What was your cyber security ah-ha moment?
Cybersecurity

Hartford Union High School
Notable Members

State of Wisconsin
City of Madison
Marquette University
Medical College of Wisconsin
DDoS Attacks Don’t Discriminate
DDoS?
Your Outward Facing IP Address
Cost to them...
<table>
<thead>
<tr>
<th></th>
<th>1 Month Basic</th>
<th>Bronze Lifetime</th>
<th>Gold Lifetime</th>
<th>Green Lifetime</th>
<th>Business Lifetime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>5.00€/month</td>
<td>22.00€ Lifetime</td>
<td>50.00€ Lifetime</td>
<td>60.00€ Lifetime</td>
<td>90.00€ Lifetime</td>
</tr>
<tr>
<td>Concurrents</td>
<td>1 Concurrent+</td>
<td>1 Concurrent+</td>
<td>1 Concurrent+</td>
<td>1 Concurrent+</td>
<td>1 Concurrent+</td>
</tr>
<tr>
<td>Boot Time</td>
<td>300 seconds</td>
<td>600 seconds</td>
<td>1200 seconds</td>
<td>1800 seconds</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>Network Capacity</td>
<td>125Gbps</td>
<td>125Gbps</td>
<td>125Gbps</td>
<td>125Gbps</td>
<td>125Gbps</td>
</tr>
<tr>
<td>Resolvers &amp; Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
<td>24/7 Dedicated Support</td>
</tr>
<tr>
<td>Order Now</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Cost to you?
Magic Box?
Cloud-Scrubbing
Thousands a month

Start talking to your ISPs about bundled services. eRate can be part of the solution...
GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED
Fear and getting over it...
Stuff with $0 cost....but people’s time
People

Tech

Process
Killer Apps
Communication and Relationships
Tips

Create good passwords
Avoiding Phishing Schemes
Run updates
Lock your computer screen
Washington County loses $87,760 in email scam

By Hannah Schwarz of the Journal Sentinel

Washington County wire transferred $87,760 to criminal bank accounts as a result of an email phishing scam, county officials disclosed Friday.

The Washington County Sheriff’s Office is investigating the scam, the department said.
Spear Phishing
Online Banking Alert

Dear member:

We detected unusual activity on your Bank of America debit card on 09/22/2014. For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at https://www.bankofamerica.com to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.
Free Training

Nathan Mielke <mielkedata@gmail.com>
to nathan.mielke

Hello

Click hear to enter your info to get free training


Nathan Mielke
Hartford Union High School
Technology Services
262.670.3236
Help Please

Monica Glorioso <monica.glorioso.hartford@gmail.com>
to Lisa.Fendt

Hello staff,

Sign for helping below

http://bit.ly/2mNjfT

-Monic
National Institute of Standards and Technology (NIST)

The organization suggests keeping passwords simple, long and memorable.
Create good passwords

Avoid Dictionary Words
Password-cracking tools that are widely available online usually try different combinations from dictionary lists.
Create good passwords

Try Personal Sentences
Think of a sentence that has personal meaning to you, then add in numbers and special characters. Try to add in uncommon symbols, such as > < ? ! - _ [ ] #.

Long, simple passwords
Create good passwords

Test your password out at - http://www.passwordmeter.com
Avoid Phishing Schemes

Take a quiz at - https://www.sonicwall.com/phishing/
Run Updates

Restart your computer
Lock your computer screen

LOCKS THE COMPUTER
Asset Management
Creating a Cyber Secure Home

1 Securing Yourself

Cyber attackers have learned that the easiest way to get something is to simply ask for it. As such, common sense is your best defense. If a message or phone call seems odd, suspicious or too good to be true, it may be an attack. Here are some examples:

Phishing emails are emails designed to fool you into opening an infected attachment or clicking on a malicious link. These emails can be very convincing; they may appear to come from a friend or organization you know. Sometimes cyber attackers even use details from your social media accounts to craft customized phishing attacks.

Someone calls you pretending to be Microsoft tech support. They claim that your computer is infected, when they are really just cyber criminals that want access to your computer or want you to buy their fake anti-virus software.

2 Securing Your Home Network


4 Securing Your Accounts / Passwords

You most likely have a tremendous number of accounts online and on your devices and computers. Here are some key steps to protecting them:

Always use long passwords that are hard to guess. Use passphrases when possible. These are passwords that have multiple words, such as “Where Is My Coffee?”

Use a different password for each of your accounts and devices. Can’t remember all of your strong passwords? We recommend you use a password manager to securely store them. This is a computer program that securely stores all of your passwords in an encrypted vault.

Use two-step verification whenever possible. Two-step verification is when you need a password and something else to log in to your accounts, such as a code sent to your smartphone.

On social media sites, post only what you want the public to see. Assume they can read your posts. Be aware of your online presence.

"As technology becomes more important in our personal lives, so does securing it. Here are some fundamental steps you should always take to help protect yourself and your family."

Lori Rosenberg - eBay

To learn more, subscribe to our monthly security awareness newsletter

www.sans.org/thehumanfactor
What do you have?
What does it do?
Who is responsible for it?
Who you gonna call?
Cloud Security

On prem best practices = off site best practices
Benchmarks – NIST & CIS
Configuration

NITS and CIS
Cyber Hygiene

Keep your computer and your digital self clean
Keeping Clean

1. Keep an inventory of hardware and software on the district network.

2. Develop a process for IT approved software installation by end users. That could include limiting installation of trusted software or prohibiting and blocking all installation without prior approval from IT. (make it easy for the users without allowing the wild west, it’s a balancing act)

3. Educate users on practicing good cyber behavior, including password management, identifying potential phishing efforts, and which devices to connect to the network.

4. Identify vulnerable applications that aren’t in use and disable them.

5. Consistently back up data and keep multiple copies. Consider using a secure cloud solution as well as on premise.
Randomware...backups, backups backups
Keeping Clean
The Big Five

1. Least Privilege
2. Segmentation
3. Encryption
4. Multi-Factor Authentication
5. Patching
Be an Active Partner

To achieve the goal of a safe and secure learning environment we need everyone's help and participation.

Keeping systems up to date and practicing good cyber hygiene can prevent lots of issues.

No matter your role Cyber Security affects you and you are part of the cyber security workforce.
Why it matters to **YOU**

On average it take **640 hours** to restore your identity if you’re the victim of identity crime.

**YOU** are the target, criminals want what you have.

Being cyber safe helps protect those **you care about**.

A child is **51% more likely** to be the victim of an identity crime then their parents.
A child is 51% more likely to be a victim of identity theft
Student records – up to $200 on the dark web
81% of events exploit identity
'Dark Overlord' hackers posted stolen student info, Johnston officials say

Sera Alexander pleads guilty to involuntary manslaughter in stepfather's death

Johnston School District

Johnston School District

thedarkoverlord
@ltdo_hackers

We’re now publicly claiming responsibility for the threats that resulted in the closure of JCSD in Iowa and 7,200 children without school.
6:19 AM - Oct 4, 2017

thedarkoverlord
@ltdo_hackers

With the student directory from JCSD we released, any child predator can now easily acquire new targets and even plan based on grade level.
8:36 AM - Oct 5, 2017

thedarkoverlord
@ltdo_hackers

We’re now publicly claiming responsibility for the vivacious assault on Splendora Independent School District.
6:18 AM - Oct 4, 2017
Johnston School District

Fear and Getting Over It

Living through a cyber security event or data breach can be a very scary thing.

Having the right level of concern is paramount, you should be concerned but not be gripped by fear.

Some of the things you can do to get a clearer picture of the cybersecurity risks you are facing:
Breach response team / plan.

Perform a risk assessment so you can best decide how to address the risks discovered way to address risk are (Avoid, Mitigate, Transfer, Accept).

All of these pieces should help you get over your fear...it's going to happen, but you have put pieces in place and have a plan.
You need another set of eyes...
Need vs Want
You need a trusted partner

• What local staff does...  
• What vendors do...
This is going to cost some $$$$
Google Apps Audit

Hartford Union High School District
**Detailed Findings:**

*Medium Priority:*

- **BIOS Unlocked**
  
  One of our biggest security concerns was with the accessibility of the Boot Order option in the BIOS. While the configuration settings in the BIOS were password protected, other options, like Boot Order, were unlocked. As we discussed during the walkthrough, there have been a few students that have loaded Linux onto these school issued laptops. While most of these students are probably harmless, it only takes one to start poking around to cause trouble. Exploiting this vulnerability was how we were able to conduct the rest of our audit.

- **Moodle not being the latest version**

  Another security concern we had was the version of Moodle. While Moodle is relatively up to date, it was not the latest version possible at the time we did our audit. This normally would not be a major concern, but this case is different. Through a popular online database of exploits, we found an SQL injection attack that affected the running version of Moodle (exploit-db.com/exploits/41828/). While this attack is relatively complicated, the information, and the value of that information, held at schools makes this a medium vulnerability.

*Low Priority*

- **Physical server room security**

  The biggest physical security concern we saw was the lack of security cameras around server rooms. While there were security cameras in the hallways, we ideally would have cameras in the server room. This would keep a record of who went into each room at what time and what they did. Having this information would be helpful to mitigate an internal attack.
Cyber insurance
Who/what is your best defense?

Create a comprehensive cyber security awareness training program with ease. Promote awareness and foster change.

LEARN MORE
Training for your technology staff
Nathan Mielke
Holy Hill Area Schools and Hartford Union High School
@ndmielke
ndmielke@gmail.com