

Behavioral & Cultural Insights

AnnexVault LLC
Groundhog Research Group™

Original publication: April 2025
Revised: 26 October 2026

Cyber threat intelligence (CTI) is evolving beyond traditional technical analysis, with behavioral and cultural insights now playing a critical role in understanding, predicting, and countering cyber threats. By examining the underlying motives, regional influences, organizational structures, and cultural adaptability of threat actors, CTI becomes a powerful tool not only for identifying attacks but also for developing proactive defense strategies. This essay explores how behavioral and cultural factors contribute to a deeper understanding of threat actors, enabling CTI teams to tailor their responses and enhance long-term security.

Why this matters to AnnexVault

This report shows how behavior, culture, and organization shape risk. Technical evidence becomes more useful when reviewers understand the people and conditions around it.

Motivation and Threat Actor Psychology

Threat actors are typically driven by diverse motivations, which shape their tactics and target selection. Nation-state actors, for instance, are often motivated by espionage, political influence, or economic advantage. Operating with state support or guidance, these actors focus on national security interests, including data theft and political disruption, aiming to gain leverage over other countries. In contrast, cybercriminals are largely driven by financial gain, targeting assets that can be quickly monetized, such as personal data, credit card information, or ransomware payments. These actors prioritize profitability, often choosing high-value, low-risk targets to maximize returns.

Hacktivists, another distinct group, are motivated by ideology or social causes. Rather than pursuing financial gain, they conduct disruptive attacks, such as website defacements or denial-of-service attacks, to raise awareness of specific issues or causes. Insider threats can involve intentional or unintentional harm by people with authorized access or organizational knowledge, including employees and contractors. Unusual access or activity outside normal hours may warrant contextual review, but no single behavior establishes malicious intent. [1] Understanding these varied motivations helps CTI teams anticipate the tactics likely to be used by different types of threat actors.

Regional and Cultural Influences

Geographic and cultural context can inform analysis of threat activity. Language, terminology, and activity timing may provide investigative leads, but they do not establish nationality, location, or motive on their own. As a specific technical example, Australia's ACSC reported that LockBit 3.0 checks for certain installed languages associated with Commonwealth of Independent States countries and may avoid execution on those systems. This behavior is not a reliable basis for treating any country or language setting as safe. [2]

Cultural significance also influences the choice of targets. Nation-state actors often select targets that align with political or ideological goals, such as critical infrastructure, media outlets, or government websites in adversarial countries. These choices may have symbolic importance, reinforcing the attackers' ideological alignment and sending a message to the target nation. By analyzing the cultural context behind target selection, CTI teams can gain insights into the

intentions and objectives of threat actors, allowing them to better predict and respond to potential threats.

Organizational Structures

The organizational structures of threat groups often resemble legitimate business models, with defined roles and hierarchical arrangements. Larger, more organized groups, such as those associated with nation-states or organized cybercrime syndicates, may include specialized teams responsible for tasks like research, development, and testing of malware. Some groups operate using a service-based approach, such as Ransomware-as-a-Service (RaaS), in which affiliates “rent” access to malicious software. In these models, profits are typically split between developers and operators, creating a structure that mirrors legitimate businesses. [10]

Within underground markets and cybercriminal forums, reputation plays a crucial role. Many forums rely on trust-based systems, where threat actors build reputations that signal reliability and credibility to potential collaborators. Misbehavior, fraud, or failure to deliver promised services often results in penalties or exclusion from the community. CTI analysts can monitor these reputation systems to identify new players or detect shifts in group dynamics, providing valuable insights into emerging threats and potential vulnerabilities within threat groups.

Cultural Adaptability in Tactics

Threat actors are highly adaptable and often adjust their tactics to suit the cultural and security landscape of their targets. Target selection can reflect an actor’s objectives, access, and available opportunities; strong national defenses do not make individual organizations immune. This adaptability extends to social engineering, where cultural knowledge enhances the effectiveness of phishing and other social tactics. Threat actors may exploit common beliefs, regional customs, or seasonal events to increase the credibility of phishing messages. For example, tax-related phishing emails are commonly sent to U.S.-based targets around tax season, while other culturally relevant events, such as national holidays, are used to tailor attacks to specific regions. [9]

Culturally familiar themes can make deceptive messages more convincing and may help attackers bypass users’ scrutiny. Understanding these culturally informed tactics helps CTI teams develop training programs for employees, enabling them to recognize and respond to culturally targeted social engineering attacks.

Cultural Indicators in Malware and Tools

Language in code comments, error messages, and malware functionality can provide investigative leads. Shared tools, reused code, and deliberate deception mean that technical artifacts must be corroborated before attributing activity to an actor or region. Ransomware negotiation behavior can vary between operators and incidents; it should not be treated as evidence of national culture. Incident-response decisions should follow organizational policy and applicable legal requirements.

Ethical and Legal Constraints

Legal exposure and operating conditions may influence criminal target selection. Some ransomware variants include language-based execution exclusions, as documented for LockBit 3.0. Such exclusions do not by themselves demonstrate protection or approval by a government, and they should not be used to reduce monitoring or defensive coverage. [2]

The following organizational factors are analytical considerations, not universal findings about defense agencies or national cultures. Their relevance should be tested against the organization's own evidence.

Hierarchy and Chain of Command

- **Behavioral Insight:** Defense agencies operate under strict hierarchical structures to maintain accountability and discipline. This can slow decision-making but establishes clear authority.
- **Cultural Insight:** Respect for rank and seniority is deeply embedded, affecting interactions and the pace of change within the organization.

Mission-Driven Culture

- **Behavioral Insight:** Commitment to national-security missions can support resilience and loyalty; effects vary by organization and working conditions.
- **Cultural Insight:** Emphasis on patriotism and service creates a culture of solidarity, though it can sometimes lead to an "us vs. them" mindset.

Risk Aversion and Caution

- **Behavioral Insight:** Risk aversion is common due to the high-stakes nature of defense work, resulting in a preference for cautious decision-making.
- **Cultural Insight:** Stability and security are prioritized over rapid innovation, with established protocols often taking precedence over novel solutions.

Diversity and Inclusion Initiatives

- **Behavioral Insight:** Recruitment and career-development practices should assess whether barriers prevent the organization from drawing on relevant skills and diverse perspectives.
- **Cultural Insight:** The U.S. Department of Defense reported that women represented 17.7% of its active-duty force in 2023, up from 17.5% in 2022. This describes force composition, not the culture of every defense organization. [3]

Adaptation to Technological Advancements

- **Behavioral Insight:** Workforce adaptation to technologies such as AI and cybersecurity tools is emphasized, with training programs supporting this shift.

- **Cultural Insight:** There's a balance between valuing traditional skills and digital proficiency, blending generational strengths to meet modern demands.

Ethics and Accountability

- **Behavioral Insight:** Defense agencies prioritize high ethical standards due to the sensitivity of their work, with systems for accountability and integrity.
- **Cultural Insight:** Honor, duty, and integrity require reporting channels that allow concerns to be raised and assessed without inappropriate retaliation. [4]

Interagency Collaboration and Competition

- **Behavioral Insight:** Collaboration between agencies, including defense and intelligence organizations, can support coordinated national-security work.
- **Cultural Insight:** Individual agency cultures can create friction, though efforts are made to align objectives and improve communication across agencies.

Continuous Improvement and Learning

- **Behavioral Insight:** Emphasis on continuous improvement is reflected in professional training, especially in fields such as cybersecurity.
- **Cultural Insight:** Programs for ongoing education promote a culture of learning, with professional military education and technical certifications being integral.

Behavioral and cultural insights in financial services often focus on understanding how customer preferences, trust, technology adoption, and socio-economic factors influence their interactions with financial institutions. Key areas include:

Trust in Financial Institutions: Levels of trust vary globally and can depend on factors like transparency, financial stability, and digital security measures.

Digital Adoption: Different demographics adopt financial technology (FinTech) at varying rates, influenced by age, region, and comfort with technology. [11]

Spending and Saving Behaviors: Income, age, and culture play a significant role in determining saving versus spending behaviors, particularly noticeable across generations like Gen Z, Millennials, Gen X, and Baby Boomers.

Use of Financial Advice Services: The reliance on financial advisors, robo-advisors, or self-directed investments can vary, with preferences differing by customer needs, access, and experience.

ESG and Ethical Investment Trends: Sustainability and social-responsibility preferences can influence investment choices, including interest in Environmental, Social, and Governance (ESG) approaches; demand varies by market and period.

Payment Preferences: Cash, digital wallets, and credit usage vary by region and demographic, and should be assessed using market-specific evidence rather than assumed from a region's digital infrastructure.

Behavioral and cultural insights are crucial in healthcare and pharmaceuticals, as they influence patient behavior, adherence to medications, and overall health outcomes. Key areas include:

Health Literacy and Medication Adherence

- Health literacy, which involves understanding and using healthcare information effectively, plays a big role in medication adherence. Difficulty understanding health information can create barriers to using medicines as intended. AHRQ recommends clear communication and checking understanding for patients at all health-literacy levels. [5]

Cultural Beliefs and Treatment Preferences

- Cultural beliefs impact treatment choices, acceptance of alternative medicine, and openness to preventive care. Certain communities might prioritize natural remedies over pharmaceuticals, while others may hesitate to seek mental health support due to stigma.

Trust in Healthcare Providers and Pharmaceutical Companies

- Trust levels in healthcare providers and pharmaceutical companies significantly impact patient behavior. Trust can affect willingness to discuss concerns and follow treatment plans; adherence also depends on access, cost, understanding, and other circumstances. [5]

Patient-Provider Communication

- Effective communication between patients and providers enhances understanding and adherence. Language barriers or misaligned cultural expectations can affect patient outcomes and satisfaction with care.

Use of Digital Health Tools by Demographics

- The adoption of digital health tools varies across demographics. Age, education level, and cultural background influence the likelihood of using digital health apps, telemedicine, and wearable health devices.

Social Determinants of Health (SDoH)

- Social factors like income, education, and neighborhood environment have a major impact on healthcare access and outcomes. Interventions should address identified social barriers and evaluate outcomes in the populations they serve. [6]

Behavioral and cultural insights are crucial within critical infrastructure (CI) because they affect how people work, respond to threats, and handle security measures. In environments like

energy, water, healthcare, and defense, the safety and stability of systems are highly dependent on the human factors embedded in their operation. Here are some core insights:

Risk Perception and Awareness

- **Behavioral Insight:** Individuals in CI sectors often perceive risk differently based on personal experiences and organizational culture. For example, the NRC's safety-culture policy emphasizes a questioning attitude, personal accountability, and effective communication in nuclear activities. [7]
- **Cultural Insight:** Different organizations or countries may have unique perspectives on acceptable risk. In some cases, risk-taking may be more acceptable, while in others, stringent risk-aversion is embedded into workplace culture.

Human Error and Decision-Making

- **Behavioral Insight:** Human error is a significant factor in CI incidents, often due to fatigue, workload, or complexity in systems. Decision-making in high-pressure situations, especially during emergencies, can lead to mistakes if protocols are not clear or personnel are not adequately trained.
- **Cultural Insight:** Training and decision-making approaches differ across CI sectors and regions. For example, some cultures may prioritize strict adherence to procedures, while others emphasize adaptability and autonomy.

Trust and Communication

- **Behavioral Insight:** Trust between individuals and departments within CI is vital for effective operations, particularly in incident response. Poor communication or lack of trust can lead to delayed responses and mismanagement of critical events.
- **Cultural Insight:** Hierarchical organizations or those with strict chain-of-command structures may struggle with communication, especially if employees feel they cannot challenge or question decisions made by superiors. On the other hand, cultures that encourage open dialogue may foster better teamwork and quicker responses.

Security Culture and Insider Threat

- **Behavioral Insight:** Employees in CI may not always prioritize cybersecurity or physical security due to complacency or lack of understanding about threats. This can make them susceptible to social engineering or lapses in protocol, which can be exploited by malicious insiders.
- **Cultural Insight:** Security awareness and role-based learning support risk management and the development of a security culture. Their effectiveness should be evaluated; these practices do not establish that a particular country or organization experiences fewer insider incidents. [8]

Adapting to Technological Change

- **Behavioral Insight:** The rapid pace of technological advancements in CI can create stress and resistance among employees who are accustomed to traditional methods. This is particularly challenging in sectors like utilities, where staff may have been in the same role for decades.
- **Cultural Insight:** Some CI sectors or regions may be more open to technological change than others, depending on factors like organizational culture, leadership style, and resource availability. Training and upskilling can support adaptation, with results depending on leadership, resources, and implementation. [8]

Compliance and Regulatory Differences

- **Behavioral Insight:** Employees in CI may sometimes view compliance as a checkbox activity rather than an integral part of security and resilience. This can lead to minimum standards rather than proactive safety and security measures.
- **Cultural Insight:** Different regulatory environments and levels of government oversight can influence how seriously organizations take compliance. Regulatory requirements can establish expectations for safety and accountability; effective implementation and oversight still need to be assessed. [7]

Resilience and Crisis Management

- **Behavioral Insight:** Resilience in CI is not just about systems but also about people. Employees who are trained in crisis management and stress resilience can respond better under pressure and help prevent cascading failures in emergencies.
- **Cultural Insight:** The emphasis on resilience varies by culture and sector. Some organizations may prioritize immediate recovery and minimal downtime, while others focus on long-term resilience planning and preparedness. Past disasters may inform preparedness efforts, but resilience should be assessed from demonstrated capabilities rather than assumed from national history.

References

- [1] CISA: Insider Threat Mitigation Guide
- [2] Australian Cyber Security Centre: LockBit 3.0 profile (2023)
- [3] U.S. Department of Defense: 2023 Demographics Profile of the Military Community
- [4] DoD Inspector General: Whistleblower Reprisal Complaints
- [5] AHRQ: Health Literacy Universal Precautions Toolkit
- [6] WHO: Determinants of health (2024)
- [7] U.S. NRC: Safety Culture Policy Statement
- [8] NIST SP 800-50 Rev. 1: Cybersecurity and Privacy Learning Program (2024)
- [9] IRS: New-client phishing scam warning (February 2024)
- [10] CISA and partners: Understanding LockBit (2023)
- [11] FDIC: 2023 National Survey of Unbanked and Underbanked Households