Title: The Talent Abroad, the Vulnerable Home: Nepal's Cybersecurity Paradox

Author: Sanskar Bhattarai

Date: 2083/02/03

Document Type: Policy Analysis Brief

Executive Summary

Nepal's own cybersecurity personnels consistently rank among the world's top on global bug bounty and ethical hacking platforms, yet Nepal's own government websites and financial systems suffer frequent cyberattacks. This brief identifies the 3 core causes: Economic Incentives that attract talents towards foreign firms, Outdated Cybersecurity Frameworks, and a System that discourages ethical hackers from reporting vulnerabilities domestically. This brief recommends establishing national vulnerabilities disclosure policy, creating a domestic bug bounty platform and operationalizing a Central National Computer Emergency Response Team of skilled IT professionals. These measures convert Nepal's dispersed human resources into a national security asset and build a sovereign cyber resilience positioning Nepal to compete with the world's leading cyber powers.

Introduction

In early 2024, a young security researcher named Samip Aryal was publicly recognized by Meta as No 1 Contributor to their White Hat Hall of Fame, earning massive bounties for identifying the 0-click Account Takeover vulnerability on Facebook. Yet, by March 2025, the entire digital infrastructure of the country suffered a humiliating collapse when a DDoS attack towards Government Integrated Data Center (GIDC) at Singha Durbar affecting over 400 government sites including the immigration systems at Tribhuvan International Airport which caused 6 international flight delays, exposing how fragile Nepal's own digital nervous system truly is. Nepal produces world class ethical hackers, yet its domestic digital infrastructures remain among the most vulnerable in South Asia.

This paper argues that disconnect is not a failure of talent, but a predictable outcome of market forces, an absent institutional framework and a legal environment that penalizes domestic vulnerability research. It also diagnoses these root causes and proposes a feasible, cost-conscious set of policy interventions to reverse the paradox.

Nepal's Presence in Global Cybersecurity Talent

1. **Global Bug Bounty Benchmarks**
   In prestigious events like HackerOne Ambassador Cup 2023, a global competition pitting national teams of ethical hackers against each other, the Nepali team finished a historic 3rd place globally [HackerOne 2023]. In 2024, Nepal ranked against the second highest award-winning nation in Meta's Bug Bounty Program beating United States and only falling behind India [Meta Engineering 2025]. Nepali researcher Birendra Sah has also ranked No 1 in Bugcrowd monthly leaderboards [Monastic 2025].

2. **Capture the Flag Benchmarks**
   In 2024, Nepali team Hack@Sec achieved 219th rank globally scoring 181.115 points by participating in 76 events [CTF TIME 2024]. The same team in 2025 achieved 58th rank globally scoring 479.381 points by participating in 69 events [CTF TIME 2025].

3. **Case Studies**
   In 2020, a Nepali researcher Saugat Pokharel discovered a privacy vulnerability in Instagram where deleted and private user data could still be accessed through data exports feature. This issue was patched and he received $6000 bug bounty from Meta [TekhLekh 2020].

   In 2024, Samip Aryal discovered a 0 click account takeover vulnerability in Facebook authentication system that prevented billions of active social media accounts from being compromised. This granted him entry into the global elite Hall of Fame rankings (Meta #1). This highlighted Nepal's presence in global cybersecurity research [Republica 2024].

Domestic Cybersecurity Deficit

1. **Government Portal Defacement**
   In 2025, the official website of Nepal's Ministry of Health and Population experienced a defacement attack, where attacker replaced the website's homepage with unauthorized messages and altered visuals. The attacker was identified to be "CaptainSmok3r", who altered official date and took over the portal [Angelwrites 2025].

   This incident forced website blackout, exposed sensitive administrative data and highlighted severe vulnerabilities in Nepal's digital infrastructures.

2. **Distributed Denial of Service (DDoS) on Government Integrated Data Centre (GIDC)**
   On January 2023, a massive DDOS on Nepal's GIDC took caused 400 government websites to be offline for several hours [The Kathmandu Post 2023].

   The attack caused significant disruptions at Tribhuvan International Airport, freezing immigration systems and forcing manual processing for travelers. Media reports reported that National Information Technology Centre lacked adequate defenses and had failed to renew security licenses which left the system vulnerable.

3. **Public Service Commission (PSC) Data Erasure Crisis**
   In April 2023, a massive system failure occurred at the central servers managed by the National Information Technology Center [TekhPana 2023]. Due to absence of backup routines, server maintenance and disaster recovery drills, the data belonging to over 60 government agencies was wiped out. The hardest hit agency was the PSC.

   The system failure instantly erased data of approximately 400,000 job applicants who had applied for civil service positions [Routine of Nepal Banda 2023]. This included permanent losses of personal documents, and exam fees. Months later, they admitted to being incapable of recovering lost applicants' records. This froze national public service recruitment, paralyzed careers of thousands of Nepali Youths and forced the agency to manually rebuild their systems.

Diagnosing the Disconnect: 3 Core Causes

1. **Economic Incentives that Attract Talent towards Foreign Firms**
   The top reason why Nepali researchers target foreign systems is because of the economic incentives they offer. Average bounty for a critical vulnerability on Meta is $20,000, reaching a maximum of $300,000 while the minimum being $500 [Meta Bug Bounty 2026] while the salary of an Ethical Hacker in Nepal is NPR 110,000 (~$715) maximum [MoCIT 2082].

   Therefore, the disparity ratio between average critical bug bounty on Meta and Ethical hacker maximum salary is 27:1. This implies that even a highly paid Nepali Ethical hacker must work for 2 years and 3 months to equal the one-time reward earned by another Nepali researcher from discovering a single critical vulnerability.

   This disparity discourages Nepali talents to work in Nepali offices and encourages them to work in highly paid global firms like Meta which also enable remote works, global recognition and career progression. There is no domestic platform which offers the same, leading ethical hackers to ignore the local job market and target only foreign firms.

2. **Outdated Cybersecurity Frameworks**
   Nepal lacks a comprehensive modern cybersecurity act. The primary legislation Electronic Transaction Act 2063 was designed for old Internet era. Social media was minimal, cloud computing was rare, AI driven cybercrimes did not exist, and critical infrastructure digitalization was limited.

   Modern cyber threats now include AI assisted attacks, misinformation on social media, data breaches on critical infrastructure digitalization and identity thefts, which the law does not adequately address. The law focuses primarily on criminalization rather than proactive cybersecurity governance.

   An outdated legal framework not only weakens security enforcement but also reduces legal clarity for investors, courts and users. The pace of technological evolution has outgrown the legal framework.

3. **System that Discourages Ethical Hackers from Reporting Vulnerabilities Domestically**
   Under the Electronic Transaction Act 2063, unauthorized access to systems can potentially be treated as cybercrime regardless of intent. This creates legal uncertainty in ethical hacking. Researchers may fear legal action, police investigations, reputational damage and institutional retaliation even when they are attempting to responsively disclose vulnerabilities.

   This fear has caused researchers to avoid reporting vulnerabilities which increase system risk. Nepal also lacks standardized reporting channels so ethical hackers often do not know how to report vulnerabilities safely.

   Institutional immaturity, where the institutions may react defensively instead of collaboratively, is a leading cause of weak national cyber resilience. International institutions like Google, Meta and Microsoft have public vulnerabilities disclosure and bug bounty programs. They collaborate with security researchers which improve their security. Such maturity remains to be seen in domestic institutions.

Policy Recommendations

1. **National Vulnerability Disclosure Policy**
   The Ministry of Communication and Information Technology should develop a Vulnerability Disclosure Policy (VDP) for all .gov.np domains. The policy must state that individuals who report vulnerabilities in good faith and abide by a defined set of rules will not face prosecution under the Electronic Transaction Act.

   The following core rules must be defined in the policy to protect researchers acting in good faith:
   - Researchers must not execute any testing that harms the confidentiality, integrity and availability of the system.
   - Researchers must give the targeted government agency time to patch the vulnerability before making it public.
   - Testing must be restricted to digital applications boundaries. Social Engineering and Physical Intrusion is excluded from Safe Harbor Protection.
   - Researchers must immediately stop all testing the exact moment a vulnerability is confirmed. Downloading, Altering and Maintaining local copies of sensitive information instantly voids legal protection.

   The VDP is low cost because it shifts the financial burden from state to a voluntary community who ask for recognition and legal protection. Nepal can leverage its massive pool of talents for virtually zero cost offering unmatchable return of investment.

2. **Domestic Bug Bounty Platform**
   Joint initiative of Public and Private Bug Bounty platforms should be developed to address the Economic Brain Drain. To ensure fiscal viability, this initiative must reject traditional capital-intensive audit models and adopt the 'Pay for Results' model.

   Traditional security auditing models mandate fixed and upfront payments regardless of vulnerabilities found or not. However, 'Pay for Results' model ensures that the fund is disbursed only upon the discovery and successful mitigation of vulnerability.

   The platform hosts time bound bug bounty programs for banks and e-government portals. Rewards can be a mix of cash and non-monetary rewards like certificates, scholarships, or opportunities to work in Cyber Bureau or CERT depending on the severity of vulnerability.

3. **Operationalizing Central Computer Emergency Response Team (CERT)**
   Currently there is no government entity with a clear mandate to receive the vulnerability reports, analyze it and take appropriate steps to patch it. Central CERT will act as a coordination hub, focused on 3 tasks:
   - Serve as the government's single point of contact for vulnerability reports submitted under the recommended Vulnerability Disclosure Policy.
   - Analyze and route incidents to the relevant ministry or agency, providing technical guidance and incident response resources by dispatching technical professionals from the country's pool of ethical hackers and private firms.
   - Conduct regular proactive, non-intrusive vulnerability scanning of all government digital assets, and patch any vulnerabilities or errors such as expired certificates, exposed login panels and known unpatched software.

Conclusion

Nepal's cybersecurity weakness is not a lack of human capital. It is paradoxically a consequence of failing to utilize the talent that the country produces in abundance. By providing legal protection, economic incentives and a home for their talent, Nepal can transform its ethical hackers into pillars of national cyber resilience.

The cost of inaction is very heavy; every defaced website and every breached database reduce citizen trust and digital economy potential. The resources to fix this are already present within the national borders. The question is whether the policy will finally recognize them.

References

I. Nepal's Presence in Global Cybersecurity Talents

Garcia, A. (2023, December 14). *The 2023 Ambassador World Cup Final: Results, Impact, and Looking Ahead*. HackerOne. https://www.hackerone.com/blog/2023-ambassador-world-cup-final-results-impact-and-looking-ahead

Meta. (2025, February 13). *Looking back at our Bug Bounty program in 2024*. Meta Engineering Blog. https://engineering.fb.com/2025/02/13/security/looking-back-at-our-bug-bounty-program-in-2024/

Monastic School/College. (2025). *Alumni success: Birendra Sah secures #1 global rank as ethical hacker on Bugcrowd for April*. Monastic School/College. https://www.monastic.edu.np

CTFtime. (2024). *Hack@Sec team statistics (2024 season)*. CTFtime. https://ctftime.org/stats/2024/NP

CTFtime. (2025). *Hack@Sec team statistics (2025 season)*. CTFtime. https://ctftime.org/stats/2025/NP

Shrestha, P. (2020, August 18). Saugat Pokharel from Nepal Awarded $6000 Bug Bounty by Instagram. TechLekh. https://techlekh.com/saugat-pokharel-instagram-bug/

Republica. (2024, February 24). Nepal's Samip Aryal tops Facebook's White Hat Hall of Fame for uncovering major flaw. *My Republica*. https://myrepublica.nagariknetwork.com/news/nepal-s-samip-aryal-tops-facebook-s-white-hat-hall-of-fame-for-uncovering-major-flaw

II. Nepal's Cybersecurity Deficit

Angel. (2025, February 20). The wake-up call: Nepal's governmental website hacks. *Angel Writes*. https://angelwrites.xyz/current-events/the-wake-up-call-nepals-governmental-website-hacks/

Shrestha, P. M. (2023, January 30). Singha Durbar server continues to face cyberattacks. *The Kathmandu Post*. https://kathmandupost.com/national/2023/01/30/singha-durbar-server-continues-to-face-cyberattacks [1, 2]

TechPana. (2023, April 26). डेटा रिकभरी नहुँदा लोकसेवा आयोगको विज्ञापन नै रद्द हुने अवस्थामा, के थियो मुख्य समस्या? [Due to lack of data recovery, the Public Service Commission's vacancy announcement is on the verge of cancellation, what was the main problem?]. *TechPana*. https://techpana.com/

Routine of Nepal Banda. (2023, April 27). Serious Issue, लोकसेवाको डाटा गायब: Personal Data of around 4 lakh applicants who applied for the Public Service Commission (लोकसेवा आयोग) is probably lost [Status update]. *Facebook*. https://www.facebook.com/officialroutineofnepalbanda/posts/serious-issue-लोकसेवाको-डाटा-गायब-personal-data-of-around-4-lakh-applicants-who-/7320505514648845/

III. Diagnosing the Disconnect

Meta Bug Bounty. (2026). *Program overview*. Meta. https://bugbounty.meta.com/
(Note: This covers Meta's direct payout matrices, documenting the minimum payout of $500, average critical payouts around $20,000, and maximum potential payouts reaching $300,000 for mobile Remote Code Execution).

Edusanjal. (2025, August 28). Salary of IT Professionals in Nepal: MOICT. *Edusanjal*. https://edusanjal.com/blog/salary-of-it-professionals-in-nepal-moict/
(Note: This provides the official breakdown of the "Norms for Cost Estimation of IT Systems Development and Consultation Services, 2082" issued by Nepal's Ministry of Communications and Information Technology, explicitly capping the monthly rate for a Vulnerability Assessor / Ethical Hacker / Application Security Engineer at NPR 110,000).