Cybersecurity Trends and Threats

2024 ANNUAL CONFERENCE

#iasboAC24

INVEST IN YOURSELF IGNITE OTHERS

Presenters:

MODERATOR INFO:

John Lavelle, Asst. Supt. for Business Services; CHSD#230
708.745.5241; jlavelle@d230.org

PANELISTS INFO:

John Connolly, Chief Technology & Operations Officer; CHSD#230
708.745.5253; jconnolly@d230.org

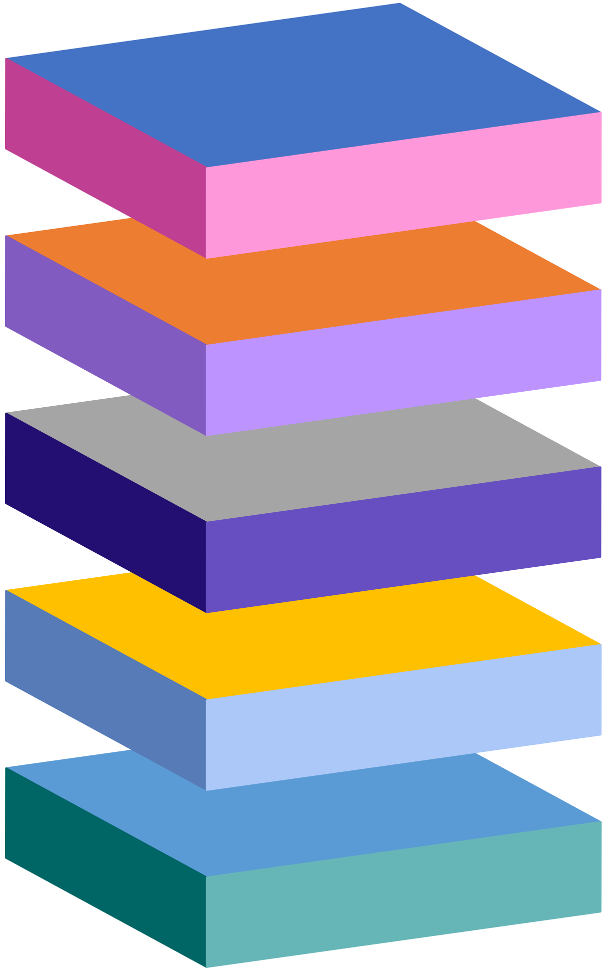
Craig Williams, Director of Infrastructure Services
630.656.7366; cwilliams@clientfirstcg.com

Consolidated High School District 230

- Large High School District in Illinois
  - 3 high schools
  - **7,600** students, **550** teachers, **300** support staff, **100** admins
- Roughly **50%** free and reduced lunch
- 1:1 with Chromebooks (since 2017-18)

INNOVATION • EMPATHY • LEADERSHIP
D230
INSPIRES & EMPOWERS

D230 Technology/Security Layers (March)



Network

Next Gen Firewall
Wireless Access Point Config
Granular Wireless Access

Application

Web Filtering
2-Factor Authentication
Drive Security/Backups
Gmail Rules / Virtru

Cloud

Two Internet Service Providers
DDoS Protection
Imperva Traffic Management

Endpoint

Next Gen Anti-Virus
Lack of Admin Rights
No Network Drives

Infrastructure

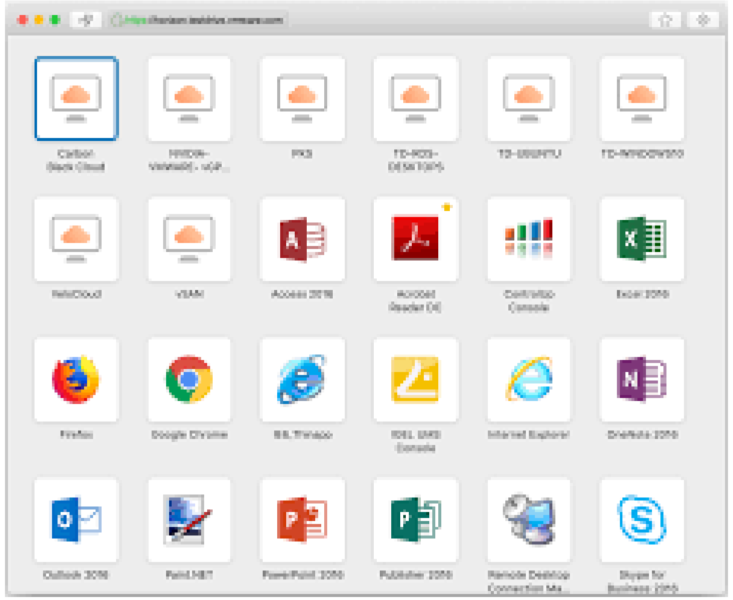
Multiple Data Centers
Granular Access Levels
Data Backup Procedures

End Users - KnowBe4 Drills

VDI for COVID: Spring ‘20 / Summer ‘20

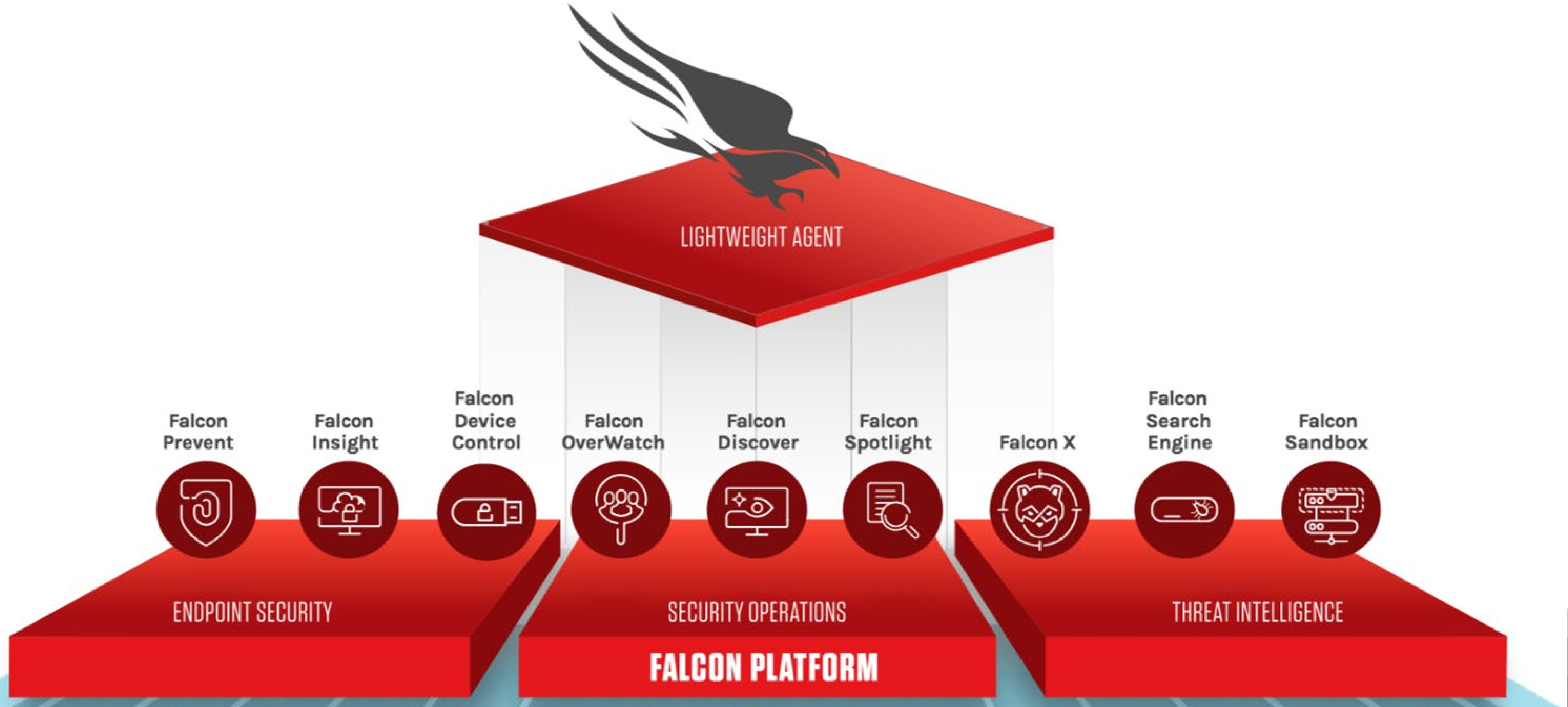
Virtual Desktop Infrastructure - Horizon VMWare

- Classes: CAD, Graphic Arts, Music,
- Staff Chromebook Applications
- Remote Support: helpdesk, AD, etc.
- Remote Desktops



No VPN Access - this is/was our system

Tuesday April 13 - EndPoint Protection



Incident #1 April 16-18

Friday, 4/16 11:30pm

- Student logs into Horizon VDI, accesses Remote Desktop designated for Music and uses old sharepoint domain admin account to access and view key servers
- Ran task manager on key servers and general viewing of the D230 virtual server environment.
- Extracted Active Directory database
- Crowdstrike Notifications make us aware

Saturday, 4/17 12:30pm

- Updated Crowdstrike agent from standard to aggressive defense on all servers. CS engineer reviewed servers to confirm all was clear.
- Reset All Staff Passwords
- Disabled Student and SP accounts

Incident #1 April 16-18

Saturday, 4/17 9:30pm

- Disabled student attempts to log in, denied. Tries the SP account, denied. Logs in with service Admin account and gets in (we did not reset these yet).
- Crowdstrike blocks a few attempt to install malicious software.
- Extracted Active Directory database (again).

Sunday, 4/18 9:30am

- VDI environment taken offline.
- Removed all domain admin accounts from VDI.

Monday, 4/19

- 9am - JC and dean meet with Student in question.
- Events were reported to insurance company (hotline on 4/17,
  email and call on 4/19) - Alliant, Corvus

Incident #1 Summary

- Bad Actor - questions on if it was student, external bad actor, etc.
- $25k Deductible for Cyber Security - I did not decline it, provided what we did and that we felt like we covered everything. Insurance company never got back to us.
- Student/Sub Password Reset - strategic language to parents for pswd reset. This was optional based on lawyer recommendation.
- Improved Security
  - VDI - segmented, Crowdstrike on VDI Desktops, desktops only for students that need them
  - Crowdstrike Antivirus/EDR expansion
  - Segmented Admin and service accounts, deleted not needed
  - Reset Pswds
  - **Upgraded to Crowdstrike 24/7 Complete on 5/3**

Incident #1 Staff Communication

Staff Communication

Subject: [Urgent] Staff Pswd Reset - Effective 12:30 Today (4/17)

In response to a security threat detected last night, **we will be triggering a staff password change at 12:30pm today (Sat, 4/17)**. Our systems that we have in place detected the threat and based on our logs, there was NO access to any personal information or data. **The password reset will block access to Skyward and any other D230 systems with the exception of Google until you are back onsite to reset your password**.

On Monday AM when back onsite, all staff members will be prompted to change their password when they log into a district laptop or computer. We will provide information on students and subs on Monday.

Incident #1 Parent/Student Pswd Change

Parent/Student Communication

Subject: D230 Student Password Change - Recommended

D230 Students,

In response to an event over this past weekend where staff and student login information may have been accessed, we are recommending a password change for all students. The systems we have in place detected the threat and based on our logs there was no access to personal information or data.

Students, please click on the link below for instructions on how to reset your password. *Note: this is for student accounts only, parent accounts were not affected*:eir password when they log into a district laptop or computer. We will provide information on students and subs on Monday.

Incident #2 Tuesday, May 4th 1:00am

3:00am Text
Device/Support Manager: “Hey, you may want to check your email, something is going on”

3:05am Call *(as I am not able to log into anything)*

Operations Manager: **“We are under attack!”**

Incident #2 Tuesday, May 4th

- Bad Actor logged in with Staff account, ran brute force on one of our domain controllers and were successful
- Dumped Active Directory
- Changed Pswd to Network Administrator account and were off and running
- Moved quickly across all servers systems
- Ransomware on VDI environment (Linux)
- Ran various variants: Pysa ransomware, Discovery tactics, powershell changes, File Share search, Google Drive Search, credential dumping, credential changing
- Crowdstrike 24/7 - Anti-virus/EDR blocked some, agent in Australia monitoring and eventually pulled plug and disabled both domain controllers. Essentially booting out the bad actor(s).

Incident #2 Tuesday, May 4th

7:00am

"In response to a security threat this AM, Skyward and other key systems are not available as we mitigate. We are working on being back online by first period and will again be triggering a staff password change. Zero hour teachers, please plan accordingly with the lack of online access. We will send updates as soon as we have them this AM.

FYI - there was NO access to any personal information or data based on our logs."

7:10am

Insurance and Corvus was engaged. IR team ready to go with SOW by noon.

Incident #2 Tuesday, May 4th

INITIAL MESSAGE TO STUDENTS, FAMILIES AND STAFF WHEN SYSTEMS WENT DOWN

District 230 Students, Families and Staff,

In response to a network security threat this morning, in a proactive manner as a precaution, we took Skyward and other key systems offline. We are working to get systems up and running as soon as possible.

For onsite students*, we will be proceeding with the regular bell schedule.*

For remote students, *we will notify you when the remote platform is back up and running and what class you should log into. Again, we are working to get this up and running as soon as possible.*

It is important to note that no personal information or data has been compromised according to our logs.

We appreciate your patience as we manage this situation. We will communicate with you as updates are available.

Incident #2 Tuesday, May 4th

- All main D230 systems came back online at 11am. Applied all critical patches to domain controllers and servers.
- Kept the VDI environment offline
- Crowdstrike reviewed all servers and systems that were accessed to remedy any files or "backdoor" options.
- Reset all staff and service account passwords. Reset the core passwords on the domain controllers.
- Forensics team kickoff call was on 5/6. The goal was to make sure we are 100% clean, the attack will not happen again, and confirm the impact/damage of the attack. This will typically take 12-15 business days.

Incident #2 Tuesday, May 4th

SENT WHEN SYSTEMS WERE BACK UP

District 230 Students, Families and Staff,

Thank you for your patience and understanding as we mitigated the network security issue this morning.

Systems are back online. Remote students should log in at 11:24 a.m. to their Period 4 class.

Thankfully, the protective systems the district has in place worked as planned this morning. The potential threat was identified by our network security partner and we were able to swiftly mitigate the issue by taking systems offline for a short period of time. No personal information or data was compromised according to our logs.

We will continue to monitor our systems and will communicate with students, families and staff if additional disruption occurs.

Again, thank you for your continued patience and understanding.

Incident #2 Summary

- External VDI was entry point
- File Share Access and scan (legacy access includes staff PII)
- Credential Access
- VDI had to be rebuilt due to pysa ransomware - complicated rebuild along with extra security precautions and 2-factor. Finalizing this week of 7/26
- Skyward: They did not or were not successfully accessing Skyward Server (we host Skyward on prem)
- Ransom Note - no specific note was sent and no data on the dark web per IR consultants
- Lawyers - we were not obligated to notify or provide credit protection, however we did. This was agreed upon and covered by Insurance company. Typically only 3% of staff take advantage of this. We were closer to 15-20%.

Crowdstrike 24/7 was a key defense

Incident #2 Staff Notification & Credit Monitoring

In response to the security incident from earlier this month, District 230 has worked with our cyber security partners to complete a comprehensive review. While we are unaware of any access to or misuse of your information, out of an abundance of caution, we are notifying you of the incident, offering you credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

- What Happened
- What Information Was Involved
- What We Are Doing (this included the IDX credit recovery information)
- What You Can Do
- For More Information

Insurance and IR Recap

D230 Emergency Team: CTO, Network Admins, Device/Help Desk, Communications Director, Asst Super of Business and Finance, D230 Lawyer

Insurance: Corvus rep, Insurance Lawyer, IR team

Terminology: “Security Incident”

Provided Notification and Credit Monitoring for 1 year - this was optional based on the findings

IR Team - top notch security experts, expected 15 days final report was more like 25-30 days. Overall painful to break down the access levels, etc.

Fall 2021-22 Aftermath

October 2021

- Blogger reaches out saying our data was dumped.
- Engage Cyber-security group and IR to grab files and analyze

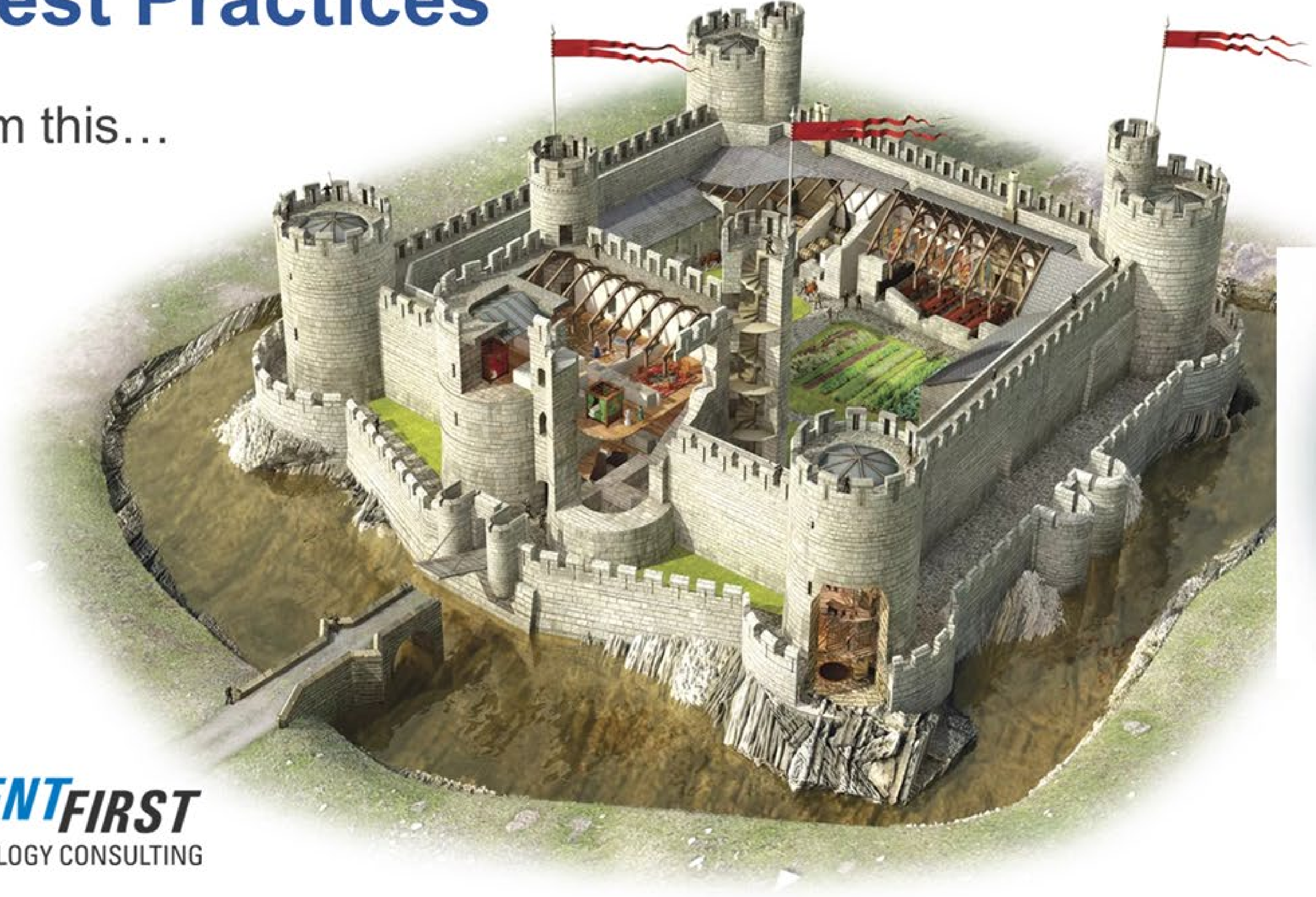
December 2021

- Results of File Scan: 99% garbage files, however one payroll file from 18-19 SY and files with students DOB.
- Letter mailed to those affected. John C sent email to current staff as heads up.
- Extension of Credit Monitoring

Pause
Feedback/Questions?

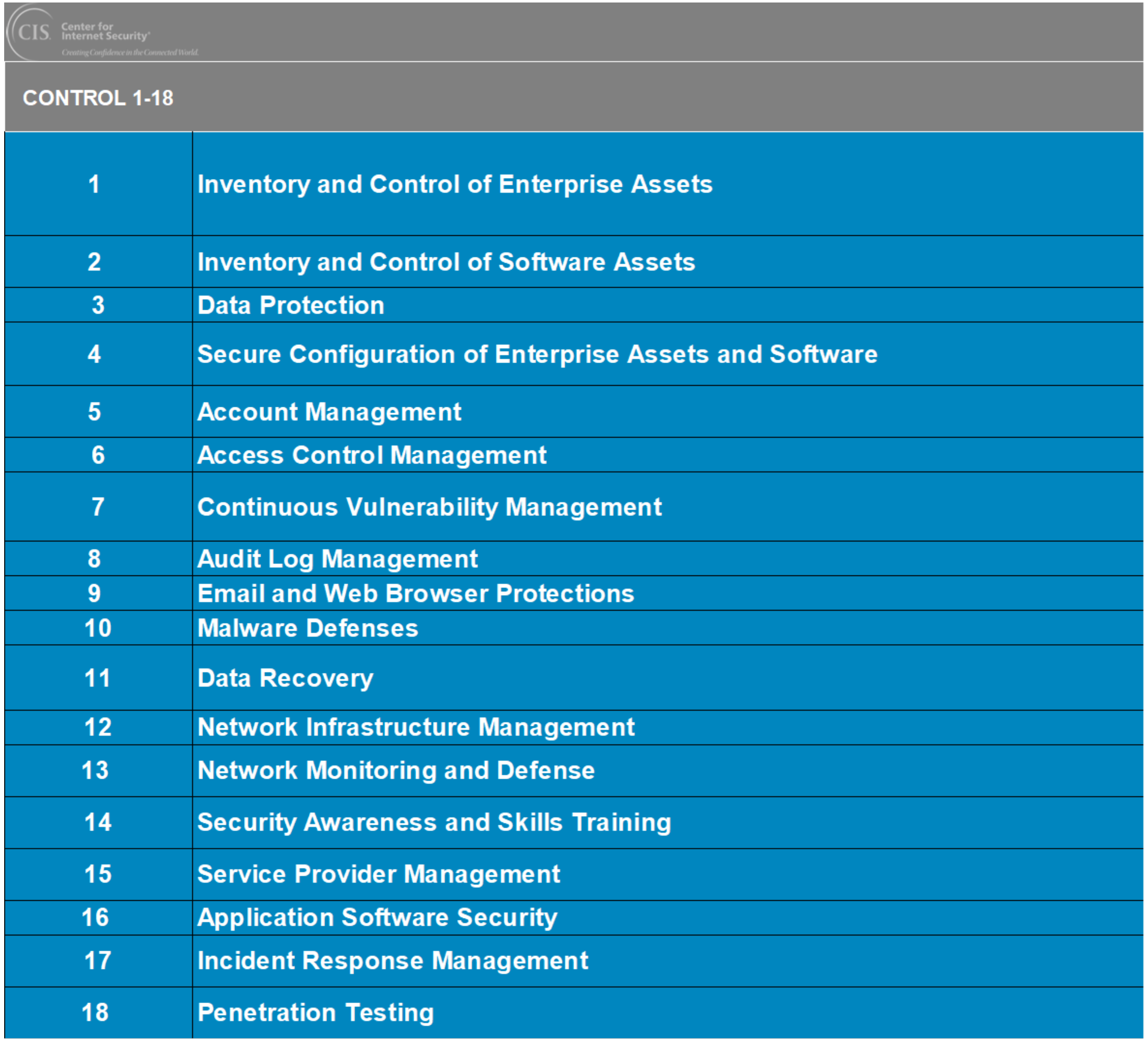
Best Practices

From this…



To this.

CLIENTFIRST
TECHNOLOGY CONSULTING



CIS Center for Internet Security
Creating Confidence in the Connected World

CONTROL 1-18	
1	Inventory and Control of Enterprise Assets
2	Inventory and Control of Software Assets
3	Data Protection
4	Secure Configuration of Enterprise Assets and Software
5	Account Management
6	Access Control Management
7	Continuous Vulnerability Management
8	Audit Log Management
9	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

ClientFirst has developed a scoring rubric to make the results easier to comprehend and implement.

The scoring profile for each subcategory questionnaire is calculated using a scale of 1 to 5 as a basis for the calculation of the score. The parent category will receive the average score for its supporting subcategories.

Scoring Definitions (1-5)

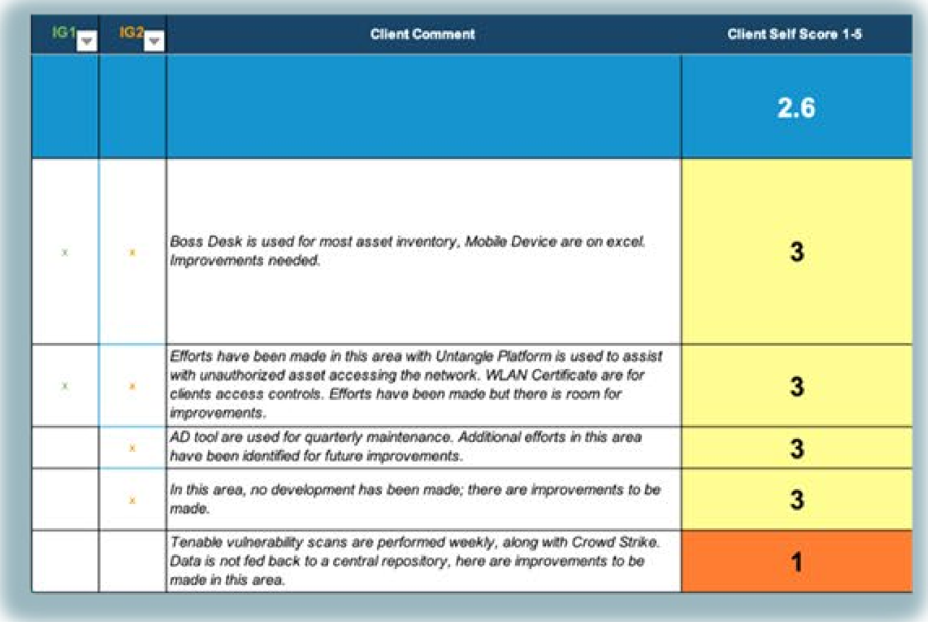
1) ***Policies and practices are absent from the organization. As a result, several areas pose an unacceptable risk and improvements are needed.***

2) ***Some efforts are in place, but they are underdeveloped. Several areas pose unacceptable risk, and there is a need for improvements in these areas.***

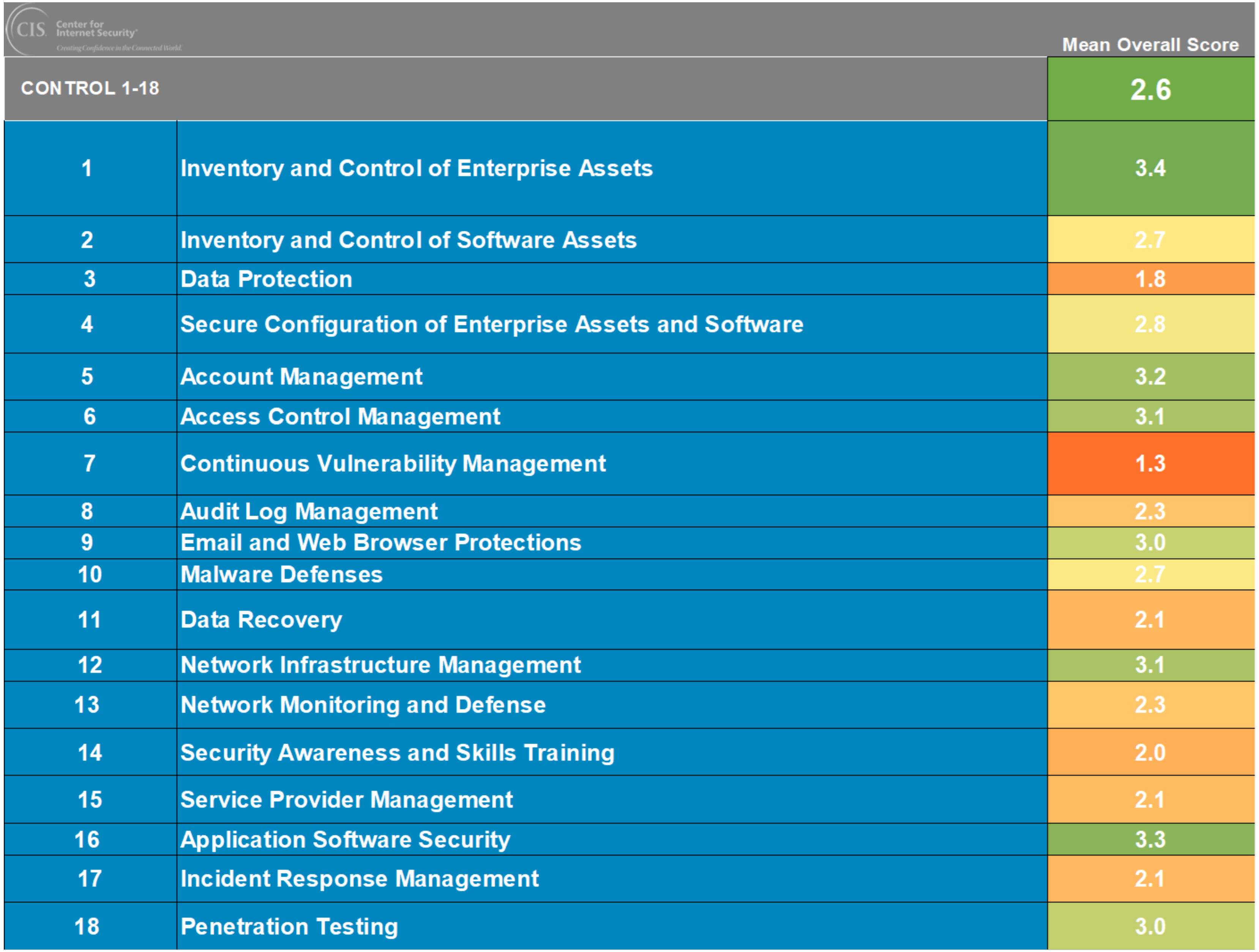
3) ***There are efforts underway to mitigate risk, or other solutions are in place to help mitigate risk if those efforts fail. However, there is a need for improvements in this area and recommendations need to be made in this regard.***

4) ***There are policies and practices in place to mitigate risk. To be fully compliant, additional efforts will have to be made.***

5) ***The practice area is fully compliant, and no additional efforts are required.***



IG1	IG2	Client Comment	Client Self Score 1-5
			2.6
x	x	*Boss Desk is used for most asset inventory, Mobile Device are on excel. Improvements needed.*	3
x	x	*Efforts have been made in this area with Untangle Platform is used to assist with unauthorized asset accessing the network. WLAN Certificate are for clients access controls. Efforts have been made but there is room for improvements.*	3
	x	*AD tool are used for quarterly maintenance. Additional efforts in this area have been identified for future improvements.*	3
	x	*In this area, no development has been made; there are improvements to be made.*	3
		Tenable vulnerability scans are performed weekly, along with Crowd Strike. Data is not fed back to a central repository, here are improvements to be made in this area.	1

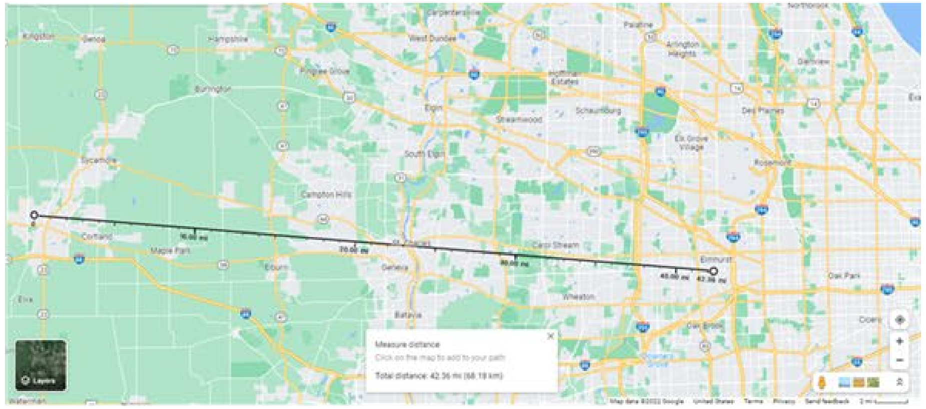


CIS Center for Internet Security
Creating Confidence in the Connected World.

		Mean Overall Score
CONTROL 1-18		2.6
1	Inventory and Control of Enterprise Assets	3.4
2	Inventory and Control of Software Assets	2.7
3	Data Protection	1.8
4	Secure Configuration of Enterprise Assets and Software	2.8
5	Account Management	3.2
6	Access Control Management	3.1
7	Continuous Vulnerability Management	1.3
8	Audit Log Management	2.3
9	Email and Web Browser Protections	3.0
10	Malware Defenses	2.7
11	Data Recovery	2.1
12	Network Infrastructure Management	3.1
13	Network Monitoring and Defense	2.3
14	Security Awareness and Skills Training	2.0
15	Service Provider Management	2.1
16	Application Software Security	3.3
17	Incident Response Management	2.1
18	Penetration Testing	3.0

Threat Prevention

- 24/7 Managed Detection & Response (MDR).
- Beyond MDR: Develop Cybersecurity Roadmap.
  - Cloud and Air-gapped Backups (25-mile rule). Immutable.
  - Network Micro-segmentation.
  - Logging and Auditing.
  - Vulnerability Management.
  - Network Access & Control.



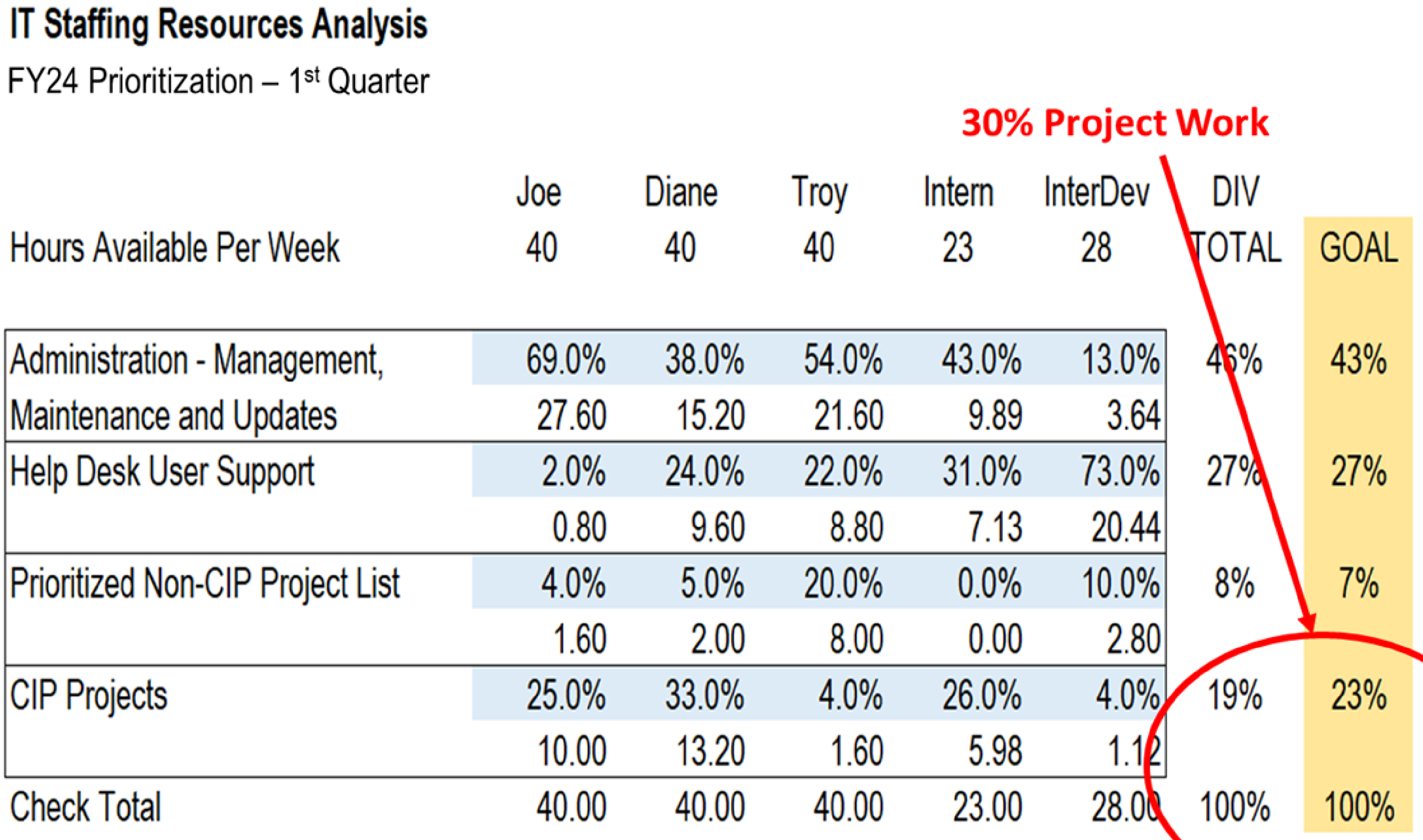
Measure distance

Click on the map to add to your path

Total distance: 42.36 mi (68.18 km)

- Follow Cybersecurity Best Practices
  - National Inst. of Standards and Technology: https://www.nist.gov/cyberframework
  - Center for Internet Security: CIS Controls v. 8

Start with the Basics - Staffing



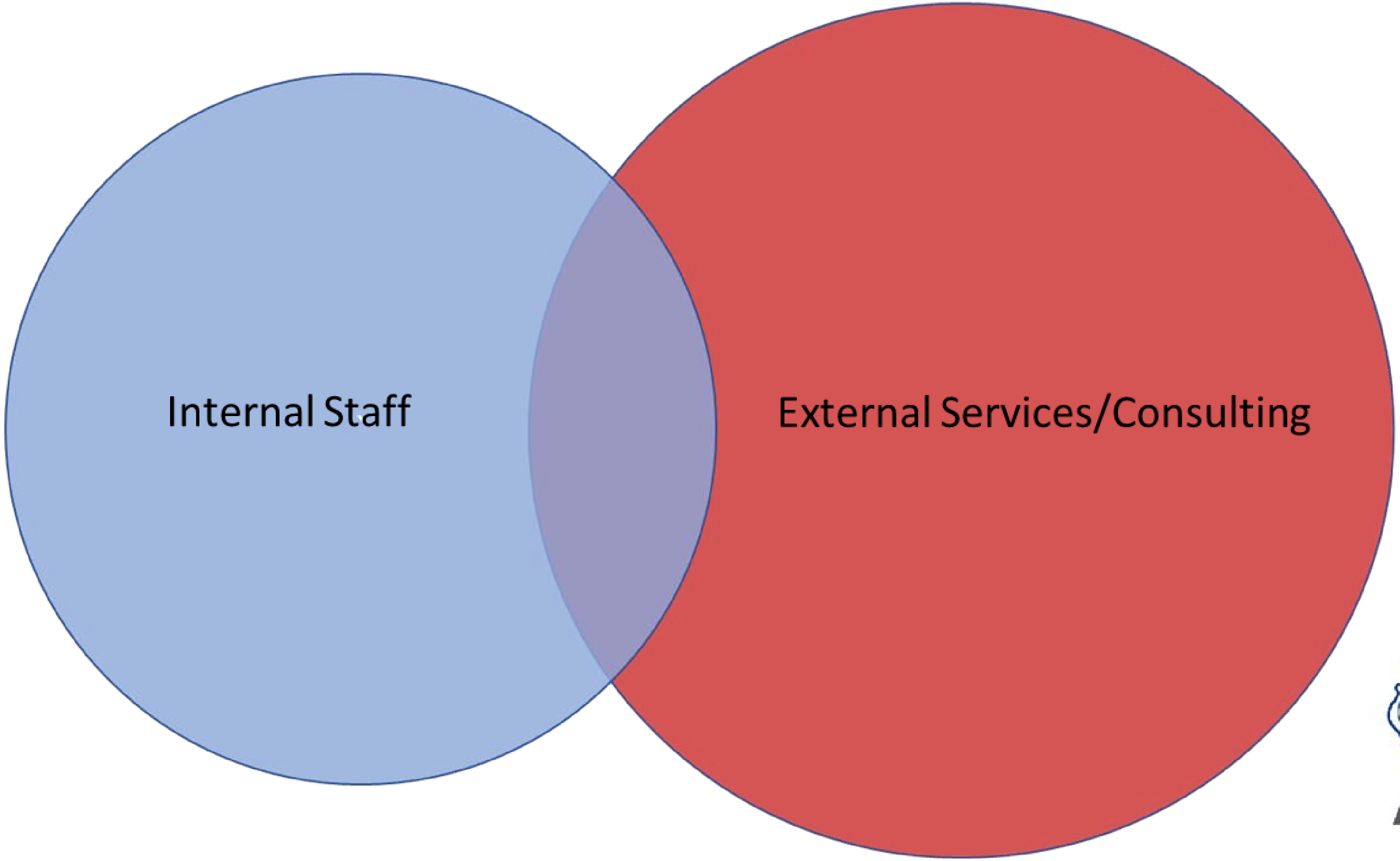
IT Staffing Resources Analysis

FY24 Prioritization – 1st Quarter

30% Project Work

	Joe	Diane	Troy	Intern	InterDev	DIV	
Hours Available Per Week	40	40	40	23	28	TOTAL	GOAL
Administration - Management,	69.0%	38.0%	54.0%	43.0%	13.0%	46%	43%
Maintenance and Updates	27.60	15.20	21.60	9.89	3.64		
Help Desk User Support	2.0%	24.0%	22.0%	31.0%	73.0%	27%	27%
	0.80	9.60	8.80	7.13	20.44		
Prioritized Non-CIP Project List	4.0%	5.0%	20.0%	0.0%	10.0%	8%	7%
	1.60	2.00	8.00	0.00	2.80		
CIP Projects	25.0%	33.0%	4.0%	26.0%	4.0%	19%	23%
	10.00	13.20	1.60	5.98	1.12		
Check Total	40.00	40.00	40.00	23.00	28.00	100%	100%

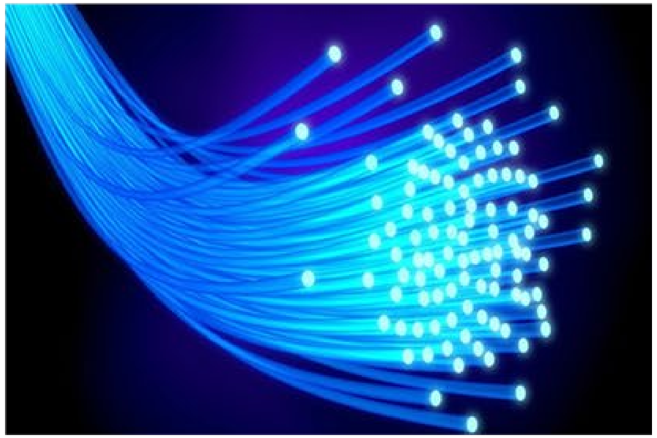
Cybersecurity Staffing



The People Factor

- Develop a strategic approach
- Provide general CyberSecurity training for all staff
- Provide comprehensive training for IT Staff

What Goes Into a Cybersecurity Roadmap



- Policies.
- Incident Response Plan.
  - No good if you don't practice it.
- Resilient Internet and Other Components.
  - Always have two tennis rackets.
- Logging & Audit Trails – forensic ability preparation.
- Security Officer monitors plan compliance.
- Add a new security application or procedure every quarter.

Top 10 Recommendations

1. Backups
2. 2-Factor on all major systems especially VDI and external facing systems
3. Proceed with security IR on first event (Cyber-security insurance) - lock down systems, etc.
4. Domain Admin Accounts - annual review and trigger options when they login
5. Host SIS and Business/HR System Offsite
6. Anti-virus on all machines - Servers especially
7. Patch Management
8. File Share - get rid of it. Get rid of files with SSN.
9. Micro-segmentation - either paid/new solution or configure existing as best possible.
10. Cyber Insurance, Communication, and Response Team
    - *What would you do if complete lock out? Payroll, etc.*

Questions and Answers

We thank you for your time!

Presenters:

MODERATOR INFO:

John Lavelle, Asst. Supt. for Business Services; CHSD#230
708.745.5241; jlavelle@d230.org

PANELISTS INFO:

John Connolly, Chief Technology & Operations Officer; CHSD#230
708.745.5253; jconnolly@d230.org

Craig Williams, Director of Infrastructure Services
630.656.7366; cwilliams@clientfirstcg.com