TRIBAL-ISAC

INFORMATION SHARING & ANALYSIS CENTER

THE PULSE

The State of Cybersecurity Within Tribal Nations

Cybersecurity Insights, Trends & Threats Across Tribal Government, Health, and Enterprises

An Annual Publication by Tribal-ISAC with assistance from TribalHub

Preface

Tribal cybersecurity is no longer a peripheral concern; it is a strategic imperative. As digital threats grow in complexity and frequency, Tribal Nations face unique challenges in protecting their sovereignty, infrastructure, and communities. From small IT teams and constrained budgets to evolving regulatory pressures and emerging technologies, tribal organizations must navigate cybersecurity with precision, resilience, and cultural alignment.

The Pulse offers a focused lens on the cybersecurity readiness of Tribal Nations, delivering insights tailored to tribal governments, health systems, and enterprises of all sizes. This publication centers on tribal-specific risk evaluation, mitigation strategies, and operational realities. It promotes collective intelligence and cross-sector collaboration to strengthen cybersecurity practices across Indian Country.

This report draws from three key sources to provide a comprehensive view of tribal cybersecurity conditions:

- **Tribal-ISAC's 2025 "Tribal Cybersecurity" Survey**, which engaged 89 IT leaders at tribes and tribal enterprises, offering firsthand perspectives on staffing, investment, planning, and threat response.
- **TribalHub's "How Prepared is Your Tribe for AI?" Survey**, based on input from 119 representatives at tribes and tribal enterprises collected during the 2025 Regional Tribal Technology Forums, highlighting readiness levels and strategic concerns around artificial intelligence (AI).
- **Gate 15's CHIEF and NATIVE Reports**, which analyze cybersecurity trends and threat activity from July 2024 through June 2025, providing context on emerging risks and sector-specific vulnerabilities.

Together, these sources illuminate cybersecurity capacity, preparedness gaps, and actionable opportunities for strengthening digital resilience of tribes and tribal enterprises. The findings are intended to inform cybersecurity professionals, government and enterprise leaders, and executives in gaming and hospitality sectors at tribes and tribal enterprises, those who shape and safeguard the digital future of Tribal Nations.

The Tribal Information Sharing and Analysis Center (Tribal-ISAC) remains committed to enabling secure collaboration, threat sharing, and coordinated response across tribal environments. Through culturally grounded, intelligence-driven cybersecurity, Tribal Nations can build sustainable defenses that honor sovereignty while navigating today's dynamic threat landscape.

Table of Contents

Executive Summary 4

Cybersecurity Resources and Investments 6

Cybersecurity Readiness 11

Threat Landscape & Response 17

Cybersecurity Frameworks & External Engagement 18

AI Planning for the Future – A Rising Cyber Threat 21

Improving Cybersecurity Posture: Insights and Resources 23

Appendix A: Tribal Cybersecurity Survey Information 28

Appendix B: How Prepared is Your Tribe for AI Survey Information 29

Executive Summary

Tribal entities are demonstrating growing strategic commitment to cybersecurity, even as operational maturity remains uneven. Most operate with small information technology teams. Over two-thirds report zero or only one dedicated cybersecurity staff member, despite facing similar regulatory pressures as larger entities. Budget allocations remain modest, with over 60% dedicating less than 20% of their technology budget to cybersecurity. Tooling receives the most concentrated investment, while staffing and training are often underfunded. Encouragingly, 73% of respondents anticipate increased cybersecurity spending in 2026, and only 1% expect a decrease, signaling a shift toward resilience and threat mitigation. However, external funding remains largely untapped, with 74% of organizations receiving no federal or state cybersecurity grants in 2025.

Cybersecurity readiness is progressing but remains fragmented. Incident response plans are widely implemented, yet disaster recovery, business continuity, and third-party risk oversight are underdeveloped. Tabletop exercises are infrequent and narrowly scoped, limiting coordinated response. While annual training is common, certification support and scalable platforms are inconsistently used, and forensic readiness varies significantly. These gaps highlight the need for structured workforce development and scenario-based testing aligned with tribal sovereignty and operational goals.

The threat landscape is dominated by ransomware, with nearly a quarter of tribal entities reporting actionable threats. Of those affected, 75% experienced ransomware in the past year, and 77% refused to pay the ransom, an encouraging sign of resilience and alignment with best practices. However, low incident reporting may reflect either strong prevention or limited detection and cultural reluctance. These findings reinforce the urgency of ransomware-focused testing, clear decision protocols, and robust recovery infrastructure.

Framework adoption is increasing, with 60% of organizations aligning with the National Institute of Standards and Technology's (NIST) governance model and 25% using custom approaches. Outsourcing is a strategic lever, penetration testing, continuous monitoring, and endpoint protection are widely contracted to external providers, while governance and continuity functions remain largely internal. Third-party risk management is gaining traction, and tribal entities rely heavily on trusted intelligence sources, with the Tribal Information Sharing and Analysis Center (Tribal-ISAC) and the Multi-State Information Sharing and Analysis Center (MS-ISAC) leading threat-sharing efforts.

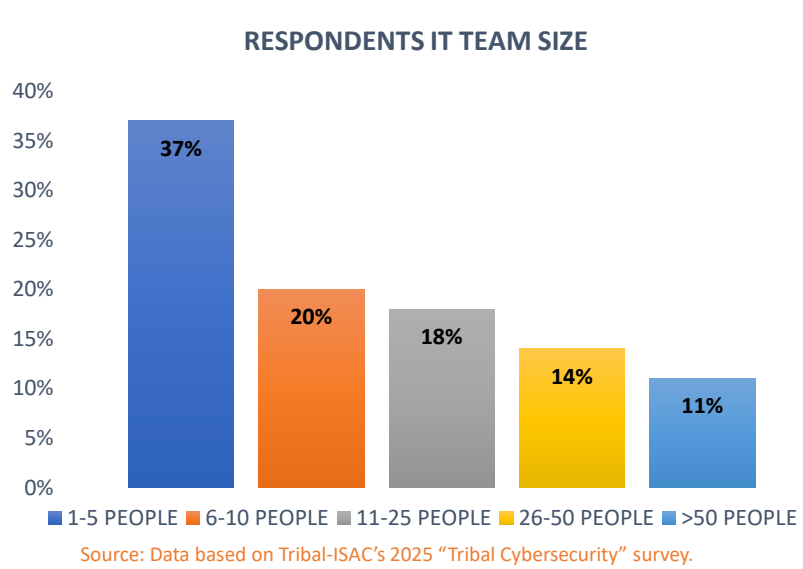
Artificial intelligence (AI) is rapidly entering workplaces at tribes and tribal enterprises, often outpacing formal governance and oversight. At TribalHub's 2025 Regional Forums, leaders acknowledged both the momentum and the risks: while most organizations report active artificial intelligence use, few have established clear policies or data protection frameworks. Preparedness levels vary widely, and strategic planning remains limited, even as AI is expected to significantly reshape operations within two years. To navigate this shift responsibly, tribal entities must prioritize AI governance as a leadership and cultural imperative, developing use policies and data safeguards that align with tribal sovereignty and uphold transparency, consent, and community benefit.

To support cybersecurity advancement at tribes and tribal enterprises, federal resources such as the Cybersecurity and Infrastructure Security Agency's (CISA's) resilience toolkit, the Secure Our World campaign, and the Tribal Cybersecurity Grant Program (TCGP) offer planning templates, cyber hygiene services, and funding pathways tailored to tribal environments. The Cross-Sector Cybersecurity Performance Goals provide a prioritized roadmap of low-cost, high-impact practices. The Tribal-ISAC plays a pivotal role in enabling secure collaboration, threat sharing, and engagement with federal partners, applying the Traffic Light Protocol to protect sovereignty and facilitate coordinated response.

Overall, the findings reflect a cybersecurity landscape at tribes and tribal enterprises that is advancing in strategic intent but still developing in operational execution. A "Resilient by Design" approach, integrating technical safeguards, cultural awareness, and long-term capacity-building, will be essential to strengthening cybersecurity maturity and sustaining continuity in an increasingly complex threat environment.

Cybersecurity Resources and Investments

This section presents a detailed analysis of cybersecurity staffing levels, budget structures, and anticipated funding shifts at tribes and tribal enterprises based on responses to key financial and operational questions in the Tribal Cybersecurity Survey. The data reflect how tribal entities are allocating internal resources, such as personnel, tools, and third-party services, to support cybersecurity programs in 2025, and how those allocations may evolve in 2026. It also highlights the role of external funding, including federal and state grants, in shaping cybersecurity priorities. The insights gathered offer a baseline for understanding current investment patterns, workforce capacity, and strategic planning across tribal communities.

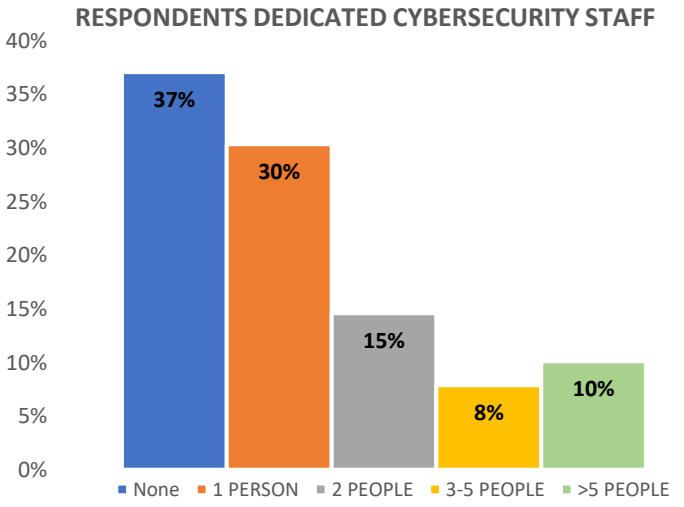


Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Across the dataset, organizations show a consistent trend of limited investment in cybersecurity personnel, both in terms of budget and headcount.

Most tribal entities operate with lean IT teams, with 37% reporting five or fewer full-time staff, highlighting broad role coverage and limited internal capacity. Within these teams, dedicated cybersecurity personnel are uncommon: 37% of respondents report having no staff solely focused on cybersecurity, while 30% have only one, and just 10% report more than five. This distribution indicates that cybersecurity responsibilities are frequently absorbed into general IT roles or outsourced to third-party providers, rather than supported by specialized internal resources. The data underscore a critical gap in workforce depth and specialization, which may impact incident response, documentation rigor, and long-term resilience.

Many tribes rely on minimal IT personnel while navigating increasingly complex infrastructures and compliance landscapes. Gaming & Hospitality typically maintain IT teams of 10–25 FTEs, with cybersecurity comprising 10–20% of staff.[1] Tribal government teams and enterprises fall short of



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

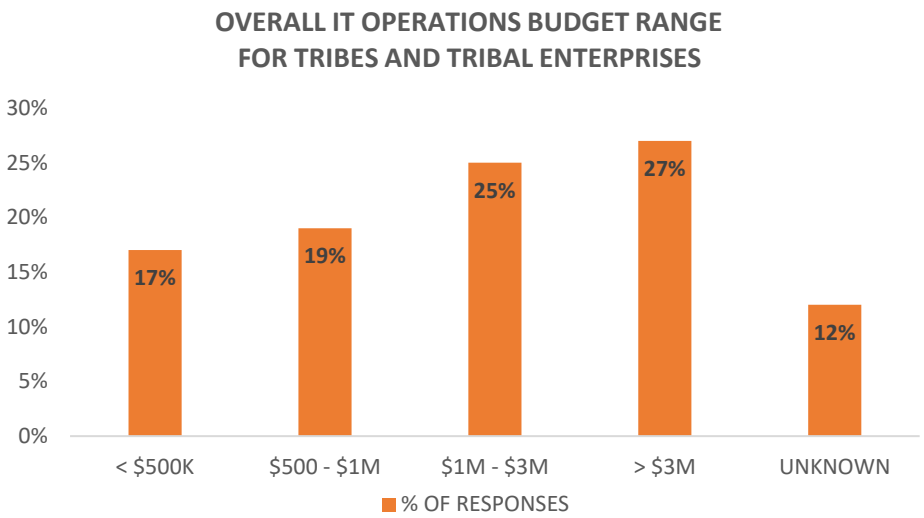
[1] **References**: Info-Tech (2023): Gaming & hospitality innovation ; www.goworkwize.com; www.workforce.com

these benchmarks despite similar regulatory and operational pressures. The absence of dedicated cyber roles in many organizations leaves critical assets exposed and slows incident response.

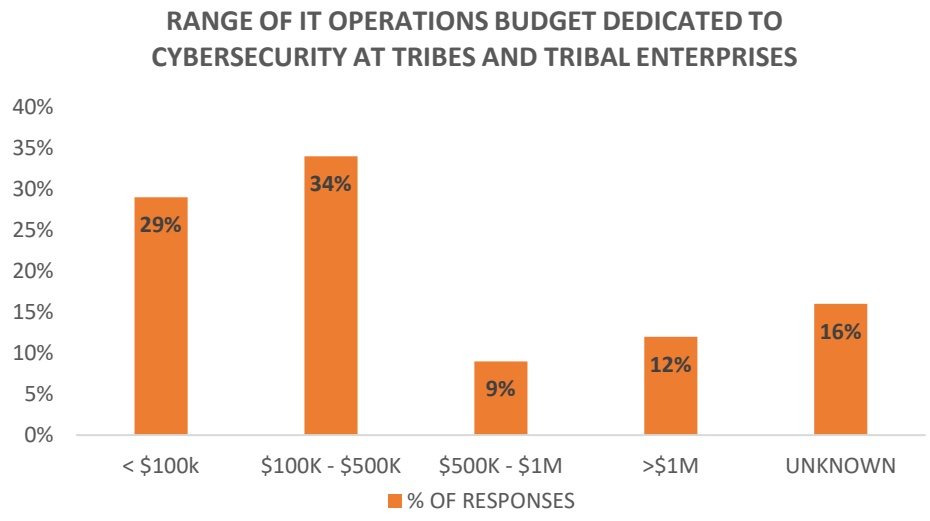
As cyber resilience takes center stage, right-sizing IT teams and diversifying skill sets are becoming essential strategies. Tribes and tribal enterprises must align technical capacity with emerging threats, regulatory demands, and operational priorities, ensuring their teams are agile, well-balanced, and equipped to adapt to evolving cybersecurity landscapes.

Cybersecurity Budget

The cybersecurity investment trends across IT budgets reveal a nuanced picture of how tribes and tribal entities are budgeting for cybersecurity relative to their overall IT spend in 2025. The survey shows that most IT budgets exceed $1 million, yet cybersecurity allocations remain modest. A large portion of respondents, regardless of total IT spend, continue to invest less than $100K in cybersecurity, often distributing those limited funds thinly across personnel, tools, and third-party services. This signals a reactive posture, with minimal capacity for strategic risk management or sustained program development.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Encouragingly, a growing segment is investing $100K–$500K, with more deliberate allocation patterns emerging. These organizations are channeling higher percentages of their cybersecurity budgets into tools and third-party services, while personnel investment remains relatively low. This suggests a reliance on external expertise and technology to compensate for lean internal teams, an approach that may offer short-term coverage but limits long-term resilience and cultural integration.

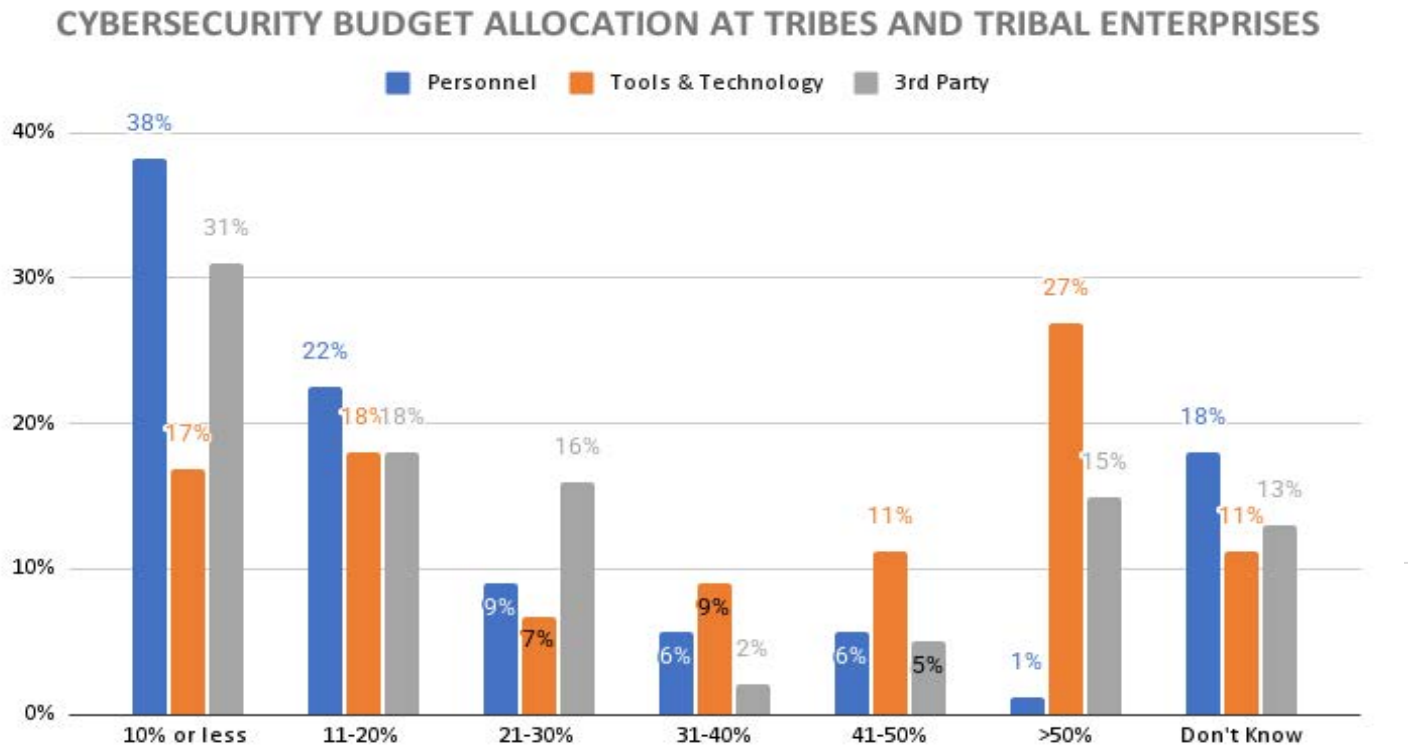
At the highest end, a small group is investing over $1 million in cybersecurity, with more than 50% of that spend directed toward internal personnel. These organizations are building in-house capacity, signaling advanced maturity and a strategic shift toward embedded, culturally aligned cybersecurity governance.

For tribal governments and executive leaders, the data underscore a critical opportunity to recalibrate cybersecurity investment in proportion to operational scale, risk exposure, and sovereignty priorities. Elevating internal capacity, especially through culturally competent personnel, will be key to sustaining trust, resilience, and transformation.

Cybersecurity Budget Allocation

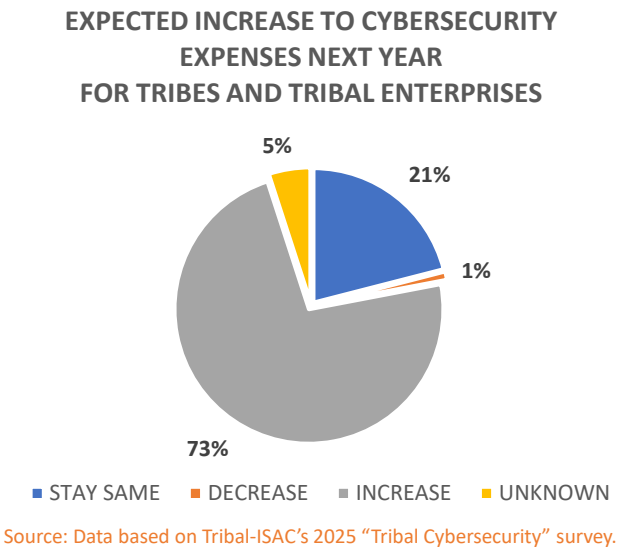
Across all tribal entities surveyed, cybersecurity budget allocation reveals a consistent prioritization of tools and technology over staffing and third-party services. Personnel investment is typically low, with most respondents allocating 10% or less of their cybersecurity budget to internal staffing, including FTEs and contractors. In contrast, tooling receives the most concentrated investment, with a notable portion of organizations dedicating more than 50% of their cybersecurity budget to tools. This pattern underscores a strategic reliance on technical solutions to manage risk, particularly in environments with constrained staffing.

Third-party services, including Managed Security Service Providers (MSSPs) and outsourced security providers, show greater variability. While many organizations allocate 10% or less to external support, a notable share report allocations exceeding 21%, with some surpassing 50%. Overall, the data reflect a tooling-first approach to cybersecurity investment, with personnel and services receiving more variable levels of funding.



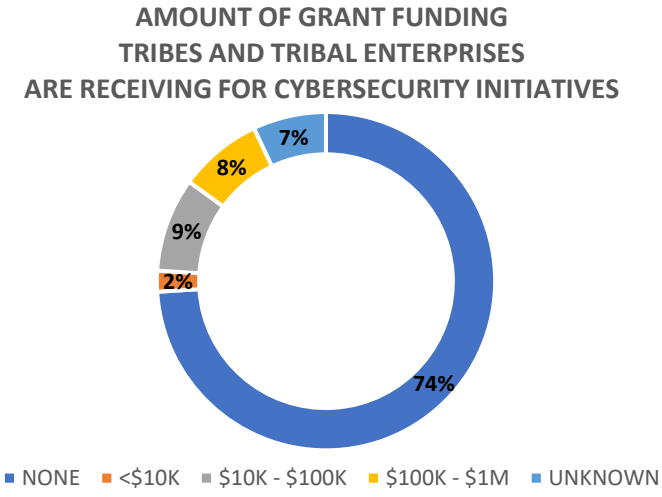
Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

A strong majority, 73% of respondents, expect their cybersecurity expenses to increase in the coming year, signaling heightened awareness of digital threats and growing investment in cyber resilience. Just 1% anticipate a decrease in spending; 21% expect costs to remain stable. This upward trend reflects a strategic shift toward strengthening defenses, meeting compliance requirements, and addressing emerging risks.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

While there are federal and state grant funds available, 74% of respondents received no grant funding for cybersecurity initiatives in 2025. Only a small portion secured external support. While some tribal entities are accessing cyber-related funding, the vast majority have yet to benefit from available grant programs.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Budget Priorities for Cybersecurity and IT in 2025–2026

The Tribal Cybersecurity Survey data highlight a clear directional shift in cybersecurity budgeting among IT leaders at tribes and tribal enterprises. Nearly one-third of respondents asking for increased budget funding in 2025 or in 2026 will request service expansion, with investments targeting new tools, platform enhancements, and third-party integrations. This signals a proactive stance on threat mitigation and infrastructure modernization. Close behind, staffing investments reflect a growing commitment to internal capability-building. Leaders are allocating funds to recruit, retain, and upskill cybersecurity talent, reinforcing the importance of workforce resilience in regulated environments.

INCREASED BUDGET FUNDING ASKS BY TRIBES AND TRIBAL ENTERPRISES	% OF RESPONSES	DESCRIPTION
SERVICE EXPANSION	32%	INCLUDES NEW 3RD PARTY SERVICES AND ADD-ONS TO EXISTING PLATFORMS
STAFFING INVESTMENT	29%	INCLUDES STANDALONE STAFFING AND COMBINATIONS WITH TRAINING OR SERVICES
TRAINING INVESTMENT	17%	INCLUDES STANDALONE TRAINING AND COMBINATIONS WITH SERVICES OR ADD-ONS
NO STATED PRIORITIES	11%	INCLUDES RESPONSES INDICATING NO CURRENT BUDGET FOCUS
MIXED/MULTI-FOCUS RESPONSES	11%	INCLUDES COMBINATIONS SPANNING ALL CATEGORIES (E.G., STAFFING + TRAINING + SERVICES + ADD-ONS)

Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Training initiatives, while less dominant, remain a critical layer, often bundled with other priorities to support broader transformation goals. Notably, a small segment reported no current budget focus, which may indicate fiscal constraints or delayed planning cycles. A subset of respondents selected multi-focus strategies, combining staffing, training, and service expansion, suggesting a more integrated approach to cybersecurity readiness. Tribal entities are balancing external solutions with internal capacity-building, positioning themselves for scalable, secure growth in increasingly complex threat landscapes.

Cybersecurity Readiness

The Tribal Cybersecurity Survey data highlight uneven adoption of foundational cybersecurity planning documents, including Incident Response Plans (IRPs), Disaster Recovery Plans (DRPs), and Business Continuity Plans (BCPs), with limited implementation of Tabletop Exercises (TTX) and Third-Party Risk Management, both of which are critical for operational resilience and supply chain security.

CYBERSECURITY PLANNING TOOLS AT TRIBES AND TRIBAL ENTERPRISES	YES	NO	DON'T KNOW
INCIDENT RESPONSE PLAN	61%	37%	2%
DISASTER RECOVERY PLAN	55%	40%	5%
BUSINESS CONTINUITY PLAN	37%	60%	3%
TABLETOP EXERCISES	44%	56%	0%

Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

While foundational planning is underway, IT teams at tribes and tribal enterprises face strategic opportunities to strengthen continuity, vendor oversight, and response validation through more comprehensive and practiced frameworks. Incident Response Plans are the most consistently adopted across IT organizations at tribes and tribal enterprises, reflecting a strong focus on immediate threat containment and operational response. Disaster Recovery Plans are in place for over half of the organizations, signaling growing attention to technical recovery readiness. Still, over half remain without formal Business Continuity Plans, highlighting an opportunity to close critical resilience gaps. In contrast, Business Continuity Planning and Third-Party Risk Management remain underdeveloped, pointing to limited preparedness for sustained disruptions and vendor-related risks. Tabletop Exercises are also infrequent, suggesting that many organizations are not actively testing their plans or validating response coordination.

CYBERSECURITY PREPAREDNESS AT TRIBES AND TRIBAL ENTERPRISES	YES	NO	DON'T KNOW
TRAINING FOR ALL EMPLOYEES	82%	18%	0%
CYBER INSURANCE COVERAGE	81%	13%	6%
FORENSICS FIRM ON RETAINER	47%	44%	9%

Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

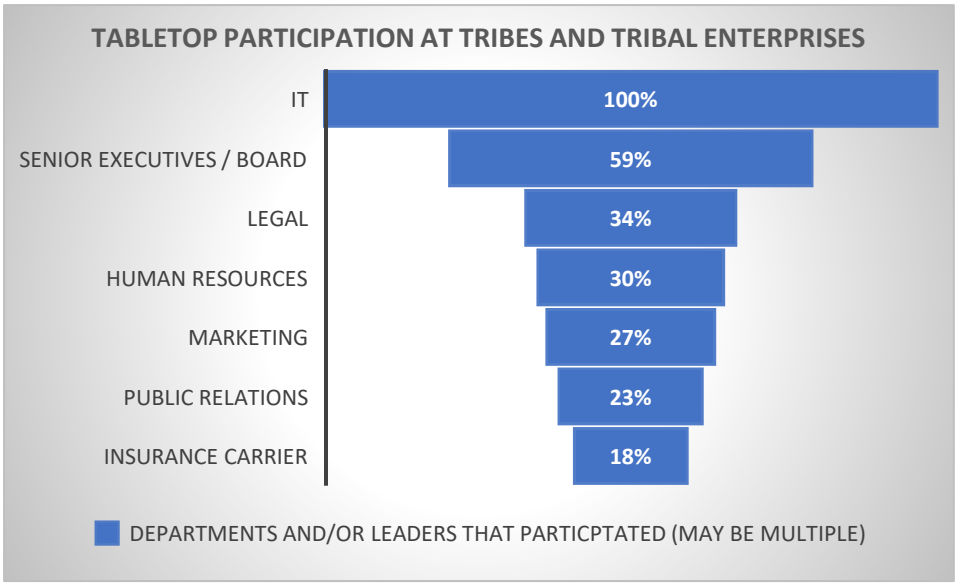
Training and cyber insurance coverage show strong adoption across tribal entities, reflecting a positive cultural investment in awareness. Forensic readiness is mixed, some organizations have formal breach response support in place, while others lack external partnerships, exposing potential gaps in incident investigation and containment.

While over half of the respondents have IRPs and DRPs, 56% have not conducted tabletop exercises revealing a critical gap in preparedness. Without regular simulation, plans may remain theoretical and untested. Roles and responsibilities can be unclear during real incidents and recovery timelines and dependencies may be misaligned with actual capabilities.

The disparity between plan adoption and exercise execution suggests a need for operational validation through scenario-based testing, cross-functional engagement to ensure plans are actionable, governance alignment to support funding, compliance, and tribal sovereignty goals.

Across tribal entities, tabletop exercises are still narrowly scoped, with most participation concentrated in IT and gaming operations. While these exercises are designed to simulate real-world incidents, their current structure often fails to reflect the complexity of actual response scenarios.

IT Tabletop exercises are consistently led by IT, with limited involvement from other key functions.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Senior executives, legal, human resources, marketing, and public relations are often absent, and insurance carriers are rarely included.

This narrow participation suggests that exercises are still treated as technical drills rather than enterprise-wide readiness efforts. Expanding stakeholder engagement is essential to building more comprehensive, culturally aligned response strategies.

Operational Focus of Cybersecurity Tabletop Exercises

TABLETOP DOMAIN EXERCISED BY TRIBES AND TRIBAL ENTERPRISES	% OF EXERCISES *
GAMING	76.3%
TRIBAL GOVERNMENT	47.4%
HEALTH	23.7%
PUBLIC SAFETY	21.1%
TRIBAL GOVERNMENT BUSINESS OPERATIONS	18.4%
INFORMATION TECHNOLOGY / SECURITY / RISK MANAGEMENT	2.6%
SIMULATED MALWARE REMEDIATION	2.6%

** Some responses included multiple selections*.

Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Gaming operations are the most frequently exercised domain, appearing in over three-quarters of all tabletops.

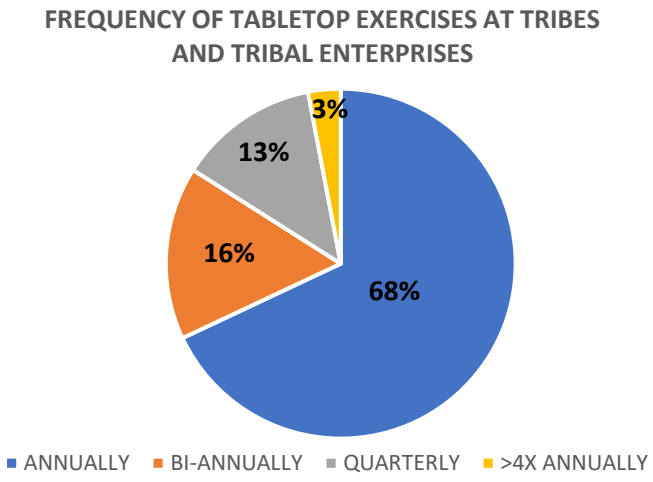
Tribal government and tribal governance areas are included in nearly half of exercises, but often without full integration with health or public safety.

Health and public safety are underrepresented, despite their critical roles in incident response and continuity.

Only 2.6% of exercises focused on technical remediation scenarios (e.g., malware), suggesting a gap in hands-on, threat-specific simulations.

Frequency of Tabletop Exercises

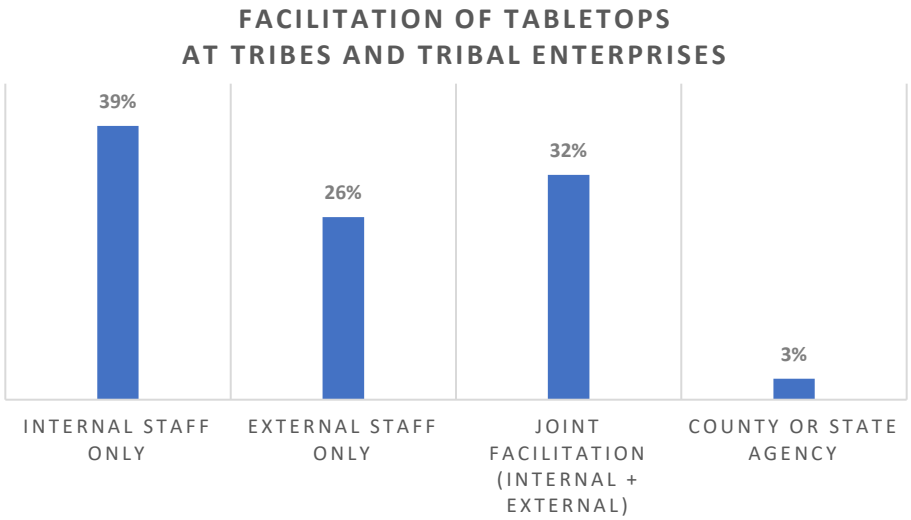
While only 44% of respondents conduct tabletop exercises, annual simulations are the most common cadence, practiced by the majority of participating organizations. More frequent testing, such as semi-annual or quarterly exercises, is less prevalent, with roughly one-third conducting simulations more than once per year. High-frequency, scenario-driven exercises remain rare, suggesting that proactive, iterative testing is still an emerging discipline across IT environments at tribes and tribal enterprises.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Facilitation of Tabletop Exercises

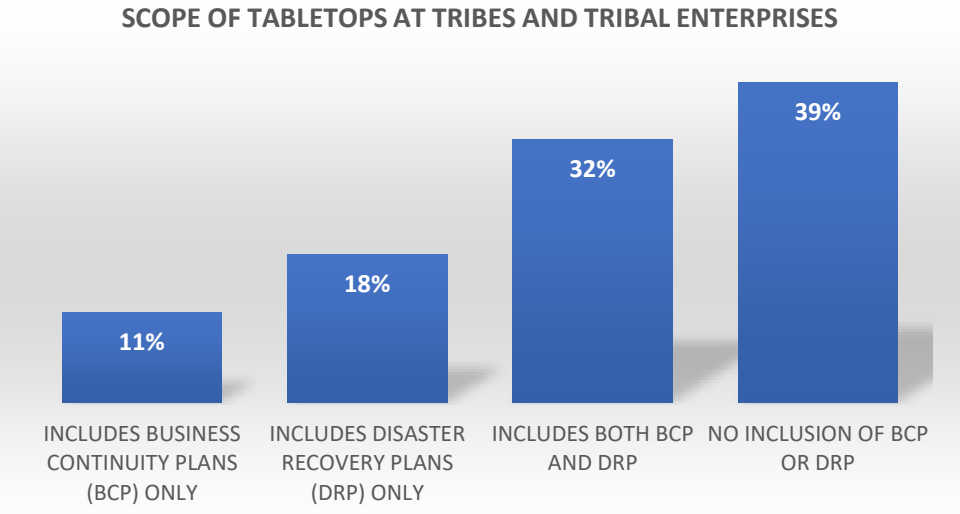
Tabletop facilitation models vary widely, reflecting differences in organizational maturity and resource access. Most exercises are led internally, while a significant portion leverage joint facilitation to balance organizational context with external expertise. Vendor-led sessions are also common, valued for their objectivity and threat modeling capabilities. Public-sector involvement, such as county or state-led exercises, remains limited.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

This mix highlights strategic choices: organizations relying solely on internal facilitation may miss opportunities for external validation, while those engaging outside partners often benefit from enhanced realism, broader threat scenarios, and stronger alignment with compliance standards.

What Do Tabletops Include?



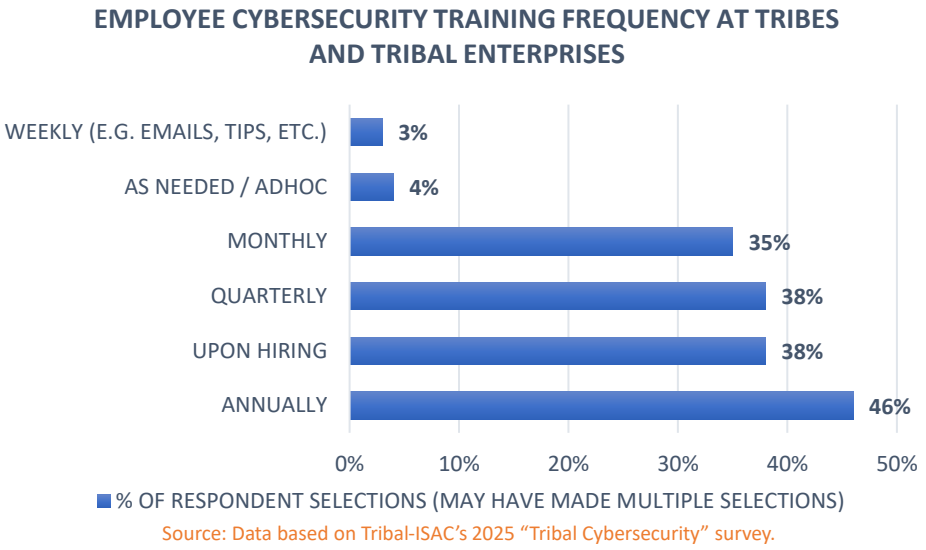
Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

The data reveal a notable gap in comprehensive resilience planning. Nearly 40% of organizations conduct tabletop exercises without incorporating Business Continuity Plans (BCP) or Disaster Recovery Plans (DRP), underscoring a lack of coordinated response and recovery alignment. Full integration of both plans, while not yet widespread, reflects best practice for cross-functional preparedness. Partial inclusion of either BCP or DRP suggests siloed planning approaches and limited enterprise-wide engagement. This distribution reflects varying levels of maturity in resilience strategy and highlights opportunities to strengthen integration across operational and technical domains.

Cybersecurity Training

Tribal organizations face a rapidly evolving cyber threat landscape, where both broad employee awareness and deep technical expertise are essential to resilience. While cybersecurity training and upskilling are often grouped together, they serve distinct purposes and require tailored approaches. The following sections outline the differences, current practices, and strategic importance of each.

Cybersecurity training is not just a compliance checkbox; it's a frontline defense against evolving threats. Employees across all functions represent both risk and opportunity. When equipped with the right knowledge, they become active participants in protecting organizational assets. Regular, role-relevant training helps reduce susceptibility to phishing, strengthens incident response readiness, and fosters a culture of accountability. As tribal and regulated environments face increasingly sophisticated attacks, investing in employee education is essential to building resilient, security-aware teams.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

The survey data show that annual training remains the most common baseline (46%), often paired with onboarding to establish foundational awareness. Quarterly and monthly cadences are gaining traction, appearing in over one-third of responses, reflecting a shift toward continuous engagement. Adaptive training models, tailored to phishing simulation results, individual risk profiles, or product changes, are emerging but still rare. Weekly awareness efforts, such as "Threat Thursday," are used by a small subset, suggesting room to expand microlearning strategies that reinforce secure behaviors in real time.

Cybersecurity training for employees builds the foundation of organizational security. It promotes secure behavior, reduces human error, and supports a culture of vigilance. While frequency and personalization are improving, tribal entities have an opportunity to expand microlearning and adaptive models to strengthen everyday awareness.

Upskilling Cybersecurity for Technical Talent

Upskilling technical talent is a deeper, role-specific investment in professional development. It targets IT staff, security analysts, engineers, and other technical roles responsible for implementing, managing, and defending systems. In this context, upskilling is not optional, it is essential to maintain operational integrity, protect tribal sovereignty, and ensure long-term resilience. Yet current approaches remain uneven. Many organizations rely on reactive or informal training, which may leave teams unprepared for emerging threats or compliance shifts. Certification support is inconsistently offered, and scalable online platforms are underused, despite their potential to deliver cost-effective, flexible learning. A small but notable segment reports no structured training at all, highlighting critical gaps in capacity and readiness.

In response to the question *"How are you continually upskilling your cyber staff?"* the most common strategy was conference attendance, cited in nearly 75% of responses, often paired with certification reimbursement or access to training platforms. This suggests that in-person learning, and peer engagement remain central to cybersecurity development at tribes and tribal enterprises but may not be sufficient on their own.

CYBERSECURITY UPSKILLING METHODS AT TRIBES AND TRIBAL ENTERPRISES	% OF RESPONDENTS*
CONFERENCE ATTENDANCE *(Includes all variations: standalone, bundled with certifications or platforms)*	74%
COMPENSATION FOR CERTIFICATIONS *(Includes direct mentions and bundled responses)*	45%
ONLINE TRAINING PLATFORMS *(Includes TribalWise, Pluralsight, Udemy, Stormwind, ACI, Info-Tech)*	15%
GENERAL TRAINING / FREE RESOURCES *(Includes "training," "free training," "state homeland security," "access to materials")*	7%
NO TIME / NO DEDICATED STAFF / NONE *(Includes "no," "none," "no time," "we don't," "no dedicated staff")*	6%

Note: Some responses included multiple selections, so percentages reflect overlapping strategies.

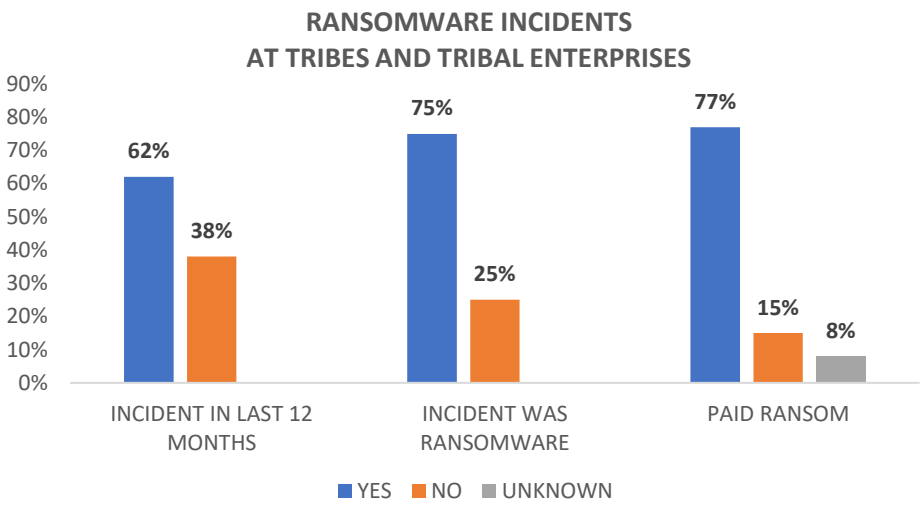
Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Upskilling cybersecurity professionals is a strategic imperative. It builds technical depth, supports retention, and prepares teams for complex threats and compliance demands. While conference attendance and certification support are common, tribal entities must move toward structured, scalable development models to close readiness gaps and build internal leadership pipelines.

Threat Landscape & Response

While most respondents report no recent cybersecurity incidents, the data reveal that a meaningful minority have experienced actionable threats, with ransomware emerging as the dominant attack type.

Nearly a quarter of respondents reported experiencing an actionable incident of significant severity where they had to implement their incident response plan. Among those who did report an incident, 62% occurred within the last 12 months, indicating that threats are not just theoretical, they are current and active.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Ransomware stands out as the most common form of attack. Of those who experienced an incident in the past year, 75% identified it as ransomware, underscoring its prevalence and disruptive potential.

Despite the severity of ransomware attacks, most organizations chose not to pay. Among those affected: 77% did not pay the ransom, 15% did pay, 8% preferred not to disclose.

This suggests a strong posture of resistance and resilience, though it also raises questions about recovery capabilities, insurance coverage, and forensic readiness, especially for those who declined to pay and had to restore systems independently. The low overall incident rate (under 25%) may reflect strong prevention efforts, or underreporting due to limited detection, documentation, or cultural reluctance to disclose. The high concentration of ransomware among reported incidents reinforces the need for regular tabletop exercises simulating ransomware scenarios, clear decision-making protocols around ransom response, strong backup, recovery, and forensic capabilities. The majority 'refused to pay' aligns with best practices but also implies a need for robust continuity planning and post-incident support.

Tribal entities should continue to strengthen their ransomware defenses while ensuring that incident response plans are tested, cross-functional, and culturally aligned. Investing in detection, reporting, and recovery capabilities will be key to maintaining sovereignty, operational continuity, and community trust in the face of evolving threats.

Cybersecurity Frameworks & External Engagement

Common Frameworks

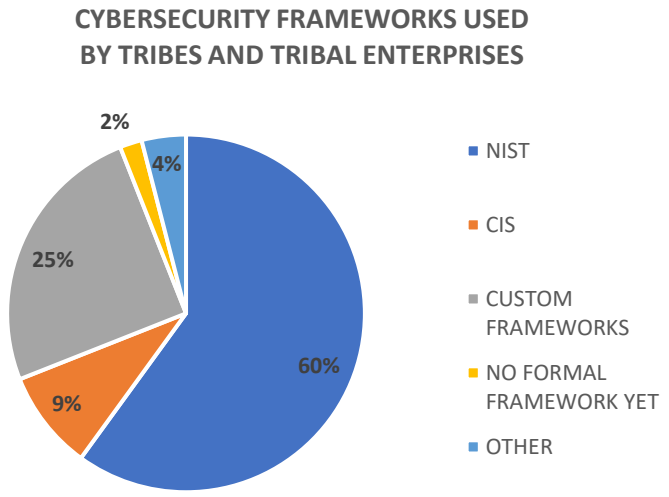
The data reveal a strong preference for formal cybersecurity frameworks, with National Institute of Standards and Technology (NIST) emerging as the dominant standard across tribal entities. However, a notable portion of respondents still rely on custom or hybrid approaches, indicating varied maturity levels and evolving governance strategies.

NIST is utilized by 60% of respondents, affirming its role as the de facto standard for cybersecurity governance, especially in tribal environments. The dominance of NIST reinforces its importance for tribal sovereignty, federal grant alignment, and structured risk management. Organizations not yet aligned with NIST may face challenges in demonstrating readiness or securing funding.

Tailored approaches to cultural or operational needs, or early-stage maturity where formal adoption is still underway is suggested by 25% reporting custom framework utilization.

The reliance on custom frameworks presents both opportunity and risk:

- Opportunity: Tailored governance models can reflect cultural values, operational uniqueness, and sovereignty.
- Risk: Lack of standardization may hinder benchmarking, compliance, and incident response coordination.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Center for Internet Security (CIS) based models (including CIS, CIS Controls, and CIS Critical Controls) collectively account for 9%, with some organizations planning to transition to NIST within 3–5 years. The CIS-to-NIST migration path suggests a practical roadmap for organizations seeking gradual maturity, especially those with limited resources or early-stage programs.

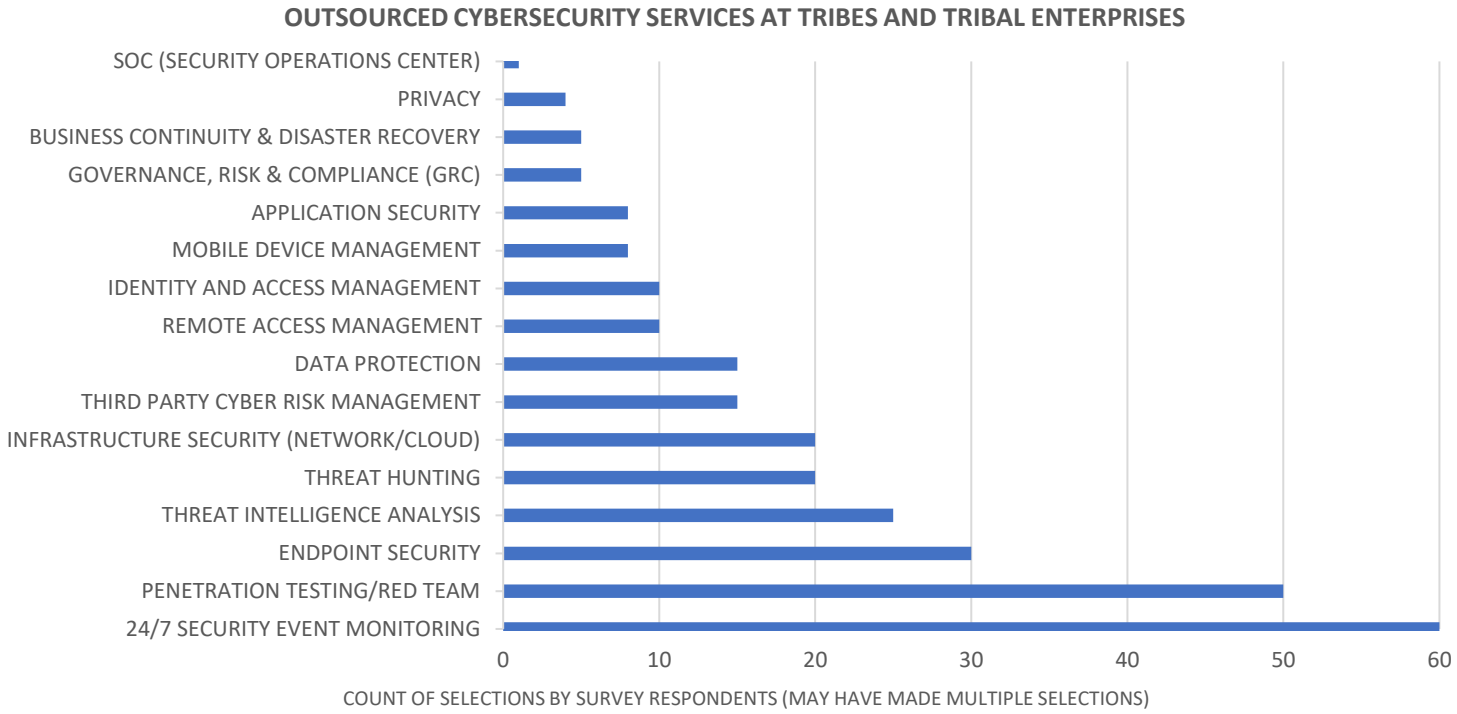
Other frameworks such as MITRE ATT&CK, HIPAA, and Palo Alto appear in isolated use cases (4%), likely to reflect specific threat modeling, compliance, or vendor-driven strategies.

A small number of respondents (2%) are not currently using a formal framework, but express intent to adopt NIST or are informally aligned with its principles.

Organizations are encouraged to promote framework literacy and crosswalks to help leaders and IT teams at tribes and tribal enterprises understand how different models interrelate and support sovereignty, resilience, and compliance.

Outsourced Cybersecurity Services Trends

As cyber threats grow in scale and sophistication, tribal entities are increasingly leveraging external partners to enhance their security posture. A review of outsourcing patterns reveals a clear stratification of services, driven by risk exposure, regulatory demands, and operational capacity.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Core services such as penetration testing, 24/7 security event monitoring, and endpoint protection are the most frequently outsourced. These functions form the backbone of proactive threat detection and response, often delivered as bundled offerings through Managed Security Service Providers (MSSPs). Their widespread adoption reflects a strategic shift toward continuous visibility and rapid containment.

Advanced threat capabilities, including threat hunting and threat intelligence analysis, are also commonly outsourced, particularly by organizations lacking in-house expertise. These services provide deeper insight into attacker behavior and emerging risks, enabling faster and more informed decision-making.

Mid-tier services like infrastructure security, data protection, and identity and access management are often added to broader engagements. Their inclusion typically depends on cloud adoption, compliance requirements, and internal capacity to manage sensitive systems and access controls.

In contrast, specialized domains such as governance, risk, and compliance (GRC), business continuity, and privacy are less frequently outsourced. These areas are closely tied to tribal sovereignty, cultural values, and strategic planning, leading many organizations to retain internal oversight or selectively engage consultants with deep cultural and regulatory fluency.

A notable trend is the growing emphasis on third-party cyber risk management, reflecting increased scrutiny of vendor ecosystems and supply chain vulnerabilities. This shift signals a maturing understanding of systemic risk and the need for holistic oversight beyond the organizational perimeter.

Across all tiers, outsourcing decisions are evolving from purely technical evaluations to more strategic assessments. Tribal entities are prioritizing vendors who not only deliver operational excellence but also align with governance structures, demonstrate transparency, and support culturally grounded cybersecurity strategies.

Staying Informed

In today's threat landscape, timely access to actionable intelligence is essential for tribal entities to safeguard sovereignty, member data, and operational integrity. Tribal entities rely on a blend of structured collaboration and informal networks to stay informed about critical cyber threats. The most trusted and widely used source is the Tribal Information Sharing and Analysis Center (Tribal-ISAC), cited by 65% of respondents, reflecting strong engagement in tribal-specific intelligence sharing. The Multi-State Information Sharing and Analysis Center (MS-ISAC) follows closely at 61%, underscoring the importance of multi-state coordination.

While formal Information Sharing and Analysis Centers (ISACs) dominate, nearly half of respondents also turn to news monitoring services and peer groups for real-time insights and contextual awareness. A smaller segment supplements their intel through federal agencies, Managed Security Service Providers (MSSPs), mailing lists, and conferences, highlighting the diverse ecosystem tribes navigate to maintain cyber vigilance.

This distribution reveals a clear preference for community-driven, trusted networks, with Tribal-ISAC at the center of daily threat awareness.

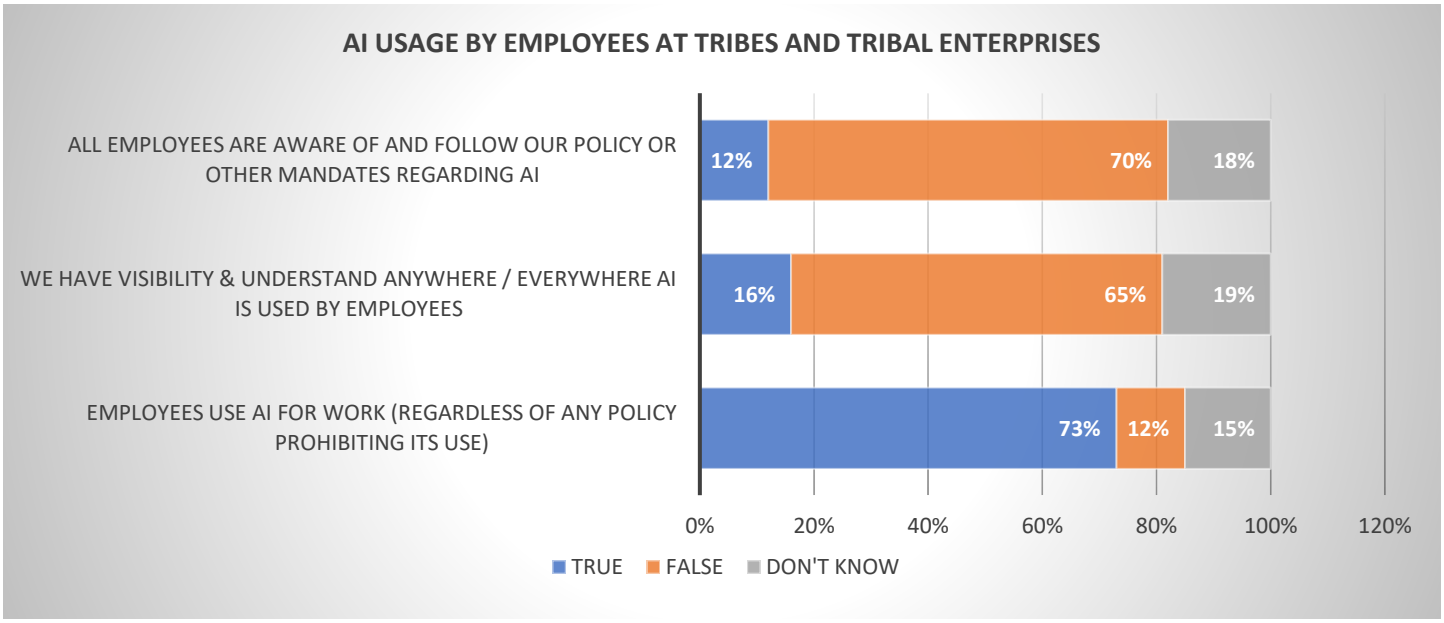
THREAT INTELLIGENCE SOURCES AT TRIBES AND TRIBAL ENTERPRISES	% OF RESPONDENTS*	DESCRIPTION
TRIBAL-ISAC	65%	TRIBAL-FOCUSED INTEL SHARING AND COLLABORATION
MS-ISAC	61%	MULTI-STATE ISAC ALERTS AND ADVISORIES
NEWS MONITORING SERVICES	44%	NEWS OUTLETS, VENDOR BULLETINS, PODCASTS, CUSTOMER RELATIONSHIP MANAGEMENT (CRM) UPDATES
PEER GROUPS	38%	INTERNAL TEAMS, INDUSTRY EXPERTS, PROFESSIONAL NETWORKS
OTHER	20%	CISA, FBI, HOMELAND SECURITY, MSSPS, MAILING LISTS, CONFERENCES, ETC.

** Some responses included multiple selections, so percentages reflect overlapping strategies.*

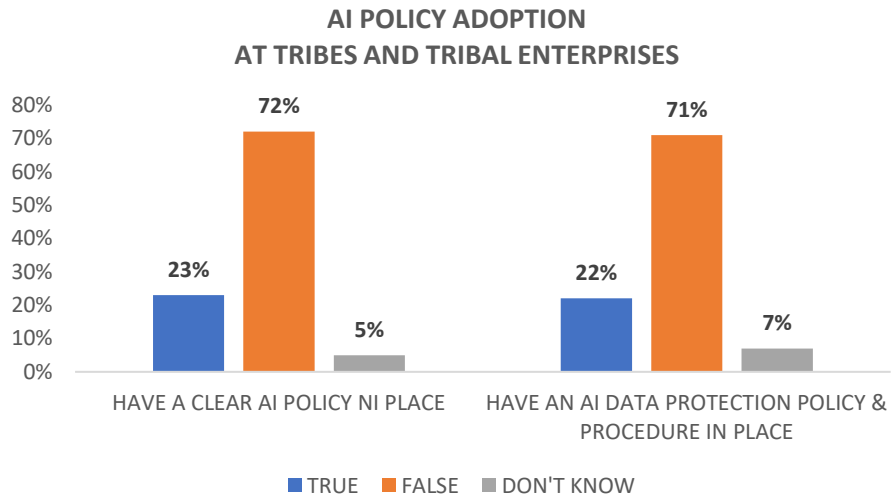
Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

AI Planning for the Future – A Rising Cyber Threat

At TribalHub's 2025 Regional Forums, Artificial Intelligence (AI) emerged as a central theme. While most tribal entities report active use of AI tools, often ahead of formal governance, few have established clear policies or data protection procedures. In some cases, AI is being used despite technical prohibitions, underscoring a lack of oversight and visibility.

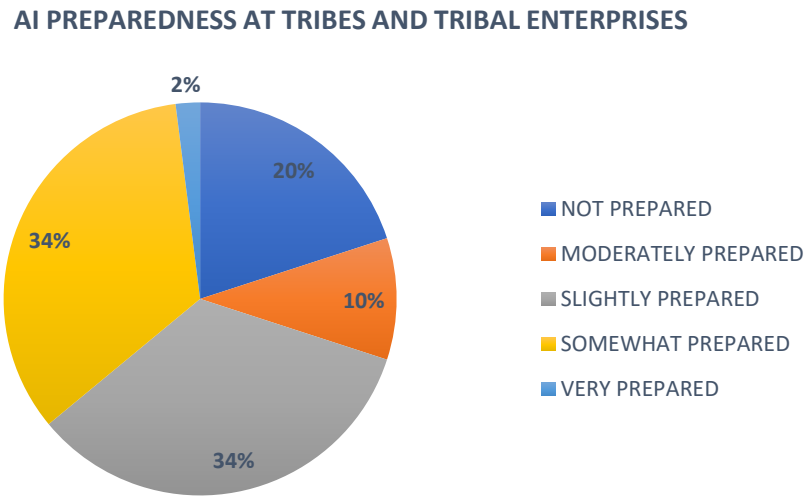


Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?" survey.



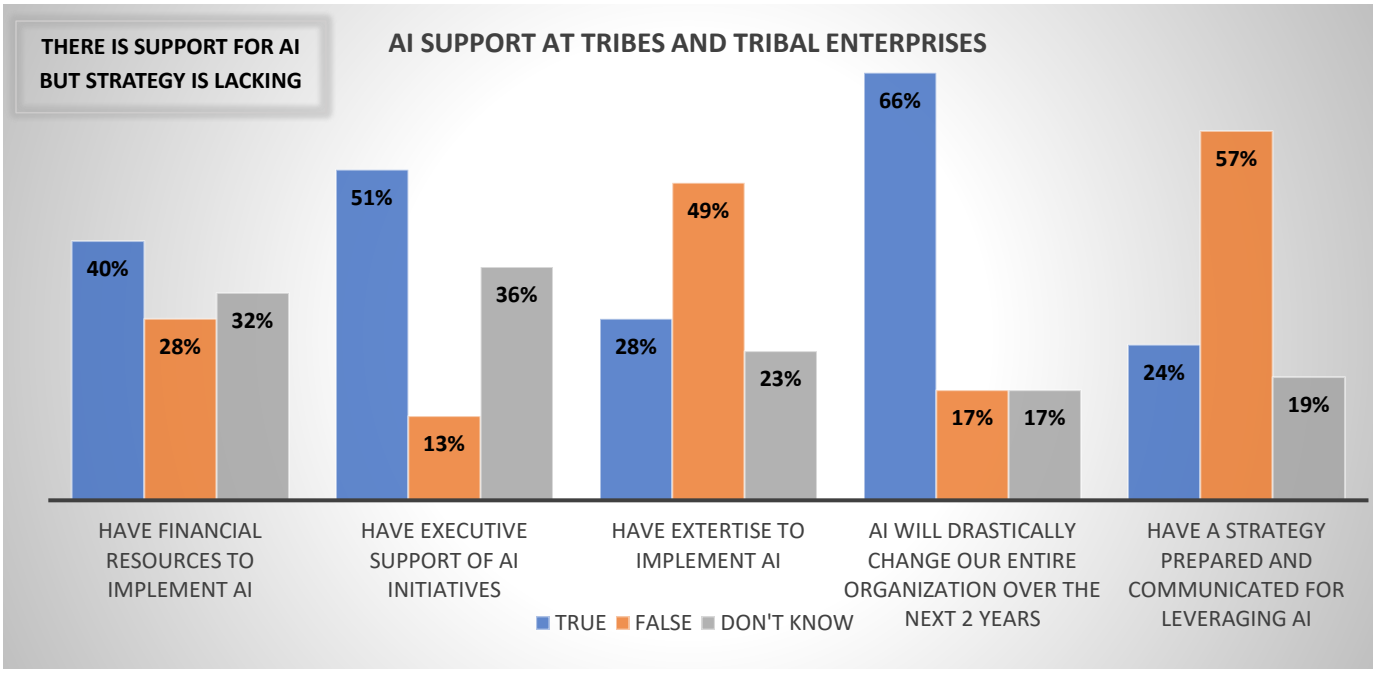
Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?" survey.

Preparedness levels vary widely. Only a small fraction feels fully ready to implement AI, while many describe themselves as moderately or slightly prepared. A notable segment remains entirely unprepared. Despite this, there is broad consensus that AI will significantly reshape tribal entities within the next two years.



Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?" survey.

Support for AI initiatives is uneven. Some organizations benefit from executive backing and financial resources, but internal expertise and strategic planning remain limited. Change management capabilities are more commonly in place, but strategic planning around AI is still lagging.



Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?" survey.

To address this gap, tribal entities must treat AI governance as a leadership and cultural imperative. Developing AI-use policies and data protection procedures, aligned with tribal sovereignty is essential. These should define acceptable use, decision-making boundaries, model training safeguards, and member data protections, all grounded in transparency, consent, and community benefit.

Improving Cybersecurity Posture: Insights and Resources

Emerging/Rising Threats & Resilience Building Measures

Gate 15 serves as a strategic intelligence partner to the Tribal Information Sharing and Analysis Center (Tribal-ISAC), delivering threat-informed, risk-based analysis that supports member resilience. Through daily alerts, monthly summaries, and quarterly insights, Gate 15 provides critical intelligence products designed to inform proactive risk mitigation across tribal entities. This section presents a curated selection of emerging and rising threat trends, along with recommended mitigation strategies shared by Gate 15 over the past year.

Ransomware remains a major threat, with a reported 126% global increase in 2024. The Cybersecurity and Infrastructure Security Agency's (CISA's) #StopRansomware Guide offers a roadmap for prevention and response. Equally as critical as technical controls are non-technical preparedness, engaging executives, employees, partners, and pre-written communication templates is highlighted as essential for coordinated response, reputational protection, and rapid recovery.

Business Email Compromise (BEC) continues to evolve in complexity, with threat actors leveraging cryptocurrency laundering, deepfake technologies, and even state-sponsored tactics to bypass traditional defenses. With over $55.5 billion in global losses since 2013, BEC is no longer just a phishing problem, it is a business risk requiring executive-level attention.

Recommended safeguards include:

- Multi-Factor Authentication (MFA): A critical barrier against unauthorized access to email and financial systems
- Phishing Awareness Training: Regular, scenario-based education to help employees recognize social engineering tactics
- Financial Controls: Dual-authorization workflows, vendor verification protocols, and transaction monitoring to prevent fraudulent transfers
- Rapid Incident Response Procedures: Pre-established playbooks and escalation paths to contain and investigate suspected BEC events

Consider integrating BEC scenarios into tabletop exercises to evaluate cross-functional readiness and executive decision-making.

Insider threats, whether from careless mistakes, disgruntled employees, or compromised credentials, pose a unique challenge due to their access privileges and contextual knowledge. These threats often bypass perimeter defenses and can be difficult to detect without behavioral context.

A multi-layered mitigation strategy includes:

- Employee Training: Foster a culture of security awareness and ethical responsibility.
- Behavior Monitoring: Use User and Entity Behavior Analytics (UEBA) to detect anomalies in access patterns or data usage.
- Access Controls: Apply least privilege principles and regularly audit permissions.
- Cross-Departmental Collaboration: Align human resources, legal, IT, and security teams to identify and respond to insider risks.
- Specialized Tools: Leverage frameworks like the Insider Risk Mitigation Program Evaluation (IRMPE) and CISA's National Insider Threat Awareness Month (NITAM) resources to assess and mature your program.

Do not overlook the importance of psychological safety and anonymous reporting channels to surface early warning signs.

New attack vectors are exploiting user trust and automation. Email subscription bombing floods in boxes with legitimate newsletters to obscure real alerts (e.g., password reset emails), while Click Fix malware uses deceptive CAPTCHA pages to trick users into executing malicious scripts.

Defensive measures include:

- Advanced Email Filtering: Use heuristics and reputation-based filtering to detect mass sign-up attempts and spoofed domains.
- Group Policy Restrictions: Limit script execution and browser behavior to reduce exposure to drive-by downloads.
- User Education: Train users to recognize fake support scams, suspicious CAPTCHA prompts, and unusual email behavior.

Consider integrating browser hardening and endpoint detection tools to catch evasive malware tactics.

Security Enhancements for Tribal Entities

As cyber threats grow in scale and sophistication, tribal entities face unique challenges in safeguarding their digital sovereignty, operational continuity, and community trust. A proactive, culturally aligned cybersecurity strategy is no longer optional, it is foundational to tribal governance, economic development, and intergovernmental collaboration.

To build a resilient security posture, tribal entities are urged to prioritize core technical controls, hygiene practices, and strategic threat awareness. The following guidance outlines key measures and resources to strengthen tribal cybersecurity.

FOUNDATIONAL SECURITY ENHANCEMENTS

Tribal organizations can strengthen baseline defenses and reduce risk by implementing the following core practices.

Comprehensive Asset Inventories
Maintain up-to-date records of hardware, software, and cloud assets to support visibility, risk assessment, and incident response.

Strong Password Practices
Enforce complexity standards, regular rotation, and password managers to reduce credential-based attacks.

Multi-Factor Authentication (MFA)
Deploy MFA across critical systems to prevent unauthorized access, even in cases of credential compromise.

Timely Patching
Leverage the Cybersecurity and Infrastructure Security Agency's (CISA's) Known Exploited Vulnerabilities Catalog to prioritize patching of high-risk systems and reduce exposure to active threats.

Secure-by-Design/Default Technologies
Procure solutions from vendors that embed security into their architecture, minimizing configuration errors and reducing attack surface.

Third-Party Risk Management
Conduct due diligence on vendors and train employees to recognize phishing tactics that exploit trusted relationships.

INCIDENT RESPONSE: PLANNING FOR THE INEVITABLE

A well-structured Incident Response Plan (IRP) is essential for minimizing damage, restoring operations, and preserving trust during a cyber event.

Establish Multi-Disciplinary Response Teams
Include IT, legal, communications, and tribal leadership to ensure coordinated action.

Conduct Regular Tabletop Exercises
Simulate realistic scenarios to test readiness, clarify roles, and identify gaps.

Develop Specialized IRPs
Tailor incident response plans for ransomware and other major threats using established frameworks (e.g., National Institute of Standards and Technology (NIST)), to improve preparedness and coordination.

Secure Incident Response Retainers
Pre-arrange contracts with external experts to ensure rapid access to forensic and remediation support.

Define Crisis Communications Protocols
Prepare messaging templates and stakeholder outreach plans to maintain transparency and control the narrative.

DATA PRIVACY: PROTECTING TRIBAL CITIZENS AND SOVEREIGNTY

Data privacy is a cornerstone of tribal digital governance. As data volumes grow and regulations evolve, tribal organizations must embed privacy into their operations.

Data Breach Response Plans
Establish clear procedures for containment, notification, and remediation.

Employee Training on Data Handling
Promote responsible data stewardship across departments.

Integration of the NIST Privacy Framework
Align privacy practices with a recognized standard to support compliance and risk management.

Privacy Impact Assessments (PIAs)
Evaluate the implications of new technologies and data uses on tribal citizens.

Transparent Communication with Stakeholders
Build trust through openness about data practices, breaches, and privacy protections.

THREAT AWARENESS & INTELLIGENCE INTAKE

To enhance cybersecurity posture and foster culturally aligned threat awareness, tribal organizations are encouraged to implement the following practices.

Formalize Threat Intelligence Intake
Establish daily or weekly briefings using Tribal-ISAC, MS-ISAC, and vendor feeds. Assign ownership to a designated cyber lead or vCISO.

Strengthen Tribal-ISAC Engagement
Promote active participation in forums, working groups, and incident sharing. Use Tribal-ISAC as a backbone for cross-tribal coordination.

Diversify and Validate Intel Sources
Supplement peer and news-based intel with structured feeds from MS-ISAC, CISA, and trusted vendors. Regularly assess source reliability.

Integrate Threat Intel into Operational Workflows
Feed intel into security information and event management (SIEM) tools, managed detection and response (MDR) dashboards, or Managed Security Service Providers (MSSP) briefings. Use threat data to inform tabletop exercises, patch cycles, and risk assessments.

Ensure Threat Monitoring Respects Tribal Sovereignty
Align practices with tribal governance, data ownership, and cultural priorities. Advocate for tribal-specific threat sharing protocols in federal and state partnerships.

Federal Resources

Tribal nations are encouraged to embrace a “Resolve to be Resilient” mindset and adopt a “Resilient by Design” approach, investing proactively in both physical and cyber preparedness. This philosophy aligns with the Cybersecurity and Infrastructure Security Agency’s (CISA) Shields Ready campaign, which emphasizes readiness not just to prevent cyberattacks, but to recover swiftly and minimize disruption when incidents occur.

Building a culture of resilience across tribal communities requires more than awareness, it demands access to practical tools, strategic guidance, and sustained support. Fortunately, several federal initiatives offer specific resources to help tribes strengthen continuity planning, incident response, and long-term cybersecurity maturity.

CISR Toolkit - The Cybersecurity and Infrastructure Security Resilience (CISR) Toolkit provides planning templates, assessment tools, and guidance for building robust continuity and response capabilities across tribal operations.

Secure Our World Campaign - CISA’s Secure Our World initiative offers actionable resources for individuals and organizations, including tribes, to improve cyber hygiene, raise awareness, and promote safe online behaviors.

Tribal Cybersecurity Grant Program (TCGP) - This dedicated funding stream enables tribal governments to advance their cybersecurity posture through strategic investments in technology, training, and governance. Recommended resources under this program include:

- Cyber Hygiene Services: Free vulnerability scanning and risk assessments for tribal networks.
- Nationwide Cybersecurity Review (NCSR): A voluntary, annual self-assessment that helps tribes benchmark their cybersecurity maturity against national standards.

To help tribes prioritize their efforts, CISA offers the Cross-Sector Cybersecurity Performance Goals (CPGs), a set of 38 voluntary practices designed to improve resilience across critical infrastructure sectors. These goals are risk-informed and impact-driven, adaptable to tribal environments, and focused on high-value outcomes. Of these, 21 goals are low-to-no-cost, and 14 are considered high-impact with low implementation complexity, making them ideal starting points for resource-constrained tribal entities.

Tribal-ISAC – How We Help…

The Tribal Information Sharing and Analysis Center (Tribal-ISAC) fosters a trusted, collaborative environment, by tribes, for tribes to share threat intelligence, exchange leading practices, and strengthen collective cybersecurity resilience. We protect tribal sovereignty by applying the Traffic Light Protocol (TLP) to all shared reports and by serving as a secure conduit between tribal entities and federal partners such as the Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI), and other critical infrastructure stakeholders. Our mission is to improve the security posture of tribal nations through culturally aligned information sharing and coordinated response.

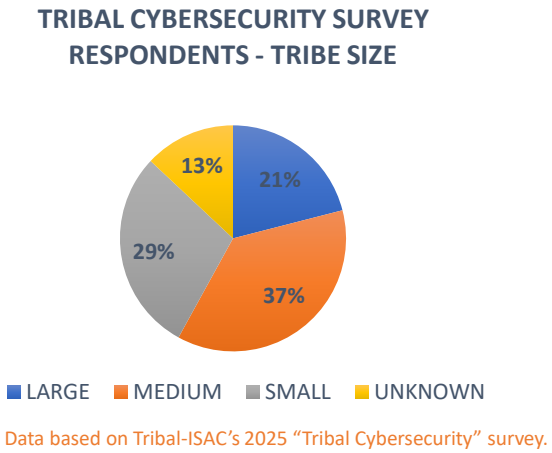
Members of the Tribal-ISAC gain access to a robust suite of resources designed to mitigate threats and support cybersecurity readiness and response at tribes and tribal enterprises:

- Discounted access to cybersecurity-focused networking events nationwide
- Community discussion board for peer exchange and collaboration
- Tribal-ISAC portal for secure document sharing
- Daily threat intelligence feeds tailored to tribal relevance
- Monthly reports and virtual meetings
- Annual tribal cybersecurity report
- Coordinated response to federal cybersecurity initiatives
- Tabletop exercise grant program
- Secure incident reporting
- Lessons learned from real-world incidents
- And much more

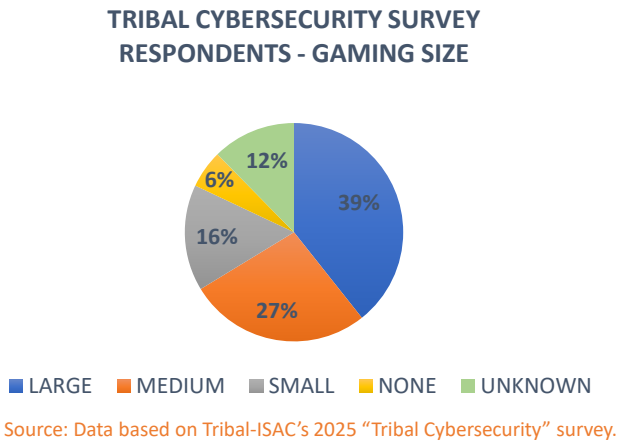
The Tribal-ISAC is a proud member of the National Council of ISACs (NCI), a coordinating body that facilitates secure information flow across key private and non-federal critical infrastructure sectors. This includes collaboration with the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Retail and Hospitality Information Sharing and Analysis Center (RH-ISAC), and other sector-specific Information Sharing and Analysis Centers (ISACs)—ensuring voices at tribes and tribal enterprises are represented in national cybersecurity efforts.

Appendix A: Tribal Cybersecurity Survey Information

The 2025 Tribal Cybersecurity Survey was distributed to 369 IT leaders at tribes and tribal enterprises. With 89 responses, the survey achieved a 24% response rate, indicating meaningful engagement across Indian Country. The response rate reflects active participation from IT leadership at tribes and tribal enterprises, despite competing priorities and resource constraints.



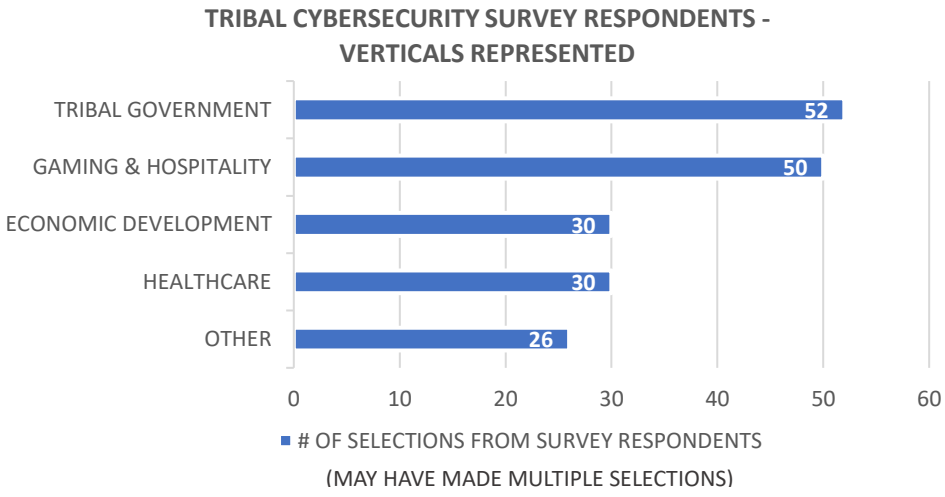
Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

Respondents span a range of tribe sizes (Large - Over 7,500 Members / Medium - 2,001 – 7,500 Members / Small - Up to 2,000 Members) and gaming operations (Large - Over 1,200 slots / Medium - 501 – 1,200 slots / Small - Up to 500 slots), with notably strong engagement from medium and small tribes, suggesting broad relevance of the survey topics.

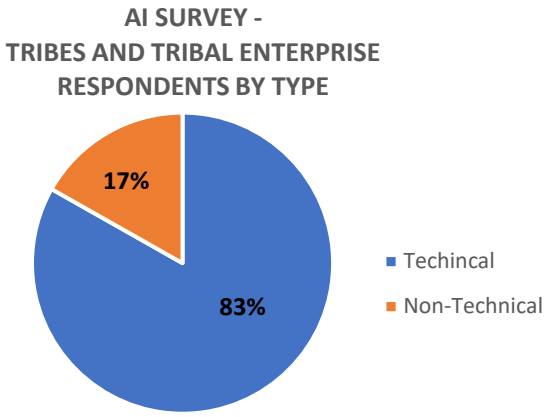
Survey participants reflected a wide range of operational domains, underscoring the interconnected nature of technology leadership across sectors. Respondents frequently cited multiple verticals, highlighting the cross-functional responsibilities of IT teams at tribes and tribal enterprises.



Source: Data based on Tribal-ISAC's 2025 "Tribal Cybersecurity" survey.

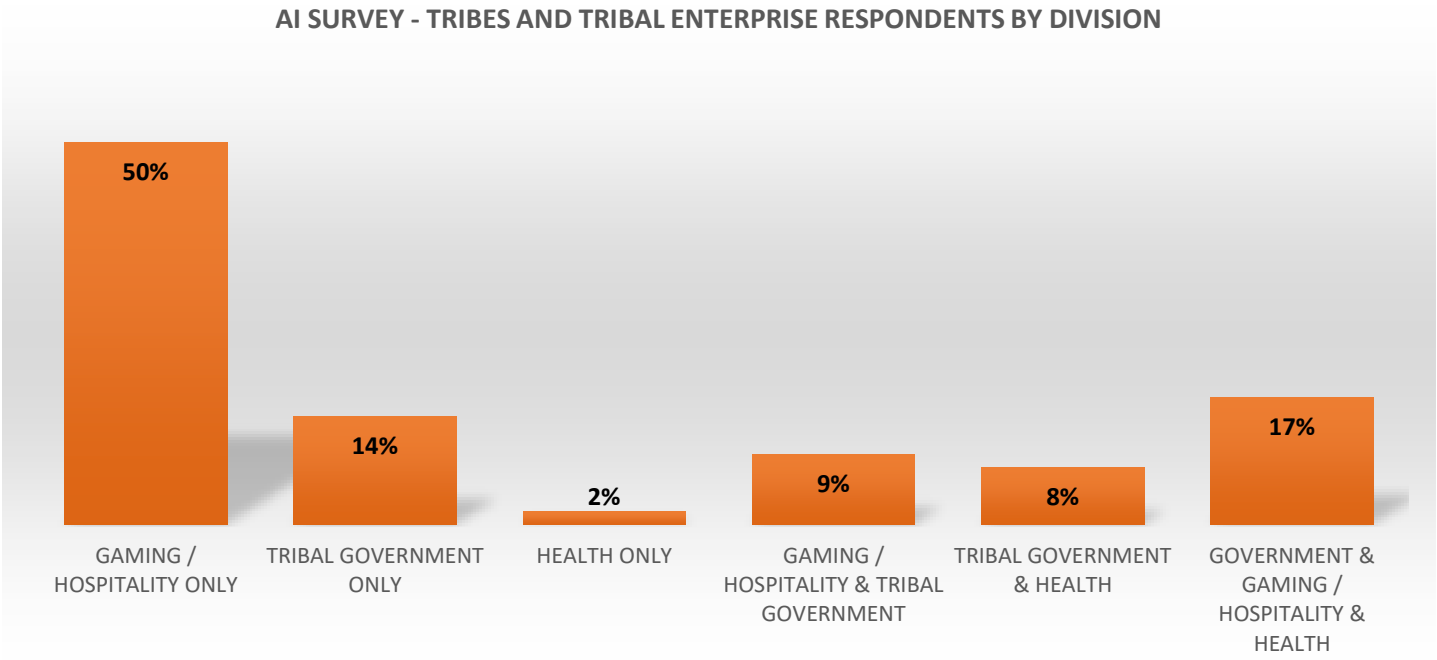
Appendix B: How Prepared is Your Tribe for AI Survey Information

Survey data from TribalHub's 2025 Regional Tribal Technology Forums reveal strong participation from technical departments, underscoring the central role of IT professionals in shaping cybersecurity and artificial intelligence (AI) strategy at tribes and tribal enterprises. While non-technical respondents were present, their representation was notably lower, highlighting an opportunity to broaden engagement across operational functions.



Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?"

Respondents spanned a variety of divisions at tribes and tribal enterprises, with Gaming/Hospitality leading in representation. Tribal Government-only and blended divisions, such as Tribal Government & Gaming/Hospitality or Tribal Government & Health, also contributed meaningfully. Health-focused roles appeared less frequently, and divisions like finance or administration were not explicitly captured in the survey categories.



Source: Data based on TribalHub's "How Prepared is Your Tribe for AI?"

Looking Ahead

Thanks to all those who participated in the surveys that enabled this first annual edition of *The Pulse: The State of Cybersecurity Within Tribal Nations - Cybersecurity Insights, Trends & Threats Across Tribal Government, Health, and Enterprises*. Your contributions have helped illuminate the cybersecurity realities facing Tribal Nations, bringing clarity to the risks, resilience strategies, and operational challenges that shape our digital sovereignty.

We look forward to your continued participation in future cycles of *The Pulse*, as we build a shared foundation of tribal-specific intelligence, strengthen cross-sector collaboration, and advance cybersecurity readiness across Indian Country. Your voice is vital to this collective effort, and your engagement ensures that *The Pulse* remains grounded in truth, relevance, and action.

To learn more about the Tribal-ISAC visit our website: www.tribalisac.org.

For more information about *The Pulse*, email us: info@tribalisac.org.

TRIBAL-ISAC

INFORMATION SHARING & ANALYSIS CENTER

TRIBALISAC.ORG
INFO@TRIBALISAC.ORG