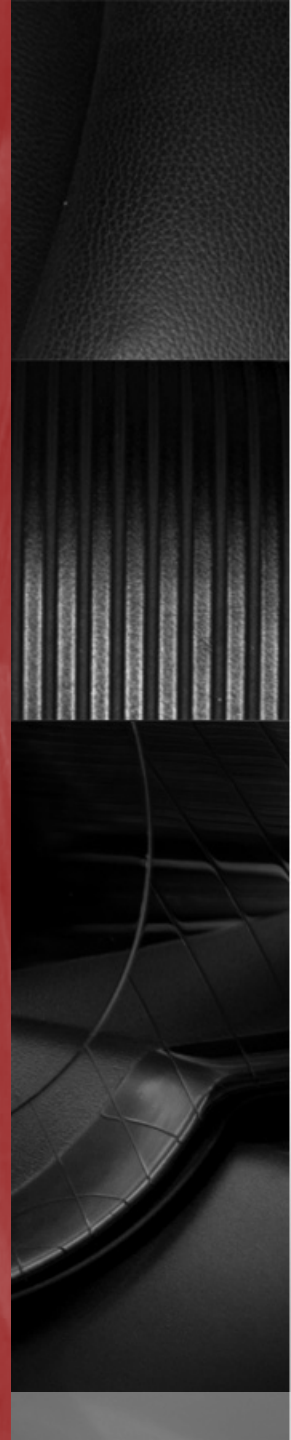
Managing Your Network: Facts and Fiction

Dealing with Hackers, Attackers, and Bandwidth Snatchers

Presenters:

Donnie Cummins – CIBER Global, LLC.

Glen Popiel – CIBER Global, LLC.



Who Are The Ciber Engineers?

- The Ciber Engineers are provided by MDE as a free technology resource to all school districts
  - Ciber has been providing this service to MDE and school districts for nearly 20 years
- The current Ciber Engineers have over 80 years of experience in the IT and networking fields, and have multiple network and vendor certifications
- The Ciber Engineers are paid on a fixed-rate contract by MDE and are an unbiased resource that you can use for:
  - Network Infrastructure and Security Assessments
  - Network Infrastructure and Server consultation and installation
  - Technical Support and Troubleshooting assistance
  - DDOS and Virus Mitigation assistance
  - Disaster Recovery
- Since the Ciber Engineers are viewed by E-rate as an extension of MDE, we can also provide:
  - E-rate Assistance
  - Assistance with preparing and evaluating RFP's
  - Technology Plan Assistance

Introduction

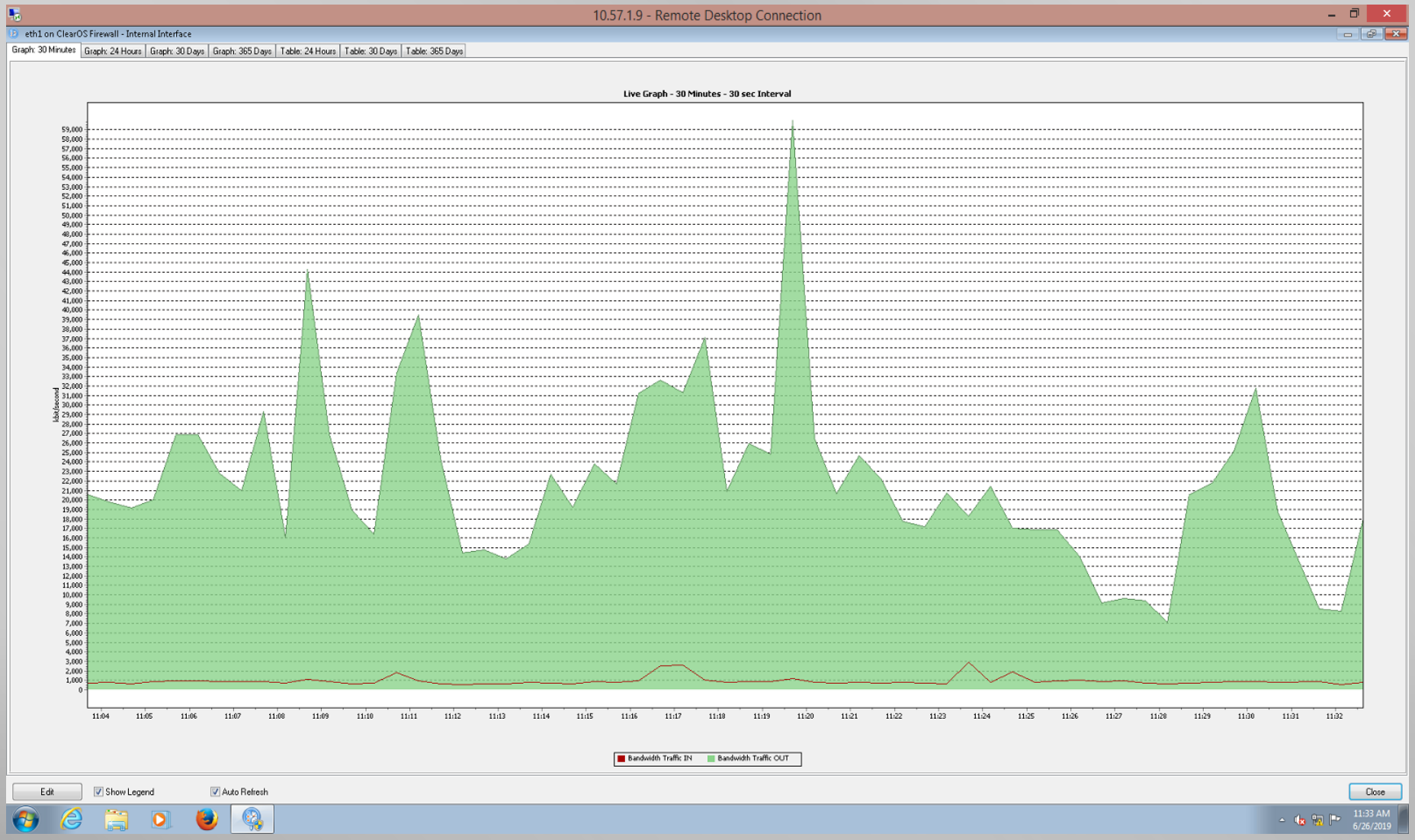
- We're here today to discuss some of the current challenges you are facing with your networks and how you can address them. These issues include:
  - Bandwidth Management
  - Denial of Service Attacks
  - Data Breaches
  - Users bypassing filters
  - Network Security

- Although it is also an important concern, we will not be focusing on or addressing network infrastructure or security issues caused by users. These should be addressed through user education and your Acceptable Usage Policy

Bandwidth Issues

- As our Internet speeds get above 250 Mb/s, online speed tests are no longer valid as bandwidth measurement tools. One service provider's engineer went so far as to say their own speed tests are not valid and they use a competitor's speed test to test and troubleshoot, but even that vendor's test did not always provide valid results. This begs the questions:
    - Are we getting what we're paying for and how do we know?
    - How can we tell we're having bandwidth-related problems?
- One answer is to measure your bandwidth utilization using SNMP (Simple Network Management Protocol)
    - SNMP is a standard protocol that allows us to read and write status and configuration information on most network devices
    - This allows us to access device statistics that shows actual bandwidth utilization based on packet count
- Tools that you can use to display and graph your actual bandwidth utilization
    - PRTG (Paessler Router Traffic Grapher)
    - Solar Winds

PRTG


10.57.1.9 - Remote Desktop Connection
eth1 on ClearOS Firewall - Internal Interface
Graph: 30 Minutes
Graph: 24 Hours
Graph: 30 Days
Graph: 365 Days
Table: 24 Hours
Table: 30 Days
Table: 365 Days
Live Graph - 30 Minutes - 30 sec Interval
kbit/second
Bandwidth Traffic IN
Bandwidth Traffic OUT
Edit
Show Legend
Auto Refresh
Close
11:33 AM
6/26/2019

Misconfigured Firewalls and Edge Devices

- We have come across a significant number of districts where a vendor has installed a firewall or other edge device, configured VLANs, etc., and the device is installed or configured incorrectly and/or the routing is incorrect
  - This issue is known as Asynchronous Routing or a Routing Loop
  - This can impact overall network performance and can cause issues with HTTPS traffic and other secure traffic
  - If any gateway IP address on your network is not at the industry standard .1 or .254 IP address, there is a strong probability that your firewall, edge device, and/or VLANs are misconfigured

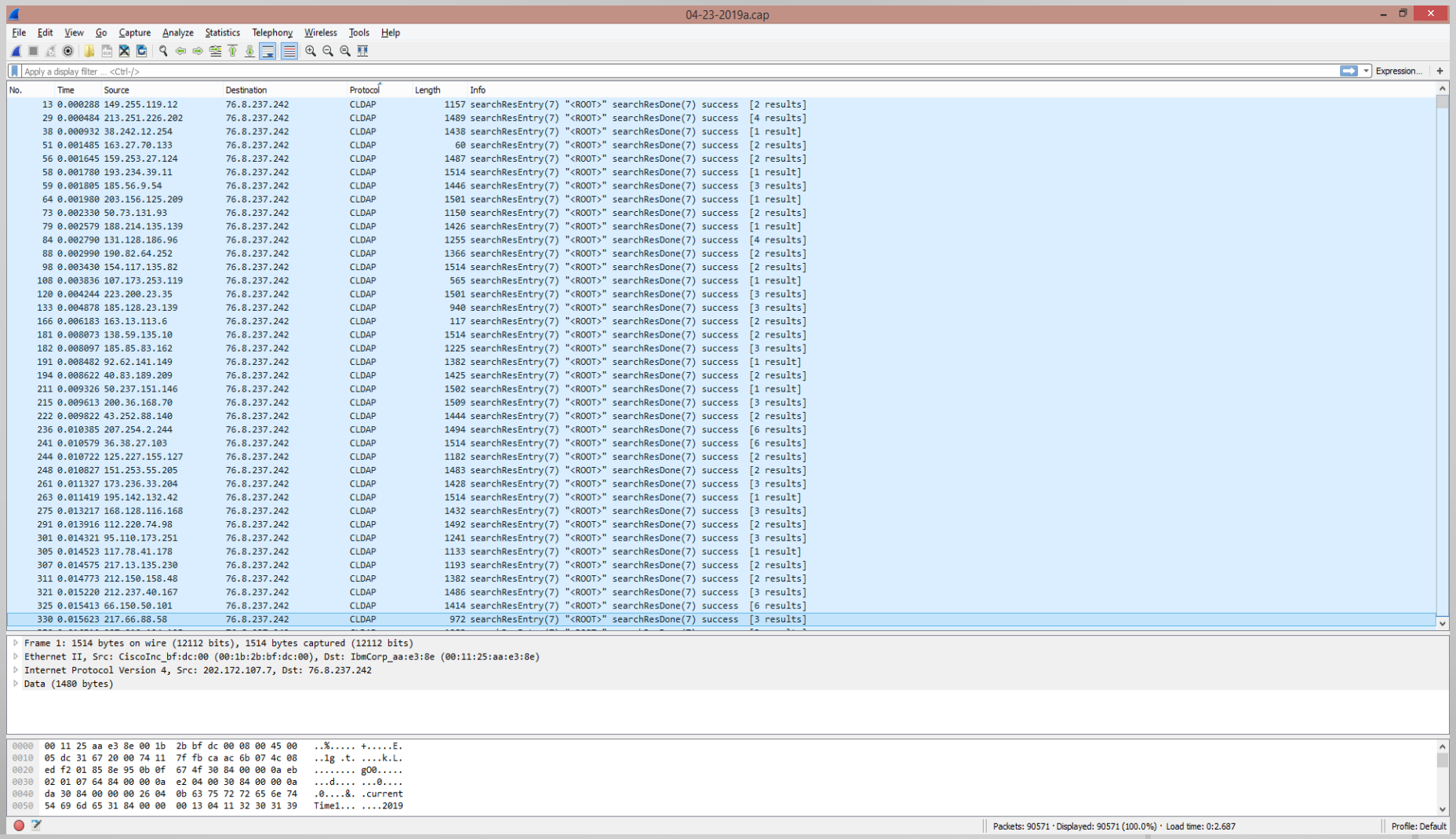
Denial of Service Attacks

- DDoS attacks in the K-12 world are becoming commonplace, especially during online testing
  - Students have figured out they can avoid testing by initiating a DDoS attack
- Attacks can be purchased anonymously online by anyone for just a few dollars per attack
- DDoS attacks cannot be mitigated locally, regardless of what your service provider tells you. They can only be addressed at the service provider level. Once the attack gets to your local Internet connection, there is nothing you can do on your end to mitigate the effects
  - Some service providers offer mitigation assistance as part of their service, others charge for it
  - A DDoS attack will prevent you from accessing your cloud-managed devices such as firewalls, etc.
- Tools that you can use to help determine that you are under attack and the type of attack include:
  - Wireshark (Ethereal)
  - PRTG
  - Solar Winds

Types of DDoS Attacks

- Volumetric Attacks
  - Overwhelms the network bandwidth and firewall CPU resources by flooding it with false data requests
- Application-Layer Attacks
  - These attacks focus primarily on web traffic in order to make the web resources unavailable to legitimate users
- Protocol Attacks
  - Focuses on disrupting and/or overloading connection tables and buffers in network equipment

Wireshark capture of a DDoS Protocol Attack



Ransomware

- Ransomware is another security issue which presents itself as a form of DDoS attack. We are seeing more and more network-level Ransomware issues
  - Ransomware will encrypt all of the files on a server or workstation and demand payment, usually in Bitcoin or other form of untraceable currency, to provide the keys to unlock the affected server or workstation
    - Even if you pay the ransom, quite often the keys you pay for don't work, and you've just wasted a bunch of money
- If the Ransomware attack vector was via a user with Administrative rights to the servers, all servers are at risk
  - You need to control all administrative access to critical network infrastructure, especially Windows servers
- If you are running Windows Hyper-V, if the host gets infected, all of your virtual servers get encrypted and are more than likely unrecoverable
  - Any network shares that are mapped to any infected server are also encrypted, meaning that your backups can be wiped out as well
- VMware runs a secure version of Linux and is immune to Ransomware. Snapshot backups allow rapid data recovery in the event that a Windows virtual machine gets infected with Ransomware
  - Virtualization Operating Systems such as VMware are preferable to Hyper-V for this reason

Other DDoS-style Security Issues

- Crypto Botnet Mining
  - This is malware that is similar to a virus, but is designed to utilize your network resources to “mine” cryptocurrency for the Botnet manager
  - Uses the cumulative computing resources of your network to generate cryptocurrency (i.e., Bitcoins)
  - An invisible CPU and network resource hog that can cause your network and affected devices to appear to run slow

DDoS Response Plan

- You should develop a DDoS Response Plan before an actual DDoS event
  - When an attack occurs, there is no time to think about the best steps to take
  - Make sure you and your staff are prepared and that everyone is aware of their responsibilities
  - Where possible, run simulated DDoS attack drills to judge the effectiveness of your response plan
- Key Response Plan elements include:
  - Systems Checklist
    - Develop a full list of assets you should implement to ensure threat identification, assessment, and mitigation
  - Form a response team
    - Define responsibilities for key team members to ensure an organized response to the attack as it happens
  - Define notification and escalation procedures
    - Make sure your team members know exactly who to contact in case of an attack
    - Include the list of internal and external contacts that should be informed about the attack, including your Internet Service Provider, law enforcement agencies, etc.

DDoS Warning Signs and Monitoring Tools

- Symptoms of a DDoS attack include:
  - Network Slowdown
  - Intermittent internal and/or Internet connectivity
  - Intermittent Internet connect

- Implement Network Monitoring tools such as PRTG and Solar Winds to alert you to possible DDoS attacks

- During an attack, use a tool such as Wireshark to capture the DDoS traffic for later analysis to help develop plans to mitigate similar future attacks

Data Breaches

- How do you know if one has occurred?
  - Most districts, if not all, do not have the tools, resources, or personnel to detect a data breach
    - School districts are the custodians of a lot of sensitive students, parent, and district personnel personal information
  - Usually the first time you hear about a data breach is from someone else
    - Users and vendors report unusual activity
    - Law Enforcement and/or other agencies notify you of a possible breach
- What are your responsibilities in responding to a breach?
  - Do not ignore a possible data breach, this is a serious event
  - Get law enforcement involved, especially the state cybercrime unit and the FBI
  - Tell the world - Warn your fellow districts and anyone else who may be similarly attacked
  - Staying silent is what the bad guys want you do, so they can continue exploiting others
- Have an Incident Response Plan

Incident Response Plan

- There are six key steps in a Data Breach Incident Response Plan
  - Analysis
  - Containment
  - Communication
  - Eradication
  - Recovery
  - Post-event Analysis

Incident Response Plan

- Analysis
  - Verify that it is an actual data breach and not a false alarm
  - Review your network and system logs for any abnormalities
  - Determine what systems have been attacked
    - Where did the attack originate from?

- Containment
  - Try to limit the spread and impact of the incident
  - Isolate the system if possible
  - Make a backup for forensic investigation

Incident Response Plan

- Communication
  - Alert everyone on the Incident Response Team
    - Include IT, HR, Legal, Operations and Management
  - Determine if law enforcement/FBI should be contacted
  - Determine if you need outside expertise to help
  - Determine if and how soon you should alert the public

- Your IRP should include a detailed communication plan, detailing who should be contacted in the case of an event, what message will be conveyed to them, and who has the authority to communicate on behalf of your organization

Incident Response Plan

- Eradication
  - Scan all systems for malware
  - Isolate and disable all accounts and services that have been compromised
  - Remove access to systems from suspect user logins
  - Change passwords, apply patches, and perform any other necessary reconfigurations

- Recovery
  - Prioritize what affected systems are most critical to operations
    - Be aware that recovery can take a while, especially if law enforcement agencies will be performing any forensic analysis

Incident Response Plan

- Post-event Analysis
  - Determine the time it took from the data breach to recovery
    - What changes can be made to improve this?
  - Are changes to policies, procedures, or equipment in order?
  - How effective was your Incident Response Plan?
    - Revise and test your new IRP with a simulated data breach drill

- Provide data security awareness training to all employees
    - Inform everyone what do, and what not to do, in the event of a data breach

Assessing Network Security Risks

- When should you perform a Network Security Assessment?
  - Industry Best Practices recommends twice a year at a minimum
  - After a security incident or breach
  - After changes to compliance laws
  - When you've made any significant changes to the network
  - When you have significant personnel changes, especially within the IT staff
- Who should you get to perform your Network Security Assessment?
  - Ciber (free through MDE)
  - Independent third-party
    - Can be expensive
    - Do not use a vendor that might bid on any recommended equipment or applications, as they may be biased in their assessments

Improving Network Security

- Use a hosted email service such as Office365 or Gmail
  - The email provider is responsible for providing security and backup
  - Use web browser access where possible
    - More resistant to viruses and other attacks
    - Ransomware won’t encrypt a remote browser-based email connection

Assessing Network Security Risks

- Tools you can use to perform Network Security Assessments include:
  - Metasploit
  - Nikto
  - Aircrack
  - Nessus
  - OpenVAS
  - Microsoft Baseline Security Analyzer

Bypassing Internet Filters

- VPN Tunnels
  - Users are bypassing the filters by using VPN tunneling apps and software such as Norton VPN
  - Since this a non-web browsing protocol, filters won't block it
  - VPN traffic can only be blocked at the firewall level
  - Many VPN tunneling apps are port-agile and difficult to block

- Tools you can use to detect and identify include:
  - Wireshark
  - Firewall Logs

- How to deal with users attempting to get around your Internet filter?
  - Enforce your AUP

Filtering Help

- CleanBrowsing.com is an inexpensive DNS-based filtering solution similar to Securely and the old OpenDNS.com filtering solutions
  - $30/month for 1000 devices, $50/month for 2000 devices
  - Easy to set up and manage
  - Provides detailed reporting
  - Recommended as a second-level filter, acting as a helping solution to your primary filter solution

Wireless Issues

- Wireless Access Points are only as fast as the slowest device on each wireless channel
- Many of our wireless systems were designed to service a large area (coverage model) with little consideration to the current ever-increasing density (density model) of wireless devices
- Wireless networks and coverage should be re-assessed on a regular basis to ensure adequate density and throughput

Other Concerns

- We need to educate our users about network security risks
  - Ransomware
  - Social Engineering
  - Smartphones are no longer immune to malware
    - More and more malware is targeting smartphones, specifically to steal access to a user's financial information
  - Keyloggers
- Increasing level of phishing and social engineering attacks
- AUP Enforcement

How to Request Ciber Engineer Assistance

- If you would like a Ciber Engineer to assist you and your district, please contact MDE or us directly

Donnie Cummins
dcummins@mdek12.org
601-946-0839

Glen Popiel
gpopiel@mdek12.org
601-209-9866

Questions?