MOREnet
Be better connected.

ENSURE READINESS FOR THE MSIP 6 STANDARD ON CYBERSECURITY AND PRIVACY

MOREnet Cybersecurity

security@more.net

More.net/blog

MOREnet is providing this information and guidance, in consultation with the Department of Elementary and Secondary Education (DESE), to assist districts and charters with successful alignment to Standard L10 E in the Missouri School Improvement Program (MSIP) 6 Standards.

MSIP 6 STANDARD

School Safety L10 - The school system actively addresses school safety and security in all facilities

E. The school system implements a cyber/privacy security plan, utilizing nationally accepted standards

To successfully meet this standard, the school district will **document its plans** to implement these Top 10 items, at a minimum.

The following industry accepted information security frameworks were referenced in the creation of this document:

NIST-National Institute of Standards and Technology

- SP 800-53, 171, CSF – Cybersecurity Framework

CIS Controls – Center for Internet Security

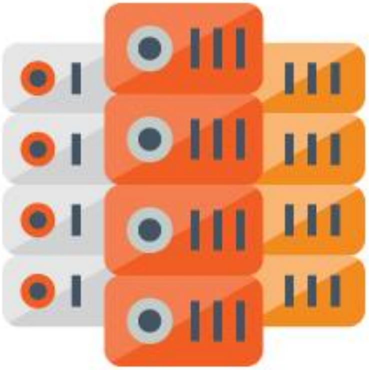
1. Inventory & control of hardware and software
2. Implement complex passwords
3. Document a plan to implement MFA
4. Develop/document a process for backups & restores
5. Implement an ongoing cybersecurity awareness program
6. Deploy endpoint protection
7. Create a plan for patching
8. Remove local administrator rights for end users
9. Develop a disaster recovery/incident response plan
10. Document a plan for protecting data privacy

INVENTORY

Hardware and Software

- Network equipment
  - Servers, switches, APs, IoT, virtual
- End user devices
  - PCs, laptops, tablets, peripherals, phones
- Cloud software, Apps
- Installed software

Authorized AND Unauthorized



CIS Controls 1 & 2-Inventory & Control
NIST SP 800-53

IMPLEMENT COMPLEX PASSWORDS

- 15-character length
- Upper/lower case
- Numbers
- Special Characters (! % ;)

CIS Control 5- Account management
CIS Control 6- Access management
NIST SP 800-63C

MULTI FACTOR AUTHENTICATION

- Employee email
- Remote access
- Privileged accounts
- Access to sensitive data

CIS Control 6-Access Control Management
NIST SP 800-63c

Be better connected.

BACKUP AND RESTORE PROCESSES*

- Documentation
  - Schedule, what, where, when, who
- Offsite
- Offline
- Test restore
  - Do not assume that all backup processes are successful

***MOREnet has a discounted solution to support your goals contact help@more.net**

CIS Control 11-Data Recovery

NIST SP 800-209

Be better connected.

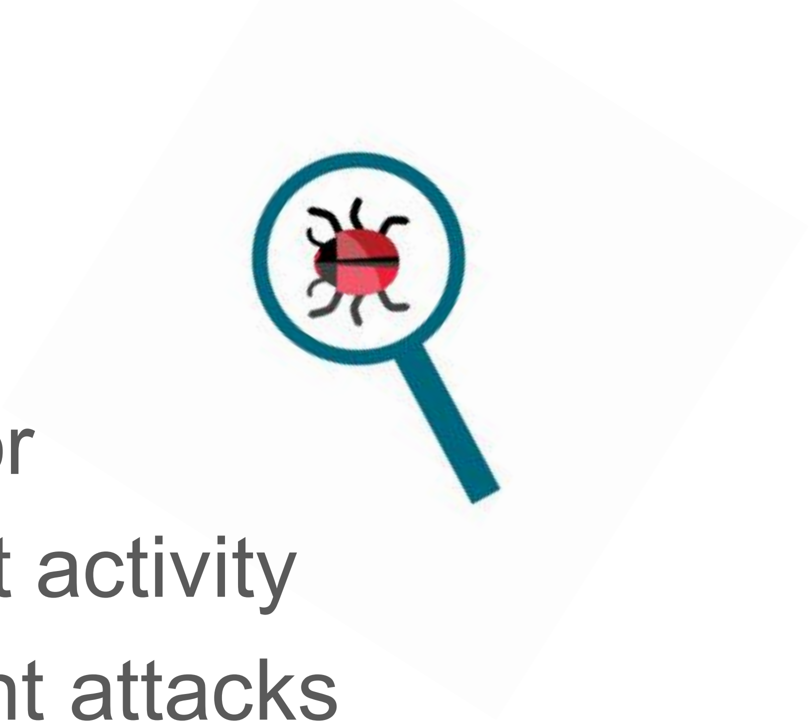
CYBERSECURITY AWARENESS*

- Develop and document a plan
- Ongoing training
- Phishing simulations

*MOREnet has a discounted solution to support your goals-Infosec IQ

CIS Control 14-Security Awareness and Skills Training
NIST SP 800-50

ENDPOINT DETECTION, PROTECTION AND RESPONSE



- Monitor
- Collect activity
- Prevent attacks
- Respond

- Next generation anti-virus
- Enable Host firewall

CIS Control 10-Malware Defenses
NIST SP 800-83

Be better connected.

PATCHING

- Documentation
  - Who, when, where, what
  - Audit process
- Hardware
  - Network equipment
  - End user devices
  - Peripherals, mobile devices
- Software
  - Operating system
  - Firmware

CIS Control 7-Continuous Vulnerability Management
NIST SP 800-40

Be better connected.

ACCESS CONTROLS

- Turn off local domain permissions for end users
- Establish a policy of least privilege
  - Access on a need-to-know basis
- Separate logins for domain administration

CIS Control 5 Account Management, 6-Access Control Management, NIST 800-53

INCIDENT RESPONSE PLAN

Develop a written incident response plan.

- Save time and money when an incident occurs
- Test the plan
- Revise and improve the plan on a regular basis

Incident Response Guide Workbook

MOREnet

CIS Control 17 - Incident Response Management, NIST SP 800-61

DATA PRIVACY*

Document a plan for protecting data privacy

- Identify PII (personally identifiable data)
- Encryption
- Safe transfers of data
- Disposal of data

***MOREnet has a solution to support your goals-Missouri Student Privacy Alliance (MOSPA)**

CIS Control 3 – Data Protection
NIST Privacy Framework

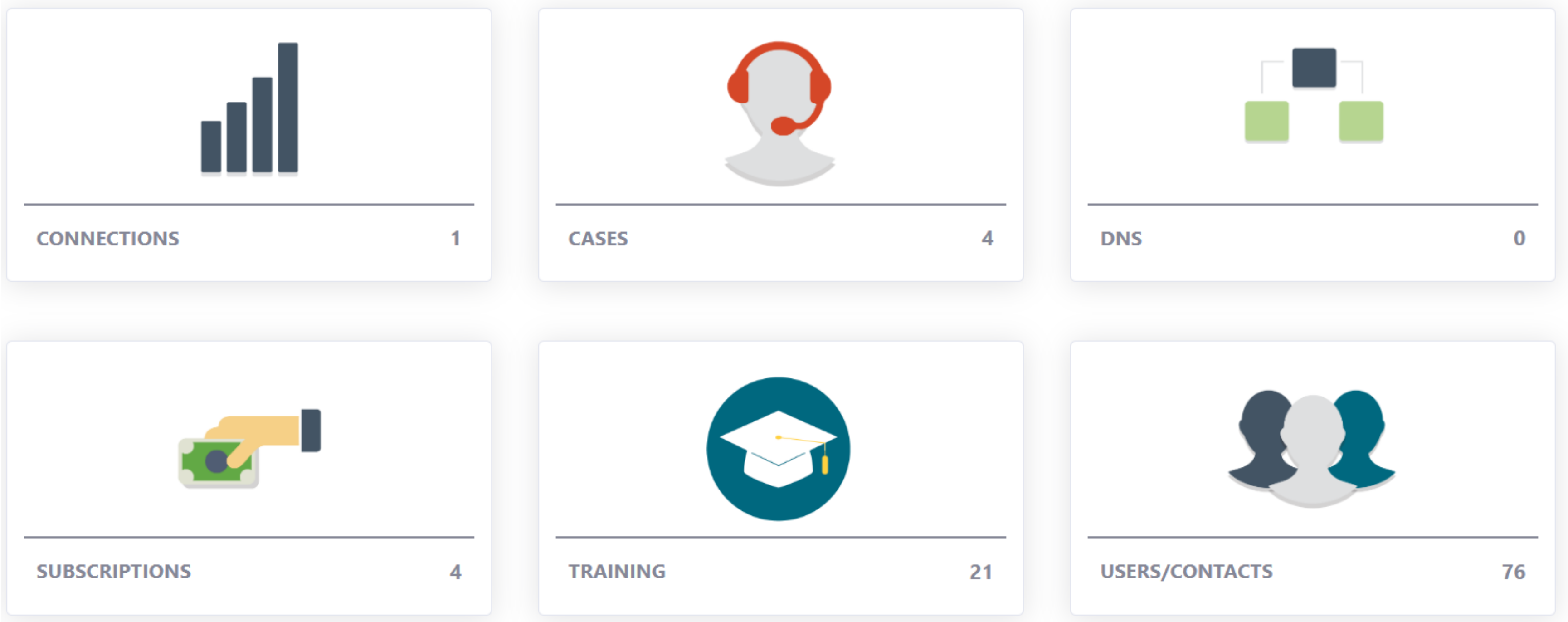
CYBERSECURITY ASSESSMENTS

MOREnet CYBERSECURITY ASSESSMENT

We can provide a comprehensive assessment to help you determine and improve your overall cybersecurity posture.

Network Consulting can pair with cybersecurity to perform a similar assessment focusing on network infrastructure.

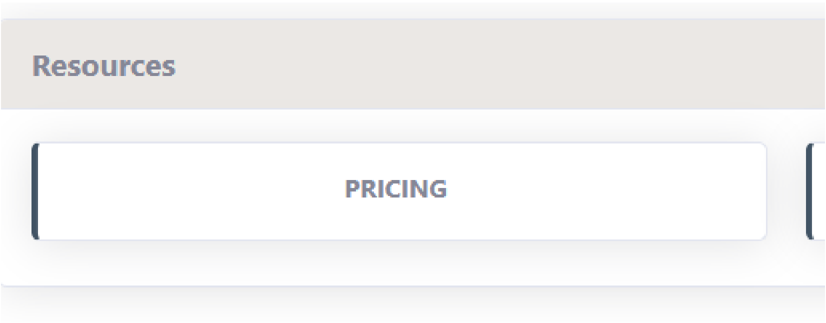
MYMORENET

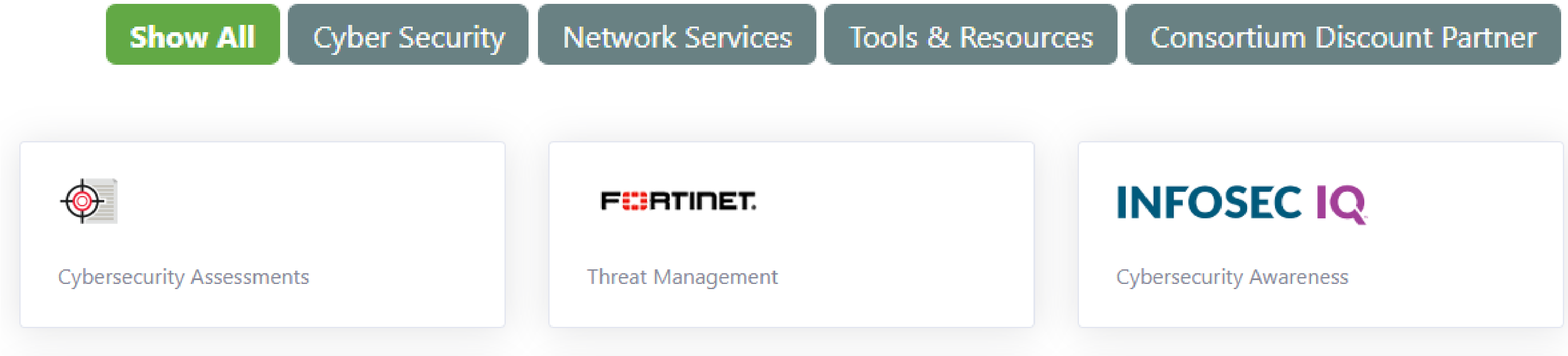


CONNECTIONS	1
CASES	4
DNS	0
SUBSCRIPTIONS	4
TRAINING	21
USERS/CONTACTS	76

Be better connected.

MYMORENET





Be better connected.

QUESTIONS?

security@more.net

More.net/blog

Top 10 ways to start your Cyber/Privacy security plan

To successfully meet the MSIP 6 standard, the school district will document its plans to implement these Top 10 items, *at a minimum*.

1. Inventory and control of hardware and software assets connected to the infrastructure physically, virtually, remotely, and within cloud environments.

2. Implement complex password requirements.
   - 15-character length
   - Upper/lower case
   - Numbers
   - Special characters (!, *, %)

3. Document your plan toward implementing multi-factor authentication (MFA), requiring MFA for:
   - Employee email
   - Remote access
   - Privileged account or access

4. Develop and document a process for offsite and offline backups and testing restore processes of critical data.**

5. Implement an ongoing cybersecurity awareness program that includes simulated phishing campaigns.**

6. Deploy endpoint detection and protection (EDP) on all managed devices.
   EDP will monitor and collect activity data, analyze, and automatically respond to identified threats or suspicious activity. Examples of endpoint detection and protection include such things as anti-virus software, malware detection software, enabled host firewall, etc.

7. Create an audited, written plan for patching hardware and software.

8. Remove local administrator rights for end users. Establish a policy of least privilege.

9. Develop a written Disaster Recovery/Incident Response Plan. Test and update on a regular basis.

10. Document a plan for protecting data privacy. E.g., Missouri Student Privacy Alliance (MOSPA), Student Data Privacy Consortium (SDPC)

** MOREnet has discounted solution options to support your goals in this specific area, contact help@more.net

MOREnet
Be better connected.

better connected.