Rochester Clearinghouse Meeting

Presented by:

ANJOLEN
Securing Your Cyber Future

Michelle Tuttle
VP Client Relations & Business Development

- Manages all client engagements
- BS degree in Communications and Marketing from SUNY Poly
- Master's degree in Cyber Security from Utica College.
- Expertise in cybersecurity, compliance, risk management and marketing/PR
- Identity Theft Prevention Expert.
- 15+ years experience in financial operations

ANJOLEN

- Specialists in cyber security, incident response and remediation
- Experience in finance/banking, education, non-profit, healthcare sectors
- Provides long-term planning and guidance to support evolving security demands
- Located in Utica, N.Y. – Clients throughout the U.S.

Introduction

- Growing Cyber Security Threats
  - Heightened cyber security awareness (Russia & China)
- Banking sector increasingly a target
  - PII
  - Cripple Economy
- Prepare for the unexpected – Be Hypervigilant
- Zero-Day Attacks
  - Anti-Virus & IDS are not effective
  - SOC Services

Proactive Measures

- Update Anti-Virus & Anti-Malware Systems
- Ensure recent backups of critical data
- Increase Monitoring of Alerts & Systems (SOC Monitoring)
- Internal & External Vulnerability/Penetration Testing
- Social Engineering Testing
- Ongoing Cyber Security Training
- Incident Response Retainer

SOC Monitoring Services

- Monitor security systems and alerts
- Prioritize security alerts
- Take immediate action

External Penetration Test

- Use simulated attacks against external firewalls and external facing systems
- Identify:
  - Open ports
  - Potential vulnerabilities
  - Methods of intrusion
  - Internal data leakage

Internal Vulnerability Assessment

- Test internal network in the following areas:
    - Policy and Procedure benchmarking
    - Network scanning
    - Access control testing
    - Data storage security testing
    - Data transmission security testing
    - Physical security analysis

Social Engineering Testing

- Attempting to improperly gain access to sensitive information or locations without proper authority, intended to gauge employee responsiveness using methods such as:
  - **Phishing**
  - **Vishing**
  - **Pretexting**
  - **Adversarial attack**

Training

- Cybersecurity Training and Awareness:
  - Customized training sessions focused on human vulnerabilities related to information and data protection
  - Diverse audience training that may be tailored to audiences such as executives, technical personnel, administrative and clerical staff
  - Adaptable training formats such as:
    - In-person training
    - Online training
    - Hybrid training

Contact Us

Anjolen Inc

www.anjolen.com

Michelle Tuttle

(315) 525-6233

mtuttle@anjolen.com

Questions

?