You Can't Patch a Shitty Culture: Operational and Social Risks

By Dominik Wilkes and Keisha Mitchell
Edited by Keisha Mitchell

When it comes to blockchain and smart contract development, there's a tendency to focus heavily on writing secure code, running penetration tests, and fixing vulnerabilities. And while these technical steps are crucial, they often overlook something equally important: the organizational culture and operational procedures that underpin a secure and resilient system.

At Creed, we've seen firsthand how many blockchain companies make the mistake of assuming that great code alone can protect them. But the truth is, you can't patch a shitty culture. Operational missteps, poor communication, and a lack of proper processes are social risks that writing great code can't solve. In this article, we'll explore the social and operational issues we've observed in blockchain companies and why they matter just as much as the code you write.

The Human Side of Security: Why Culture Matters

It's easy to get caught up in the technical details of cybersecurity—fixing bugs, securing APIs, and reviewing smart contracts. However, at the heart of many breaches and failures isn't a lack of technical knowledge, but a failure in organizational culture. A company's internal dynamics—how teams communicate, how decisions are made, and how security is integrated into daily operations—can be just as much of a risk as poor coding practices.

Blockchain companies, especially startups, are often fast-moving and focused on delivering results quickly. In the race to build the next big thing, security and operational procedures sometimes take a backseat. This leads to a culture where the focus is solely on shipping product, rather than building in security from the ground up. While speed and innovation are key drivers in blockchain, this "move fast and break things" mentality can leave critical vulnerabilities that are ignored or minimized until they explode into a full-blown crisis.

Operational Risks: When Procedures Don't Scale

Blockchain projects often grow rapidly, and with that growth comes increased complexity. Operational procedures that worked well in the early days of a project may no longer be adequate as the company scales. In many cases, teams are left without clear ownership, unclear roles, or a well-defined chain of command. Without the right processes in place, this can result in several risks that code alone cannot

solve.

A common issue is the **lack of clear ownership**. In some blockchain organizations, there is uncertainty about who is responsible for specific tasks, particularly in the realm of security. This ambiguity often results in critical gaps in areas such as patch management, incident response, and code reviews. When no one is specifically accountable for these processes, security becomes fragmented and incomplete, leaving the organization vulnerable to potential threats.

Another problem is a reactive, rather than proactive, approach to security. Many blockchain companies only address security concerns after a problem arises, typically after an exploit or breach has been discovered. This reactive mindset leads to constant firefighting, preventing the organization from focusing on long-term strategic planning. An effective security posture, however, requires proactive planning, continuous risk assessments, and fostering a culture of ongoing improvement.

Finally, **inconsistent documentation** is a frequent challenge. Blockchain teams often prioritize development speed, sometimes at the expense of creating and maintaining comprehensive documentation. As a result, processes may not be well-documented, leading to confusion when it's time to audit or troubleshoot issues. The lack of documentation also hinders knowledge transfer when employees leave or new team members join, which can slow down the response to emerging security risks.

Social Risks: Culture Eats Security for Breakfast

The human side of blockchain companies is just as critical as the technology side. Poor communication, a lack of transparency, and a toxic culture can undermine even the best technical work. While coding practices and technical solutions are key, there are significant social risks that can't be fixed simply by writing great code.

Poor Communication Between Teams: Many blockchain companies consist of cross-functional teams, including developers, auditors, business teams, and leadership. However, when communication is lacking, silos form, and critical information about risks and vulnerabilities may not be shared across departments. This disconnect can lead to security measures being poorly implemented, with team members unaware of the potential risks they're facing.

Ego and the "Not My Problem" Mentality: In some blockchain environments, there is a heavy focus on individual brilliance, where developers or team leads work in isolation. This "I'm a great developer, security is someone else's responsibility" mindset leads to neglected or ignored security practices. Developers may assume their code is secure, but this lack of collaboration between development, security, and operations teams creates a fragmented and incomplete security strategy.

Overconfidence and Overpromising: Another common issue is overpromising features, timelines, or security guarantees to investors, clients, or the community. This overconfidence often results in cutting corners to meet deadlines, which includes overlooking crucial security practices. Underestimating the complexity of a project and failing to incorporate security early on usually leads to vulnerabilities that are only discovered under pressure, resulting in costly fixes and potential breaches.

Burnout and High Turnover: The blockchain industry is a fast-paced sector, and burnout is a prevalent issue. When employees are pushed to their limits, they may rush through tasks, including security reviews, or fail to follow standard procedures. High turnover further compounds the problem, as it means knowledge isn't retained, disrupting continuity and leaving gaps in the system. This lack of stability can make it challenging to maintain a consistent and effective security posture.

Social risks are often overlooked in favor of a sole focus on technology and coding. However, addressing these issues within the team and organization is crucial for developing a robust and sustainable security strategy.

Security Culture: Building a Strong Foundation

So, how can you mitigate these operational and social risks that can't be addressed simply by writing great code? It ultimately comes down to establishing a robust security culture that permeates every level of the organization. Here are some practical ways to get started:

Foster Open Communication: Encourage communication and collaboration across teams. Security is not just the responsibility of the security team or developers—it's everyone's responsibility. By holding regular security check-ins or risk assessments involving all stakeholders, you ensure that everyone is aligned and aware of the current security posture. This transparency helps prevent silos and ensures that risks are addressed collectively.

Define Roles and Responsibilities Clearly: Ensure that ownership of security tasks is clearly defined and documented. From patch management to incident response, it's crucial to know who is responsible for what. Clear role definitions ensure that security tasks are not neglected or left unfinished, preventing critical gaps from forming in your security strategy.

Adopt a Proactive Security Approach: Shift away from a reactive security model. Security should be integrated into your ongoing processes, including regular risk assessments, code reviews, and the integration of threat intelligence. These tasks should not only be performed when an exploit is discovered but should be embedded into the development cycle to anticipate and prevent potential threats.

Cultivate a Growth Mindset: Encourage continuous learning and improvement within your team. Whether it's staying up to date with the latest security best practices or improving internal processes, fostering a culture of growth helps avoid complacency. Recognizing and rewarding individuals who identify gaps in security or make improvements to existing practices can boost morale and strengthen the overall security framework.

Address Burnout Early: A strong security culture relies on a team that is both focused and well-rested. Avoid pushing your team to their breaking point and prioritize work-life balance. A motivated and well-supported team is far more likely to remain engaged and productive, thereby reducing the risk of mistakes due to burnout.

When these operational and social risks are addressed through intentional cultural practices, you can

create a security-conscious environment that supports both sustainable growth and a resilient security posture. It takes practice, but it’s not impossible.

Conclusion: Great Code Alone Won’t Cut It

While writing great code is essential for securing your blockchain project, it’s not enough. Organizational and cultural risks must also be addressed to build a resilient security posture. Proper security comes from a culture where security is everyone’s responsibility, processes are well-defined, and communication is open.

At Creed, we’ve seen how neglecting the human and operational sides of security often leads to avoidable risks. A thorough risk assessment highlights these vulnerabilities, and it’s up to you to take action. Don’t just patch your code—patch your culture too. Only then can you build a truly secure and resilient blockchain project.

If you're ready to tackle both technical and social risks, take The Creed, we can help. Contact us today to schedule your risk assessment and take the first step toward a stronger, more secure blockchain project.