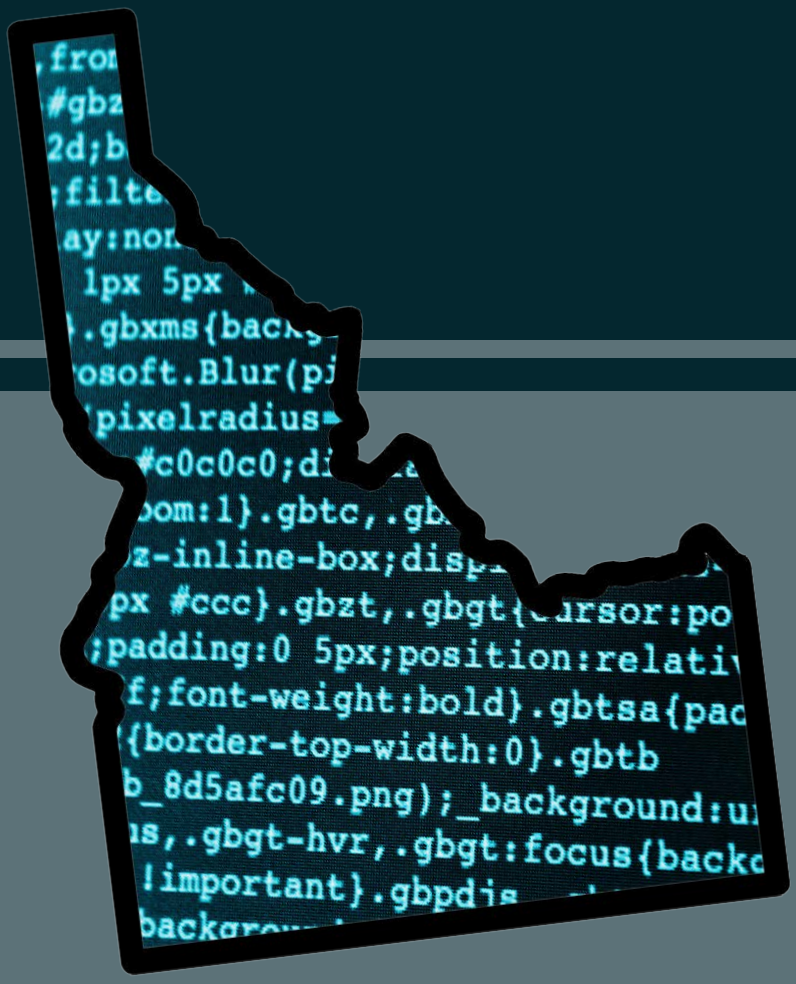
Idaho Cybersecurity

4th Annual Interdependencies Summit

Event Summary



April 26, 2018
St. Alphonsus Regional Medical Center
Boise, Idaho

CRDR
Center for Regional Disaster Resilience

Contact:

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

Eric Holdeman
Director
Center for Regional Disaster Resilience
206-443-7723
eric.holdeman@pnwer.org

Executive Summary

Executive Summary

The Idaho Cybersecurity Interdependencies Summit was held April 26, 2018 in Boise, Idaho at the St. Alphonsus Regional Medical Center. More than 200 participants from both public and private sectors, and from across the Pacific Northwest took part in the Summit that focused on emerging cyber and technology disruptions; regional resources and incident reporting; current trends and best practices in the public and private sector; and building a diverse and effective cyber workforce. Attendees also completed a simulation exercise to better understand the escalation of a cyber incident and thresholds for reporting and requesting resource assistance.

Brad Richy, Director, Idaho Office of Emergency Management, spoke at the event along with other experts on emerging technology and workforce training. He encouraged participants to improve their own cyber plans by challenging their planning assumptions, gaining a greater understanding of their interdependencies and by building relationships with others across the state and region.

Background

The Summit was the fourth event in a multi-year initiative in collaboration with the Pacific Northwest Economic Region's Center for Regional Disaster Resilience developing a public/private sector partnership for resilience in the state of Idaho. Previous events focused on training for small businesses, workshops focused on cyber interdependencies, and cyber threats. The Pacific NorthWest Economic Region (PNWER) is a statutory, public/private non-profit created by statute in 1991 by Idaho and nine other states and Canadian provinces with the mission of increasing regional collaboration. More information including meeting reports and deliverables can be found at www.regionalresileince.org/cyber-security.

Development

The event was developed over the course of seven months through a series of conference calls and meetings. In addition to Idaho Office of Emergency Management and PNWER CRDR, planning team participants included Idaho Department of Labor, Micron Technologies, Idaho Director of Information Security, Idaho Division of Human Resources, City of Nampa, Idaho Power, St. Lukes Health System, and Idaho Technlogy Council.

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 communication across agencies and organizations. There needs to be a greater awareness of resources available for both training and responding to a cyber incident. Relationships should be cultivated beforehand to share resources and facilitate a comprehensive response.

The importance of user education was highlighted several times during speaker presentations and participant discussion. Human error is the cause of many cyber incidents and ongoing training is needed for the whole organization, not just personnel involved in IT. Users of all levels and ages need education on their exposure to cybersecurity threats.

Every public and private organization faces cybersecurity risk and should develop a comprehensive cybersecurity plan. The cyber incident plan should incorporate all applicable divisions within the organization and be tested regularly through different scenarios. The State of Idaho offers tools for developing cybersecurity plans and responding to cybersecurity incidents, though access to these tools was not widely known.

The need for diverse workforce training was stressed by several speakers and during participant discussion. Diverse backgrounds, both demographically and educationally, contribute to a more resilient and prepared workforce. Participants were encouraged to engage with their local K-12 education system to

inspire students to consider STEM careers. The best way to prevent cyber incidents is to focus on the people and behavior- recruit, train and retain a high-quality workforce. This begins with Idaho's youth.

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

- Facilitate information sharing on training, resources, and best practices incident response plans. Develop training materials and regular webinars and other training opportunities to help organizations grow cybersecurity plans and facilitate information sharing. A "hotline" for immediate assistance would be helpful as well as templates for checklists and response escalation.

- Organizations should integrate incident response plans with emergency management channels and organization (NIMS/ICS).

- Government, businesses of all sizes, and law enforcement need to build relationships, improve collaboration and encourage information sharing on plans, threats and significant cyber incidents.

- Cyber leaders from critical service providers, major employers and critical infrastructures across the state should explore the development of a Cyber Resilience Coalition to encourage the sharing of information and to continue to build trust.

- Regular communications should include the judicial system with data on common cyber crimes and how to aid successful prosecutions of threat actors.

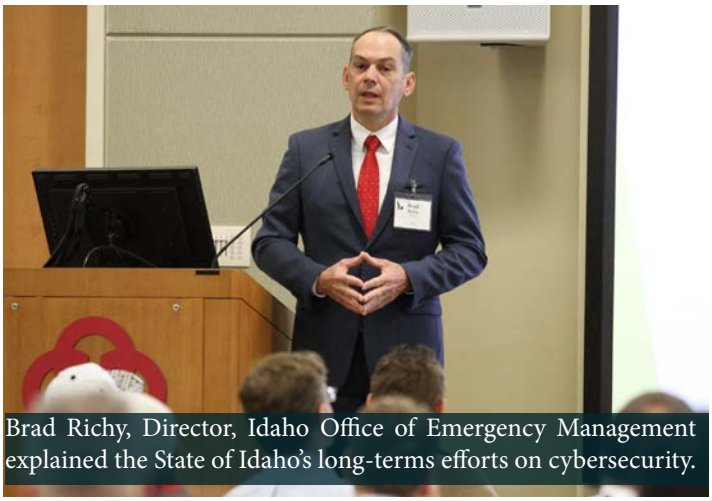
- Public-private partnerships are needed to successfully recruit, retain, and train a capable and diverse cyber workforce. Leadership should collaborate with the K-12 and higher-education system on inspiring students to enter the cybersecurity field.

- The cost for professional cybersecurity outsourcing is prohibitively high for many small/medium sized governments and businesses. Greater communication among these types of organizations is essential to learning and exemplifying best practices.

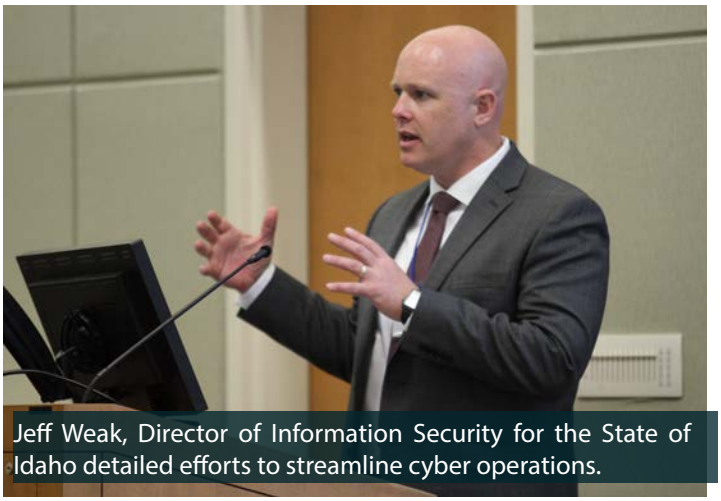
- In addition to concerns of cost and internal expertise planning, cyber preparedness has to be prioritized within small/medium enterprises. Providing affordable cybersecurity assistance, response plan templates, forums for exchanging information and free networking events are significant for smaller entites.

Over 200 cyber/IT and other professionals from all over Idaho participated in the Summit to explore best practices and share resources.

Event Summary



Brad Richy, Director, Idaho Office of Emergency Management explained the State of Idaho's long-terms efforts on cybersecurity.



Jeff Weak, Director of Information Security for the State of Idaho detailed efforts to streamline cyber operations.

Opening and Introduction
Brad Richy, Director, Idaho Office of Emergency Management

Brad Richy, Director of the Idaho Office of Emergency Management, opened the Summit by welcoming attendees and explaining the Summit as the latest iteration of a long-term effort. Idaho is a target of cyber threats and it is increasingly important for all stakeholders, both public and private, to develop cyber incident reporting guidelines and learn how best to ask for assistance. He encouraged attendees to network during the day and to convey the important lessons back to their institutional leadership.

Jeff Weak, State of Idaho Director of Information Security

Jeff Weak, Director of Information Security at the State of Idaho presented an overview of recent state IT initiatives including Legislation: HB 607 which created the Office of Information Technology Services under the Office of the Governor. The office is responsible for IT services and cybersecurity policies within the state and aligned statutory authorities. DIS and OCIO were combined and entail 30 FTEs with a $5.3M budget.

The State is also working on developing Idaho's response to incidents using CIS critical controls, NIST cybersecurity framework, and cybersecurity awareness training. Weak also stressed the importance of third party management, vulnerability assessments and penetration testing. The number one threat is the human factor which is why consistent cybersecurity awareness training is crucial to developing a cyber culture.

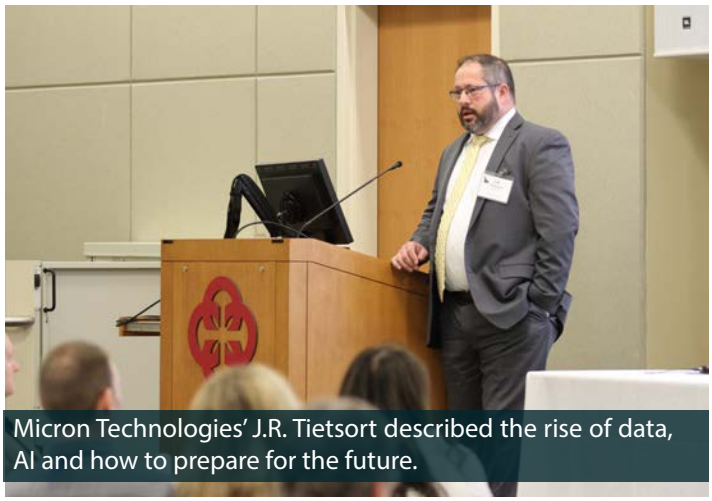
What's Coming in the Future and How Can We be Prepared? - J.R. Tietsort, Chief Information Security Officer, Micron Technologies

J.R. Tietsort, Chief Information Security Officer at Micron Technologies provided an overview of technology disruption. The millennial and gen z generations have grown up with Internet at their disposal, able to understand technology and even write code at a young age. Internet penetration was 45% in 2009 and is now over 60%. Combine this with the accelerating growth in technology and the stage is set for disruption.

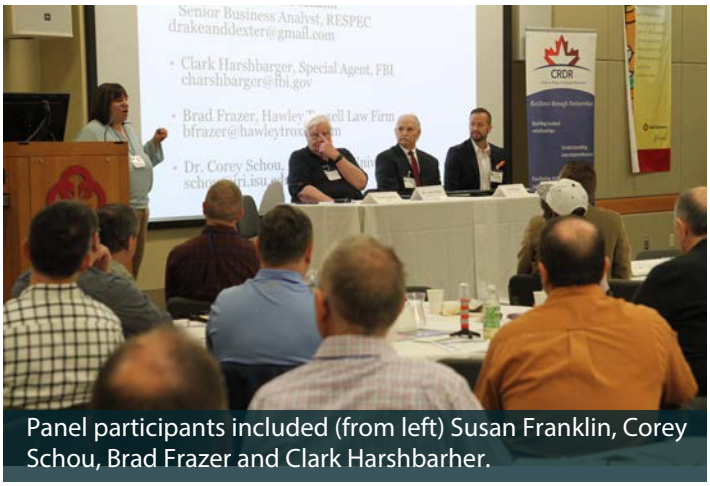
Data is the new "oil." It is being monetized and stored. Data is compounding and algorithms in machine learning are leading to artificial intelligence (A.I.). A.I. and advanced compounding machine learning have the potential to impact every industry from healthcare (research) to manufacturing (anomaly detection) and logistics (efficiency). A.I. is a double-edged sword; do A.I. objectives line up with our own? Ex: Increased productivity may not be widely distributed and mass surveillance may battle with data privacy.

Tietsort addressed the Internet of Things (Iot), the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data. Iot has the potential to transform industries as it blurs the lines between physical environments and data analytics. Automation will enable new levels of efficiency while threatening existing industries.

Data collection is increasingly leading to convenience and privacy erosion.



Micron Technologies' J.R. Tietsort described the rise of data, AI and how to prepare for the future.



Panel participants included (from left) Susan Franklin, Corey Schou, Brad Frazer and Clark Harshbarher.

Merger and acquisition trends are increasing with brick and mortar companies buying tech companies and vice versa. Private networks are changing the boundaries of the Internet, i.e. appliances in the home connecting to a power company, medical appliances connecting to remote monitoring services and shipped packages connecting to logistics services.

The continued growth of the internet and increasing number of devices is leading to ransomware growing to a $1 billion industry. Continued attacks threaten user trust of the Internet consequently reducing economic potential. However, convenience forces users back to the platform, where they become numb to data loss issues.

An increasingly connected physical world means that a cyberattack does not stay in cyberspace. Cyber incidents are increasingly blurred. Threat actors include nation states, but also surrogates, political movements, even independent actors which are supported by disinformation campaigns. Large cyber attacks frequently require a multi-stakeholder response with the government and private sector working together. The traditional approach of governments is ill-equipped to respond rapidly to emerging tech advancement. National security concerns must be weighed versus privacy and freedom rights. Government must avoid falling further behind technological change and must avoid disproportionate and harmful regulations in response to growing cyber threats. Nationalist strategies threaten valuable cross-border data flows.

Preparation and resilience are key. The public and private sectors must both be at the table to make decisions and respond. Sufficient risk planning needs to be a part of business operations for small and medium size companies and all organizations should be thinking about resiliency and continuity, focusing on value protection. Strategic planning is necessary to understand how advancing tech can disrupt the business model.

Panel: Regional Resources and Assistance: Whom to Contact for Incident Reporting and Assistance

Moderator Susan Franklin, Senior Business Analyst, RESPEC
Members of the panel included:
Clark Harshbarger, Special Agent, FBI
Brad Frazer, Hawley Troxell Law Firm
Dr. Corey Schou, Idaho State University

Clark Harshbarger, Special Agent, FBI describe the role of the FBI in cyber crime. It is impossible for everyone to come to him when there is an incident. The government can be slow and even case law is behind on current threats. Harshbarger explained that there is not yet law that defines specific elements of ransomware as illegal, but their are other elements that can be prosecuted.

His suggestion is to retain a civil attorney on standby to give advice on business and legal obligations. The FBI prefers that all data and logs are kept for evidence for use by the U.S. Attorney's Office. However, that may not be suitable for the business. There are few post-breach reporting requirements from very narrow federal cases. It is important to note

that saved emails may be susceptible to discovery in a trial, consequently there is a liability risk.

Data has value; the average breach cost is $50,000 for a medium enterprise under an umbrella insurance policy. Affected parties should acknowledge the worth of their data when contacted by the FBI or their lawyers. Businesses must have a plan in place when data is compromised. Is there an alternate way to get data into your business operations?

IC3.gov is a central government repository for all cybercrime. It's important for affected parties to report incidents because information is disseminated to all jurisdictions relevant to the case. Harshbarger explained that when he approaches the U.S. Attorney with a case, the first decision is determining the venue and who is responsible for handling the case.

Brad Frazer, Hawley Troxell law firm, reviewed the legal implications of cyber incidents. There are specific data reporting obligations and when an enterprise is hacked, it should be reported accordingly. However, once the news is public, people will be able to sue. His strong advice is to know the legal obligations before an incident and to have a plan prepared.

Idaho code section 28 -51-105 is the data breach reporting statue. In civil litigation there are two conditions to proceed – standing and damages. The 9th Circuit recently ruled in the Zappos case that if data is hacked and personal identifiable information, (PPI) is compromised, the plaintiff does not need prove standing or monetary damages to proceed with the lawsuit. This greatly affects future case law and Frazer suggests due diligence.

States have different breach reporting statues. Attendees at the Summit must be proactive and seek updated information.

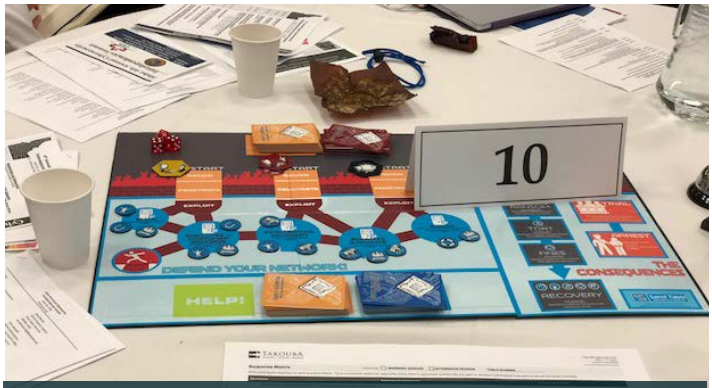
Dr. Corey Schou, Idaho State University spoke on Evaluating Interdependent Systems Cyber Range Simulators. Why do an organization's systems operate they way they do, and what are the policy, human and IT variables involved? A simulator can help understand these underlying process.

Looking at a traditional organization chart, where is the information system? Every organization chart is an example of internal interdependence. But the lines that connect all the boxes are the information system. An accounting department may have excellent cyber practices but the marketing department may create vulnerabilities. Dr. Schou recommended more consideration be given to how people work together and to their interdependencies. Organizations need to focus on establishing analytical skills, operating system awareness, penetration testing, interpersonal skills, social engineering techniques and pen-testing tools familiarity.

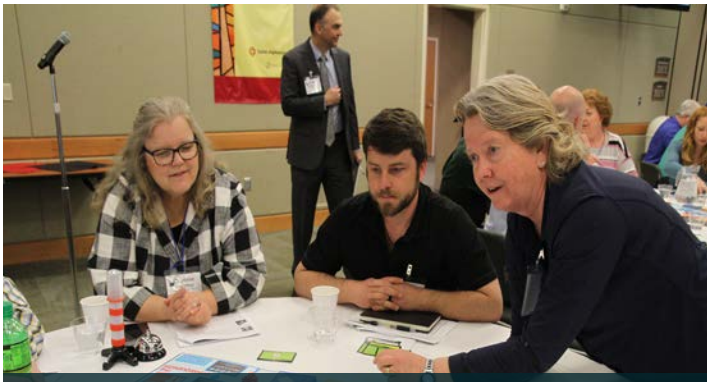
The Idaho State University's simulator allows people to play with the system, apply patches and see the effects. Users can model their own institution's system organization. Ethics, cyber kill chain, offensive tools and social engineering can all be tested.

Penetration testing provides businesses with the opportunity to increase their security posture. Testers use methods normally employed by malicious threat actors. Penetration testing is heavily technical and requires specialized training. Cyber range simulations can provide the best means for training penetration testers. These simulations must be realistic and immersive. Areas for further research include gamification of cyber ranges for training purposes, and ways to fully integrate ethics and social media into cyber range simulations.

Cybersecurity interactive simulations exercise



In small teams, attendees interacted with the game scenario and shared their experiences with cyber incidents and response.



The simulation guided participants from the initial stages of a cyber intrustion to defender responses and potential legal proceedings.

Cybersecurity Interactive Simulation Exercise

James Rollins, Managing Partner at Takouba Security, introduced the simulation by explaining the current landscape. It is a new cold war and foreign cyber adversaries are effective. The risks are very high because borders are meaningless and barrier to entry is low. It is common to think that organizations only need to build a higher wall and keep patches up to date. However, a player's entire cyber protection is based on the decisions of the team.

The simulation exercise gave participants a firm understanding of how cyber-adversaries work their way into a domain, appreciation of the costs associated with a cyber incident, a general understanding of their organization's vulnerabilities and capabilities to respond to a cyber iincident, and a general understanding of what community resources are available.

Attendees actively engaged with the game process throughout the day for thirty minutes at each session. During game play, the cyber incident would escalate and participants requested assistance from state and federal authorities.

Participant Discussion:

There is a broad range of preparedness. Generally smaller organizations lack plans, budgets and people, whereas the public sector has the clearest procedures and policies. The process of developing a response plan can be prohibitively expensive and time consuming for small businesses.

Companies may have plans but employees do not know them or how to discern the severity of incidents in order to follow the plans. Concrete indicators, scenarios, and examples seem necessary to convey the risk associated with different types of breaches.

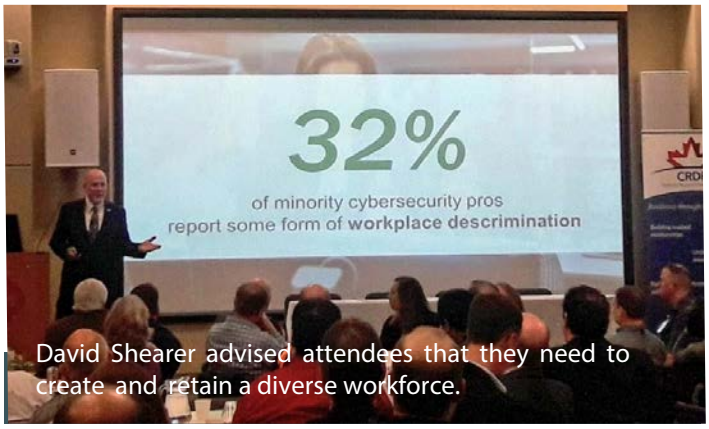
How should stakeholders be included? At what point during the escalation? Public relations, Attorney General's Office, insurance, IT director, ic3.gov, C levels, others who will be affected are all stakeholders.

There is a distinction between public, private, and publicly traded companies with varying levels of triggers. Government organizations and utilities have the most clear response plans, but employee understanding of these procedures is not well established.

The cost for professional cybersecurity outsourcing is prohibitively high for small business. Greater communication among small businesses is essential. Standardizing processes for backups, information sharing, and personnel training are potential actions to improve preparedness and resiliency.

Luncheon keynote: David Shearer

CEO of (ISC)², Largest IT Certifying Organization in the World

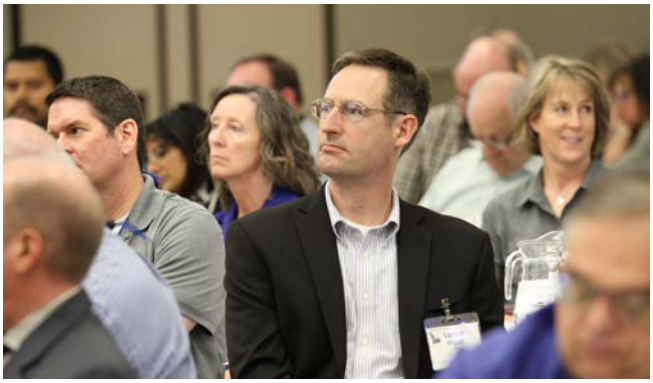


David Shearer advised attendees that they need to create and retain a diverse workforce.

Mr. Shearer spoke on recruiting and retaining an effective workforce. CIOS average only 18 months with an employer, which shows that people want to work where their opinions matter. People want to buy into the mission and act ethically. It is important for organizations to invest in training and certifications. To attract employees, invest in the latest technology, view cybersecurity as more broad than just technology and invest in training and certifications. Organizations need to develop the right strategy; where is IT located and how do people collaborate? Analyze the business process and educate users on cybersecurity.

Shearer explained there is a dearth of talent and a need to incease underrepresented groups. The workforce tends to be white, older, and male. Organizations need to prepare for the millennial generation. Diverse workers problem-solve issues differently. Life experiences and uncommon educational backgrounds add to the strengths of a workforce. Pay discrepancies, discrimination, and hiring bias are barriers to recruiting and retaining a diverse workforce.

Shearer reminded all that cybersecurity is our responsibility, and if we do not do it well, we will be out of business.



Panel: Current Trends and Best Practices from Public and Private Sector Perspectives

Moderator: J.R. Tietsort, Micron Technologies

Members of the panel:
Mark Wennstrom, Regional CIO, Trinity Health/St. Alphonsus Regional Medical Center
Susan Buxton, Administrator, Idaho Division of Human Resources
Daniel DeCloss, Director of Security, Scentsy
Fran Caprai, Director of IT, The Amalgamated Sugar Company

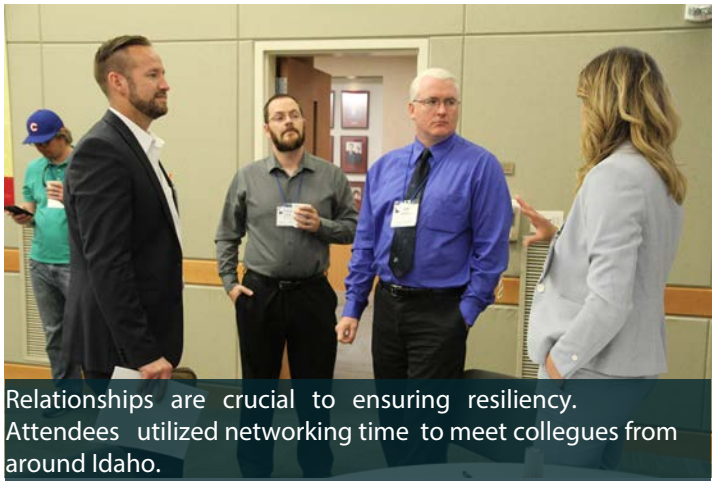
Fran Caprai explained the producers co-op manages critical agronomic data. The processes are proprietary and use SCADA systems. In addition to the chemical engineering data, there are human resources data and general business data. Their experiences have reminded them that human behavior is the weak link.

Daniel DeCloss reviewed Scentsy's reliance on relationship building. The 1100 person company needs to protect 6000 identities of sellers. Intellectual property is also a valuable asset vulnerable to hacking.

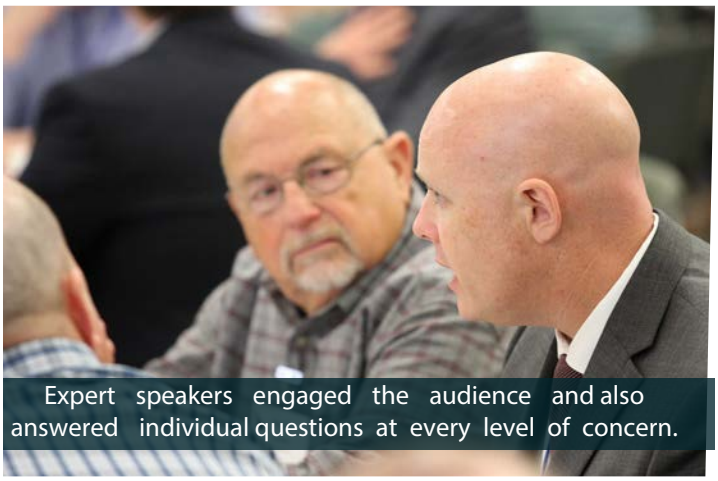
Susan Buxton explained the DHR has 25,000 employees working with tax data, licensing, and unemployment, labor, and disability benefits. Hospitals and veteran homes generate personal health information. The staff in all the IT departments work to keep the systems up the date and also inform the legislature of procedures. DHR began an annual training requirement for all state employees in 2017.

Mark Wennstrom, pointed out that healthcare systems are significant targets because of their valuable information and unfortunately old legacy systems pieced together. The enterprise information security team in the corporate office is the fastest growing financial and staffing part of Trinity.

Buxton added the Idaho Division of Human Resources abides by public records act so the agency has to ensure people aren't accessing additional data. The focus is on external threats and internal threats. The cybersecurity task force established mandatory training which is critical because the workforce is siloed in a



Relationships are crucial to ensuring resiliency. Attendees utilized networking time to meet collegues from around Idaho.



Expert speakers engaged the audience and also answered individual questions at every level of concern.

federated system. The curriculum was directed to each level of access and ensured everyone had the same training. 95% of the workforce have finished the mandatory training.

Caprai recalled that IT was once housed in the accounting department at The Amalgamated Sugar Company. There was not a focus on IT or promoting best practices, therefore initial years were focused on getting basics in place. Now the company can focus on training. An earlier breach showed how to communicate internally and externally.

DeCloss pointed out that since the workforce are 1099 contractors, Scentsy is unable to command training but can emphasize through an online portal of tips, tricks, and best practices. Scentsy has conducted pen testing. This year, the organization will focus on advanced purple team events and other advanced training. DeCloss added there are decent frameworks available like NES. The objective is to simulate the activity of an intruder and check if the defenders can detect.

Trinity Health requires mandatory employee education and quarterly phishing exercises. Wennstrom said the goal is to make employees aware that they need to be more careful. For example, a flag is placed on incoming emails from external address. Employees are educated to slow down and be cautious when interacting with external messages. This lowers the percentage of people falling for phishing schemes.

Historically, medical devices were standalone and the biomedical shop and IT did not communicate. Now all devices are attached to the network.

Because devices are attached to patients, they are FDA regulated. It is time consuming and costly to get FDA approval so vendors do not upgrade backend systems. Some devices are still running Windows XP. Devices are not managed by IT but by the vendor so hospitals are 100% reliant on the vendor to manage security. The critical engineering employees tasked to support devices are not structured under IT so it is difficult to communicate and collaborate effectively.

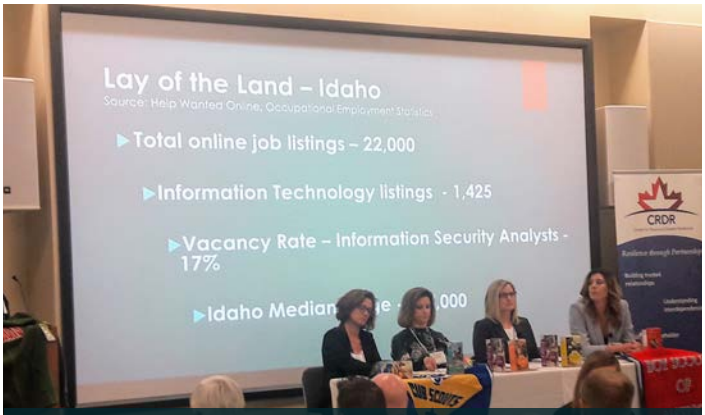
Scentsy created is own custom training to increase interest. Some of it is remedial but as users become more aware of risk, they are open to having a discussion on reaching end results without shortcutting security. DeCloss recommended organizations use games and other incentives to encourage people to participate.

Panel: Cyber Career Education and Talent Development

Moderator Georgia Smith, Deputy Director, Idaho Department of Labor

Members of the panel included:
Mackenzie Brown, Research Principal, OPTIV
Alisa Bondurant, Director for Talent, Idaho Technology Council
Dr. Sherawn Reberry, Director of Education Programs, Idaho Digital Learning Academy
Shawna Hofer, St. Luke's Health Systems

Georgia Smith presented Idaho data that vacancy rates are very high. Employers need to be competitive in this industry and follow the salary in neighboring states. Students that are actively seeking employment



Panel participants encouraged the audience to commit to reaching out to studetns and diverse populations.

make their decisions within the first year of education so onboarding is critical. Internships are proving effective for Idaho employers.

Dr. Sherawn Reberry, added that organizations in the public sector need to be creative in offering work-life benefits. Cybersecurity can feel like a thankless job so they need to be shown appreciation. Employees want to feel passionate about the organization and the mission.

Mackenzie Brown warned of a severe overturn rate because good employees will be poached. Organizations need to understand employees and develop relationships. Either invest in your people or you will need to hire a new person and it will take a year for them to be onboarded to understand your cybersecurity system and business.

Attendees asked the panelists how to engage with students in rural districts. Reberry explained the development of a curriculum for volunteers to use in the online classroom and in mentoring. Virtual tours can also be used to inspire students. All of the panelists recommended the audience reach out to schools and other youth organizations to offer mentoring services. Smith added that the Girl and Boy Scouts have a curriculum for scouts and local community members.

It is important to reach the community that does not have a background in cybersecurity. Professionals can visit high schools or small businesses. The industry needs to also think about the best way to advocate for women and other non-traditional employees to increase diversity in problem-solving.

It will be much easier to secure the future workforce if we start teaching from an early age. Organizations should be creative in their hiring strategies and think outside of the box of traditional applicants.

Possible next actions include using our employers to provide experiential learning, internships or registered apprenticeships. Opportunities for students to come into the workplace and engage with hands-on learning will inspire the future workforce.

There are jobs open but the information sharing is lacking. The industry needs to do better about connecting with people.

Scenario Hotwash and Key Takeaways

To close the day, participants shared their key takeaways and recommendations for cybersecurity in Idaho. Based on their input, and the input provided through feedback forms, several key takeaways were identified. Participants considered the conference very good overall. Several commended the efforts Idaho is making towards securing a diverse workforce. Other participants echoed the lessons that neighbors will be the first ones to help after an incident. Idaho needs to improve public-private partnerships and information and resource sharing. Participants also expressed a desire for more frequent trainings, suggesting webinars and online materials would be useful in between opportunities to gather in-person.

Recommendations

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

- Facilitate information sharing on training, resources, and best practices incident response plans. Develop training materials and regular webinars and other training opportunities to help organizations update cybersecurity plans and facilitate information sharing. A "hotline" for immediate assistance would be helpful as well as templates for checklists and response escalation.

- Organizations should integrate incident response plans with emergency management channels and organization (NIMS/ICS).

- Government, businesses of all sizes, and law enforcement need to build relationships and improve collaboration and encourage information sharing on plans, threats and significant cyber incidents.

Recommendations continued

- Cyber leaders from critical service providers, major employers and critical infrastructures across the state should explore the development of a Cyber Resilience Coalition to encourage the sharing of information and to continue to build trust and sharing information.
- The judicial system should be kept current on common cyber crimes to aid successful prosecutions of threat actors.
- Public-private partnerships are needed to successfully recruit, train and retain a capable and diverse cyber workforce. Cyber workers should collaborate with the K-12 and higher-education system to inspire students to enter the cybersecurity profession.
- The cost for professional cybersecurity outsourcing is prohibitively high for many small/medium sized governments and businesses. Greater communication among these types of organizations is essential and where possible learn from larger entities' best practices.
- Many factors aside from cost and internal expertise impact cyber preparedness including the need for communication among organizations and the prioritizing of cybersecurity within small/medium enterprises. Providing affordable cybersecurity assistance, response plan templates, forums for exchanging information and making points of contacts more clear for certain industries are steps organizations can take to be more cyber resilient.

I enjoyed all of the meeting dynamics, especially the board game table top discussions which gave an opportunity to get to know people - *participant*

The Summit was very useful in meeting and discussing these issues with a broad range of backgrounds, i.e. public/private, military/civilian, etc. - *participant*

The biggest take-away was the future of the changing workforce - *participant*

Our community is definitely becoming aware and increasing our involvement in these issues - *participant*