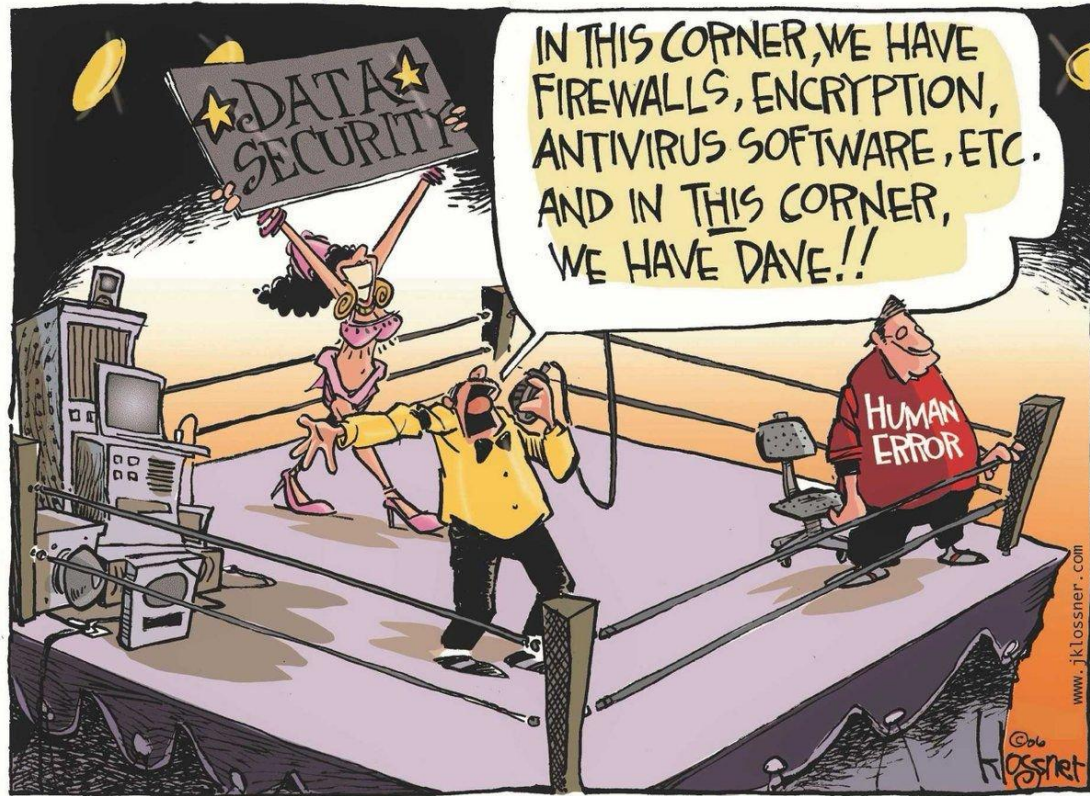




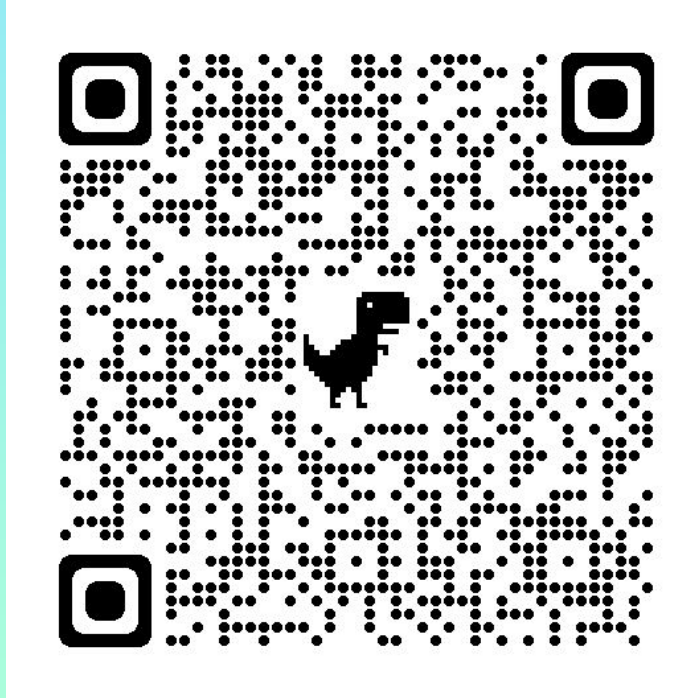
Creating A Cyber Secure Culture

Julian Smith – Hoover City Schools



**Reduce the
amount of
Daves in your
environment!**

Cyber Security is Everyone's Job!



Leadership

01

Finance

04

Public Relations

02

Human Resources

05

Facilities

03

Technology

06

01

Leadership



01 - Leadership

- Understand cyber security basics and best practices enough to enable sound decision making
 - Establish a routine reporting process for cyber risks within the organisation
 - Regularly commission objective risks assessments of the organisation
- Include cyber risks in the district's risk management process
 - Avoid treating cyber risks as a separate matter to only be handled by the technology department
 - Understand the organizational impacts of cyber incidents
 - Conduct exercises and decision making drills to familiarize yourself and district with how to respond to a disaster & security incident
- Develop and maintain organization information security policies and standards
 - Ensure organizational security policies are appropriately implemented, institutionalized, and communicated
- Adequately fund cybersecurity resource requests
 - Digital assets cannot be protected without human and technical resources
- Leadership is the most important factor influencing awareness and mindset
 - Deep technical knowledge is not required from leaders. Instead, leaders should model good personal security habits based on sound guidelines.

01 - Leadership

Planning

Managing and mitigating overall cyber-related risks

Governance

Establishing effective governance controls

Culture

Establishing a cyber-secure culture within the organization



02 Public Relations

02 - Public Relations

- Communicate the importance of cybersecurity matters to internal stakeholders
 - Collaborate with each department to achieve best practices on utilizing and sharing data securely
- Understand the potential impact of a cyber incident on the organization, including parent & student trust
- Develop a communications plan for the inevitable cyber incident
 - Participate in internal Incident response planning
 - Know what to say and what not to say during an incident

02 - Public Relations

**Brand
Management**

**Organizational
Awareness**

**Public
Communication**

03

Facilities



03 - Facilities

- Securing physical systems from compromise due to all hazards including physical & cyber risks
 - IoT devices
 - Door Systems
 - Alarm
 - Video Systems
- Ensure appropriate physical security controls are implemented at facilities
 - Deterrence – Boundary restrictions
 - Denial – Locked vault doors
 - Detection – Using motion detectors
 - Delay – Cable lock on a laptop
- Maintain environment that is conducive to proper functioning of IT infrastructure
 - HVAC
 - Flooding
 - Fire

03 - Facilities

Physical security controls

IoT device security

04

Finance



04 - Finance

- Understand the many different business effects of cyber threats
 - Loss of credibility
 - Legal liabilities
- Provide sufficient funding to enable success of the school's cybersecurity strategy
 - Hardware and software costs
 - Vendor support
 - Differentiate between must-haves and nice-to-haves
- Develop a complete view of security related spending
 - Can be spread across multiple areas and budget allocations
- Cyber incident response plans should incorporate how to purchase needed equipment or services in the event of an incident
 - Contingency plan for if financial systems are attacked and how to ensure continuity with minimal disruption
 - Consider purchasing cyber risk insurance to offset the financial impact of security incidents
 - Ensure the response plan includes costs associated with services such as credit monitoring for affected individuals

02 - Finance

**Financial
Support**

Liabilities

**Incident Response
Plan**



05 Human Resources

05 - Human Resources

- Ensure cybersecurity knowledge, skills, and abilities are incorporated into employee training and development
- Background checks
- Increase efforts at attracting and retaining employees filling cybersecurity roles
- Protect access to human resources management platform by using best practices
 - Strong passphrases
 - Unique passphrases for each critical account
 - Multi-factor Authentication
 - Use encryption to share sensitive information when possible
- Work with IT to manage employee account lifecycle
 - Immediately notify pending or actual termination of employees
 - Update directories with new status to ensure cascading of permissions changes across platforms and applications

05 - Human Resources

**Employee
Training**

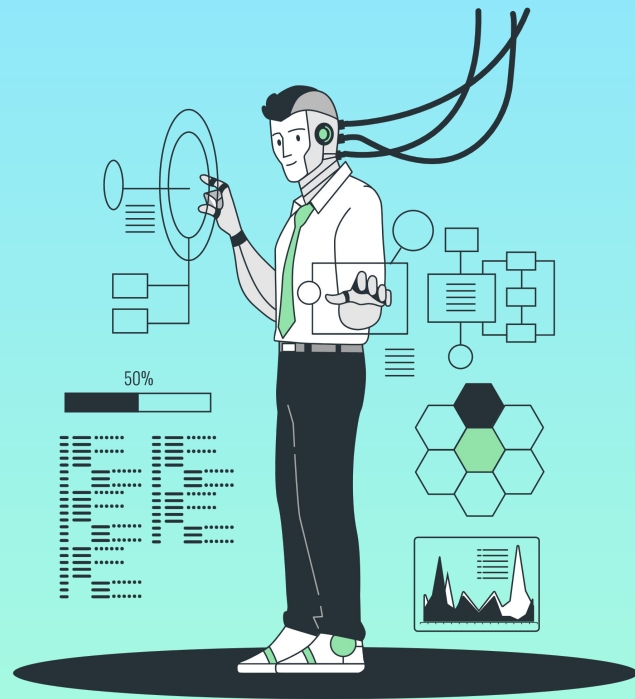
Staffing

**Employee
Data**

**Insider
Threats**

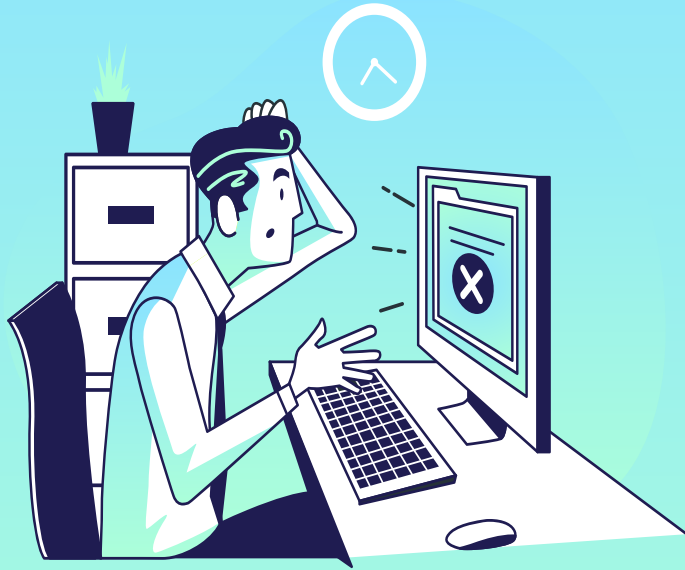
06

Technology



06 - Technology

- Provide technical expertise in support of the organization's cybersecurity program
 - Maintain current knowledge in cybersecurity tools, techniques, and procedures
 - Cross-train other IT roles with security functions
 - Collaborate with other business functions across the organization
- Implement a robust cybersecurity program with appropriate technical and process controls consistent with the organization's risk mitigation strategy
 - Leverage exist cybersecurity frameworks such as NIST, CIS Controls
 - Work with external entities such as consultants and auditors to ensure you are utilizing the appropriate tools
- Integrate security into IT design, architecture, deployment, and routine operations
 - Consider security upfront, not as an afterthought
- Establish and help enforce robust security policies for employees, contractors, vendors, students, with codified acceptable use policies to enforce accountability



While multi-layered security
protections are important,
particularly if implemented in an
automated fashion, the
organization is still relying on
individuals to
do the right things

Do the right thing

- Exercise caution when using information systems; if you are unsure or sense you may be doing something risky, seek guidance from responsible individuals
- Fully understand your role and take personal responsibility for knowing how your organization addresses cybersecurity risks
- Be willing to learn, since technology is continually evolving
- Know how to handle, control, store, transfer and dispose of information in your organization
- Protect your assets by physically safeguarding your computer, mobile devices, and non-electronic information
- Follow your organization's security procedures for facilities and prevent unauthorized access via social engineering tricks
- Use the best authentication capabilities your organization offers for controlling access to computers, mobile devices and the information services and applications you use
- Use encryption for information in transit and at rest

THANKS!

Do you have any questions?

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik** and illustrations by Stories

Please keep this slide for attribution.

