CYBERSECURITY UPDATES

Dwight Levens
Executive Director of Technology

OaklandSchools

Agenda Overview

- Cybersecurity Insurance
- Data Security Threats | Mitigation Strategies
- Oakland Schools Cybersecurity Initiatives
- Current Legislative Actions Supporting Cybersecurity
- What can you do as finance leaders
- Resources


CYBER
INSURANCE

Cybersecurity Insurance Market Conditions

- Increased Deductibles - Substantial increase in the marketplace
- Renewals – Application process more challenging
- Lower Limits – Creating sublimit on amount of coverage
- Limited Market – Less Appetite in the marketplace, will drive increased costs
- Vulnerability Testing – Testing to conduct risk analysis
- Coinsurance – District paying for portion of claim cost
- Extortion / Ransom – District paying for portion of claim cost

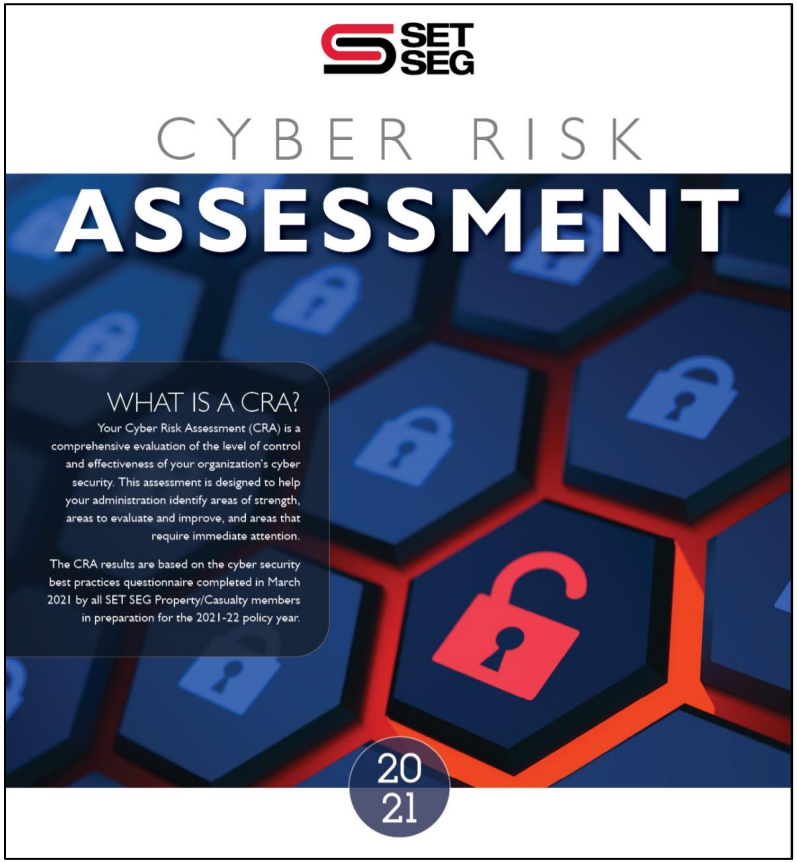
Source: SET SAG, 2021 Superintendents Presentation

Future Requirements from Insurers

- Phishing Training
- Multi Factor Authentication (MFA) – remote access / critical information
- Backups offline / inaccessible to outsiders / encrypted / regularly scheduled
- Limiting administrative access
- System security patches updated
- Close open ports

Source: SET SAG, 2021 Superintendents Presentation

Cyber Risk Assessments Now Required From Insurer



CYBER RISK SUMMARY

	QUESTION	RISK	RESULT
1.	How frequently do you conduct security awareness training and phishing tests?	*Never*	
2	Do you back up critical servers and data regularly offline? If so, how frequently?	*Daily*	
3.	How often do you test the offline backups?	*Annually*	
4.	Do you have an established and regularly tested Business Recovery Plan and Incident Response Plan?	*Yes*	
5.	Do you enforce Multi-factor Authentication (MFA) for all staff?	*Yes*	
6.	How often do you apply security patches to your systems and install antivirus updates?	*Daily*	
7.	Have you ensured that school employees do NOT have administrative rights to school devices and applications?	*Yes*	
8.	Do you use an Endpoint Protection Product (EPP) across your enterprise?	*Yes*	
9.	Do you have separate networks for district owned and managed devices versus Bring Your Own Devices (BYOD)?	*Yes*	

CRA FOLLOW UP

Please review your results and determine the areas that require action.

Your SET SEG Account Executive will be contacting you to discuss your CRA results, support resources, and security planning, as well as the impact these risks may have on your cyber insurance coverage if left unaddressed.

IMPORTANT NOTICE: The cyber security best practices outlined in this document will likely be required for SET SEG Property/Casualty Pool members in 2022. Members will be required to complete a follow-up questionnaire later this year. Failure to address moderate or high risk areas could jeopardize your ability to maintain cyber coverage through the SET SEG Property/Casualty Pool.

Source: SET SAG, 2021 Superintendents Presentation

SET SAG Ransomware Protection Ratings

Minimum

- End-Point Protection (EPP)
- Email tagging
- Enable MFA for Office365
- Disable Macros
- Patching
- Remote Access – secure RDP behind MFA VPN
- Incident response process
- Regular back-ups stored offline
- Phishing training / education
- Firewalls

Stronger

- Establish secure baseline configuration
- Filter web browsing traffic
- Use protective DNS
- Regularly test back-ups
- Disconnect back-ups from network
- Separately stored, unique back-up credentials

Best

- End-point detection and response (EDR) tools
- Intelligent email evaluation
- Centralized log monitoring
- Encrypted back-ups
- Network segregation
- Web isolation
- Application permissions

Source: SET SAG, 2021 Superintendents Presentation


CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
HUMAN ERROR
DATA SECURITY THREATS
SPYWARE
SOFTWARE ERROR
STOLEN INFORMATION
CYBER ATTACKS
PASSWORD CRACKING
FRAUD
HACKING
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

Education Data Breach Stats 2021

Frequency

- 1,332 incidents
- 344 with confirmed data disclosure

Data Compromised

- Personal (61%)
- Credentials (51%)
- Other (12%)
- Medical (7%)

Top Patterns

- Social Engineering
- Miscellaneous Errors
- System Intrusion represent 86% of breaches

Threat Actors

- External (80%)
- Internal (20%)
- Multiple (1%)

Actor Motives

- Financial (96%),
- Espionage (3%),
- Fun (1%),
- Convenience (1%),
- Grudge (1%)

Source: Verizon, 2021

Ransomware Stats

148%
Increase in ransomware attacks, fueled by the pandemic

$154,108
Average ransom demand in Q4 2020

1 in 3,000
Email messages that contain malware (email phishing is also included in the top three ransomware attack vectors)

21 days
Average days of downtime in Q4 2020 (+11% from Q3 2020)

4,000
Average number of ransomware attacks that have occurred daily since Jan. 1, 2016

4.7 million
How many misconfigured RDP ports are open to the internet

Source: SET SAG 2021 Superintendents Presentation and Marsh LLC

Ways To Mitigate Your Cybersecurity Risks

- Obtain the appropriate cybersecurity insurance policy for your organization
- Regularly audit and discuss your cybersecurity preparedness including Incident response and business continuity planning
- Utilize strong passwords organization wide
- Implement two-factor authentication (2FA)
- Ensure that you have a comprehensive system backup process that includes offline copies
- Regularly install security patches and software patches for critical security updates
- Evaluate what's on your network
- Ensure that internet-facing systems or servers are secure, not running out of date operating systems and are up to date on security patching

User Training

- District wide cybersecurity awareness professional development / training
  - Invest in a cybersecurity awareness training platform that includes internal phishing attempts
  - Work to include data privacy and cybersecurity into your organizational goals and culture
  - Individual departments dedicate time to discussing their responsibilities in protecting data and systems
- Conduct internal phishing attempts and assessments

Essential Cybersecurity Practices for K12

Know how to protect user experience

- Disable unnecessary services & ports
- Utilize a (VPN) Virtual Private Network
- Two Factor Authentication
- Disable legacy protocols
- Enable workstation firewalls
- Monitor devices for misconfigurations

Know how to protect systems & data with backups

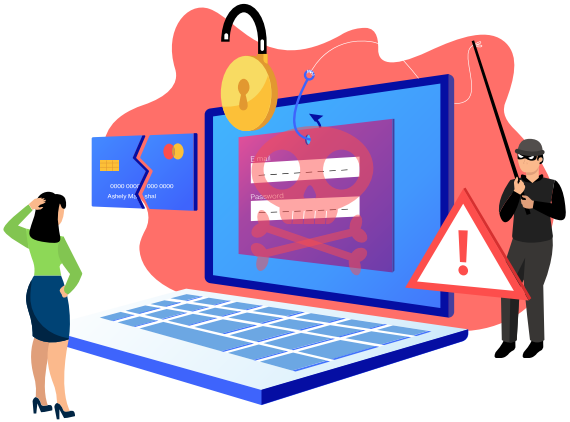
- Use a comprehensive backup strategy (incremental - full)
- Ensure all critical files, databases, and documents are backed up on a regular basis
- Multi location (on and off site)
- Include configuration files
- Use encryption
- Test & Verify backups (and test again)

Know how to protect user devices

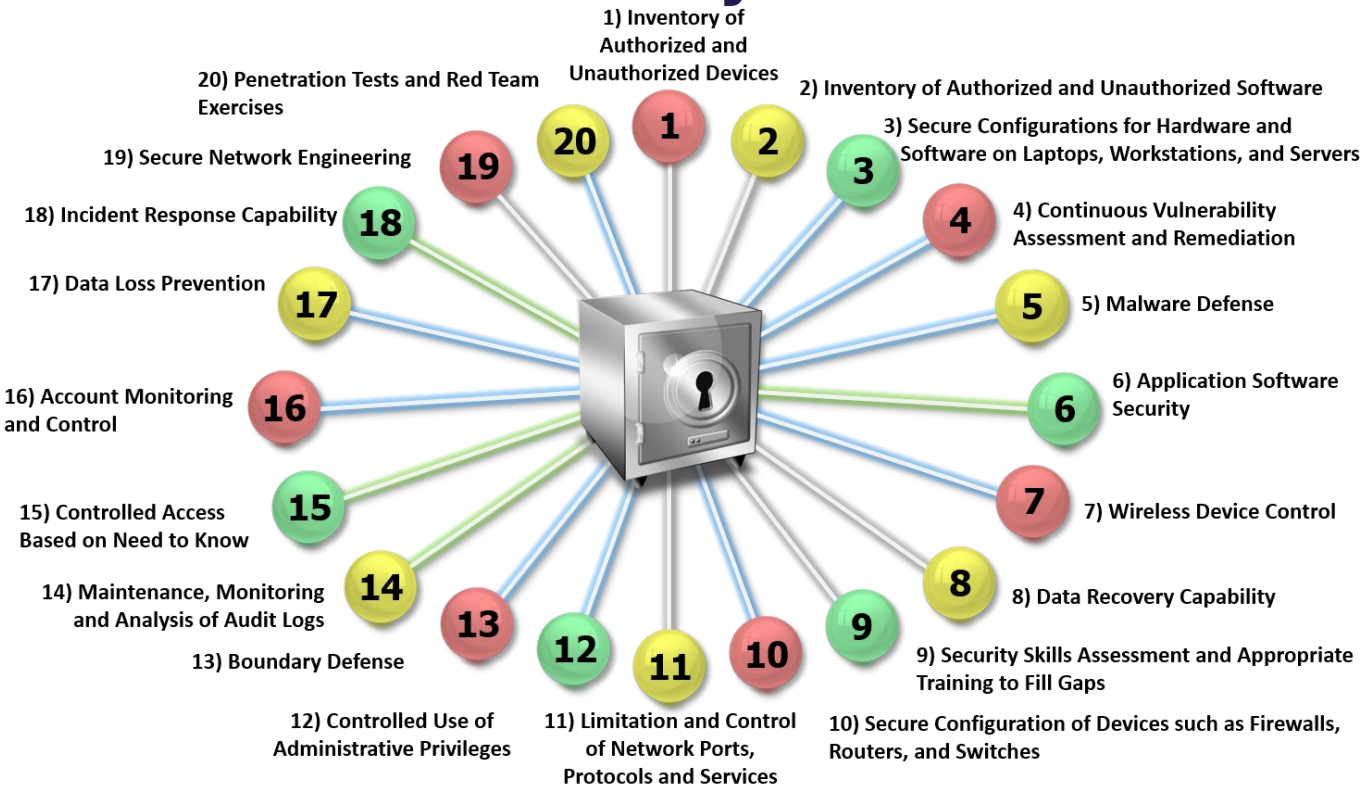
- Install Anti-Malware software
- Scan removable media (USBs)
- Include only necessary protocols and services of the operating system

Know to deploy secure devices

- Use an image deployment tool and track deviations



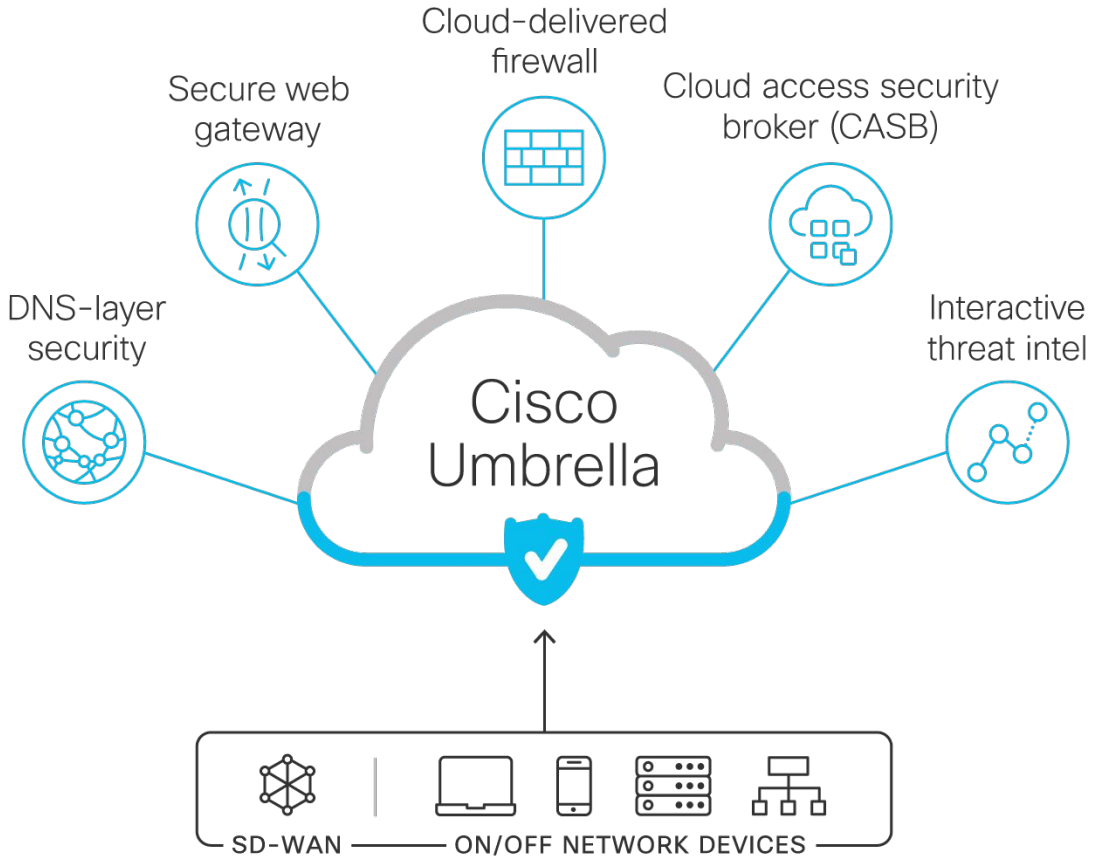
SANS Top 20 Essential Security Controls For Effective Cyber Defense



Oakland Schools Efforts To Support District Cybersecurity Improvements

CISCO Umbrella

- No cost to districts
- Cloud delivered security web content filtering tool
- Offered to all ONE Network districts
- Covered under the ONE Network for 3 years
- Not too late to take advantage

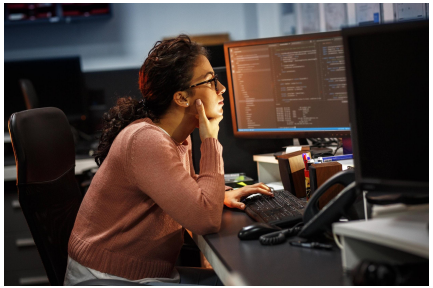


Security Information and Event Management (SIEM)

This is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system. The Securely Managed service sends immediate notification of a security threat and provides direct access to highly skilled engineers who are monitoring the network. SIEM provides districts a savings of approximately **$8,000** a month in operating charges. Available at no cost to districts.

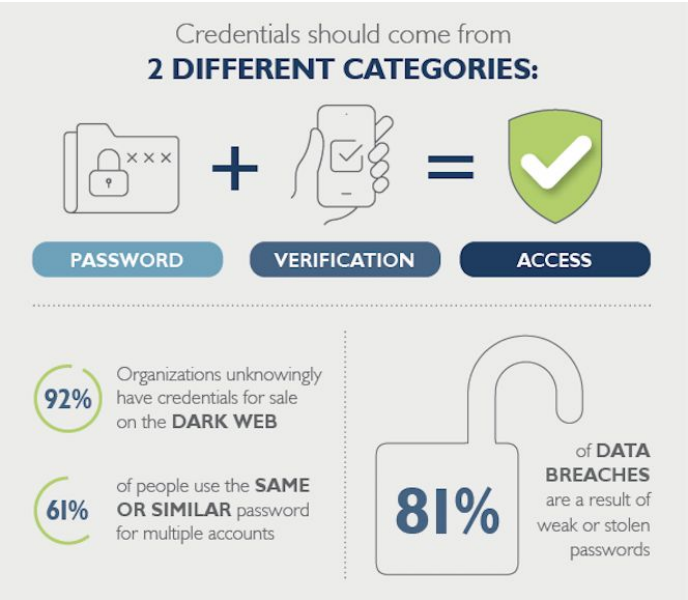
Internal and External Penetration testing

- No cost to districts
- Available to all 28 public Oakland County school districts
- Oakland Schools provides a laptop to districts to place on their internal networks to search for vulnerabilities
- Each district receive their testing outcomes in a custom report containing findings and recommendations
- The service includes a Phishing exercise to assess district users' vulnerability to be phished.



Two Factor Authentication – 2FA

- Selected platform: Cisco Duo
- Used by Oakland Schools directly
- All field service districts will utilize this security measure for the following: Google Workspace, MiStar and Office 365)



Source: SET SAG

Current Legislative Actions Supporting Cybersecurity

- The K-12 Cybersecurity Act
- Senate Bill No. 672

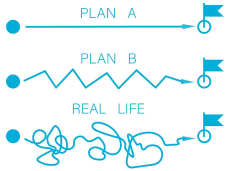
- On its own, the legislation is fairly simple: It authorizes the director of the Cybersecurity and Infrastructure Security Agency (CISA) to conduct a study within 120 days of the specific risks impacting K–12 institutions. Following that, the director will develop, within 60 days, recommendations for cybersecurity guidelines for K–12 schools, based on the results of the study. And following that, within 120 days, will create an online training toolkit for "officials" at K–12 schools.

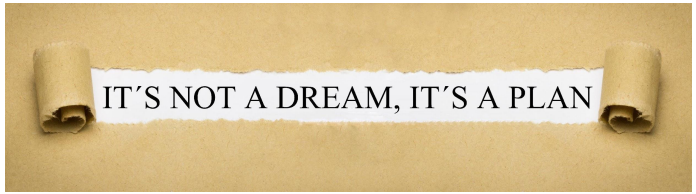
Source: The Journal, October 2021

- In 27 states there were over 100 cybersecurity bills introduced in 2020 as identified in a report from COSN.

What can you do?

- Engage with the technology leader in your district to learn where your district stands regarding the current best practice recommendations
- Ask if your district is taking advantage of the ONE Network cybersecurity initiatives
- Work with your technology leader to find a funding source for the recommendations
- Serve as a champion for the necessary changes some of which will impact users' familiar experiences
- Develop an incident response plan
- Develop a Business continuity plan





Resource Toolbox

Cybersecurity Best Practice Resources:

- MISECURE.ORG
  METL 20 Essential Cyber Security Practices
- The 18 CIS Critical Security Controls
- DTMB - Michigan Cyber Partners and the CIS Controls
- SET SAG Cyber Risk and Liability Presentation
- Michigan.gov/cyberpartners
- CIS Controls Self Assesment Tool
- Michigan Cyber Command Center

Incident Response Resources:

- MI Sample Cybersecurity Incident Response Plan Template
- MI Sample Incident Response Planning Companion Presentation

Cybersecurity Awareness Month Resources:

- Cybersecurity "Start with the basics" resource
- CISA 2021 Cybersecurity Awareness Month Partner Presentation You Can Utilize Complete With Speaker Notes
- CISA 2021 Cybersecurity Month One Pager
- Cybersecurity Awareness Month 2021 Partner Toolkit