Education Networks of America (ENA) sponsored and developed this white paper in collaboration with eLearn Institute and TechEdvantage. Dr. Tom Ryan, Chief Executive Officer of the eLearn Institute, was the senior analyst and Mr. James Aldridge, Principal of TechEdvantage, was the principal analyst. Dr. Ryan served in public education for 31 years as a teacher and high school principal as well as the Chief Information Officer of Albuquerque (NM) Public Schools for 11 years. Mr. Aldridge has worked in information technology for over 10 years and most recently served as the Chief Technology Officer for Metropolitan School District of Warren Township (IN). We thank Dr. Ryan and Mr. Aldridge for their overall guidance and authoring of the white paper.

ENA would like to extend a special thanks to the technology leaders of the school districts who participated in the vignettes included in the white paper. Their insight and recommendations regarding network security strategies in their districts will be immeasurably helpful to school districts nationwide. Participants include:

**Broward County Public Schools (Florida)**
*Mr. Tony D. Hunter, Chief Information Officer*
*Mr. Douglas G. Pearce, Director of Technical Support Services*

**Huntington County Community School Corporation (Indiana)**
*Mr. Thomas Ashley, Director of Technology*
*Mr. Ryan Wall, Network Engineer*

ENA also thanks Cory Ayers, our Director of Architecture, and Jay Power, our Director of Solutions Engineering, for their overall guidance and contributions to the white paper.
Introduction – Network Security Takes Center Stage

Providing a safe place for students, teachers, and administrators is essential for facilitating great teaching and learning. In today’s hyperconnected world, school district networks have become the foundational core for using and sharing instructional resources, information, data, and business applications.

With increasing threats to network security as well as a rapidly escalating number of ways to breach current defenses and gain unauthorized access to data and personal information, it is imperative that school districts implement stringent security practices to protect their students, staff members, and networks from virtual intruders.

District technology leaders take the responsibility of providing safe learning environments very seriously, but securing a network is a complex task that is impossible to achieve without the end users’ cooperation. In addition to implementing preventative network security design and configuration measures, technology leaders must develop policy strategies that inform stakeholders of risks, instruct on the skills necessary to assure safe use, and enforce security procedures and protocols. Ongoing network security monitoring, management, and communication are essential components of any strong district-wide network security program.

Security experts advise that security incidents are inevitable and that it is not a matter of if, but when an incident will occur. The Education Network Security in a Hyperconnected World white paper provides insight into potential network security threats impacting today’s school districts. It also shares key considerations and best practices every school district can implement for improving their network security as well as preparedness when an incident does occur. It shares the experiences and recommendations of two school districts—Broward County Public Schools (Florida) and Huntington County Community School Corporation (Indiana). The white paper as well as this Executive Summary include a Network Security Recommendations Checklist that serves as a quick reference guide for developing a comprehensive district-wide network security strategy.

As a leading network service provider for school districts nationwide, ENA hopes the information shared in this white paper assists school systems with their planning and prevention of network security threats and incidents.

ENA Education Networks of America®
WHY IS NETWORK SECURITY SO IMPORTANT?

Network security is becoming increasingly important with technology’s growing role in facilitating education and business operations in school districts. With greater use come more risks due to the additional complexities and configurations required to manage user access and identities across the network. As a result, school districts (and businesses in general for that matter) have experienced a significant increase in network security incidents. District technology leaders are concerned about protecting their digital resources and users. Many are identifying and implementing steps to improve their overall network security and to prepare for and mitigate security incidents when they occur.

Protecting school district networks from external unauthorized access as well as inappropriate use by internal users—such as students and employees—can be daunting. Striking a balance between widespread accessibility and stringent security is difficult, especially when known users can intentionally or unintentionally threaten the system. Both unintentional and intentional incidents can cause significant damage to poorly secured networks in the form of data loss, unforeseen network outages, and accidental breaches of confidential information by unauthorized individuals.

Network security problems have multiplied with the adoption of online assessments. States and school districts nationwide have experienced interruptions in their online testing due to network disruptions from distributed denial of service (DDoS) attacks. The increase in the number of DDoS attacks can partly be attributed to the ease with which even unsophisticated users can find and pay for a service to launch an attack. These services are often inexpensive, ranging from five to thirty dollars. Essentially, for the equivalent of a day or week’s worth of lunch money, an individual can purchase a DDoS attack that disrupts a school district’s network service and ultimately delays testing. Although purchasing a DDoS attack is cheap, their ramifications can be very costly to a school district. With the reliance on the network for instructional and administrative applications, any time the network is compromised, the result is a disruption in education and operations—the equivalent of a Snow Day or what now can be termed a Digital Snow Day.

A general awareness and understanding of the various threats that exist will help every school district remain vigilant about network security. The good news is that many of these threats are preventable. The not so good news is that no organization, including Fortune 500 companies, is exempt from attack. No entity can be 100 percent secure, 100 percent of the time. But with proper planning, processes, communication, and professional development, school districts can be prepared to prevent and mitigate many of the most common threats.

Buying a DDoS attack is easy and cheap. “It used to take a tech-savvy hacker to compromise the system, now it’s a credit card.”

Douglas G. Pearce, Director, Technical Support Services, Broward County Public Schools, Florida
TYPICAL NETWORK SECURITY THREATS INCLUDE:

- Distributed denial of service (DDoS) attacks
- Infection of systems by unauthorized or hostile software (virus, malware)
- An attempt at unauthorized access
- Unauthorized systems changes (hardware, software, or configuration)
- Compromised information integrity (damage to data)
- Loss of information confidentiality (theft of data)
- Misuse of services, information, or assets
- Theft of physical IT assets
- Damage to physical IT assets
- Reports of unusual system behavior
Key Considerations for School District Network Security

It is important to note that the success of any district initiative requires executive level engagement and sponsorship. Network security incidents impact the entire school system, which is why it is important to adopt a cross-functional team approach when developing a district-wide network security plan. Key departments to include when building a team are instruction, information technology, human resources, school police, communications, and legal services. Because every department is at risk, every department should be engaged in the safe and secure operations of a school district network.

“Everything new in the district involves IT.”
Tom Ashley, Director of Technology, Huntington County Community School Corporation, Indiana

Engaging managed Internet service providers adds an enhanced level of network security. Managed service providers deploy network monitoring systems that can proactively detect network trouble and assist in identifying network security incidents.
WHAT SHOULD EDUCATION TECHNOLOGY LEADERS DO?

A solid plan to address district-wide network security includes four main strategic areas:

1. **Policies and Procedures** – Clear policies and procedures are essential for maintaining network security in a school system. They also set the stage for proper executive sponsorship and responsibility to maintain ongoing ownership and relevance. Commonly-employed policies include acceptable use policies, remote access policies, and digital or electronic communications policies. These policies need to be clear, practical, and easy to enforce. The white paper describes these policies and successful implementation suggestions.

2. **Communications and Professional Development** – Once a district creates and establishes its policies, the next step is to craft an effective and impactful communications and professional development strategy. District stakeholders—teachers, staff members, volunteers, students, and parents—must be made aware of the importance of good security practices, the significant consequences incidents or breaches can have, and the policies and procedures that must be adhered to in order to provide a safe and secure network environment.

3. **Prevention Measures** – Simply stated, the best defense is preparation and prevention. Comprehensive network security is dependent on multiple prevention measures that work together to avert intrusions, attacks, and breaches. The key prevention measures to consider include infrastructure design and systems configuration, access control and authentication, and network monitoring.

4. **Incident Response and Mitigation** – As stated earlier, no network is 100 percent secure, 100 percent of the time; therefore, having an incident response plan and complementary mitigation strategy in place is critical for every school district. Developing an incident response plan requires the active involvement of a cross-section of district personnel. An effective incident response plan includes several components, all of which are outlined in the white paper. However, preparation, communications, and restoration are the three most critical components. Solid mitigation strategies limit your exposure, protect against the human factor, and build a strong line of defense.

These four strategic areas are outlined in detail within the white paper. We have also included a Network Security Recommendations Checklist with this Executive Summary, as well as the white paper, as a quick reference guide for district technology leaders to assist with developing a comprehensive, district-wide network security strategy.
Conclusion

Network security threats are real and looming. Experts predict that these types of incidents are on the rise and will only become more frequent, rendering every school district vulnerable to attack. For this reason, every school district should have a network security strategy in place to address the inevitable.

As described above, developing a comprehensive network security strategy involves implementing an integrated mosaic of four strategic areas of focus and action items including policies and procedures, communications and professional development, prevention measures, and incident response and mitigation plans. In addition to these strategic areas of focus, school leaders from Broward County Public Schools (FL) and Huntington County Community School Corporation (IN) offer the following recommendations.
As school systems continue to make the shift to digital, having reliable and healthy network environments will become more critical to carrying out the education mission and business operations of school districts. In today’s hyperconnected world, school districts need to adopt a holistic approach when creating their network security strategies. From forming strategic partnerships with managed service providers to effectively leveraging cloud-based resources to developing impactful stakeholder communications, district technology leaders must take steps now to protect their network from attack. The components detailed within the white paper provide district technology staff with the blueprint they need to create an effective and impactful approach to safeguarding their network security.
Network Security Recommendations Checklist

This checklist is designed to assist in a quick review of your K-12 district or school’s network security planning. It includes key areas such as planning, policies, communications and professional development, and technical infrastructure design and prevention measures. The checklist is intended to help identify gaps in your planning or prevention processes with the intention of improving network security.

INSTRUCTIONS

Use the checklist as a tool to research and collect information on your district’s or school’s network security best practices. In the box next to each category, rate your level of readiness using the following scale:

0 = No evidence of best practice exists
1 = Awareness – Some verbal awareness exists, but it is not documented or communicated
2 = Adaptation – Some documentation exists for some of the best practice components, but it has not been updated in the last 12 months or is incomplete
3 = Best Practice – Evidence has been updated in the last 12 months and is well documented and communicated

Planning

Executive Sponsorship

There is an executive leadership team that meets regularly to address network security health and wellness. There is a role and responsibility matrix that identifies accountability, sustainability, reporting, and communication. Team should include leaders from a number of different stakeholder groups, such as:

• Technology
• Human Resources
• Legal
• Instructional
• Communications

Network Risk Assessment

The District/School conducts periodic network risk assessments which:

• Identify network security assets
• Identify the risks and threats corresponding to these assets
• Define the potential loss or impact to the system from the identified risk or threat
• Evaluate direct and indirect effects/costs of these risks
• Recommend remediation for risks. Include level of effort and cost associated with mitigation
Security Policies and Procedures
The District/School has developed published security policies that correspond to the school’s instructional, operational, and technical design.

Communications
The District/School has developed proactive communications strategies.

Professional Development
The District/School has ongoing professional development and documentation.

Incident Response Plan
The District/School has created an incident response plan and procedures that include the following areas:

- Description of roles and responsibilities of team members and external service providers – know who to call and what they can do to help.
- Identification of possible risks and development of corresponding risk mitigation strategies
- Preparation for unique incidents that may require unique responses
- Verification that an incident really did occur. Verification of an incident before you communicate is essential as communication that is not accurate contributes to an erosion of trust.
- Restoration of instructional and/or business continuity. Continuity plans are business plans not IT plans. How do you keep the “lights on” when technology is off?
- Communication procedures that identify who needs to be communicated to and in what timeframe. Communication must be clear about what happened and what steps are being taken to mitigate the incident. Focus on issue resolution instead of finger pointing.
- Communications templates that can be used in an emergency. They can be altered to fit the incident, but having them prepared in advance saves time.
- Security audit process to determine how the incident occurred and identify the vulnerability and potential continued risk
- Remediation or mitigation strategy to make sure the risk does not continue
- Evaluation process to review and improve the security evaluation process

Policy Development
Policies form a foundation for any network security program. Policies define how organizations will approach security, how staff and students are to approach security, and how certain situations will be handled. The following are considered baseline best practices for policy development.

The District/School has a number of policies that were developed and approved by the Executive Sponsorship team.

The District/School has a current Acceptable Use Policy for Staff and Students defining the intended uses of the network that includes, but is not limited to, the following areas:

- Who should and should not have access to the network
- Clearly defined prohibited activities based on past experience “use cases”
- Blanket statements that address engaging in unlawful activities
- A Monitoring Disclosure statement
- Consequences for non-compliance
The District/School has a Digital Communications Policy to assist in preventing viruses and malware as well as define issues surrounding cyberbullying, defamatory communications, and social networking. The Digital Communications Policy includes, but is not limited to, the following areas:

- Appropriate use of written, audible, and visual communications
- A statement defining types of security issues (e.g. malware, viruses, spoofing)
- A Monitoring Disclosure statement
- Consequences for non-compliance
- The person(s) in charge of enforcing the policy
- Contact information for reporting malicious or suspicious activity
- Clear statements concerning FERPA, COPPA, CIPA, PPRA

The District/School has a Remote Access Policy that defines standards for connecting to the organizational network from outside of the physical network and security standards for devices that are allowed to connect. The Remote Access Policy includes, but is not limited to, the following areas:

- Clear definition of secure remote access methods (e.g. OOB, VPN, SSH) and clear definition of unauthorized, non-secure methods (e.g. RDP, telnet, http)
- Statement of internal resources available through secure remote access
- Statement of internal resources not available through remote access
- Anti-virus and malware prevention software standards needed on devices used for remote access
- Guidelines for requesting, approval, and denial of remote access

Communications and Professional Development

Communications and professional development (PD) should be provided for all individuals who have access to network resources or the Internet (teachers, staff, administration, students, volunteers, and parents). PD should be delivered frequently and in a variety of easily accessible formats such as documentation, webinars, face-to-face instruction, videos, and online classes. The following are considered baseline best practices for network security professional development:

- Distribute and communicate Acceptable Use and Digital Communications Policies to all district stakeholders listed above with acknowledgement or receipt to appropriate administrator or staff
- Make all policies available to everyone online
- Distribute and communicate the legal definition of state and federal laws and regulations (e.g. FERPA, COPPA, CIPA, and PPRA) to all school personnel
- Make definitions of state and federal laws and regulations available to everyone online
Provide real-world examples of threats and attacks that have already occurred in other districts to all internal personnel

Provide everyone with basic knowledge of and common vocabulary for possible threats such as virus, malware, phishing, and social engineering

Provide all users with tips and recommendations for proper system access etiquette, including:
- Protect your password, do not display or give out
- Use an alphanumeric password that is at least 8 characters long
- Refrain from using a district account for personal use
- Do not allow a user to use a computer you have already logged into
- Log out of a computer when you are finished or walk out of your room
- Refrain from logging into more than one station at a time
- Do not open any attachments from others that you do not know
- Do not open any attachments with the file extension (.exe)
- Do not respond to emails asking for sensitive information
- Report any suspicious activities or emails

Infrastructure Design

Careful attention to infrastructure design and systems configuration will create security standardization directly contributing to reduced vulnerabilities, threats, and attacks. Having a clear understanding of every network component and its configuration capabilities is very important. A regular assessment of infrastructure should be performed to identify each network supporting device and its function within the organization’s infrastructure. Best practices are outlined below.

Internet Access. Some best practices include:
- Use filter lists that match the District/School’s Acceptable Use Policy
- Consider bandwidth shaping to decrease non-critical application usage to preserve bandwidth if availability is restricted
- Distribute Network Address Translation of public IPv4 addressing across locations or private networks
- Where possible, scan for malicious payloads (e.g. email, http, ftp)
- Engage a network service provider that has DDoS mitigation capabilities and strategies in place to assist you

General inventory of current security technologies. Performing an end-to-end network supporting device identification assessment can uncover the information technology leaders need to address critical security gaps. The components may include:
- Firewall
- Router and switch infrastructure
- Wireless network devices
- VPN
- Networked end user devices
- Intrusion prevention
- Content security
- Identity management
Selected network supporting devices are listed below along with best practice recommendations.

**Firewall best practices include:**
- Latest patches and updates are installed
- Effective filters are in place to prevent malicious traffic from entering the perimeter
- Unused ports are blocked by default
- Unused protocols are blocked by default
- ‘Deny All’ should be the default posture on all access lists – inbound and outbound
- IPsec is configured for encrypted communication within the perimeter network
- Intrusion detection is enabled at the firewall
- Careful use of 1:1 Network Address Translations (NAT)
- Use of Port Address Translations (PAT) for Internet facing services
- Distribute NAT addressing between locations and services
- Logging enabled and audited
- Routine audits for unused or legacy rules
- Employ management user authentication and authorization with user accounting
- Routinely back up configurations and audit changes

**Router best practices include:**
- Latest patches and updates are installed
- Standardize router configurations
- Assign static IP addresses to all management interfaces
- Block known vulnerable ports
- Use only secure routing protocols that use authentication
- Use the most secure remote access method your platform offers (typically the newest version of SSH)
- Disable telnet and other remote access methods not used
- Use strong passwords for both remote and local connections
- Ingress and egress filtering is enabled, incoming and outgoing packets are confirmed as coming from public or internal networks
- Web-facing administration is disabled
- Directed broadcast traffic is not received or forwarded
- Unused services are disabled
- Logging is enabled and audited for unusual traffic or patterns
- Large ping packets are screened
- Restrict remote access to only known management networks
- Employ management user authentication and authorization with user accounting
- Routinely backup configurations and audit changes
Switch best practices include:

- Latest patches and updates are installed
- Standardize switch configurations
- Assign static IP addresses to all management interfaces
- Use strong administrative passwords
- Use VLANs to segregate traffic types and reduce broadcast domains
- Unused administrative interfaces are disabled
- Unused services are disabled
- Available services are secured
- Employ management user authentication and authorization with user accounting
- Routinely backup configurations and audit changes

Wireless network device best practices include:

- Use SSIDs that cannot be easily associated with your school
- Do not broadcast SSID not meant for casual use
- Use 802.11x for authentication to your wireless network so only approved devices can connect
- Use the strongest encryption method possible, WPA2 Enterprise preferred
- Never use WEP encryption
- Only permit guest network connectivity to connect to the Internet, not to internal resources
- Apply bandwidth restrictions to guest or open networks

Access Control and Authentication

Access control and authentication are two of the most important foundations of network security. In short, these are the fundamentals of who can access your systems and resources as well as authenticate that these individuals are who they claim to be. If these two pieces are not addressed appropriately, any other security efforts could be rendered ineffective. The following are best practice recommendations:

Access control and authentication

- Implement password management solution(s) (e.g. identity management, single sign-on)
- Keep passwords confidential (don’t write password down)
- Create strong password guidelines
  - Password should be at least 8 characters long or longer
  - Use complexity - alphanumeric, upper case, lower case, symbols
  - Don’t reuse passwords
  - Force password changes every 90 days
**ENA** is the leading provider of managed Infrastructure as a Service (IaaS) solutions to K-12 schools and libraries. In 1996, ENA created one of the first statewide K-12 networks in the U.S. and has earned a reputation as experts in the design, deployment and management of broadband, Wi-Fi/LAN, voice and video solutions. Today, ENA manages multiple statewide and district-wide networks, including 15 of the largest school systems in the country, successfully serving approximately 5,000 sites; 570 school districts; 3.2 million student, educators, and administrators; 280 libraries; and 3.2 million librarians and patrons. We understand the business and mission of the communities we serve, and all of our solutions are designed to meet technology needs and allow for maximum flexibility while minimizing the burden on our customers’ administrative and technical resources.

For more information, please visit [http://www.ena.com](http://www.ena.com) or call 866-615-1101.

**The eLearn Institute** is a non-profit organization that is dedicated to transforming education through the effective use of digital learning tools. The central focus of the institute is to help schools and districts design, build, and “own” their eLearning programs. As a trusted partner and aggregator of digital resources, the eLearn Institute will help connect online educators and organizations to appropriate resources as they (a) develop appropriate eLearning models, (b) select quality content, (c) provide professional development for teachers, administrators, and staff, and (d) select appropriate hardware, software, and systems to build a high quality eLearning program. The eLearn Institute understands that having the right digital tools is one half of the challenge that educators and schools face, and using these tools effectively to building transformative educational models that support great learning is the other half of the challenge. The institute assists schools to create a facilitated community of online educators to share best practices, effective learning models, and new ideas specific to online and blended learning.

For more information, please visit [http://www.elearninstitute.org](http://www.elearninstitute.org).

**TechEdvantage** is an education technology consulting firm headquartered in Indianapolis, Indiana. TechEdvantage serves as a leading technology consulting firm for K-12 Schools and Higher Education through its experienced consultants, strategic vision, and the ability to serve as a client advocate by remaining manufacturer neutral. TechEdvantage is a trusted partner in the areas of strategic planning, technology assessment, operational analysis, information security, and digital learning design and integration.

For more information, contact James Aldridge, Principal of TechEdvantage at jaldrige@techedvantage.com.