Nancy Laney, CyberAB Registered Practitioner
Owner PEAK Complyance CyberAB Registered Practitioner Organization

Nancy Laney is President and Owner of PEAK Complyance, a division of Laney ITC (RPO) in Southern Oregon, focusing on bringing the expertise of over 30 years of compliance design and implementation within reach of the SMB in the defense industrial base. She is a CMMC Registered Professional and has professional certifications in Project Management (PMP), Healthcare Information and Management Systems (CPHIMS), and has implemented many certification standards including ITIL, HIPAA, CIS and NIST.

Nancy's mission is to make the complex understandable; to distill the possibilities of best practices to exactly what is needed for small business.

Prior to launching both her MSP (PEAK IT Security & Services) and PEAK Complyance, Nancy served as an IT consultant, Corporate IT Director, Program Manager, as well as New Construction IT Project Manager in healthcare related fields for national healthcare companies.

https://www.linkedin.com/in/nancylaney/
Current State of Manufacturing

- **60%** Legacy Systems Lacking Updates
- **25%** Formal Incident Response Plan
- **35%** Cybersecurity Training
- **45%** Lack Segmentation IT and OT networks
- **25%** Cyber Disruption

www.cobalt.io/blog/cybersecurity-statistics-2023
Threats to IT & OT Manufacturing

- 95% Data Breaches Due To Human Error
- 96% Focused on Monetary Gain
- 38% Server Security Misconfigurations
- 14% Prepared to Defend Cyberattack
- 60% SMB Owners Think they are NOT a Target

www.cobalt.io/blog/cybersecurity-statistics-2023
"Legacy devices were often deployed on flat networks, at a time when the need for security took a back seat to other priorities, such as high availability and performance."
Incident Response & Business Continuity

**Incident Response Plan**

- Preparation
- Detection & Analysis
- Containment, Eradication, Recovery
- Post Incident Activity

**Business Continuity**

- Disaster Recovery
- 3-2-1-1-0
- Immutable Backups
- Air gapped
- Critical
- Business Priorities
- Downtime
Network

DMZ & Firewall
- Public Facing Ports
- Configuration Documentation

Segmentation
- Unmanged Hubs
- VLANs
- Access Control Lists
- 802.1x
- DHCP/IPs
- Layers of security
- Documentation
Endpoints

**Configuration Management**
- Patch/update
- Domain Joined
- Manage Stale AD
- Full Disk Encryption
- LAPS
- No Personal SW

**Anti-Virus**
- Endpoints
- Servers
- AV Current
- Behavior Based
- Zero-Trust
Users

- Training
- Human Shield
- Train Often
- Phishing Campaigns
- Cheat Sheets
- Password Strength
- Password Manager

- Least Privilege
- Role Based Access
- MFA
- 2FA
- MFA
- TOTP
1 Day Away

1. Immutable Backup & Test it
2. Relentless Patching
3. Upgrade to current versions
4. Anti-Virus
5. 2FA on EVERYTHING
6. Strong Passwords
   a) Password Manager
7. Network Segmentation
8. Incident Response Plan
9. PingCastle/Testimo
10. ATP Recommendations
Thank you!

Nancy@peakitss.com

3.5 Million

# of Open Cybersecurity Jobs in 2023 waiting to be filled

Thank you!

PEAK IT SECURITY & SOLUTIONS