Executive Responsibility Track

For non-IT leaders, this non-technical track informs and engages executives to understand risks, integrate security into business planning, and communicate and implement a culture of cybersecurity across their tribe or enterprise.

Topic	General Summary of What We'd Like Covered
Cybersecurity's Role in Protecting Sovereignty	Every leader in a tribe or tribal enterprise plays a role in protecting the sovereignty of that tribe. In this session, our presenter will discuss where cybersecurity plays a key role in protecting sovereignty. Whether it is protecting data, operations, or digital assets, the understanding of sovereignty is a unique but critical part of every native american organization.
Executive Cyber 101 - the common foundational cyber policies, procedures, and operations to know	This session is all about removing the tech talk and sharing the foundational basics of organizational cybersecurity with any non-technical leader. Leave this session understanding the core components and infrastructure that define cybersecurity operations in your own organization.
Cybersecurity Budgeting - an executive perspective and guide to budgeting and sharing risks	Understanding how much to budget for cybersecurity resources and services is a challenge for every leader or executive. How can you understand the proper balance of risk versus cost? This session will provide guidance on how to be more confident in setting and understanding your cybersecurity investment and understanding what that level of investment means to your organization.
Cyber Insurance - what to expect and what to ask for	Cyber insurance has changed as cyber threats have changed. Costs have increased and in many cases, what is covered has been reduced. Join this session to learn about what executive leaders should know to prioritize your cyber insurance to maximize benefits with reasonable cost. More clearly understand what cyber insurance covers (or not), common policy mistakes, and where your own tribe or tribal enterprise may be at risk.
The Executive Role in Creating a Culture of Security	The culture of any tribe or tribal enterprise is set and controlled primarily from leadership. It is a fact that the IT and cybersecurity team cannot create a "culture of security" without the support, understanding, buy-in, and practice from their leadership. This session will uncover the keys for leadership to assist their technology team in creating a truly effective culture of security.

Strategic Cybersecurity Track

For CIOs, CISOs, technology minded business leaders and professionals, this track offers strategic insights on mitigating risk, technology alignment and best operational business practices designed to maximize cyber preparedness.

Topic	General Summary of What We'd Like Covered
Cyber KPIs and Metrics - what you need to share with the executive team	Can't get the necessary cyber funding? Executives' eyes glaze over when you start talking to them about cybersecurity risks and challenges. In this session, we will uncover effective cyber metrics and KPI's that you can present in a manner that leadership will want to see, hear, and understand. We all win when cyber risks and challenges are better understood across the organization.
The Journey to Cyber Maturity - an open discussion presented from a small, medium, and large tribe perspective	Join this session to hear from leaders representing small, medium, and large tribes or tribal enterprises as they uncover the challenges and roadmap to increasing cyber maturity across organizations with different levels of resources. Everyone needs to cover cybersecurity 24x7x365, but what does that look like based upon the size of your own tribe or tribal enterprise?
Cybersecurity Policy and Data Governance	At a time when many tribes and tribal enterprises are still trying to get effective and fully implemented cyber, AI, and data policies in place, how can we best use our available resources to prioritize and implement what puts us most at risk? Why is data governance critical to cybersecurity and how can resource-constrained tribes achieve even basic data governance across the organization?
AI's Effect on Cybersecurity - staying informed	AI can be used for good but it can also be used for nefarious purposes. Nowhere is this more clear than in the world of cybersecurity. Attend this session to learn about how the quickly changing AI landscape is creating both new challenges and new solutions for your organization.
Tabletop Cyber Exercises (TTX) - creating your own TTX to engage both the executive and technical teams	Practice is essential to effective preparedness and tabletop exercises are a fantastic way to test your readiness to respond to whatever cyber threats you may face. They are also a critical tool in helping your non-technical leadership team understand the important and immediate role they need to be prepared for in the event of any serious cyber issue. In this session, you will learn how you can create your own tabletop exercises designed to improve preparedness and to uncover gaps in your existing response plans.
Security Awareness Training - keeping it meaningful and effective	As threats advance and change, our security awareness programs need to change as well. Learn about tools, practices, and new techniques that keep security awareness meaningful and effective from on-boarding an employee through their entire work journey.
The Value of Third-Party Assessments and How to Engage for Meaningful Results	Third-party cybersecurity assessments and testing need to be a regular and critical part of any organization's cyber preparedness strategy. Assessments should be more than vanilla exercises designed primarily to check off the annual compliance or regulatory requirement check boxes. Join this session to learn what makes third-party assessments more meaningful and how to engage more effectively in the future.

Cybersecurity in Practice Track

For front-line IT and cyber professionals, this technical track dives into hands-on strategies, advanced tools, and real-world challenges for protecting tribal organizations.

Topic	General Summary of What We'd Like Covered
Vulnerability and Patch Management - a success story	Join this session as we hear from tribes that have successful vulnerability and patch-management programs in place. Learn about their journey and current challenges in protecting their network and network devices.
The Cybersecurity AI Tools You Need to Know About Now	This session is all about identifying and learning about the most current AI tools and tactics that a front-line cybersecurity technical team needs to be aware of. As AI continues to quickly change the cybersecurity landscape, we all need to stay on top of what this means for our cyber preparedness.
Cyber Threat Hunting - the tricks and tools as you mature as a threat hunter	Put on your cyber technical hat as we dive into the progression and maturity of cyber threat hunting. Our presenters will work their way through tips and tricks for those just beginning on the threat hunting journey and moving to more complex methods and tools used by more experienced threat hunters.
Business Email Compromise (BEC) - technology solutions to a people problem	BEC remains at or near the top of the list of vulnerabilities for organizations across the world. In this session, we will discuss and learn what technical resources can be doing to improve identification and prevention of this continuing threat.
Cybersecurity on a Budget - protecting your tribe when you have little or no dedicated cyber resources	No matter how few resources, budget, and tools you have to work with, you are still expected to provide 24x7x365 cybersecurity. Fair or not, that is the reality for most tribes and tribal enterprises. Attend this session to learn about how the technical cyber team can deliver the most with a limited budget.
Hacker 101 - WiFi cracking - see and learn the tools of your potential adversaries	We all depend on WiFi—here is your chance to watch and learn about WiFi cracking. See what far too many threat actors already know about WiFi vulnerabilities. We will start easy with WPA, then move to WPA2psk using tools like Kismet, Airmon-ng, Airodump-ng, and Aircrack-ng or Hashcat to break into a network. Time permitting, we will show Wardriving and WiFi Pineapple to demonstrate how these attacks can be automated or simplified, and insert Evil Twin attacks to set up a man-in-the-middle type attack.
Hacker 102 - using open source intelligence tools (OSINT)	Ready to take an even deeper technical cyber learning drive? If so, this session is for you. Watch and see how to use tools like TheHarvester, Powermeta, and Recon-ng to gather information, then spin up a rudimentary phishing site using SocialPhish or a similar tool getting Hashes. Pretend you have an implant in a network and use tools like SCCMSecrets, Impacket, and Responder to get a new identity. Then use Bloodhound to see the path forward to a crown jewel.