Ten Ways (not really) to Provide Stronger Security for Your Data

DATAG Fall Meeting
October 4, 2019

About Us

Kieran O’Connor

Exec Dir: Planning, Dev., and Technology

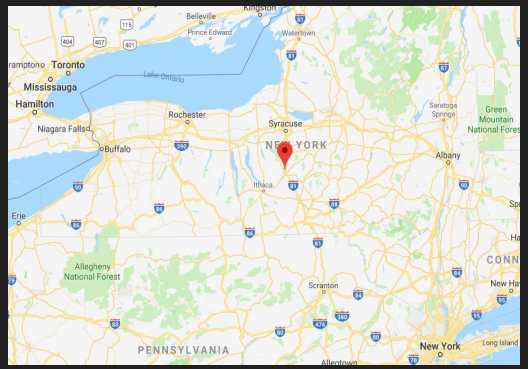
East Syracuse Minoa Schools

3,400 students

PreK-12

@koconnoresm 315-396-7686

koconnor@esmschools.org



Josh Finn

Chief Technology Officer

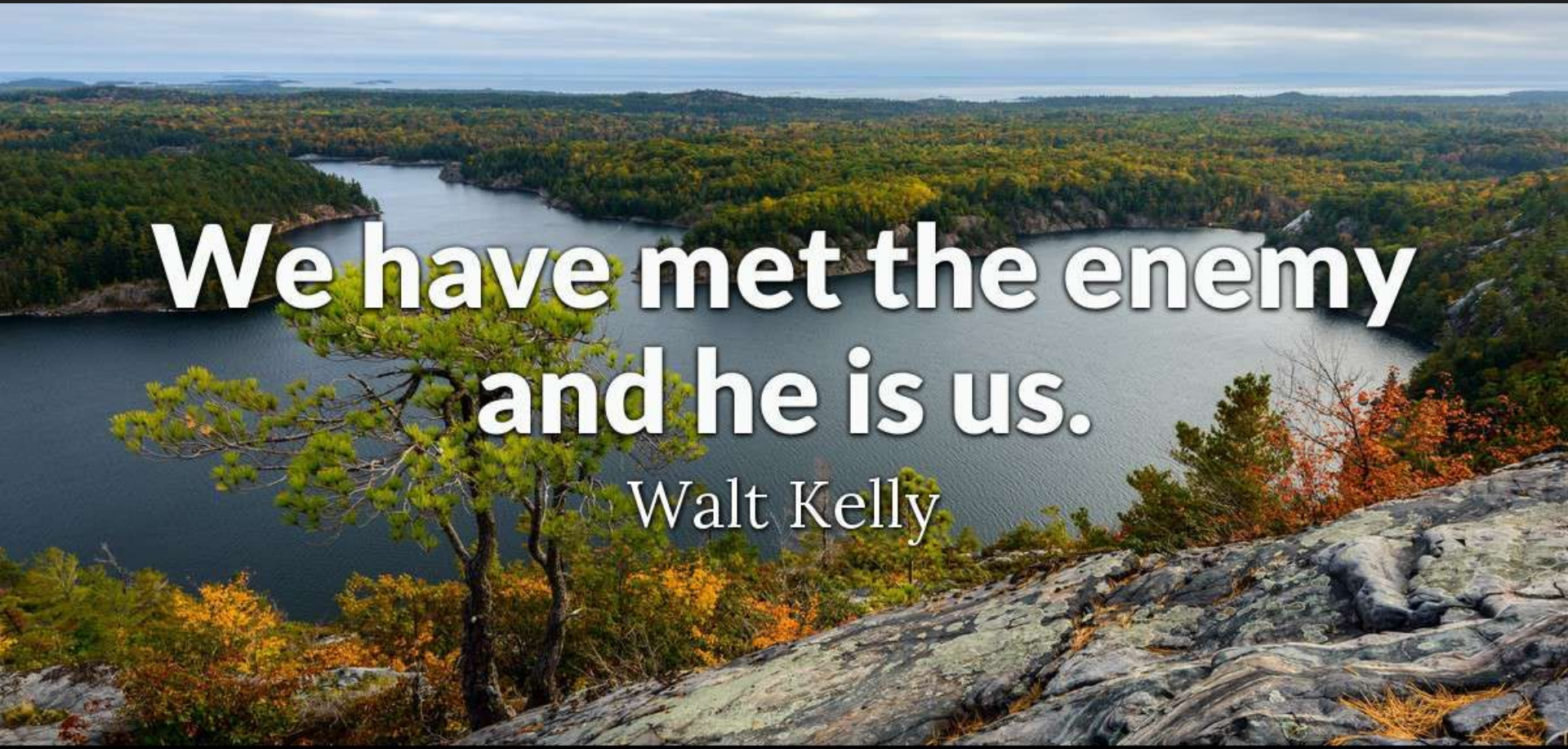
Homer Central School District

1,900 Students

PreK-12

@jfinnis20

Jfinn@homercentral.org



“Manage your risk by managing the way you think about employees.” - KOC

The Employee Lifecycle

- Before Employment - Build an environment of security
- During Employment - Support employees to make good choices
- After Employment - Ensure all loops are closed
- Continual Review - Keep your processes up to date

Before employment - Overview

User Management

- Who gets an account & what access is granted? (Matrix)
- Security controls

Data Classification, and who has access to what data

- Public
- Internal
- Confidental
- Restricted Confidential

Position type	Google	Schooltool	Network Logon	District-wide Public	Building Teacher Public	Building Staff Public	School Dude	Voicemail / Changes	nVision	H:drive	staff intranet
District-wide Administrator	y	y	y	y	y	y	y	y	n	y	y
Building Administrator	y	n	y	y	y	y	y	y	n	y	y
Non-Instructional Supervisor	y	y	y	y	y	y	y	y	n	y	y
Network Admin	y	n	y	y	n	y	y	y	n	y	y
Lan Tech	y	n	w/a	w/a	n	w/a	n	n	n	n	w/a
Nurse	y	n	y	y	n	y	y	y	n	y	y
Head Custodian	n	n	w/a	w/a	n	n	n	n	n	n	w/a
Custodian / Custodial Worker	y	n	y	y	n	n	y	y	n	y	y
Food Service Manager	y	n	y	y	n	n	n	n	n	n	y
Food Service Worker	y	n	y	y	n	n	y	y	n	y	y
Mechanic	n	n	n	n	n	n	n	n	n	n	n
Delivery Person	y	w/a	y	y	n	y	y	y	y	y	y
Transportation admins									n		
Bus Driver	y	y	y	y	y	n	y	y	n	y	y
Secretary or Typist	y	w/a	y	y				w/a	n	w/a	y
Teacher / school psychologist/OT/PT / Speech Pathologist	y	w/a	y	y				n	n	n	y
Teaching Assistant	y	w/a	y	y	n	y	y	n	n	n	y
Teaching Assistant (Long Term)	y	y	y	y	y	y	y	y	n	y	y
Teacher Aide	y	n	y	y	n	y	y	y	n	y	y
Student Teacher	y	n	w/a	w/a	n	w/a	n	n	n	n	w/a
Daily (Per-Diem) Sub	y	n	y	y	n	y	y	y	n	y	y
Long Term Sub	n	n	w/a	w/a	n	n	n	n	n	n	w/a
Regular Sub	y	n	y	y	n	n	y	y	n	y	y
Sub Counselor	y	n	y	y	n	n	n	n	n	n	y
Sub Nurse (regular)	y	n	y	y	n	n	y	y	n	y	y
Sub nurse (long term)	n	n	n	n	n	n	n	n	n	n	n

Note: this is fake data

Before Employment

Security Controls

- Password requirements
  - Length
  - Complexity
  - Expiration
- Aging out of accounts
- No Generic Accounts
- IT only has admin rights
- Accounts for BOCES/other outside staff---BOCES staff use their own accounts
- Vendors/Contractors

Before Employment

Security Controls

- Least privilege
  - Beware privilege accumulation
  - Same person: different logins for different roles
- Audit Logs
  - Computer Login
- Single Sign On--risks/rewards
- 2 Factor Authentication

	Data Classification				
	Public	Internal	Confidential	Restricted Confidential	Notes
Data Type					Also note
Financial Data			server at BOCES		
State Reporting files			server at BOCES		
BOE documents	server		server		
Employee Data			server		
Data exports (list all)					
Email	server, mobile phone		server, mobile phone		
Negotiations				server at BOCES	
Student Data: SMS			server		some data subject to FERPA
Student Data: Clever			server		
Student Data: Library system			server		
Staff Directory		server			
Reference					
IT Governance Manual					
https://www.osc.state.ny.us/localgov/pubs/lgmg/itgovernance.pdf					

Note: this is fake data

During Employment - Overview

- Policies and Procedures
- Ongoing Training
- Attack Vectors
- Security and vigilance as a culture

During Employment

Policies and procedures - Know them and keep updated!

- Confidentiality Agreements
- Staff Acceptable Use Policy (AUP)*
  - Staff use of Social Media
  - Personal use of equipment
- Student Grading Information Systems
  - Categorization of system users

* Mandated policy

During Employment

Policies and procedures - Know them and keep updated!

- Data Networks and Security Access
  - Inventory Assets
  - Physical Access
  - DR Planning
- Information Security Breach and Notification*
  - Definition of Breach
  - Notification requirements

* Mandated policy

During Employment

In my role to support the educational mission of the [redacted] District, I understand that I may have access to School District, BOCES, or other districts' data (such as student grades, health or family information, district emergency plans, financial documents, security procedures, … etc.).

I understand that I will only access data or information for which I have a legitimate business purpose. Accessing data is only in conjunction with my job responsibilities.

I am not to share (electronically or otherwise), reproduce, distribute, or discuss any accessible data with any person or entity not directly involved with the job responsibilities of my position.

I am not to share my access codes (network, building, phone… etc.) unless directed by my administrative supervisor. Additionally, I will not provide information to any staff members, students or the public unless directed to by my administrative supervisor on how the district network is set up, monitored, protected, or vulnerable.

If there are any doubts in this regard, I will obtain clarification and permission from my administrative supervisor.

My signature confirms that I have read and understand the above Confidentiality Statement.

Signature _____ Date _____

Print Name _____

During Employment

Ongoing Training

- Simulate Phish
- KnowBe4 (one option)
- Meet with Business Office folks. Often.
- Digital Security Training is now mandated under 2-d

During Employment

Attack Vectors

- Email
  - Problems
    - Phishing
    - Spearfishing
    - Whaling
    - Spam
  - Solutions
    - Encryption
    - Banners/External Email notices
    - Password protect files in transit
    - Strip attachments
- Phone (Vishing)
- In person

During Employment

Security and vigilance as a culture

- See Something Say Something
- Phish Bowl
- Eliminate flash drives
- Additional training for those who need it

After Employment

Offboarding

- Look to coordinate thru HR
  - Be aware other departments may provide accounts too!
- Process to suspend all accounts immediately
- Refer to account matrix
- Badge & Key collection
- Exit survey

After Employment

Building/Dept. Information	Staff Responsible	Sign-off/Completed
Classroom materials returned	Supervisor	
Computer inventoried	Supervisor	
Copier code removed	Supervisor	
District-owned curriculum materials returned	Supervisor	
*Exit interview requested**	Supervisor	
Exit questionnaire provided	**See below*	
Future contact information provided	Supervisor	
I.D. badge returned	Supervisor	
Maintenance notified for keypad access removal	Supervisor	
Miscellaneous keys returned (elevator, copy room, storage closet, etc.)	Supervisor	
Outstanding expense forms submitted	Supervisor	
Parking hang tag returned	Supervisor	
Payroll notified	Supervisor	
Room/building key returned	Supervisor	
Teacher handbook returned (K-8)	Supervisor	
Tech dept notified • Disable computer access • Remove from staff web • Voice mail changed	Supervisor, then Tech Dept	
Thank you letter for service	BOE/Superintendent	
**Please notify Director of Instruction to schedule interview or to request exit questionnaire*	Supervisor	

Continual Review

Build procedure to maintain desired level of security

- Onboarding/Offboarding
- Ongoing Reviews
- Audit
  - Inside
  - Outside
- District* Security Committee (meet 3-4 times a year)

Resources

IT Governance, NY Comptroller

IT Contingency Planning

Wireless Tech and Security

QR code handout to this presentation

Account Matrix template

Data Classification template

Resources

Check Comptroller reports for ideas, here are samples:

- Dover: locking server rooms, excluding all but IT
- Finn Academy: IT policies
- Ellicotville: User Training and personal internet use
- Honeoye: IT only audit, references personal use and personal items on H drives
- Dansville: Policies, training, personal use
- Cazenovia: Policies, PPSI
- Hamburg: DR, Policy, Training