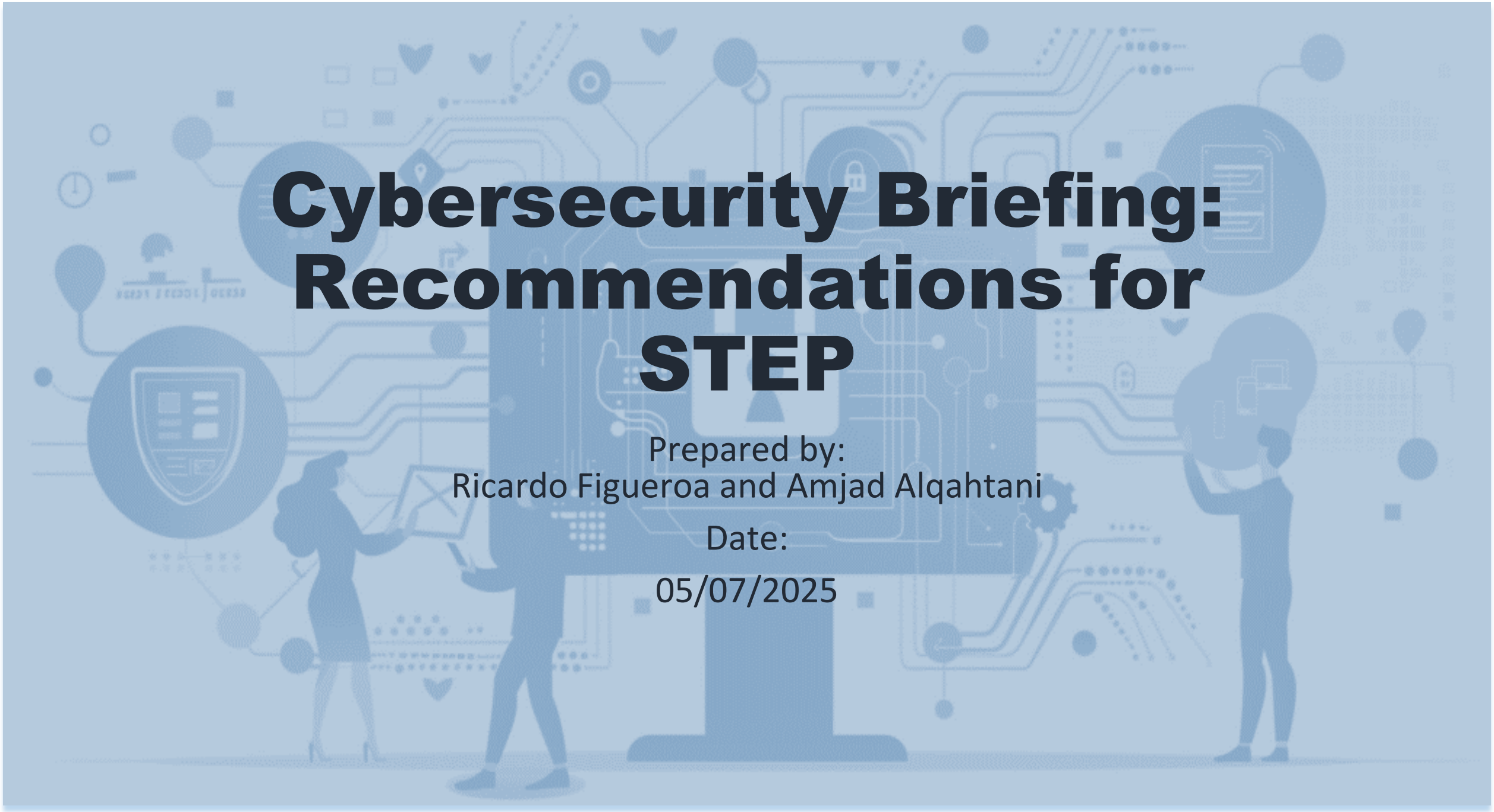


Cybersecurity Briefing: Recommendations for STEP

Prepared by:
Ricardo Figueroa and Amjad Alqahtani

Date:

05/07/2025

CEO Introduction

- CEO: Team, I’ve seen the report on our cybersecurity posture. Can you please explain where we really stand?

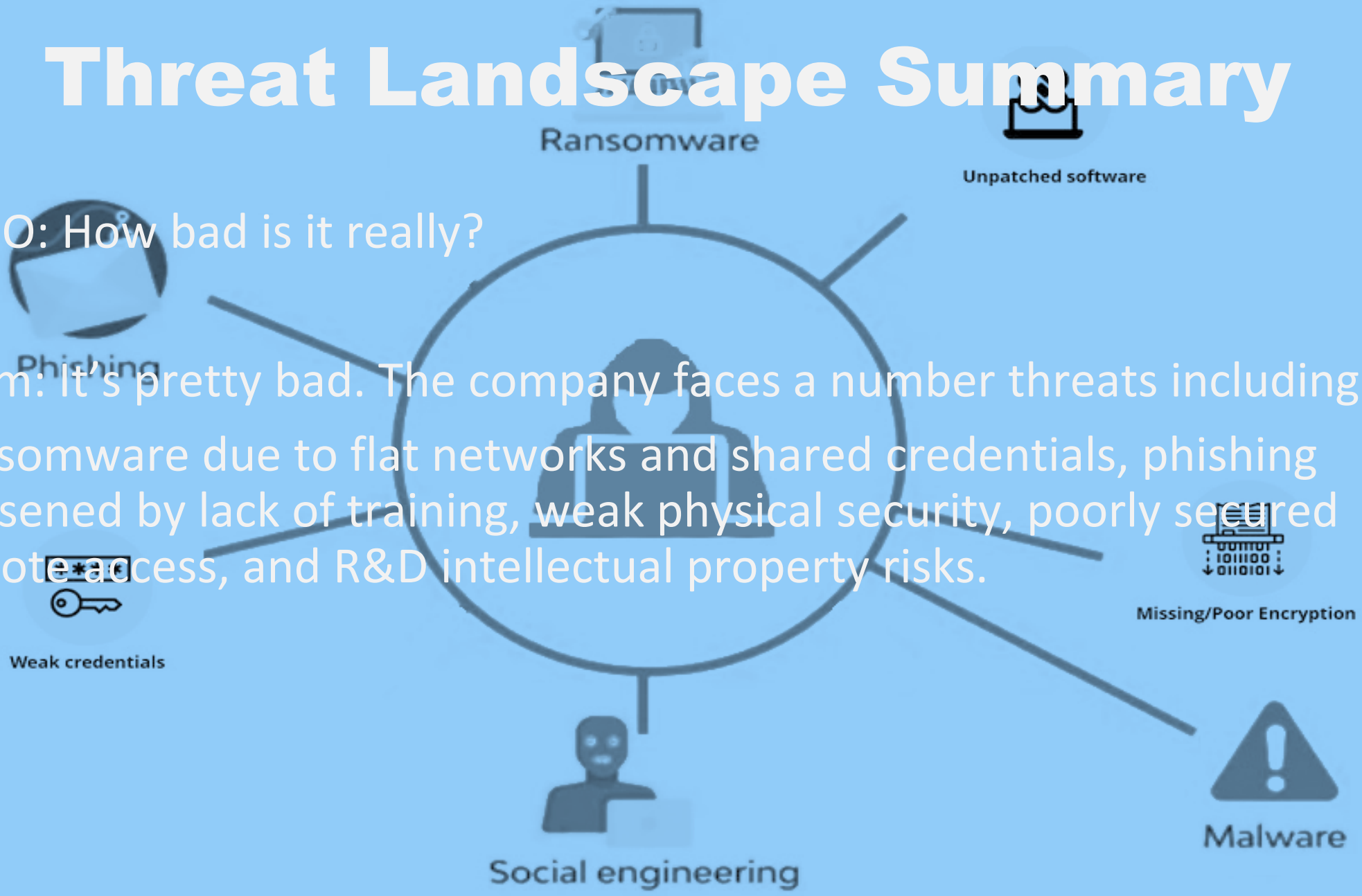
- Team: Absolutely! STEP is at serious risk from cyberattacks, especially ransomware, phishing, insider threats, and credential misuse. These threats could cripple operations if not urgently addressed.

Threat Landscape Summary

- CEO: How bad is it really?

Team: It’s pretty bad. The company faces a number threats including:

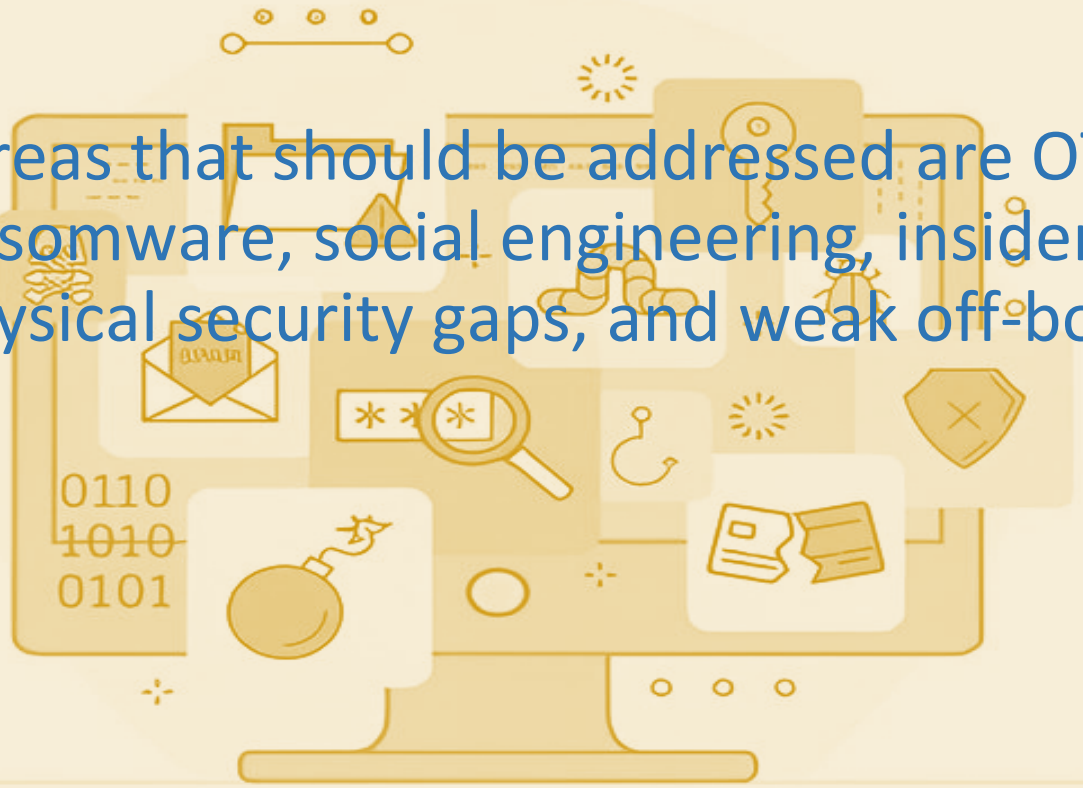
Ransomware due to flat networks and shared credentials, phishing worsened by lack of training, weak physical security, poorly secured remote access, and R&D intellectual property risks.



Top 7 Organizational Risks

- CEO: What are the top areas I should worry about?

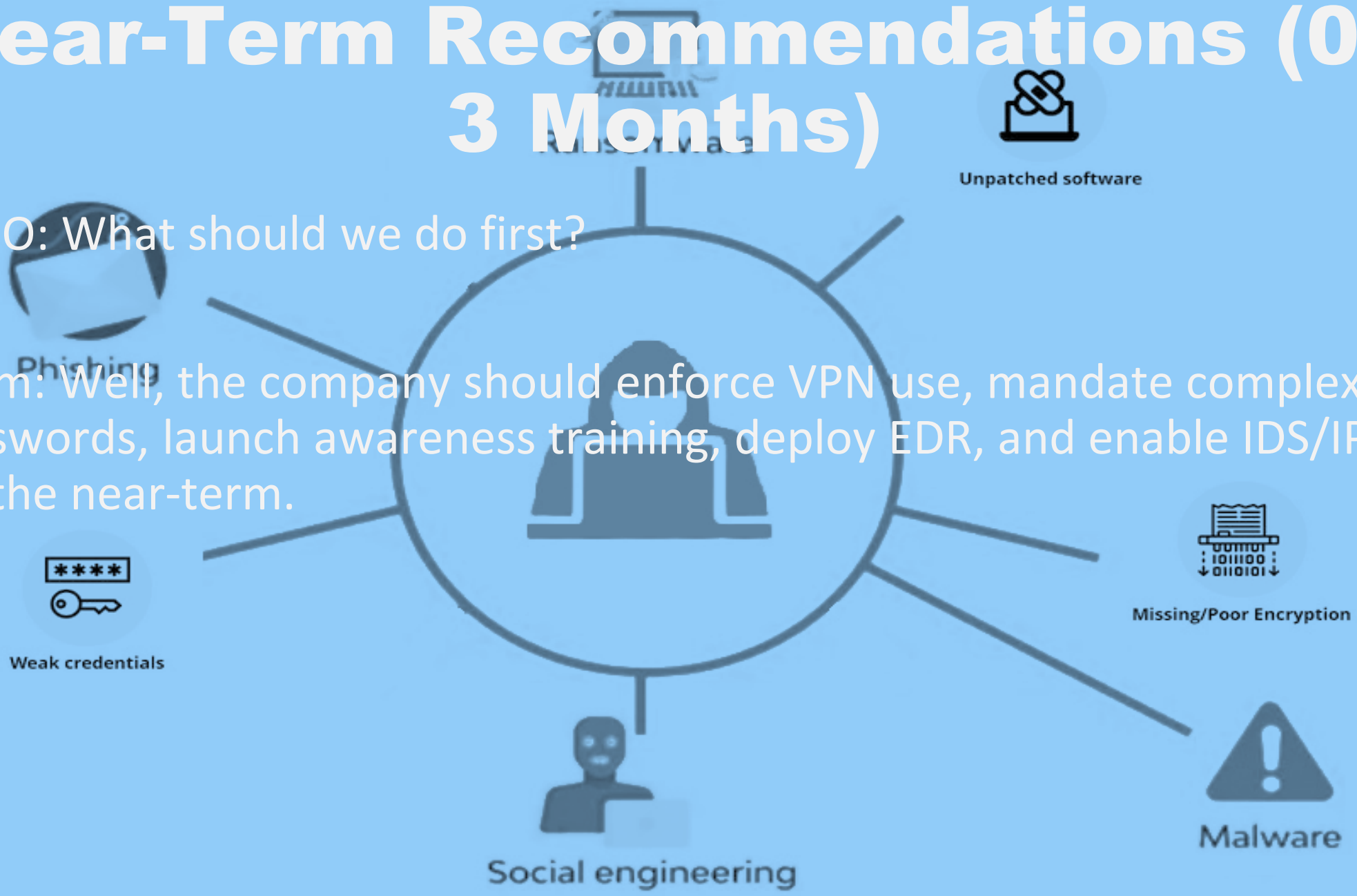
- Team: Well, the areas that should be addressed are OT system compromises, ransomware, social engineering, insider threats, R&D data breaches, physical security gaps, and weak off-boarding to name a few.



Near-Term Recommendations (0–3 Months)

- CEO: What should we do first?

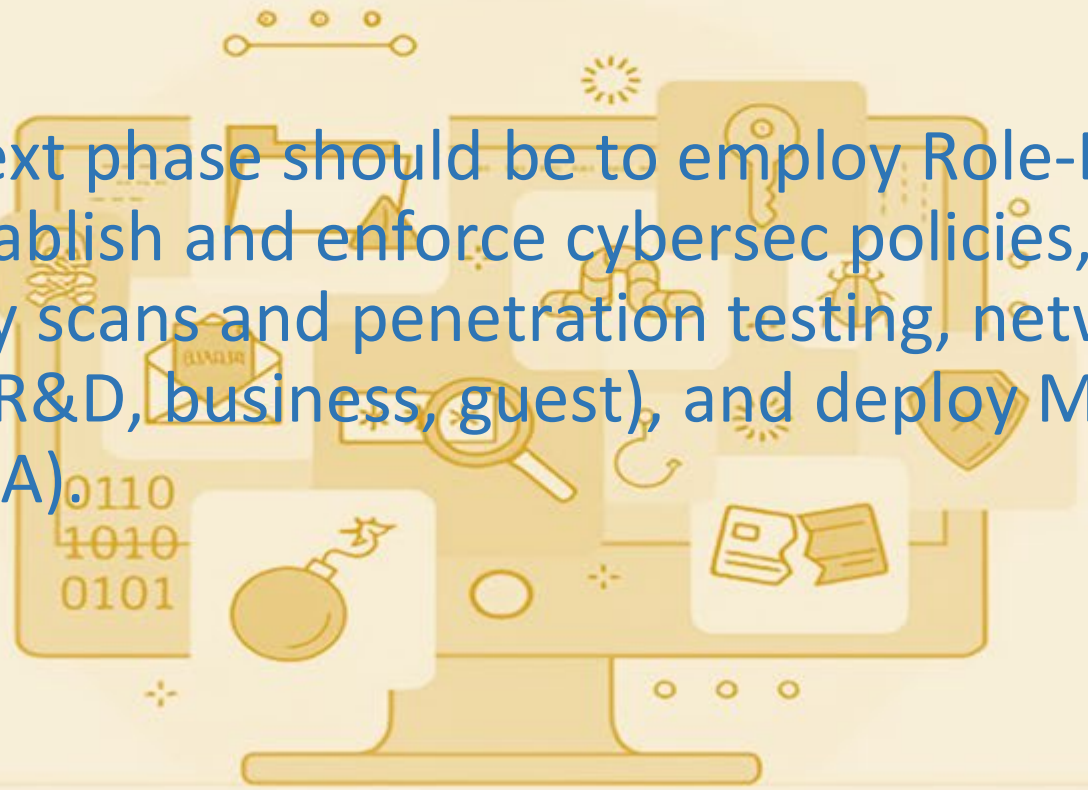
Team: Well, the company should enforce VPN use, mandate complex passwords, launch awareness training, deploy EDR, and enable IDS/IPS for the near-term.



Mid-Term Actions (4–9 Months)

- CEO: What’s the next phase?

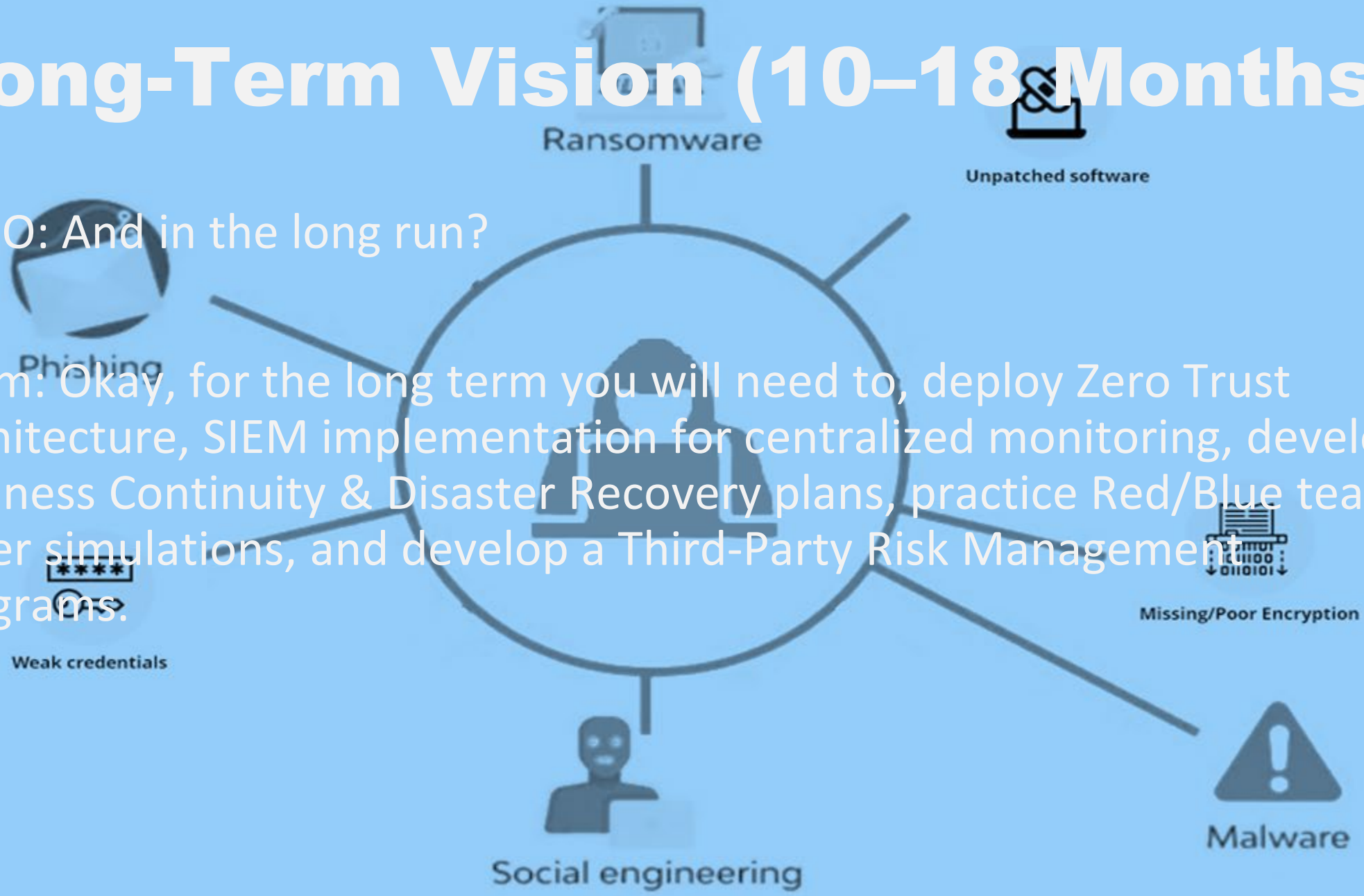
Team: Okay, The next phase should be to employ Role-Based Access Control (RBAC), establish and enforce cybersec policies, perform regular vulnerability scans and penetration testing, network segmentation (OT, R&D, business, guest), and deploy Multi-Factor Authentication (MFA).



Long-Term Vision (10–18 Months)

- CEO: And in the long run?

Team: Okay, for the long term you will need to, deploy Zero Trust Architecture, SIEM implementation for centralized monitoring, develop Business Continuity & Disaster Recovery plans, practice Red/Blue team cyber simulations, and develop a Third-Party Risk Management programs.



Core Policies to Implement

- CEO: What kind of policies do we need?

- Team: For the core policies, the company will need to Implement

Security Policies that spell out the rules for passwords, access control, and remote work. A security plan to ensure incident response, backup, disaster recovery, and a security program for endpoint management, SIEM, SOC, awareness training, and lastly a compliance and audit program.

Required Security Plans

- CEO: What about the required security plans?
- Team: We recommend an incident response plan, a backup & recovery plan, and a disaster recovery plan.

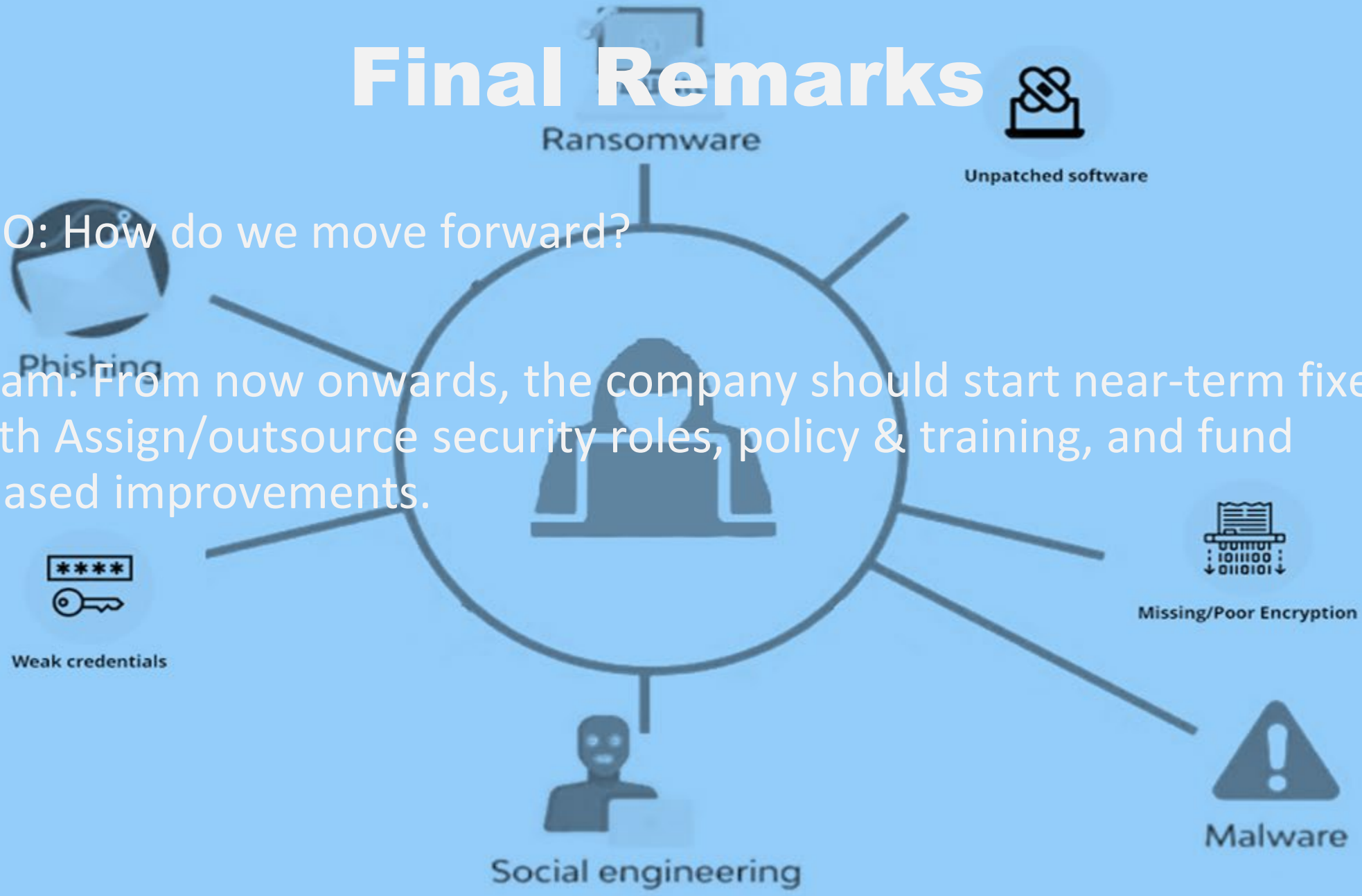
Strategic Programs

- CEO: What programs will keep us ahead?

- Team: Strategically, the company needs an awareness training program, security ops program, audit & compliance program, as well as an endpoint configuration, perimeter protection, and app whitelisting & data classification programs.

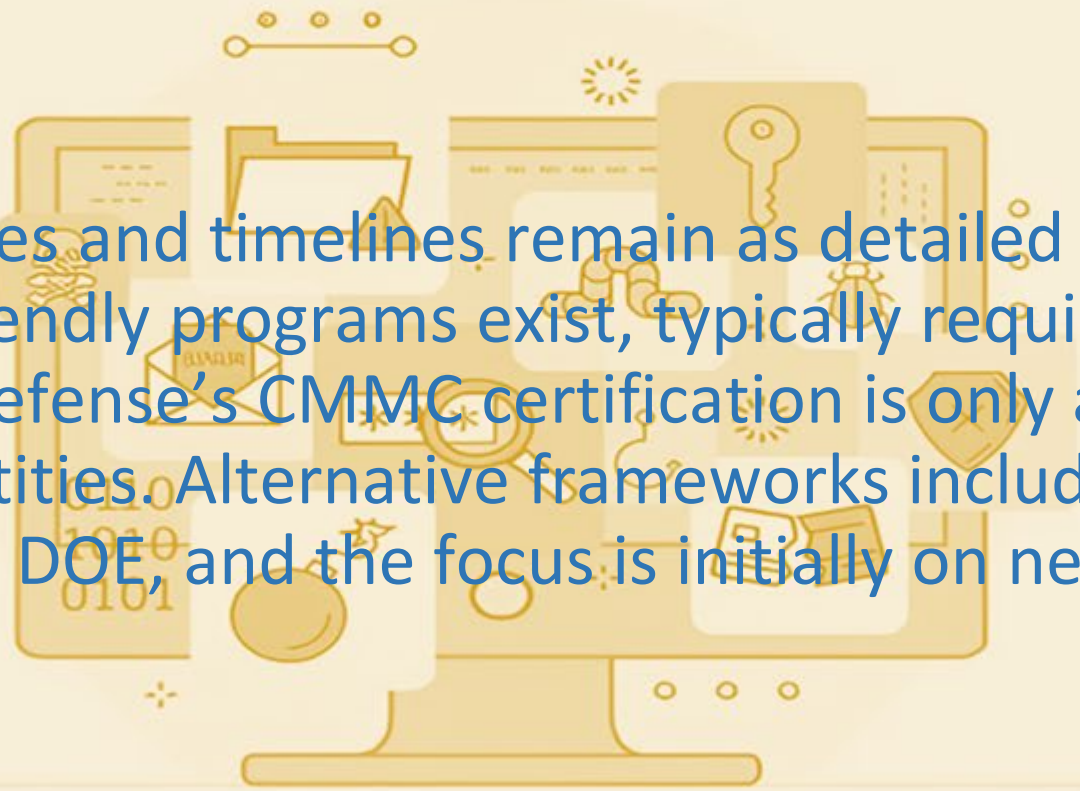
Final Remarks

- CEO: How do we move forward?
- Team: From now onwards, the company should start near-term fixes with Assign/outsource security roles, policy & training, and fund phased improvements.



Q&A

- CEO & Exec Team: Great! Let us discuss priorities, budgets, and timelines.



Team: Sure, priorities and timelines remain as detailed in the report. Multiple budget-friendly programs exist, typically requiring third-party involvement. InfoDefense's CMMC certification is only available to DoD-recognized entities. Alternative frameworks include NIST's CSF or partnering with the DOE, and the focus is initially on near- and mid-term goals.

Closing Remarks

- Thank you for your time.
- Prepared by: Ricardo Figueroa and Amjad Alqahtani
- Contact:
  - ricardo.figueroa@my.utsa.edu
  - amjad.alqahtani@my.utsa.edu