Timestamp	What is you name?	What is your current role/position?	How many years of experience do you have in IT or
########	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 thr
Multinational Enterprise	Yes	Traditional perimeter-based models rely on firewal

2. How would you describe the core value of Zero T	3. Which identity verification methods (MFA, SSO,	4. What challenges have you faced when implemer
Zero Trust ensures that no user, device, or applicat	Multi-factor authentication (MFA) combined with c	Implementing identity verification technologies oft
Zero Trust minimizes the attack surface by enforcin	Biometric MFA, such as fingerprint or facial recogn	Integrating MFA across hybrid systems—on-premis
Zero Trust ensures access is granted based on verif	Passwordless authentication combined with hardw	Integration with diverse cloud platforms and legacy
Zero Trust ensures ongoing verification of user ider	MFA via authenticator apps strikes an optimal bala	User fatigue from additional authentication steps is
Zero Trust transforms access from location-based t	FIDO2-based passwordless authentication combine	Integrating identity verification with complex syste

5. How do you assess the trustworthiness of device	6. What common issues arise when enforcing devi	7. From your experience, how do users typically re
We use endpoint management tools to assess devi	Common issues include unpatched operating syste	Initially, users expressed frustration with stricter cc
We use Mobile Device Management (MDM) tools t	Unpatched student laptops, missing antivirus softw	Students often resist stricter controls like MFA due
We use certificate-based authentication tied to dev	Delayed patches, non-standard device configuratio	Initially, stricter controls like MFA and device verifi
Device trustworthiness is assessed by checking OS	Unpatched or misconfigured systems, particularly s	Users initially resist stricter controls like MFA due t
We use continuous device health validation via Enc	BYOD fragmentation, inconsistent OS updates, and	Early pushback came from employees frustrated by

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 wit
Last year, a phishing attack targeted an employee's	The biggest barriers include legacy system incompa	Balancing security and convenience involves imple
A stolen student laptop attempted to access our le	Limited funding is a major barrier, as universities o	We balance security and convenience by implemer
An attacker attempted to access our admin portal	Legacy authentication protocols, common in hybric	We use adaptive authentication with risk scoring to
During a phishing simulation, an attacker's attempt	Complex policy configuration and a lack of awaren	Balancing security and convenience involves explai
A consultant's laptop, lacking required security upc	Complex migration from legacy systems to Zero Tru	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 ir	13. What role do you think device verification will
Start by implementing MFA across all critical syster	Identity verification will likely shift toward continuc	Device verification is critical for securing remote ar
Begin with MFA across all critical systems, such as s	Behavioral biometrics, such as keystroke dynamics	Device verification is vital for securing remote and
Begin by segmenting access based on user roles ar	Identity verification will evolve toward AI-driven tr	Device verification is critical for securing remote ar
Define clear identity governance policies and tiere	Identity verification will move toward frictionless s	Device verification is essential for securing remote
Inventory all identities and devices to establish visi	Identity verification will leverage AI-driven continu	Device verification is central to securing remote an

14. Are there industry standards or frameworks (e.	15. If you could give one key piece of advice to org		
NIST SP 800-207 provides a robust framework for Z	Adopt Zero Trust as a mindset, not just a technology solution. Start with small, high-impact areas like M		
NIST's Cybersecurity Framework provides a flexible	Focus on cultural change as much as technology. Educate users—students, faculty, and staff—about the		
NIST SP 800-207 provides a comprehensive Zero Tr	Focus on visibility, automation, and culture. Gain complete visibility into users, devices, and data flows		
ISO 27001 provides a structured approach to secur	View Zero Trust as a continuous learning process. Start with small, impactful steps like MFA and device		
NIST's Zero Trust Architecture (ZTA) provides a com	Trust nothing, verify everything, and adapt continuously. Start with high-impact controls like MFA and c		

IFA for critical systems and expand gradually to avoid overwhelming users or infrastructure. Focus on visi			
e 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 overh			
checks, then scale to comprehensive policies. Engage users early through education to build acceptance.			
levice verification, then scale to comprehensive policies. Invest in visibility—know your users, devices, ar			