

Timestamp	What is your name?	What is your current role/position?	How many years of experience do you have in IT or cybersecurity?
#####	Nguyen Quoc Hung	Cybersecurity Architect	12 years
#####	Tran Thi Minh Anh	IT Security Manager	8 years
#####	Le Van Duy	Network Security Engineer	15 years
#####	Pham Duc Long	Cybersecurity Lecturer	10 years
#####	Do Thanh Binh	CISO	18 years

What type of organization do you primarily work w	Does your organization currently use any form of Z	1. In your view, what are the main weaknesses of t
Financial Institution	Yes	Traditional perimeter-based security models rely h
University	Partially	Traditional perimeter-based models assume that th
Cloud Service Provider	Yes	Traditional models place excessive trust in internal
University	Theoretical	Traditional perimeter defenses assume external th
Multinational Enterprise	Yes	Traditional perimeter-based models rely on firewal

2. How would you describe the core value of Zero Trust? 3. Which identity verification methods (MFA, SSO, etc.) are most effective in a Zero Trust environment? 4. What challenges have you faced when implementing Zero Trust, and how did you overcome them?

Zero Trust ensures that no user, device, or application is trusted by default. Multi-factor authentication (MFA) combined with conditional access policies is most effective. Implementing identity verification technologies often requires a phased approach.

Zero Trust minimizes the attack surface by enforcing least privilege access. Biometric MFA, such as fingerprint or facial recognition, is highly effective. Integrating MFA across hybrid systems—on-premises and cloud—can be challenging.

Zero Trust ensures access is granted based on verified identity and device health. Passwordless authentication combined with hardware security modules (HSMs) is effective. Integration with diverse cloud platforms and legacy systems is a common challenge.

Zero Trust ensures ongoing verification of user identity and device health. MFA via authenticator apps strikes an optimal balance between security and user experience. User fatigue from additional authentication steps is a challenge.

Zero Trust transforms access from location-based to identity-based. FIDO2-based passwordless authentication combined with hardware security modules is effective. Integrating identity verification with complex systems is a challenge.

5. How do you assess the trustworthiness of devices? 6. What common issues arise when enforcing device policies? 7. From your experience, how do users typically react to stricter controls?

We use endpoint management tools to assess device health. Common issues include unpatched operating systems and non-standard configurations. Initially, users expressed frustration with stricter controls.

We use Mobile Device Management (MDM) tools for policy enforcement. Unpatched student laptops, missing antivirus software, and inconsistent updates are common. Students often resist stricter controls like MFA due to inconvenience.

We use certificate-based authentication tied to device identity. Delayed patches, non-standard device configurations, and BYOD fragmentation are common. Initially, stricter controls like MFA and device verification caused pushback.

Device trustworthiness is assessed by checking OS version, patch level, and configuration. Unpatched or misconfigured systems, particularly in BYOD environments, are common. Users initially resist stricter controls like MFA due to perceived inconvenience.

We use continuous device health validation via Endpoint Protection. BYOD fragmentation, inconsistent OS updates, and non-standard configurations are common. Early pushback came from employees frustrated by additional security steps.

8. Can you share an example where identity or dev 9. In your opinion, what are the biggest barriers or 10. How do you balance security requirements with

Last year, a phishing attack targeted an employee's The biggest barriers include legacy system incompatibility. Balancing security and convenience involves implementing

A stolen student laptop attempted to access our learning management system. Limited funding is a major barrier, as universities often lack resources for advanced security. We balance security and convenience by implementing

An attacker attempted to access our admin portal through a social engineering tactic. Legacy authentication protocols, common in hybrid environments, pose challenges. We use adaptive authentication with risk scoring to

During a phishing simulation, an attacker's attempt to steal credentials was thwarted. Complex policy configuration and a lack of awareness among users are barriers. Balancing security and convenience involves explaining

A consultant's laptop, lacking required security updates, was used to access internal systems. Complex migration from legacy systems to Zero Trust architectures is a barrier. We balance security and convenience with SSO and

11. What policies or best practices would you reco 12. How do you see identity verification evolving in 13. What role do you think device verification will i

Start by implementing MFA across all critical system Identity verification will likely shift toward continuous Device verification is critical for securing remote access

Begin with MFA across all critical systems, such as email Behavioral biometrics, such as keystroke dynamics Device verification is vital for securing remote and

Begin by segmenting access based on user roles and Identity verification will evolve toward AI-driven trust Device verification is critical for securing remote access

Define clear identity governance policies and tiered Identity verification will move toward frictionless self Device verification is essential for securing remote

Inventory all identities and devices to establish visibility Identity verification will leverage AI-driven continuous Device verification is central to securing remote access

14. Are there industry standards or frameworks (e.g., NIST SP 800-207, ISO 27001, etc.) that can help guide the implementation of Zero Trust?	15. If you could give one key piece of advice to organizations implementing Zero Trust, what would it be?	
NIST SP 800-207 provides a robust framework for Zero Trust.	Adopt Zero Trust as a mindset, not just a technology solution. Start with small, high-impact areas like MFA and device security.	
NIST's Cybersecurity Framework provides a flexible approach to risk management.	Focus on cultural change as much as technology. Educate users—students, faculty, and staff—about the importance of security.	
NIST SP 800-207 provides a comprehensive Zero Trust framework.	Focus on visibility, automation, and culture. Gain complete visibility into users, devices, and data flows.	
ISO 27001 provides a structured approach to security management.	View Zero Trust as a continuous learning process. Start with small, impactful steps like MFA and device security.	
NIST's Zero Trust Architecture (ZTA) provides a comprehensive framework for Zero Trust.	Trust nothing, verify everything, and adapt continuously. Start with high-impact controls like MFA and device security.	

IFA for critical systems and expand gradually to avoid overwhelming users or infrastructure. Focus on visibility and importance of Zero Trust to reduce resistance and build trust. Start with high-impact measures like MFA before implementing controls. Automate compliance checks and access policies to reduce manual overhead. Conduct regular audits and updates. Engage users early through education to build acceptance. Implement device verification, then scale to comprehensive policies. Invest in visibility—know your users, devices, and			