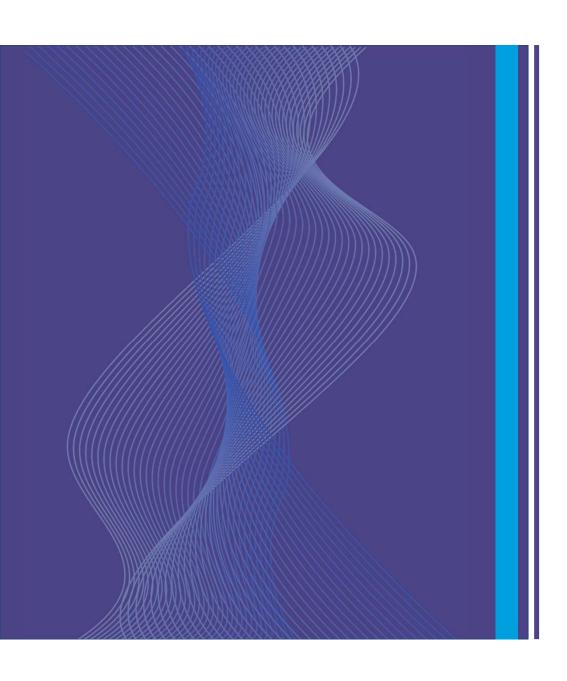


Cyber risks and Best Practices

Wednesday, May 11th, 2023





Pat Heller

Vice President, FI Sales

Adam Ward

Business Development Manager

Marquise Davis

Cyber Security Services Manager

Joe Stouffer

IT Application Support Analyst II

Agenda

- Cyber Risk Best Practices
 - Password Security and Management
 - Multifactor Authentication
 - EDR >>> MDR
 - Backup/Data Protection
 - O365 Conditional Access Policies
- Anatomy of an Email Compromise
 - With Joe Stouffer and Marquise Davis
- Recap and Questions

Password Security and Management

- Longer Passwords
- No More Password Hints
- No More Secret Questions Out of Band
- O365 Admins only non-mailbox accounts
- Password Managers













Multifactor Authentication

- 1. O365 Enable MFA for all users
- 2. O365 Enforce with Conditional Access Policy
- 3. O365 Require Authenticator App
- 4. Consider DUO for internal MFA to network
- 5. Always require MFA for remote users









EDR >>><< **MDR**

- 1. EDR Endpoint Detection & Response (Baseline)
- 2. MDR Managed Detection & Response





Backup/Data Protection

- 1. Test Automated Testing
- 2. MFA protection on any cloud storage platforms
- 3. Credentials are separate non-network credentials
- 4. Store data on separate non-Microsoft platform
- 5. Protections and Controls for Backup Segmentation
- 6. Backup Office 365



Conditional Access Policy – Business Premium

- 1. Block Non US Logins
- 2. Block Legacy Authentication
- 3. Block Logins from Outside Bank & Branch External IPs
- 4. Require MFA for All Users
- 5. Require MFA for Specific Programs Externally (Teams)



Anatomy of an Email Compromise

- 1. Vendor or other party is compromised by Phishing Attack
- 2. Email all contacts found with Sophisticated Phishing Attack
- 3. Collect phished credentials from duped parties
- 4. Immediately login to O365 portal if not blocked:
- 5. Check for admin rights if available, create new admin account
- 6. Create inbox rules to delete / move emails from original compromised vendor
- 7. Analyze what data can be accessed, download anything from One Drive/Sharepoint that appears to have passwords or email contact lists
- 8. Start Process over again with new compromised organization



Q&A

Pat Heller – pat.heller@scantron.com

Adam Ward – <u>adam.ward@scantron.com</u>

Marquise Davis – <u>marquise.davis@scantron.com</u>

Joe Stouffer – <u>joe.stouffer@scantron.com</u>

