



Final Project: Improving Information Assurance at Fullsoft

Presented by Antonio Seen

Date: 5/11/25

Regulations and Compliance Requirements

- - HIPAA
- - SOX
- - HITECH
- - SEC Cybersecurity Disclosure
- - GDPR
- - PCI DSS
- - NY SHIELD Act

Importance of Regulatory Compliance

- - Legal and financial protections
- - Customer trust
- - Investor confidence
- - Audit readiness
- - Data breach liability mitigation

Recommended Risk Framework: NIST RMF

- - Structured 6-step approach
- - Real-time risk monitoring
- - Supports DevSecOps and CI/CD
- - Public sector and IT alignment

Why Use NIST RMF?

- - Audit and compliance readiness
- - Integration with security ops
- - Continuous assessment
- - Trusted industry framework

Summary of the Malware Incident

- - Originated via USB
- - Source code accessed
- - Incomplete logging
- - Delayed detection

Lessons from the Breach

- - Improve EDR solutions
- - Disable unverified USB use
- - Train employees
- - Strengthen access controls

Security Gap Analysis Plan

- - Evaluate access and threat controls
- - Review AI integration
- - Use ISO 27002 and NIST 800-53
- - Align with internal policies

Organization-Wide Collaboration

- - Involve IT, legal, ethics, and security
- - Workshops and surveys
- - Leadership alignment

Business Continuity Management

- - Test backups
- - Remote access plans
- - Malware scenarios
- - Revise response plans

Immediate Countermeasures

- - EDR upgrades
- - 24/7 log monitoring
- - MFA enforcement
- - Targeted training

Long-Term Prevention Strategy

- - Red teaming
- - Threat intelligence feeds
- - Secure coding
- - Yearly audits

Summary: Toward a Secure Fullsoft

- - Apply NIST RMF
- - Learn from breaches
- - Fill identified gaps
- - Act fast, plan long-term

Questions & Discussion

- - Thoughts?
- - Suggestions?
- - Concerns?

References

- Capgemini Research Institute. (2019). Reinventing cybersecurity with AI.
- Microsoft. (2021). The state of cybersecurity.
- National Institute of Standards and Technology. (2022). Risk Management Framework (RMF).
- U.S. Department of Health and Human Services. (2022). HIPAA for professionals.
- U.S. Securities and Exchange Commission. (2023). Cybersecurity Risk Management Disclosure.
- Whittaker, M., et al. (2018). AI Now Report 2018.
- SecureOps. (n.d.). The Hack on Sony Group Pictures.
- CISA. (n.d.). Protecting Against Malicious Code.