



# Kaukauna Utilities

Cybersecurity Lessons Learned

Don Krause

Manager of Information  
Technology at Kaukauna  
Utilities



The graphic features a dark gray background with faint, concentric circles. A bright blue rectangular box is centered, containing the text 'Cybersecurity Lessons Learned' in white. The box has a small triangular point at the bottom center.

# Cybersecurity Lessons Learned

## Presentation Format

**Situation, Lessons Learned, and Actions taken.**

**NOTE the STAR for FREE or easy to implement Actions.**

SITUATION

ALL shared files in a single common (S)hared drive.

S:\


Lesson Learned

Anyone with rights to this folder allows malware to infect EVERY file!

Action Taken

We changed and now group files by purpose.

We restrict access based on AD group membership.





## Scope

**My responsibilities go beyond just the Utility, I am also responsible for the City of Kaukauna.**

**Some of my resources were chosen to encompass City Government.**

## SITUATION

**ALL** shared files in a single common  
(S)hared drive.

**S:\**



## Lesson Learned

**Anyone with rights to this folder allows  
malware to infect EVERY file!**



## Action Taken

**We changed and now group files by purpose.**

**We restrict access based on AD group membership.**



SITUATION

# Network Performance



## Lesson Learned

**10+ years ago...**

**Security cameras conflicting with other devices.**

**Last year...**

**Guest Wifi consumed nearly all internet bandwidth**



Action Taken

## Network Segmentation

**We implemented VLANS to reduce the size of any 1 network. We separate DATA, VOICE, SCADA, and SECURITY devices.**



## Continuous Improvement

**We further segmented our network by physically isolating guests.**

**We have a dedicated internet connection and NO shared Switches.**

## SITUATION

**Limited capabilities and visibility of  
our firewall.**



## Lesson Learned

**Next generation firewalls performed more dynamic analysis of inbound traffic, including sandboxing and provide better insight to the data.**

Action Taken

**We implemented a Fortinet Fortigate  
firewall**



SITUATION

**No Resources Available for  
cybersecurity**





## Lessons Learned

# **Municipalities have a TON of resources!**

ISAC – Information Sharing & Analysis Center

CIS – Center for Internet Security

US-CERT - Cybersecurity and Infrastructure Security Agency

WI CRT – Cyber Response Team

Fusion Center

WI National Guard



Actions Taken

**We joined E-ISAC and MS-ISAC**



**MS-ISAC<sup>®</sup>**

Multi-State Information  
Sharing & Analysis Center<sup>®</sup>



## Continuous Improvement

**Attend annual summits to stay informed**

- 1. WI Governors Cybersecurity Summit (Sep)**
- 2. APPA Cybersecurity Summit (Nov)**
- 3. MS-ISAC annual meeting (Apr)**

Continuous Improvement

**I am taking SANS courses to understand cyber incident handling.**



## Continuous Improvement

**We are utilizing the CIS Controls as a framework for documenting our policies and procedures to prove compliance.**



## SITUATION

**Users are clicking on links in emails  
and opening files containing  
viruses.**



## Lesson Learned

**Users were not aware of the hazards in email messages.**



## Action Taken

### **Peer based end user training**

**We brought in a trainer and required all staff to attend – specifically focused on phishing email identification.**





## Action Taken

To ensure our users know IT sent out the email we **purposely did NOT** use `helpdesk@ku-wi.org`

We created a new domain for our IT department AND we do not use the generic HELPDESK user.

## Continuous Improvement

**We subscribed to a service to randomly test our end users with phishing emails.**



## Continuous Improvement

**There is a cost to testing your users...**

**At the WI Governors Cybersecurity Summit I learned that the State has secured GREAT pricing for this service for municipalities with a different provider.**

**INFOSEC**<sup>TM</sup>

## SITUATION

End Users don't know  
what cybersecurity is.

## Lesson Learned

# October is Cybersecurity Awareness Month

Department of Homeland security has materials available for FREE to help you.

We use the posters and calendars





## Action Taken

**KU has a GREAT safety culture.... I've asked to incorporate cyber into that culture by presenting at the October all employee Emergency Action Plan training.**

**I used a Jeopardy style game created by the Department of Homeland Security.**

SITUATION

Outdated Website



## Lesson Learned

**We needed a web platform that is always monitored and actively developed against to ensure vulnerabilities are quickly corrected.**



Action Taken

We migrated to a new website running  
on the **WordPress** Platform.



WORDPRESS



Action Taken

We migrated to a highly responsive web developer and provider – **Digisage**

[ **digi**sage ]

## Action Taken

We implemented **Cloudflare** as our front side DNS filter for our new website:

**KaukaunaUtilities.com**

**Favorite Feature: Under Attack Mode**





## Action Taken

**We signed up for the FREE Web Profiling Tool / scanning service provided by MS-ISAC to check our public website regularly.**



**MS-ISAC<sup>®</sup>**

Multi-State Information  
Sharing & Analysis Center<sup>®</sup>



## Continuous Improvement

**We migrated to Quad 9 DNS server, a FREE Service.**

**9.9.9.9**

The system uses threat intelligence from more than a dozen of the industry's leading cyber security companies to give a real-time perspective on what websites are safe and what sites are known to include malware or other threats.

<https://quad9.net>



SITUATION

# Workstation Compliance



## Lesson Learned

**Primary threat vectors are...**

- 1. eMail**
- 2. Local Admin Rights**
- 3. Patches**

Action Taken

We implemented an **AristotleInsight** appliance to monitor workstations.



Sergeant **Laboratories**





## Continuous Improvement

**We took advantage of FREE membership to CIS SecureSuite.**

**They offer file scanning tools, hardened server images, and workstation baselines.**



**CIS SecureSuite<sup>®</sup>**  
Membership

SITUATION

**Old Version of Microsoft Exchange  
for our Mail Server**



## Lesson Learned

**Email is the highest targeted system, we needed a layered approach.**

Action Taken

**We replaced our Exchange Server with Microsoft Office 365.**



## Action Taken

**We implemented email filtering, archiving, and encryption.**

**We automatically encrypt any email containing sensitive info like SSN or CC#**

**Every Link is re-directed and sandboxed before opening for our users.**





## Continuous Improvement

**We implemented an SPF record to help prevent spoofed emails.**

**We also use our inbound mail filter to restrict mail based on SPF.**

SITUATION

**Not Involved!**



Lesson Learned

**Get Involved**



## Action Taken

**We worked with the National Guard to conduct a cybersecurity tabletop.**



## Continuous Improvement

**We worked with the National Guard again... to provide them a live network to test their equipment and skills.**



## Continuous Improvement

**I joined the WI Cyber Response Team to help with incidents and build a network of professionals I can talk with about cybersecurity.**



**CYBER RESPONSE TEAMS**  
State of Wisconsin

1. Breakup Data and authorize by groups
2. Breakup your network into segments
3. Join an ISAC
4. Peer Based User Training
5. NO Helpdesk@YourDomain.Com
6. Check out INFOSEC for phishing testing
7. Cyber Awareness at Safety Training
8. Web Profiling Tool from MS-ISAC
9. Quad9 DNS
10. CIS Cyber Security Suite

# Don Krause

Manager of Information Technology at Kaukauna Utilities

[DKrause@ku-wi.org](mailto:DKrause@ku-wi.org)

