are you protecting one thing through another thing? How many vendors do you have? Do you trust them? This is a global issue--computer chips

from China have to be cleaned before we put them into our military jets.

We should be coordinating cyber threats at the national level. There has been a lot of push back on this idea because there are concerns about privacy issues. The fact is, we all need to be talking to each other. We can't keep up with the current level of attacks going on. According to CISCO, there are more devices on the internet than there are people in the world. This is growing to include not only the things we think of as internet connected, like phones and laptops, but increasingly the use of smart appliances like our refrigerators or thermostats. Everything is electronic, and 90% of all communication is electronic.
Eight years ago if two companies were negotiating a merger and traded proprietary data in the process, they would only need to wipe the drives if the deal fell through. But now, if that happened, we would need to wipe drives, the cloud, home computer and portable devices. How do we get to that info and make sure it is erased? More of your life is on the cloud. The University of Washington pharmacy is using the cloud. Pacemakers and wireless crash carts are on the cloud. Are we comfortable with that?

When developing defenses, we have to ask: Does it work? Have we tested it? Do we need to have an exercise? Layers of security are necessary. The biggest problem is that people create policy and don't follow them.

Phillips shared further examples of emerging technology that will change the cyber security picture in the coming years:

- Virtual machines: Can be placed inside a thumb drive and inserted into a computer to collect data without leaving proof that information was removed.
- Hacker monitoring: Where hackers access a network in order to leave spyware and track a person or organization, rather then attempting to compromise their systems or extract stored data. As an example, truckers have been tracked via Facebook as a way of tracking where they will make stops. This leaves their cargo vulnerable.
- Drones: Unmanned craft controlled from afar are a growing interest. For example, drone cargo ships: If it's out at see unmanned and a machine reboots because of a hacker, what happens to the cargo?
- Cars: Modern automobiles use computers for managing the majority of their function. She shared an example of a video in which is 14-year-old hacked a car as a demonstration of what kind of access he could gain.

One of the biggest questions arising with this changing technology is the question of who is responsible for protecting data, and who has the responsibility if systems are compromised. Data passes between government, corporations, cloud providers, and individuals. There are many different zones of safety and security--it is a fact of life that there will be a zone you don't have control over.

Current Threats featuring Kevin Brennan, Cyber Task Force, FBI

"It would be very expensive to try to infiltrate a company for ten years to gain access to secure systems; it costs almost nothing to sit in another country sending phishing emails"

Overall, cyber crime is the number three priority for the FBI, which investigates cyber terrorism, state sponsored intrusions, and financially motivated attacks.

We aren't talking about terrorists using the internet for communication but instead the threat of them breaking into infrastructure and disabling systems, causing systems to destroy themselves, or releasing a harmful or noxious substance.

Brennan shared a few examples of cyber vulnerabilities and attacks including: In 2000 Vitek Boden comprised the sewage system in a city in Australia; In 2011, Houston put their water system online rather than pay for a

3rd shift operator, increasing its risk; and the release of the mariposa virus in 2001 on a power plant, delaying relaunch of the plant for three weeks and causing significant financial damage.

It is cost effective to try to attack systems remotely: It would be very expensive to try to infiltrate a company for ten years to gain access to secure systems; it costs almost nothing to sit in another country sending phishing emails. It is very low risk and the competitor doesn't have to invest ten millions of dollars in chips or boards.

A lot of people don't think they have sensitive info. We expect government and military contractors to be targets. We don't expect basic commodity projects to be attacked. For example, law firms don't seem to be a likely target, but patent information may be more easily accessible on their systems the through the paten owner.

Theft of data, and access to CI are only two of the targets. Financial theft is also a key goal. Sometimes this is done with phishing emails and spoof transactions--they can send thousands, and even if only 1% work, the rewards are still substantial. Sometimes DDOS attacks are used as a distraction as they work another end of your security. Unfortunately, if you have been victimized, you are never going to see that money again. We need to encourage IT to track trends and share them with business continuity and other security folks to look for patterns.

What can you do beforehand to help/prevent crime? Think before you click. Ensure you're using secure networks, and sending information to the correct addresses. Usernames and passwords are not enough protection--If a secondary protection is offered, take it up.

All we can do is arrest guys but that cannot bring your money back

An Ounce of Prevention: Preparing Now for Effective Breach Response featuring Sean Malone, Principal Security Consultant, Fusion X

"Whether a breach is in the New York Times or not depends on how well you can detect hijackers and how well you respond in the first 24-hours."

Breach response is the goal: security incidents are going to happen. Instead we have to define what is a major incident? An incident that has potential for affecting the organizations ability to complete its objectives.

We must have multiple controls in place, and for every control ask, what if it fails? How will you know that it failed? These layers of control give the opportunity to detect an attack and gives time to implement response. The first control to be bypassed is the network perimeter -- by now you know that the perimeter is increasingly irrelevant. In fact, a very small percentage of intrusions come from traditional sources. What we have relied on for security before shouldn't even be considered a line a defense. For example, a domain administrator account is not hard to access -- it's just one more username and password. Assume that this control has failed because it will fail. In 90% of assessments Fusion X does, they get access into the domain admin account within in two days.

In building your plans, you must review your controls, factors of authentication, and information silos. Monitor usage of highly privileged accounts, and audit the accounts on your system, including login success and failure records. Know how quickly changes can be made to the system as a whole from a domain admin account. Malone explained that as an attacker, as long as he has one account left, he can go back in and get new passwords, and the IT will have to start all over again. You have to have plan in place to do so.

Whether a breach is in the New York Times or not depends on how well you can detect hijackers and how well you respond in the first 24-hours. It's best to assume access control will fail and build your security response accordingly. Both for day to day security events and during major breach, the response plan is important. It cannot just be a document you produce that one and two people have read and haven't used it in 3 years. During an exercise, point to the 3 most senior people in the room and kick them out--Now see

how the plan unfolds.

Having a clear authority is crucial. The lead needs to make a decision between competing priorities such as getting an intruder out of the network or getting enough information to get a coordinated response which increases the chance of eradicating them on the first attempt. As part of the incident response, you need a separate communications infrastructure. You need clean devices that have never been connected to the corporate network; basic cellular modems too so the attacker can't see traffic. Have a separate email system. Assume an attacker can read email in the system. This may be a pain, but you can operate with a higher level of insurance that your plans are your plans and attacker isn't one step ahead.

Know your environment, including what data do you care about, where is it sited, what value does it have for an attacker, what system holds it and what controls prevent an attacker from accessing systems where critical information is located? If you can't answer those questions, you can't make informed decisions. In the middle of an attack, you don't want to have talk to a dozen different people before you can have idea of what to do

Washington State Community Cyber Security featuring Matt Modarelli, Cyber Security Manager, Washington Emergency Management Department

"Cyber security is not just an IT issue, it is a matter of public safety."

Modarelli emphasized the importance of approaching cyber security as a community issue and integrating cyber emergency preparedness and response efforts into all phases of emergency management and business continuity. The State emergency management division has been working hard to inculcate cyber security into all existing emergency management processes and programs across the state. The overall goal is to strengthen public, private, and tribal partnerships for the improvement of the state's overall cyber security posture.

Through the use of a Community Cyber Security Maturity Model (C2M2), Washington State's Emergency Management Division has implemented a number of enhancements to existing programs like plans and analysis, exercises and training, and community outreach. This focused approach has enabled the state to measure progress and identify gaps and areas for improvement.

Modarelli also talked of the importance of engaging corporate officers, agency leaders, and elected officials statewide on current cyber threats and vulnerabilities to ensure executive support and funding of cybersecurity initiatives. Ultimately, the response to a cyber emergency impacting the people, property, economy, and environment of Washington State will require a coordinated response.

Communicating with Media and Customers featuring Jack Whitsitt, Principal Analyst, EnergySec

"When a CEO opens their mouth, they are making a cyber security pronouncement. Ones and zeros will move based on how people react to their message."

Our choice of words, language, and attitude changes how people ingest and react to our message; we need to be aware of the context and intersections of the perspectives.

We all have different perspectives on what cyber security is. On Google, the peak searches of the word cyber come for the "cyber Monday" sales after thanksgiving. An image search turns up a lot of menacing keyboards with padlocks, but very little actually informative depictions. If you are cyber professional, you're talking about ones and zeros. It is becoming an in increasingly exciting topic, even spawning a new CSI: Cyber. It is not, however, a discipline yet--we can't even decide how to spell it. Is it cyber security or cyber security? We need

to build the discipline with new people from a variety of perspectives and backgrounds. We may not always know about someone's training, but that doesn't mean they don't have a valid perspective. Cyber security must be looked at in a multitude of different ways, and you need to be able to explain your actions in a way that makes sense to employees, the public, and your IT folks, and doesn't increase your vulnerabilities.

When a CEO opens her mouth, they are making a cyber security pronouncement. Ones and zeros will move based on how people react to their message. Keeping open channels of communication within your organization can help ensure you are prepared--announcements about non-cyber issues can have cyber repercussions. By communicating with IT staff about issues that might prompt hackers, your organization can be more prepared for response. In a world where cyber security is exciting and confusing, you just don't know where incident is going to end up. It matters who we are because it affects how we see grudge holders.

What is communication? It is successfully imparting messages in a two way process that creates meaning. It is important that it is a two way process. Our choice of words, language, and attitude changes how people ingest and react to our message; we need to be aware of the context and intersections of the perspectives. Cyber security can be the lens for our message, but we need to take the audience into consideration, aiming for explanation over fear. There are many elements you have to manage in cyber security. Only a small part is technology. Time, language, and geography are also components. Be aware that they don't see the world just in the business sense. We need to value perspectives, and train our staff to do the same. It isn't about enemies versus our organization. Instead our communications should express information not bias.

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 and direct future regional projects.

- Develop a database of resources, including sources of information and templates for planning, for use throughout the Puget Sound
- Integrate cyber security with physical security as part of a company-wide security integration.
- 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.
- Develop a functional exercise in the Puget Sound to help test plans and partnerships.
- Integrate cyber security into all exercises and planning