BGIN Block#12 Meeting Report

- BGIN is a multi-stakeholder discussion body / distributed think tank.

Cybersecurity Information Sharing Framework

bg in

blockchain
governance
initiative
network

The Global Network for Blockchain Stakeholders™

BGIN Block#12

Cybersecurity Information Sharing Framework

Date: Monday, March 3, 2025

Location: Tokyo, Japan

Duration: Approx. 90 minutes

Summary

Presentation by NIST

- NIST (National Institute of Standards and Technology) presented updates on the Cybersecurity Framework (CSF) and community profiles. NIST CSF version 2.0 was released recently (1-year anniversary in February 2024) with significant updates:
    - Addition of a new sixth function: "Govern", which surrounds and supports the original five functions (Identify, Protect, Detect, Respond, Recover).
    - Maintains alignment with international standards (e.g., ISO 27001, COBIT), and introduces online mappings/crosswalks for broader usability.
    - Framework is risk-based and designed for flexibility depending on organization type and needs.
    - Updated resources include quick-start guides tailored for SMEs, ERM integration, and CSF tiers.
    - CSF has been translated into multiple languages, including Japanese, and used internationally (notably in Japan since v1.0).

Community Profiles Overview:

- NIST National Cybersecurity Center of Excellence (NCCoE) facilitates collaborative problem-solving. Community profiles are developed by groups of companies (sectors, subsectors, or shared technology use cases). Different from organizational profiles (individual company targeting current vs. desired cybersecurity posture). Community profiles are templates for groups to manage shared cybersecurity/privacy risks.

- Benefits include:
    - Common taxonomy and shared goals.
    - Alignment with multiple standards.
    - Shared expertise and reduced individual burden.

- Profile structure includes priorities, rationale, informative references, and optionally examples and dependencies.

- NIST has created/posted profiles for threats like ransomware, semiconductors, cyber-physical systems, and more.
- Resources to help communities get started include a draft profile development guide and template.

Feedback and Participation:

- NIST encourages global participation, including non-U.S. entities.
- No formal agreement is required to participate in profile development, but other collaborations (e.g., lab tools) may require a CRADA agreement.

Q&A Highlights:

- On measuring CSF effectiveness:
    - Metrics are a challenge due to CSF's risk-based and flexible structure.
    - Metrics may vary by sector; standardized measurements are difficult but enterprise-focused guides (e.g., NIST SP 8286 series) help integrate with Enterprise Risk Management (ERM).

- Concerns around recent Bybit hack ($1.5B) linked to DPRK threat actors.
    - Emphasized the need for a crypto-specific CSF profile, modeled after the ransomware profile, to address unique risks like key management, blockchain-specific vulnerabilities, etc.
    - Urged NIST and BGIN to collaborate on creating such a profile and enhance real-time threat intelligence sharing, referencing frameworks like STIX/TAXII and CVE/NVD.

- NIST acknowledged the idea and expressed interest in following up, noting:
    - Profiles can evolve into tools/resources later (e.g., for CVEs or automated sharing).
    - It is feasible to extend existing frameworks or create mappings tailored for blockchain and DeFi.

- Participants also discussed the need for domain-specific scoping and realistic timelines for profile development.

<u>Presentation by MITRE</u>

- MITRE is a nonprofit organization that works in the public interest with U.S. government agencies like DHS and DOD. Known for the MITRE ATT&CK framework, which systematically documents adversary tactics and techniques based on real-world attack data. ATT&CK maps adversary behavior from initial access to impact, including reconnaissance, privilege escalation, lateral movement, data collection, exfiltration, and more. ATT&CK is widely used by defenders, SOC teams, red teams, threat hunters, and

vendors for threat modeling, detection development, and understanding attacker behavior. MITRE has extended its approach to focus on attacks targeting digital assets, launching a new framework called ADAPT (= Adversarial Actions in Digital Asset Payment Technologies). ADAPT is designed to track and categorize techniques unique to Web3, DeFi, and digital asset ecosystems.

- ADAPT includes many of the same tactics from ATT&CK, such as initial access and execution, but also adds new tactics and techniques specific to crypto:

    - Smart contract logic manipulation
    - Exploitation of gasless (gas-free) RPC endpoints
    - Flash loan exploits
    - DeFi protocol misconfiguration
    - Misrepresentation in off-chain communication (e.g., social engineering or phishing)

    - Layering funds using privacy tools, DEXs, and cross-chain bridges
    - Cross-chain swaps to move funds across blockchains
    - Price oracle manipulation
    - Taking advantage of frontend vulnerabilities

- Unlike ATT&CK, which is strictly based on documented real-world attacks, ADAPT includes both observed and theoretically possible (hypothetical) techniques to anticipate future threats.

- A real case study of a Bybit-related attack was used to demonstrate ADAPT's utility:

    - Attacker crafted a malicious transaction that altered logic in a smart contract wallet.
    - The wallet used a Gnosis Safe multi-sig setup.
    - One of the Bybit executives approved the malicious transaction, likely after being socially engineered.
    - Funds were moved into a contract controlled by the attacker.
    - The attacker obfuscated the trail by using chain-hopping and layering tactics.

- MITRE analysts mapped each step of this attack to specific techniques in ADAPT. The example showed how ADAPT helps break down complex, multi-step attacks in the crypto world. MITRE emphasized the importance of developing a shared understanding of threats across the crypto ecosystem. ADAPT provides a "common language" to describe and analyze attacker behavior in Web3. MITRE plans to open-source ADAPT and encourages the community to contribute and collaborate.

- The speaker also emphasized that many attacks now span multiple parties (wallets, protocols, exchanges), so shared frameworks like ADAPT help teams across companies

understand the full scope of an incident.

- MITRE highlighted the value of information sharing — detection techniques and indicators can be shared in formats like STIX for better collaboration across vendors and defenders.

<u>Discussion on the worksheet</u>

Player Category

- Debate over classifying CERTs and MITRE: MITRE is a nonprofit, FFRDC, and contractor for the US government. Decision: MITRE and similar entities should fall under government entities, not research institutions.
- Suggestion to enumerate pain points and concerns of each category to help clarify roles in the taxonomy.
- A layer-based model (inspired by the CFTC TAC DeFi report) was proposed, with categories like:
  - Protocol layer (e.g., Layer 1 foundations)
  - Network layer (e.g., validators, RPC nodes)
  - Application layer (e.g., DeFi frontends, wallet providers, VASPs, exchanges)
- Recognized the overlap between blockchain developers, suppliers, operators, and suggested refining those categories.
- Suggestion to distinguish between individual open-source developers and corporate developers due to different incentives and information sharing structures.
- Highlighted that developers work across layers, so roles might be repeated.
- Importance of archetypes was emphasized—categories that reflect informational control and response capability.
- Suggestion to keep a high-level breakdown (apps, protocol, network) and then dive deeper into blockchain-specific subcategories.
- Recognized the need for flexibility and future expansion—framework can evolve, starting with a concise, actionable model.

- Security Experts
  - Roles

        - The part of their role will be ingesting information which will inform a variety of different security services, providing threat intelligence or providing security assessments of certain vendors and platforms
        - The role is to leverage threat information to constantly update security assessments and services. For example, the role related to information sharing, related to wallet services would be that a security firm would leverage information shared with them to inform things like their recommendations on using a specific wallet.

    - Incentives
        - The incentive is to get access to the latest threat information so that you can best defend against it. “Access to broader threat intelligence for better security solutions” is the incentive which captured that the DPRK attack information access. They get intel from other groups and practitioners.

    - Challenges
        - At a higher level, it is about reluctance and unwillingness to share information. Is it a challenge by the security expert or instead by the service provider? It is more of a challenge by the service provider, but the security expert also needs to understand this challenge by the service provider.

- Academia

    - Roles
        - Regarding “contribute to standards through sharing of technical expertise and knowledge”, academia is training people to do all stuff so it might be better to change it to “train people through ～”

    - Challenges
        - Access to data / speed and lack of peer review process

    - Conflicts of Interest
        - Limited access to data is not a conflict of interest. But it depends on who’s giving you the data and who’s giving you the funding. Let’s say, if you get data from a blockchain analytics company, you can never say that they do anything wrong. Or if you get money from an exchange, you can never say that they made a mistake, which is a traditional conflict of interest.

- Law Enforcement Authorities

    - Challenges
        - Regarding “Privacy of consumers,” it is really privacy in general because at least 10 years ago in the US, no company wanted to call the FBI because they were worried that the FBI would go see you’ve been doing

something else bad and you are now in trouble. There is privacy for consumers and enterprises.

- Financial Regulatory Authorities
    - Challenges
        - We cannot divide cybersecurity risk and financial risk. Sometimes people claim that they were hacked but they are not always really hacked. It might be on purpose.
- Crypto-focused ISAC
    - Challenges
        - They lack the power to enforce. It is not something that can tangibly fixed unless they make it part of the terms of membership of an ISAC
        - If you think of enforcement from regulators, it's more of a feature to incentivize members sharing information. We also need to take into account that incentive matters but the goal is not to share information but to reduce the attack surface of the industry.
        - If participants say they are not sharing, they are not getting value from the ISAC, which means that the ISAC doesn't have a reason to exist.
- VASPs
    - Challenges
        - Some VASPs use their own wallet systems, while others use third-party systems. They lack the common schemes of wallet infrastructure between the member VASPs. There is an issue of the absence of mature security assessment methodologies across different types of applications, wallets and others. (This applies to ISACs that are trying to help VASPs better secure themselves. If there is a framework to evaluate open source software and third party vendors, it would be great!)
- Expansion of the common format for cryptocurrency fields that are sticks compatible, then is something that the ISACs need in order to be successful. This can be a point of further action between BGIN and the ISACs. (SEAL is working on defining common formats for storing things such as cryptocurrency addresses and has joined OASIS CTI TC to upstream those changes.)

Next Steps:

- The speaker discusses the importance of turning the discussion into something tangible, operational, and actionable for stakeholders, especially in the context of cybersecurity information sharing.
- Emphasizes that nothing from the discussion will be lost or deleted—everything written down will be used to create a useful document.

- The team plans to compile all the input into a foundational document focused on taxonomy and ecosystem modeling for information sharing in blockchain cybersecurity.
- This initial document will cover roles, responsibilities, and categories of players involved in the ecosystem. It will serve as a “capstone” or starting point for a potential series of documents. The goal is to draft a high-level document that explains the framework, the roles of various entities, and how they interact.
- The speaker asks for volunteers to help draft or “hold the pen” for the document. Many participants express willingness to help; some raise their hands or are acknowledged as key contributors.
- The first draft is targeted for completion around April. The document is expected to be short (5–10 pages), not an extensive technical report.
- If successful, the team might aim to submit it as an ISO standard, which is described as a monumental opportunity for BGIN and the broader blockchain community.