As cybersecurity vulnerabilities become more prevalent across the nation, this resource is designed to provide an overview of the current threat landscape and offers district leaders a reminder of important protections that should be implemented to help mitigate risks associated with recent cyber threats.

**EMOTET** INFILTRATES AND DEPLOYS
**TRICKBOT** STEALS CREDENTIALS AND SPREADS
**RYUK RANSOMWARE**

**SYSTEM PROTECTION REMINDERS**

- **VULNERABILITY MANAGEMENT**: Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.
- **SYSTEM BACKUPS**: Ensure backups for critical systems are in place and audit backups for completion and functionality.
- **SYSTEM HARDENING**: Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.
- **IDENTITY MANAGEMENT**: Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.
- **APPLICATION SECURITY**: Only use district approved softwares, audit system access, and isolate critical infrastructure.

**SYSTEM PATCHING TARGET TIMEFRAMES**

- **SECURITY AND CRITICAL**: 1 to 3 WEEKS
- **HIGH PRIORITY**: 1 to 2 MONTHS
- **LOW PRIORITY**: 3 to 4 MONTHS

Ensure ALL staff members are trained on Data Security best practices, particularly Email Phishing Recognition.
**VULNERABILITY MANAGEMENT**

Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PATCH MANAGEMENT</strong></td>
<td>Patch known vulnerabilities that apply to all systems, software, and components in your environment. Critical systems should be prioritized, however all systems should be patched in the recommended timeframe.</td>
</tr>
<tr>
<td><strong>HARDWARE INVENTORY</strong></td>
<td>Keep an inventory of authorized devices and detect unauthorized devices. Know what devices are connected to your network at all times so they can be monitored.</td>
</tr>
<tr>
<td><strong>SOFTWARE INVENTORY</strong></td>
<td>Keep an inventory of authorized software and detect unauthorized software. Know what software is in use so you can be sure it is secured and patched appropriately.</td>
</tr>
<tr>
<td><strong>NETWORK PORTS</strong></td>
<td>Limit and control network ports. Ensure ports no longer in use are closed and open ports are limited in scope where possible.</td>
</tr>
<tr>
<td><strong>WIRELESS ACCESS CONTROL</strong></td>
<td>Secure and segment wireless networks, including elimination of open networks. Guest networks should not have access to networked resources.</td>
</tr>
<tr>
<td><strong>DEACTIVATE ACCOUNTS</strong></td>
<td>Deactivate the user accounts of those no longer in need of access, including former employees. Accounts of inactive users are often exploited as warning signs are less likely to be noticed.</td>
</tr>
</tbody>
</table>

**FIVE STEPS FOR MANAGING SYSTEM VULNERABILITY**

- **SCAN**
  - Perform weekly external and internal network scans
- **PLAN**
  - Deploy and implement an alert mitigation plan
- **PRIORITIZE**
  - Make patches and fixes a high priority
- **VALIDATE**
  - Test and validate patches and fixes before deployment
- **DEPLOY**
  - Apply validated patches and fixes as soon as possible
Ensure backups for critical systems are in place and audit backups for completion and functionality.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BACKUP CREDENTIALS</strong></td>
<td>Only accounts needed for backup operations should be able to connect to backup storage systems. Backup systems should be kept as isolated as possible to prevent the spread of infections to backups.</td>
</tr>
<tr>
<td><strong>DOMAIN BACKUPS</strong></td>
<td>Backup servers should not be bound to the district domain. Isolating backup servers from the domain prevents the spread of malware to the backup server via compromised domain credentials.</td>
</tr>
<tr>
<td><strong>FILE SYSTEMS</strong></td>
<td>Leverage different file systems for backup storage when feasible. Machines running Linux often function as backup repositories.</td>
</tr>
<tr>
<td><strong>OFFLINE STORAGE</strong></td>
<td>One of the best defenses against propagation of ransomware encryption to the backup storage is to have offline storage. Examples: • Replicated VMs • Storage snapshots • Cloud Connect backups • Rotating (Media) • Tapes</td>
</tr>
<tr>
<td><strong>REGULAR TESTING</strong></td>
<td>Test backups and systems on a regular basis. Monitoring backups for completion and regularly conducting test restores helps ensure backup integrity.</td>
</tr>
<tr>
<td><strong>BACKUP LOGS</strong></td>
<td>Document and maintain a log of all system backups, testing schedules, and retention periods. Accurate log documentation can greatly increase recovery time.</td>
</tr>
<tr>
<td><strong>CURRENT IMAGE</strong></td>
<td>Keep and maintain an up-to-date image for machines to assist in recovery. Update image with each new Microsoft Build (typically semi-annually).</td>
</tr>
</tbody>
</table>

**REASONS FOR DATA LOSS**

- **UNINTENTIONAL ACTION**
  - Mistaken deletion of files or partitions
  - Computer virus attacks
  - System hacking

- **INTENTIONAL ACTION**
  - Intentional deletion of files or partitions
  - Hard drive formatting

- **FAILURE**
  - Hardware failures
  - Power failures
  - System crash

- **DISASTER**
  - Thunderstorms, earthquakes, floods, fire, etc.
NEW YORK STATE REGIONAL INFORMATION CENTERS
DATA SECURITY THREAT LANDSCAPE

SYSTEM HARDENING

Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ANTIVIRUS</strong></td>
<td>Ensure anti-virus software is installed on all systems and up to date. Anti-virus solutions that utilize behavioral analysis and artificial intelligence are more effective than definition based systems.</td>
</tr>
<tr>
<td><strong>LOCAL ADMINISTRATOR PASSWORD SOLUTION</strong></td>
<td>Utilize LAPS for the local management of domain computers. LAPS is a Microsoft tool that sets a unique password for every local administrator computer account and stores it in Active Directory.</td>
</tr>
<tr>
<td><strong>PASSWORD POLICY</strong></td>
<td>Update password policies to reflect best practices. Consider increasing length requirements on passwords and decreasing complexity requirements</td>
</tr>
<tr>
<td><strong>DOMAIN CONTROLLERS</strong></td>
<td>Do not install additional software on domain controllers. Do not install additional non-critical roles. Only mechanisms required for functionality and security should exists on domain controllers.</td>
</tr>
<tr>
<td><strong>SECURE ADMIN WORKSTATION</strong></td>
<td>Use a dedicated Secure Admin Workstation (SAW) to only perform administrative tasks. Day-to-day office work (e.g. email, web usage, etc.) should be conducted on a separate machine.</td>
</tr>
<tr>
<td><strong>ENABLE DOMAIN AUDIT LOGS</strong></td>
<td>Enable Audit Policy Settings with Group Policy. See the attached Audit Policy Settings page for recommended settings.</td>
</tr>
<tr>
<td><strong>SERVER MESSAGE BLOCKS</strong></td>
<td>Disable the outdated file and print sharing protocol Server Message Blocks Version 1 (SMBv1). Use SMBv2 or SMBv3.</td>
</tr>
<tr>
<td><strong>OPERATING SYSTEM UPDATES</strong></td>
<td>Apply critical and security patches within 2-4 weeks. Ensure Microsoft Windows patch MS17-010 is installed.</td>
</tr>
<tr>
<td><strong>OPERATING SYSTEM FIREWALL</strong></td>
<td>Limit and control system firewall ports. Ensure ports no longer in use are closed and open ports are limited in scope where possible.</td>
</tr>
</tbody>
</table>

**LAYERED APPROACH TO SYSTEM HARDENING**

- DEVICE
- APPLICATION
- COMPUTER
- NETWORK
- PHYSICAL
- POLICIES, PROCEDURES, AWARENESS
Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>APPROPRIATE PERMISSIONS</strong></td>
<td>Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.</td>
</tr>
<tr>
<td><strong>DOMAIN ADMINISTRATORS</strong></td>
<td>There should be no day to day user accounts in the Domain Admin group. Network admins should have 2 Active Directory accounts: 1. Day to day work and office functions with no admin privileges 2. Privileged account that is used exclusively for tasks requiring administrative level permission</td>
</tr>
<tr>
<td><strong>LEAST PRIVILEGED ACCESS</strong></td>
<td>Follow the Least Privilege Access model for assigning account permissions. All users should log on with an account that has the minimum permissions required for their work.</td>
</tr>
<tr>
<td><strong>ADMINISTRATOR ACCOUNTS</strong></td>
<td>The Domain Administrator account should exclusively be used for the domain setup and Domain-related disaster recovery. Domain Administrator account credentials should be an exceptionally strong password and stored in a highly secure location.</td>
</tr>
<tr>
<td><strong>PASSWORD USE</strong></td>
<td>Password reuse should be set to Never Reuse for all users where possible. Passwords from older data beaches are being leveraged in current attacks.</td>
</tr>
<tr>
<td><strong>SERVICE LOCKDOWN</strong></td>
<td>Service accounts should only have the necessary access levels required for their specific tasks. Reasons for the service account existence should be noted.</td>
</tr>
<tr>
<td><strong>MULTI-FACTOR AUTHENTICATION</strong></td>
<td>Multi-factor authentication should be used with all privileged accounts. Multi-factor authentication provides additional verification on the identity of the user.</td>
</tr>
</tbody>
</table>

**IDENTITY LIFECYCLE**

- **PROVISION**: Create
- **PASSWORD REQUESTS**: Enable
- **ACCESS**: Exit
Only use district approved softwares, audit system access, and isolate critical infrastructure.

### System Isolation

Legacy systems and applications that may require EOL software or do not allow for up to date patching should be isolated from other systems.

When possible, these systems should have internet connection disabled or limited in scope.

### Use Approved Software

Know what systems are in use in your district so protections can be put in place.

Technology management tools should be vetted before use.

### Monitor System Logs

Monitor system logs for signs of compromise.

Examples:
- Repeated failed logins
- Logins from strange locations/IPs
- Logins at unusual hours
- Users performing atypical tasks

### Password Reuse

Login credentials should not be used across multiple systems.

Compromised credentials are often used to attempt to access other systems.

### Review Accounts

Review Accounts regularly to ensure they need to remain active.

Focus on newly created accounts and admin accounts when conducting reviews.

---

**Components of Application Security**

- **Endpoint Security**
- **Application Security**
- **Network Security**
- **Content Security**

NOTE: The increased information logged can take up a lot of additional space on workstations and servers. Please set up retentions accordingly.

<table>
<thead>
<tr>
<th>SETTINGS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACCOUNT LOGON</strong></td>
<td>Ensure ‘Audit Credential Validation’ is set to ‘Success and Failure’</td>
</tr>
</tbody>
</table>
| **ACCOUNT MANAGEMENT** | Audit ‘Application Group Management’ is set to ‘Success and Failure’  
Audit ‘Computer Account Management’ is set to ‘Success and Failure’  
Audit ‘Other Account Management Events’ is set to ‘Success and Failure’  
Audit ‘Security Group Management’ is set to ‘Success and Failure’  
Audit ‘User Account Management’ is set to ‘Success and Failure’ |
| **DETAILED TRACKING** | Audit ‘PNP Activity’ is set to ‘Success’  
Audit ‘Process Creation’ is set to ‘Success’ |
| **LOGON/LOGOFF** | Audit ‘Account Lockout’ is set to ‘Success and Failure’  
Audit ‘Group Membership’ is set to ‘Success’  
Audit ‘Logoff’ is set to ‘Success’  
Audit ‘Logon’ is set to ‘Success and Failure’  
Audit ‘Other Logon/Logoff Events’ is set to ‘Success and Failure’  
Audit ‘Special Logon’ is set to ‘Success’ |
| **OBJECT ACCESS** | Audit ‘Removable Storage’ is set to ‘Success and Failure’ |
| **POLICY CHANGE** | Audit ‘Audit Policy Change’ is set to ‘Success and Failure’  
Audit ‘Authentication Policy Change’ is set to ‘Success’  
Audit ‘Authorization Policy Change’ is set to ‘Success’ |
| **PRIVILEGE USE** | Audit ‘Sensitive Privilege Use’ is set to ‘Success and Failure’ |
| **SYSTEM** | Audit ‘IPsec Driver’ is set to ‘Success and Failure’  
Audit ‘Security State Change’ is set to ‘Success’  
Audit ‘Security System Extension’ is set to ‘Success and Failure’  
Audit ‘System Integrity’ is set to ‘Success and Failure’ |