



Cyber Time:
Are you ready for an
attack?



EDUCATION

Cyber breach at Centennial School District keeps computer systems down

Hacker releases Las Vegas school district student, employee information after officials refuse ransom demands

K-12 EDUCATION

Guilderland Central Schools Hit With Malware Attack

SECURITY

Houston School District Forced to Negotiate with Hackers

EDUCATION NEWS

Hackers post 26,000 Broward school files online

Sheldon ISD forced to pay nearly \$207K after hackers targeted servers

Why Schools...

- Student and Family Information
- Student IEP/IDEA
- Employee Information (Retiree Information)
- Payment and Bank Information
- No cyber loss prevention plans
- Small IT staff
- Lack of funding

Why Schools...

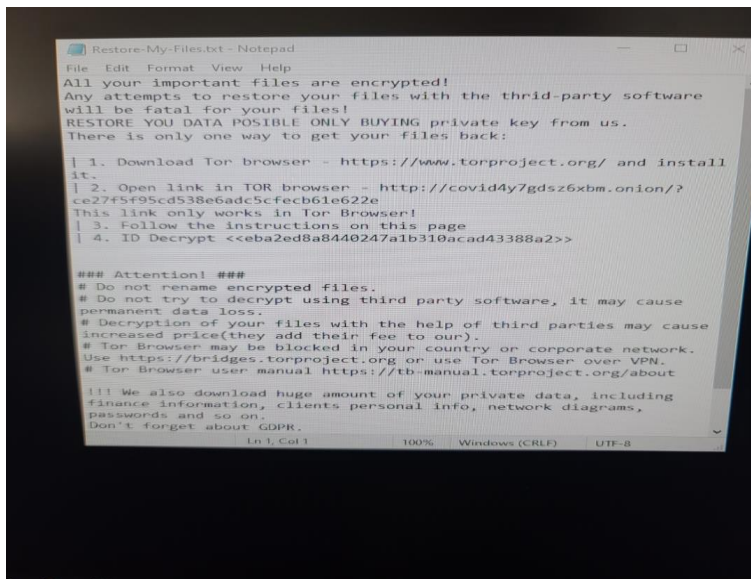
Doug Levin, national director of the school K12 SIX, said districts are appealing targets for several reasons – ***but are also often financially under-resourced, meaning their technology might not have all the latest updates to prevent incidents. They also have an incentive to pay so they're up and running again quickly.***

What is ransomware?

- Ransomware ever-evolving malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
- Malicious actors then demand ransom in exchange for decryption.
- Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.

Table Top...

What would you do if you walked in to your office on July 28th, and when you turned your computer on and it said....



```
Restore-My-Files.txt - Notepad
File Edit Format View Help
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software
will be fatal for your files!
RESTORE YOU DATA POSSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install
it.
| 2. Open link in TOR browser - http://covid4y7gdsz6xbm.onion/?
ce27f5f95cd538e6adc5cfecb61e622a
This link only works in Tor Browser!
| 3. Follow the instructions on this page
| 4. ID Decrypt <ceba2ed8a8440247a1b310acad43388a2>>

### Attention! ###
# Do not rename encrypted files.
# Do not try to decrypt using third party software, it may cause
permanent data loss.
# Decryption of your files with the help of third parties may cause
increased price(they add their fee to our).
# Tor Browser may be blocked in your country or corporate network.
Use https://bridges.torproject.org or use Tor Browser over VPN.
# Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including
finance information, clients personal info, network diagrams,
passwords and so on.
Don't forget about GDPR.
Ln 1, Col 1          100% Windows (CRLF) UTF-8
```

McFarland July 28, 2020, 2:18am

- Systems affected:
 - 18 servers
 - Back-up servers
 - Wireless system
 - All networked computers
 - Phone system
 - HVAC system
 - Safety system
 - Alarm systems
 - Camera systems
- Systems not affected
 - Student Management System (IC)
 - Finance/HR System (Skyward)
 - Recreation Management System
 - Website (CMS 4 Schools)
 - Google/Gmail

McFarland.....

- **Crisis Response team met per Crisis Management Plan at 8am on 7 28 2020**
 - Team determined communication plan
 - Get the whiteboards out
 - On site staff
 - Remote staff
 - Parents/community
 - Team determined priorities
 - Payroll and Finance
 - Buildings, Safety and Security
 - Team determined next steps
 - Contacted 3rd party Network consultant
 - Contacted Insurance

McFarland...

Action

On 7/29/2020, we determined that our full network was encrypted. Via our Insurance company EMC/Hartford Boiler Company, we assembled the following team:

- Heartland Business Services, on-site 3rd party network team
- Arete, Forensics team,
- Coveware, Ransom Negotiators, Decryption Tool Team

Between 7/29/2020 and 8/6/2020, School District, Coveware and Arete determined that we would negotiate with Lock2Bit. While ransom note did not indicate exfiltration of data, we were unable to determine if files on some servers that may have contained Personal and Financial information had been compromised.

McFarland...

While the above was being dealt with, the school district technology department, Heartland Business and other school district employees were working on the following:

- Set up wireless hotspot wifi network and computers
- **Acquired replacement hard drives**
- Built new images
- Removed all old hard drives and destroyed them
- Formatted new hard drives using toaster systems

McFarland...

Ransome and Decryption Process

- 8 6 2020, paid bitcoin ransom
- 8 19 2020, encryption tool was moved from testing to restoring servers
- 8 19 2020 to **9 14 2020**, servers brought back on line

McFarland...

Insurance

- You pay them and they work for you!
- Incident communication
- Cyber policy from \$100,000 to \$250,000
 - Ransome limit increased from \$10,000 to \$25,000
 - Ransome was \$23,000, (started higher)
- **Cyber policy excludes labor costs for employees**
 - **Worked with Insurance to explain contractor vs employee**
 - **District recouped all labor costs**
- **Cyber policy excludes hardware replacement costs**
 - **Worked with Insurance company to show cost benefit between labor and acquired hardware**
 - District recouped hardware costs for hard drives using Marine (equipment) Policy

McFarland...

Interesting Notes (Setting the Stage)

- District Network Engineer out of state
- Disgruntled technician
- Network Security Technician credentials used to breach network security
- Date of initial network compromised 6 26 2020 and again on 7 23 2020
- School District was training teachers on new software canvass and deploying mobile devices
- Finance Audit was scheduled for 8 2 2020
- No Summer School, but Recreation and Pool were operating

McFarland

Key Take Aways

- Get ready for the long haul
- Test, test, test the system
- Back up, Back up, Back up
- Cloud Systems, save the day
- Its good to also be lucky
- Communicate, Communicate, Communicate
- Human element, Breath, this is not your fault or your organizations fault, unless...

YOUR Network...GET busy...

Multi Factor Authentication for System Access (MFA)

RDP (Remote Desktop Protocols)

Privileged accounts

Anti-virus/malware software

Employee training on cyber safety and social engineering

Email Security: Quarantining and Screening

- Spam Quarantine Notification

- Warning External Email

Robust Patching Policy

Software up to date

Encryption of Sensitive Data

Operational Continuity Plan

- Must be in writing

- Be prepared to share with the underwriter

Regular Backups

- Daily is best

- Data Backup stored in a separate location

- Socially distance your backup from your data

Cyber Insurance

- How much is enough?
 - Cost of Incident
 - Time down vs Cost
- Know how your insurance will respond
 - Beyond the Policy, how can they help
 - Define and understand key player roles
 - Who will they send you too?

Cyber Insurance...

A few ABSOLUTE requirements and Questions you will be asked to get cyber insurance....

- Do you use multi-factor authentication (MFA) to secure all remote access?
- Do you use multi-factor authentication (MFA) for cloud-based email account access?
- Do you protect all of your devices with anti-virus, anti-malware, and/or endpoint protection software?
- Do you regularly back up critical data? If so, how often?
- Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?

Can't hide, avoid or ignore....

WPR: “Ransomware, phishing and cyberattacks are increasingly hitting Wisconsin school districts” - <https://www.wpr.org/ransomware-phishing-and-cyberattacks-are-increasingly-hitting-wisconsin-school-districts-most>

Business Insurance: “Schools hit with Cyber Price Hikes” - <https://www.businessinsurance.com/article/20210712/NEWS06/912342944/Schools-hit-with-cyber-price-hikes>

Help is Out There!

- Wisconsin Cyber Response Team
 - The Cyber Response Teams (CRT) strive for a safer, stronger environment for users by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners. It is a never ending battle with malicious actors but working with different teams and people, like you, only increases our chances of success.
 - Every team includes representatives from the Department of Justice
- Don't hesitate, call right away, even if you aren't sure something is going on! They are here to help!
 - Save this number to your phone! (800)943-0003

Resources

- Cyber Awareness Training
 - [KnowBe4](#)
 - [InfoSecIQ](#)
- [MS-ISAC \(Multi-State Information Sharing and Analysis Center\)](#)
- [Hudson Data Privacy/Cyber Security Information](#)
- [Wisconsin Department of Public Instruction Cyber Security Resources](#)
- [CoSN/ASBO Toolkit](#)

Resources

- [Ransomware Reference Materials for K-12 \(CISA\)](#)
- [Cyber Threats to K-12 Remote Learning Education \(CISA\)](#)
- [Ransomware Tip Sheet \(CISA\)](#)
- [Ransomware Safety Video \(CISA\)](#)
- [Ransomware Guide \(CISA/MS-ISAC\)](#)
- [Session Resources](#)

Resources...

<https://www.helpsystems.com/blog/break-time-6-cybersecurity-games-youll-love>

<https://www.cisa.gov/stopransomware>

<https://www.k12six.org/>

“

“The cost of investing time, money and procedures in cyber security outweighs the cost of having a cyber incident.”

Thank you to contributors of
this presentation:

Jen Lotze, Hudson SD

Marty Malloy, M3 Insurance