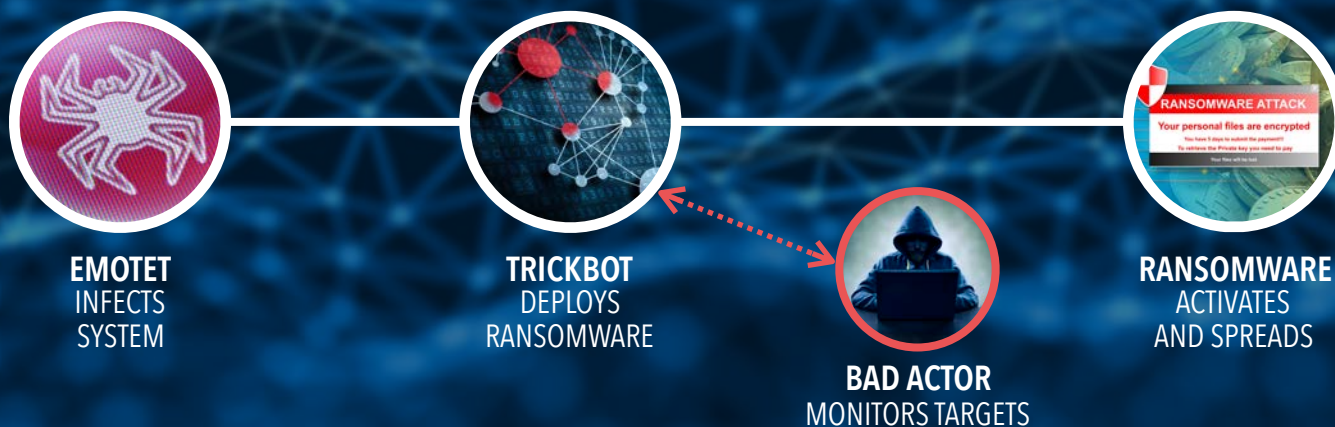


As cybersecurity vulnerabilities become more prevalent across the nation, this resource is designed to provide an overview of the current threat landscape and offers district leaders a reminder of important protections that should be implemented to help mitigate risks associated with recent cyber threats.

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.



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

SYSTEM PATCHING TARGET TIMEFRAMES

TYPE OF UPDATE	COMPLETE WITHIN
SECURITY AND CRITICAL	1 to 3 WEEKS
HIGH PRIORITY	1 to 2 MONTHS
LOW PRIORITY	3 to 4 MONTHS

DATA SECURITY **THREAT LANDSCAPE**

VULNERABILITY MANAGEMENT

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

	DESCRIPTION	NOTES	
PATCH MANAGEMENT	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.	
HARDWARE INVENTORY	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.	
SOFTWARE INVENTORY	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.	
NETWORK PORTS	Limit and control network ports.	Ensure ports no longer in use are closed and open ports are limited in scope where possible.	
WIRELESS ACCESS CONTROL	Secure and segment wireless networks, including elimination of open networks.	Guest networks should not have access to networked resources.	
DEACTIVATE ACCOUNTS	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.	

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

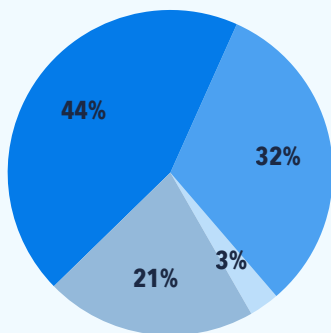
DATA SECURITY **THREAT LANDSCAPE**

SYSTEM BACKUPS

Ensure backups for critical systems are in place and audit backups for completion and functionality.

	DESCRIPTION	NOTES	
BACKUP CREDENTIALS	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.	
DOMAIN BACKUPS	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.	
FILE SYSTEMS	Leverage different file systems for backup storage when feasible.	Machines running Linux often function as backup repositories.	
OFFLINE STORAGE	One of the best defenses against propagation of ransomware encryption to the backup storage is to have offline storage.	Examples: <ul style="list-style-type: none"> • Replicated VMs • Storage snapshots • Cloud Connect backups • Rotating (Media) • Tapes 	
REGULAR TESTING	Test backups and systems on a regular basis.	Monitoring backups for completion and regularly conducting test restores helps ensure backup integrity.	
BACKUP LOGS	Document and maintain a log of all system backups, testing schedules, and retention periods.	Accurate log documentation can greatly increase recovery time.	
CURRENT IMAGE	Keep and maintain an up-to-date image for machines to assist in recovery.	Update image with each new Microsoft Build (typically semi-annually).	

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.

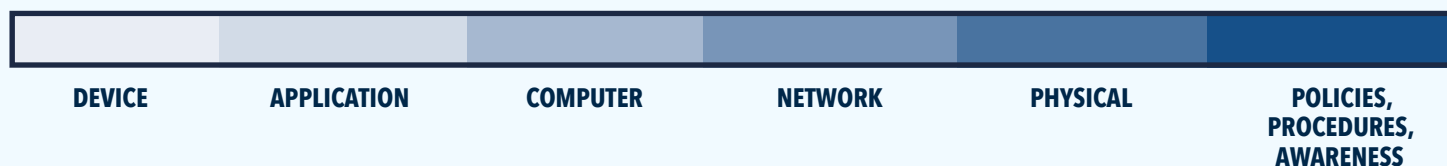
DATA SECURITY **THREAT LANDSCAPE**

SYSTEM HARDENING

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

	DESCRIPTION	NOTES	
ANTIVIRUS	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.	
LOCAL ADMINISTRATOR PASSWORD SOLUTION	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.	
PASSWORD POLICY	Update password policies to reflect best practices.	Consider increasing length requirements on passwords and decreasing complexity requirements	
DOMAIN CONTROLLERS	Do not install additional software on domain controllers. Do not install additional non-critical roles.	Only mechanisms required for functionality and security should exist on domain controllers.	
SECURE ADMIN WORKSTATION	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.	
ENABLE DOMAIN AUDIT LOGS	Enable Audit Policy Settings with Group Policy.	See the attached Audit Policy Settings page for recommended settings.	
SERVER MESSAGE BLOCKS	Disable the outdated file and print sharing protocol Server Message Blocks Version 1 (SMBv1).	Use SMBv2 or SMBv3.	
OPERATING SYSTEM UPDATES	Apply critical and security patches within 2-4 weeks.	Ensure Microsoft Windows patch MS17-010 is installed.	
OPERATING SYSTEM FIREWALL	Limit and control system firewall ports.	Ensure ports no longer in use are closed and open ports are limited in scope where possible.	

LAYERED APPROACH TO SYSTEM HARDENING



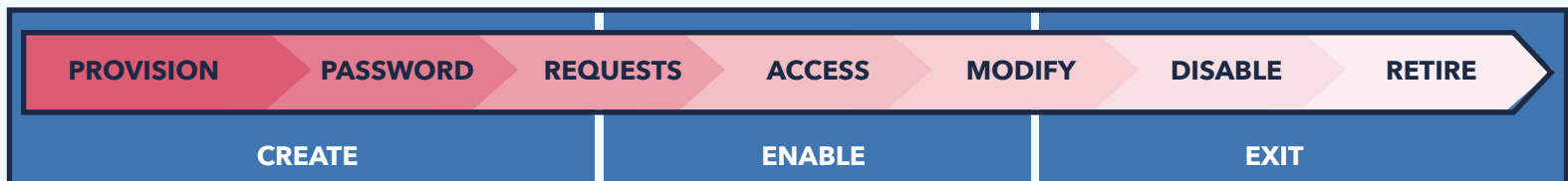
DATA SECURITY **THREAT LANDSCAPE**

IDENTITY MANAGEMENT

Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.

	DESCRIPTION	NOTES	
APPROPRIATE PERMISSIONS	Ensure accounts have appropriate permission levels.	Domain Admin accounts should never be used to access workstations.	
DOMAIN ADMINISTRATORS	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	
LEAST PRIVILEGED ACCESS	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.	
ADMINISTRATOR ACCOUNTS	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.	
PASSWORD USE	Password reuse should be set to Never Reuse for all users where possible.	Passwords from older data beaches are being leveraged in current attacks.	
SERVICE LOCKDOWN	Service accounts should only have the necessary access levels required for their specific tasks.	Reasons for the service account existence should be noted.	
MULTI-FACTOR AUTHENTICATION	Multi-factor authentication should be used with all privileged accounts.	Multi-factor authentication provides additional verification on the identity of the user.	

IDENTITY LIFECYCLE



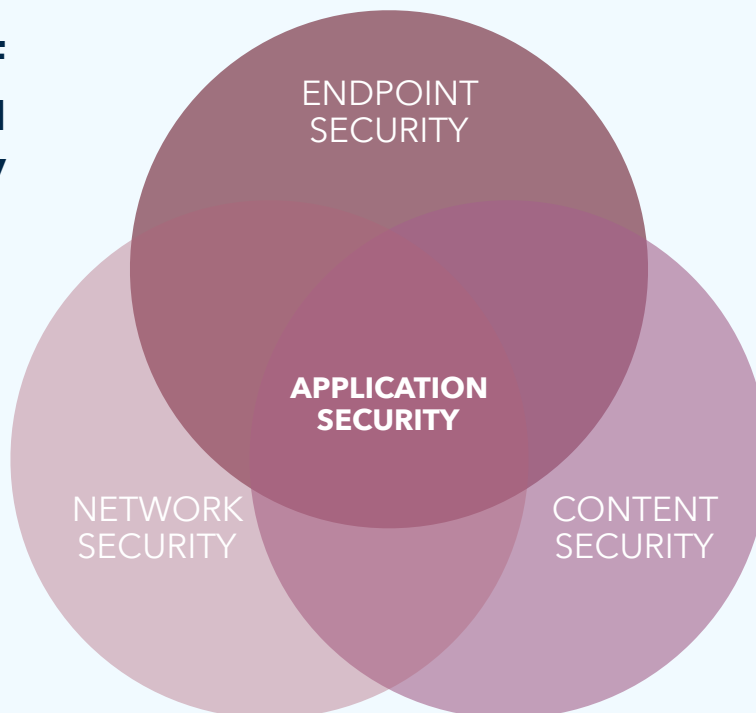
DATA SECURITY **THREAT LANDSCAPE**

APPLICATION SECURITY

Only use district approved softwares, audit system access, and isolate critical infrastructure.

	DESCRIPTION	NOTES	
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: <ul style="list-style-type: none"> • 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



DATA SECURITY **THREAT LANDSCAPE**

AUDIT POLICY SETTINGS

Enable Audit Policy Settings with Group Policy. Audit Policy settings are configured in group policy and applied to all computers and servers. Computer Configuration -> Policies - Windows Settings -> Security Settings -> Advanced Audit Policy Configuration.

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

	SETTINGS
ACCOUNT LOGON	<ul style="list-style-type: none"> ■ Ensure 'Audit Credential Validation' is set to 'Success and Failure'
ACCOUNT MANAGEMENT	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Audit 'PNP Activity' is set to 'Success' ■ Audit 'Process Creation' is set to 'Success'
LOGON/LOGOFF	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Audit 'Removable Storage' is set to 'Success and Failure'
POLICY CHANGE	<ul style="list-style-type: none"> ■ 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	<ul style="list-style-type: none"> ■ Audit 'Sensitive Privilege Use' is set to 'Success and Failure'
SYSTEM	<ul style="list-style-type: none"> ■ 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'

