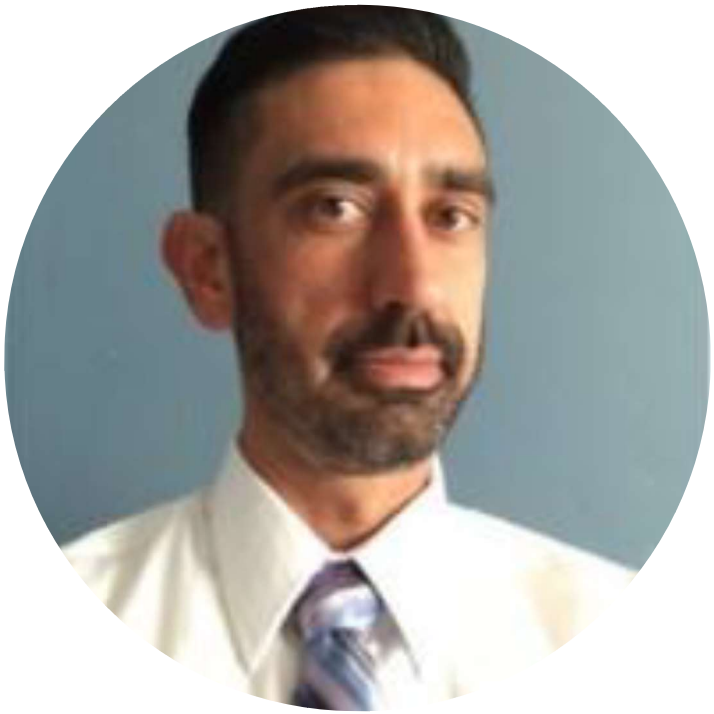
New Mexico Medical Society

Noon-Zoom: Cybersecurity

March 28, 2024

Krishna Goradia



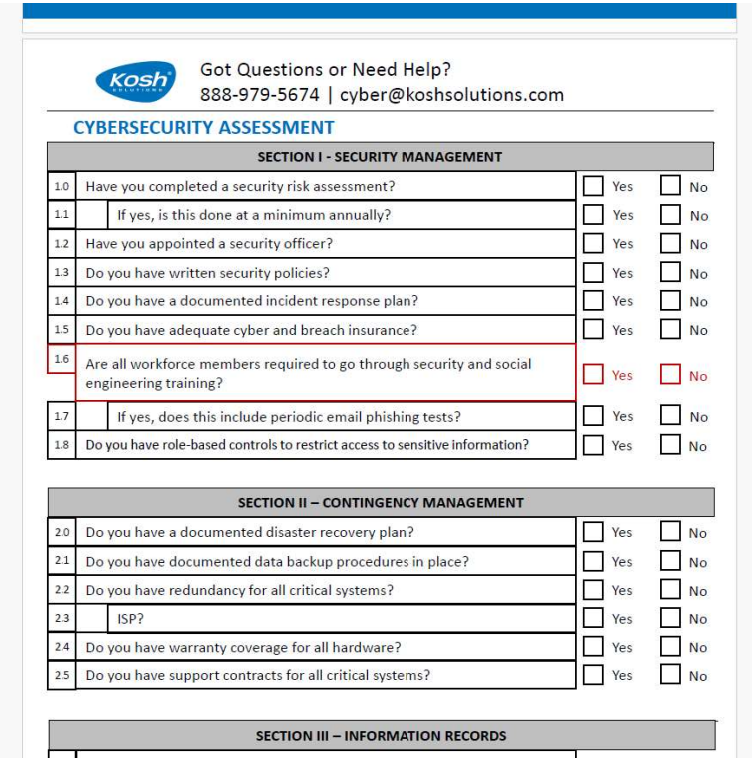
Agenda

- Course Objectives:

  - ✓ Understand how to apply the Cybersecurity Checklist to your organization.
  - ✓ Understand which components on the checklist are critical in nature.
  - ✓ Understand how cybersecurity relates to cyber insurance and some of the current requirements of insurance providers

- Evaluate your score

Cybersecurity Checklist



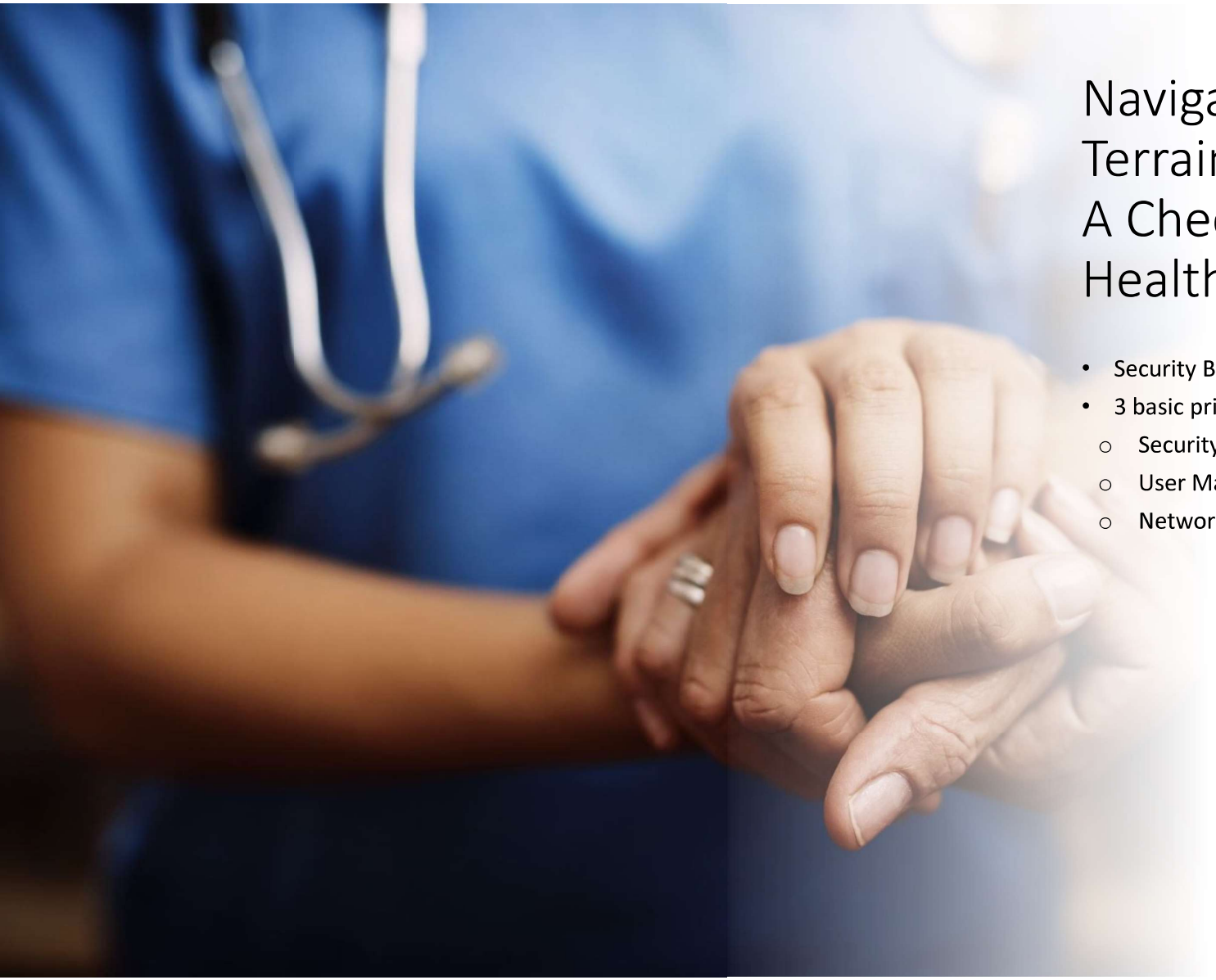
Got Questions or Need Help?
888-979-5674 | cyber@koshsolutions.com

CYBERSECURITY ASSESSMENT

SECTION I - SECURITY MANAGEMENT			
1.0	Have you completed a security risk assessment?	Yes	No
1.1	If yes, is this done at a minimum annually?	Yes	No
1.2	Have you appointed a security officer?	Yes	No
1.3	Do you have written security policies?	Yes	No
1.4	Do you have a documented incident response plan?	Yes	No
1.5	Do you have adequate cyber and breach insurance?	Yes	No
1.6	Are all workforce members required to go through security and social engineering training?	Yes	No
1.7	If yes, does this include periodic email phishing tests?	Yes	No
1.8	Do you have role-based controls to restrict access to sensitive information?	Yes	No

SECTION II – CONTINGENCY MANAGEMENT			
2.0	Do you have a documented disaster recovery plan?	Yes	No
2.1	Do you have documented data backup procedures in place?	Yes	No
2.2	Do you have redundancy for all critical systems?	Yes	No
2.3	ISP?	Yes	No
2.4	Do you have warranty coverage for all hardware?	Yes	No
2.5	Do you have support contracts for all critical systems?	Yes	No

SECTION III – INFORMATION RECORDS



Navigating the Cyber Terrain: A Checklist for Healthcare Security

- Security Breach or Incident.
- 3 basic principles
  - Security Management
  - User Management
  - Network Controls

Security Management

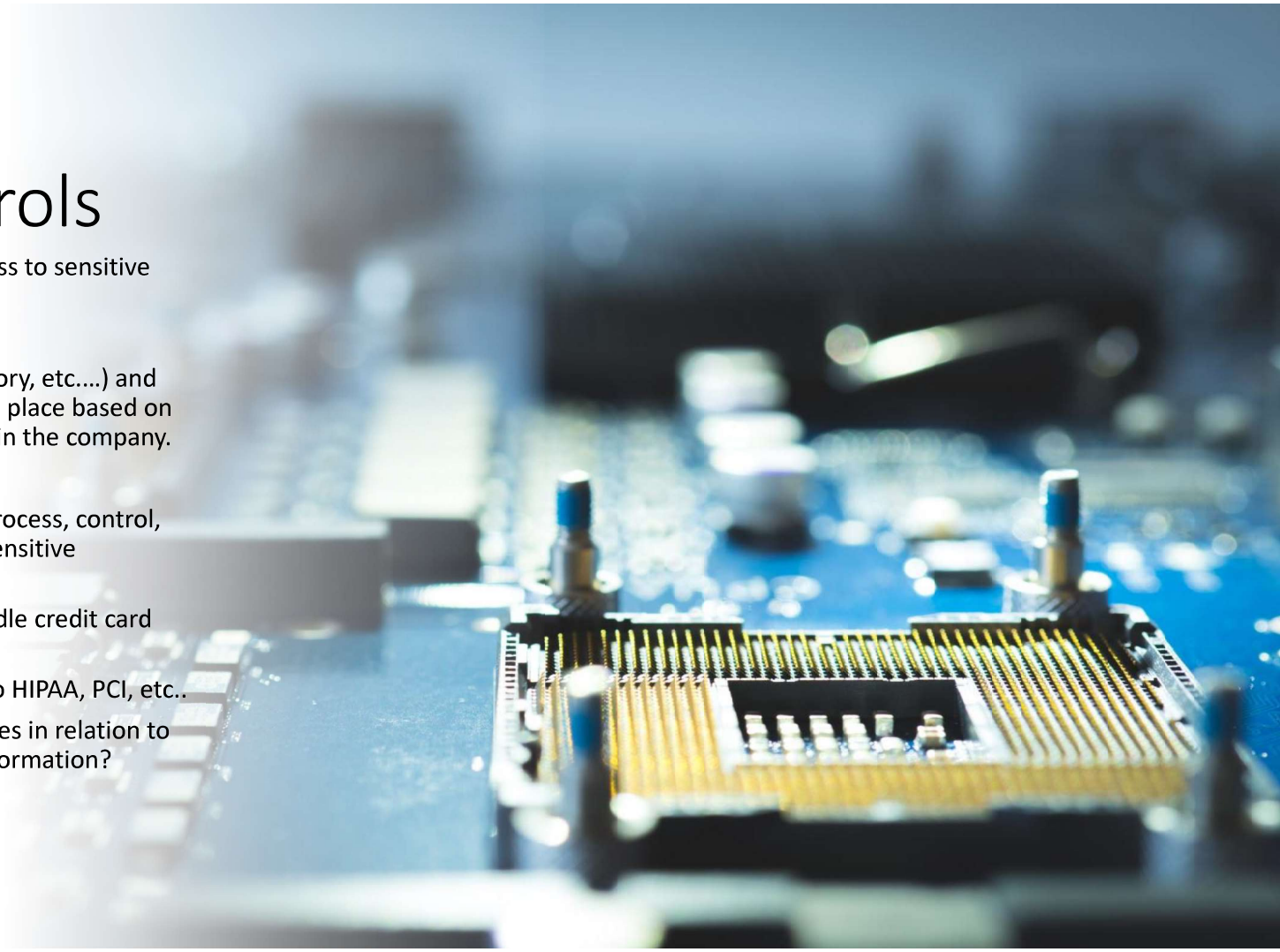
- Have you completed a security risk assessment?
  - Minimum annually
- Have you appointed a security officer?
- Documentation:
  - Written security policies
  - Incident response pan
  - Cyber and breach insurance

End User Security

- All workforce members need to go through regular security and social engineering training
  - What is security training
  - What is social engineering
- Periodic email phishing tests
  - SLAM method:
    - Sender: look at the address that sent you the email
    - Links: hover over links to see where they really point
    - Attachment: do not download
    - Message: look for urgency in the message and errors

Network Controls

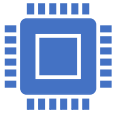
- Role-based controls to restrict access to sensitive information
  - What are these?
    - (MS 365, Active Directory, etc.…) and physical controls are in place based on the role of the person in the company.
- Information Records
  - Do you collect, store, host, process, control, use or share any private or sensitive information?
  - Do you process, store or handle credit card information?
    - How does this relate to HIPAA, PCI, etc..
  - Have you reviewed the policies in relation to storing and collecting this information?



Contingency Management

Documented disaster recovery plan

What is it? Why does it need to be documented?



Do you have redundancy for all systems?

What does this mean exactly? For what systems?

ISP – single or failover?

Support contracts for all critical systems?

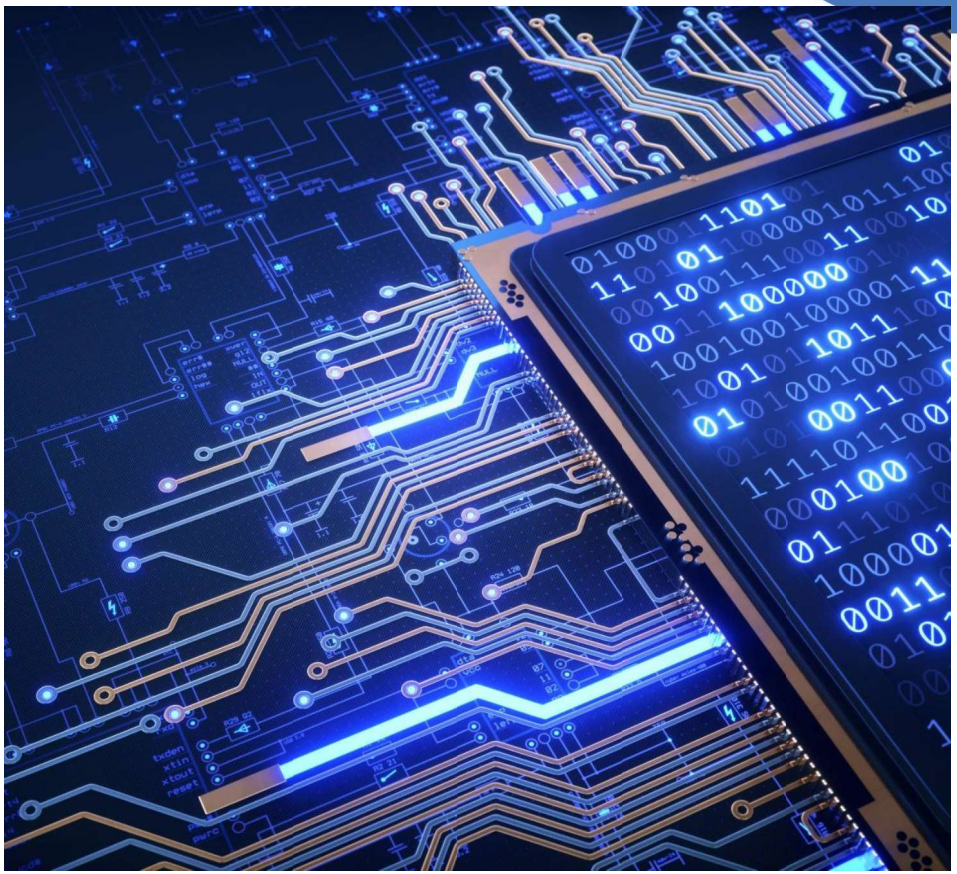
How do you define what is critical?

Infrastructure & Security Controls

- Are all systems and devices fully patched and on the most up to date versions?
- Do you have anti-virus on all servers, workstations and endpoints? Is it Next-Gen?
- Do you use endpoint detection and response tools that include centralized monitoring and logging of all endpoint security across your business?
- Do you use a cloud provider to store data or host applications?
    - Do you use MFA to secure all cloud provider services?
    - Do you have a firewall protecting both your office(s) and your cloud environment
- Is all your network equipment connected to a UPS? Especially servers

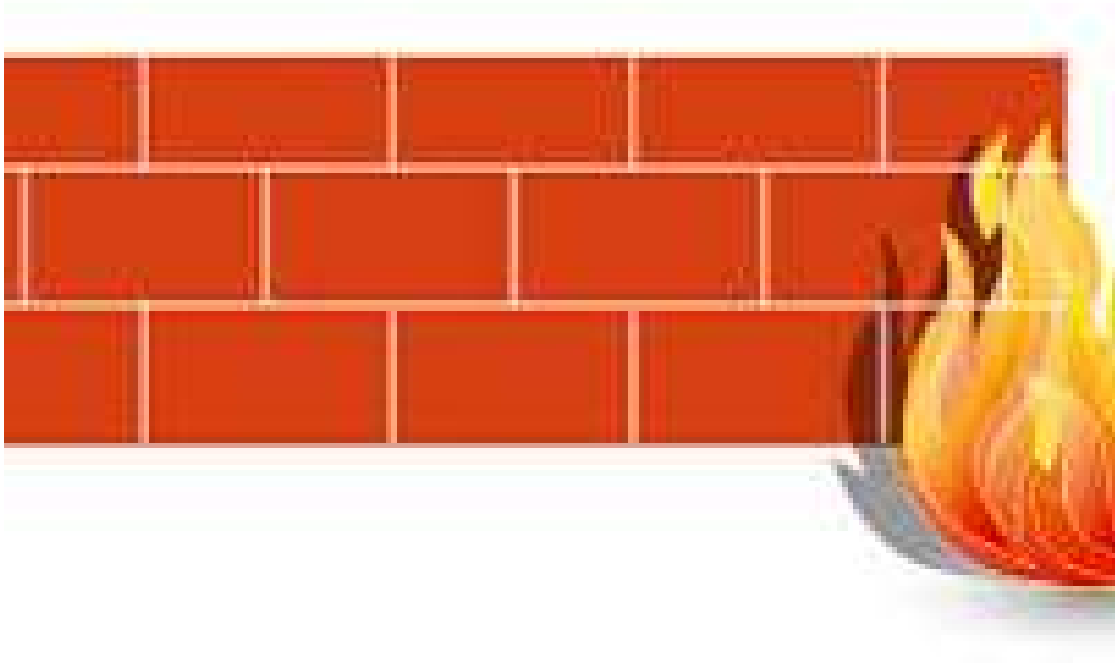
Infrastructure & Security Controls

- Do employees protect and not share passwords?
- Email
  - Are emails prescreened for potentially malicious attachments and links?
    - a. Is there a sandbox to test before delivery? Can users access email through web or non- corporate devices?
    - b. Does the access require MFA?
  - Is email encrypted?
  - Do you allow remote access to your network or information?
  - Do you use MFA to secure all access?



Infrastructure & Security Controls

- Servers
  - Do you use a data backup solution?
    - How frequently does it run?
    - Estimated amount of time it would take to restore essential functions
    - Are backups encrypted?
    - Are backups kept separate from your network?
    - Are backups secured with different access credentials from other administrator credentials?
    - Do you use a cloud-syncing service? Is it protected by MFA?
    - Have you tested a successful restoration of a file in the last 6 months?
      - How about of a server?
  - Are you able to test the integrity of backups prior to restoration to ensure they are free of malware?



Advanced Security Controls

- Do you have a firewall in place at your office(s)?
  - Does it provide UTP? IPS, Anti-X, URL filtering
  - Is it patched and up to date?
- Do you scan the dark web for potentially cracked passwords?
- Do you encrypt all sensitive and confidential information stored?
- Do you perform vulnerability and penetration testing on a periodic basis?

My Score

Add up all of your yesses to get your score

0-29	30-44	45-51
High Risk	Medium Risk	Low Risk

Key Take-Aways

- End user training (a/v and a firewall is not sufficient) - everyone in the org needs to be aware and participate in security
- Security is not static – has to be looked at and updated regularly as in-office systems change and as technology changes
- Backups save people, firewalls with UTM, MFA, on-going user security (Pii) training
- Cybersecurity insurance

Free Useful Resources

- Kosh Solutions free Cybersecurity Checklist: Cybersecurity PDF | Kosh Solutions
- Kosh Solutions free dark web scan: email or call Kosh to get started.
- Breach calculator: Free PHI Breach Cost Calculator | PII Protect (pii-protect.com)
- Cybersecurity Awareness Quiz for your staff: email or call Kosh to get started.