Council of the Great City Schools

# Cyber-Security in Today's K-12 Environment

*By Member Districts of the Council of the Great City Schools*

Baltimore City Public Schools

Fresno Unified School District

OCPS

Miami-Dade County Public Schools

# About the Council of the Great City Schools

The Council of the Great City Schools is the only national organization exclusively representing the needs of urban public-school districts. Composed of 69 large city school districts, its mission is to promote the cause of urban schools and to advocate for inner-city students through legislation, research, instructional support, leadership, management, technical assistance, and media relations. The organization also provides a network for school districts sharing common problems to exchange information and to collectively address new challenges as they emerge to deliver the best education for urban youth.

# Cyber-Security in Today's K-12 Environment

## By

## Member Districts of the Council of the Great City Schools


Fall 2017

# Table of Contents

Introduction ..... 7
Establishing a Holistic Security Strategy ..... 9
Security Planning for K-12 Education Systems - Fresno Unified School District ...11
Resilience ..... 11
Collaboration ..... 12
Socialization ..... 13
Security Operations - Fresno Unified School District ..... 15
Authenticating Identity, Authorizing Access ..... 15
Incident Response ..... 17
Preventive Measures Against Attacks ..... 18
Disaster Recovery and Business Continuity Process ..... 19
Security Awareness - Miami-Dade County Public Schools ..... 21
Communication: A Key Component ..... 21
Security Testing ..... 23
Software Development Security - Baltimore City Public Schools ..... 25
A Lifecycle Approach ..... 25
Benefits ..... 28
Communication and Network Security: Designing and Protecting Network Security - Seminole County Public Schools ..... 29
Challenge ..... 29
Solution Overview ..... 29
Solution Details ..... 30
Working Toward Learning Continuity ..... 31
It's Really a Revolution, Not an Evolution - Broward County Public Schools ..... 33
Identity Management ..... 33
DDoS Attacks and Social Engineering ..... 34
Network Health ..... 34
Network Security Recommendations ..... 34
Conclusion ..... 37

# Introduction

## Welcome to the Digital Age of Education

Technology has ushered in a new era for teaching and learning in classrooms from kindergarten through high school, with digital learning tools now an integral part of the K-12 education environment. Students are living in a world where horizons for learning extend well beyond the classroom, school building, school district, and even any individual state. With these expanded horizons comes a responsibility for educators to provide environments where students are empowered to achieve academic and personal goals, be well prepared for success in college and career, and be productive, responsible citizens in our fast-paced and interconnected world.

Equipping our children with the 21st century skills they need for our digital age requires turning traditional classrooms into a digital-learning ecosystem and ensuring teachers have the professional skills and unfettered access to the tools they need for 21st century teaching and learning. This new environment requires considerable investment in infrastructure, hardware, software, online resources, and professional development.

This digital transition is not only happening in classrooms, but also in school district administrative and operational offices. Everything is going digital—from transportation and the management of food services to communication systems, procurement processing, and everything in between. Reliance on a digital network and the applications running over them are now mission critical. In fact, the latest "IT Leadership Survey" from the Consortium for School Networking (CoSN) identified the following top three priorities and challenges for school district IT leaders:

1. Mobile learning
2. Broadband and network capacity
3. Cybersecurity and student data privacy

As such, throughout this report, the reader should keep the following minimum considerations of recognized best practices and industry trends in mind.

### *Increased infrastructure capacity.*

The State Educational Technology Directors Association (SETDA) has developed recommendations for broadband capacity in school districts, based on the number of students served ("The Broadband Imperative II: Equitable Access for Learning," 2016). Based on these recommendations, large school districts (more than 10,000 students) should ramp up internet service to 2.0 Gbps and wide area network (WAN) services to at least 10.0 Gbps per 1,000 users by 2020-21 to stay ahead of the burgeoning demand for broadband access.

### *Increased focus on security.*

School district networks are being used for instruction, business, and information sharing on an ever-increasing scale and are increasingly interconnected. As recommended in the white paper published by Education Networks of America, the eLearn Institute, and TechEdvantage in collaboration with the Consortium for School Networking (CoSN) ("Education Network Security in a Hyperconnected World," 2016), education technology leaders should have a solid districtwide network security plan that includes (1) policy and procedures that address network use, (2) communications and professional development for all school-district stakeholders, (3) network intrusion prevention measures, and (4) incident response and mitigation strategies.

### *Increased reliance on cloud computing.*

As school districts move toward cloud-based solutions for instructional and business applications, the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and other related privacy rules and regulations add a layer of complexity to network implementation. School districts must ensure that personally identifiable information is securely stored, processed, transmitted, and otherwise managed according to established standards (Consortium for School Networking, "Protecting Privacy in Connected Learning Toolkit," 2014).

# Establishing a Holistic Cyber-Security Strategy

With the escalating rise in frequency and variety of security incidents and attacks affecting school districts, it is essential to establish a holistic approach to security. Developing a holistic strategy helps to focus efforts on different and critical components of the K-12 education technology infrastructure that must be secured. There are several security "layers" to consider that range from physical security to cloud security. It is important to differentiate each of these layers and develop a security strategy for each as outlined below:

1. Physical Security — In schools, physical security is very much about the security of brick and mortar buildings themselves as well as the students, faculty, and staff that learn, teach, and work in them. With so much focus on securing technology, it can be easy to overlook the interrelationship between physical security and cybersecurity, but one of the success stories provided by the Fresno Unified School District shows that close monitoring of network and content security tools can help children in need.

2. Network Security — Network security is focused on ensuring there isn't any unauthorized traffic flowing across the network, that no one is abusing or gaining illegitimate access to network-connected resources and that sensitive information is secured while it is traversing the network (data in motion). In schools across the nation, distributed denial of service (DDoS) attacks have been used to disrupt online testing and other important assessment activities. DDoS attacks are a form of network resource abuse, and mitigating those attacks is a critical component of network security. Seminole County Public Schools, for instance, discusses their three-pronged approach to designing and protecting network security later in this report.

3. Application Security — Application security is about eliminating software vulnerabilities that could lead to security breaches. As Baltimore City Public Schools demonstrates later in this report, thinking about application security throughout the application lifecycle--and particularly in the early requirements-gathering and design phases--is critical to overall application success and cost effectiveness.

4. Content Security — Content security is focused on protecting data at rest (for instance, in a database) and on complying with various local, state, and federal requirements for data security and privacy. In schools, discussions of content security are highly intertwined with discussions of student data privacy. Many organizations combine content security and application security into a single process, but as software development projects in K-12 become more sophisticated, and different teams work on the data layer and application tiers, thinking of content and application security separately can be helpful in ensuring a positive overall security posture. This can be a complex project, but Broward County Public Schools works to strike a balance between complexity and simplicity—as described in this report.

5. End-Point Security — End-point security is traditionally concerned with keeping malicious or otherwise unwanted and unauthorized software and users off your endpoint devices. Particularly in 1:1 environments, end-point security includes asset location tracking and processes for eliminating sensitive data from and reporting lost or stolen devices. Miami-Dade County Public Schools shares their approach to embracing multiple device initiatives while maintaining a secure network environment.

6. Cloud/Data Center Security — As noted above, schools are moving more and more towards cloud-based solutions. Cloud/Data Center security is focused on ensuring a school district's core computing resources, whether hosted in the cloud or on premises, are appropriately patched and segmented to prevent unauthorized access and contain any unauthorized access if it does occur. Cloud-based data centers and services are rapidly growing within the K-12 community as they provide multiple operations and cost-saving benefits. Using cloud resources provides both a security approach as well as new security considerations as highlighted in this report by the Fresno Unified School District and the Broward County Public Schools.

This white paper outlines key considerations for establishing secure environments, particularly for the large urban school districts that are part of the Council of the Great City Schools. Contributions from educators and information technology experts in the Baltimore City Public Schools, Fresno Unified School District, Miami-Dade County Public Schools, and Seminole County Public Schools provide recommendations, best practices, and examples addressing the important components of establishing a holistic security strategy.

# Security Planning for K-12 Education Systems

## Fresno Unified School District

**This section addresses:**

*• Network Security • Physical Security • Application Security*

## Resilience

### *Background and rationale.*

Large school districts are complex organizations, systems of systems, that include the coordination of educational platforms and practices (e.g., curriculum, instruction, learning, assessments, etc.) delivered to large numbers of students, and conducted with multiple operational logistics (e.g., transportation, food services, warehouse, facilities, and maintenance). A world-class, 21st century, education can no longer tolerate extended outages at schools or downtime for critical services, just as these things cannot be tolerated in other professional-service organizations. Technology infrastructure must be designed to withstand attacks and failures of systems' components where such resilience is warranted relative to probability, cost, and impact of failure. Even so, technological systems will inevitably fail, so education organizations have the responsibility to be ready and able to withstand system failures and continue operating while protecting their stakeholders.

### *Success story: Recovery from network outage.*

There are numerous success stories and exemplars related to resilience. Districts are moving to managed or self-provisioned dark fiber with built-in monitoring rather than the virtual-shared environment of carrier-managed switched ethernet. Resilience can also mean multiple logical and physical paths that connect schools to the local educational agency's internet hub.

During the first cycle of student testing using the Smarter Balanced Assessment Consortia, the Fresno Unified School District experienced a failure in a carrier-managed switched ethernet. The IT team was ready with line-of-sight radios to bridge between geographically proximate sites. On the morning of the second day, without a definite time for restoration of services by the carrier, the IT team deployed the radios and bridged two schools, creating a new pathway to the internet so both schools could continue testing.

### *Best Practices:*

- *Move to security embedded into services*
- *Identify and recognize risks and vulnerabilities as well as the interconnected nature of K-12 ecosystems*
- *Design systems and services with a design-for-failure mindset*
- *Design for resilience*
- *Consider the benefits of a diverse combination of technologies and providers*

## Collaboration

### *Background and rationale.*

Just as educational reform requires teachers to move out of silos and work within professional learning communities, so too does protection of critical information assets require collaboration within IT units, across district departments, beyond district boundaries with external partners, and to users of information assets. This is especially true in the interconnected, complex IT ecosystems found in the K-12 sector.

IT departments must work across teams to ensure the entire technology stack is secure from design to build, test, deploy, and patch; from server to endpoint; from private to public cloud; and across the interchanges with external agencies and partners. IT departments must move beyond their silo to collaborate with purchasing, facilities, human resources, and other areas to build a stronger security posture.

A district's partnerships with other agencies and partners can be leveraged to improve services to students, staff, and stakeholders. These partnerships can increase a district's attack surface and yet--with priority given to security, intentional design, and project practices--they can deliver the intended outcomes without substantial security risks.

### *Success Story: Student in crisis.*

In a crisis, collaboration must be swift. An incident occurred in the Fresno Unified School District where the content filter administrator became aware of a student searching topics related to suicide. The system administrator collaborated with teachers on special assignment who used the district's Student Information System to identify the student's school and schedule. The team contacted the principal and school counselor, so the student could be pulled from the classroom and receive counseling that might have prevented a tragic outcome.

### *Best Practices:*

- *Leverage partnerships with agencies and external entities to improve security controls*
- *Establish a culture of vigilance and ongoing audit of those controls*
- *Expand security resilience beyond cybersecurity into the design of processes, the organizational culture, and the executive suite*
- *Establish and enforce an acceptable-use policy that provides enforceable guidance on what is and is not acceptable in the use of district IT assets*
- *Establish data-sharing agreements that structure partner relationships with clear provisions for indemnification, data governance, security expectations, and conditions for remedy or termination*
- *Encourage a culture of collaboration by setting clear expectations for collaborative behavior within departmental routines*
- *Create incident response plans that clearly identify roles, communication protocols, and expectations for escalation to ensure incident resolution*

## Socialization

### *Background and rationale.*

Security compromises are often the result of social engineering or an attack that capitalizes on normal behavioral responses. For example, ransomware preys on people's curiosity and spear phishing targets specific users. Whaling attacks go after high-value targets, such as a fiscal services employee who receives a spoofed email from the superintendent requesting a copy of every W2 for the last year. The bounty for the hacker includes the name, address, and social security number of every employee in the district. A key aspect of any effective security program clearly must be socialization that ensures people adopt better practices.

### *Success Story: Password policy.*

A tiered password policy allows different groups of users, including staff and students, to have different requirements for password complexity. Staff members with limited need to use student data can have less complex password requirements than do data handlers or system administrators. Levels of complexity can be applied to students by grade level, according to the scope of access and ability of the student.

*Success Story: Device configuration management.*

The Fresno Unified School District uses Microsoft System Center Configuration Manager to track the known state of IT assets and process the initial configuration, patching, updating, and validation of configurations. The improvement and socialization of these practices across data center, network, and desk-side support staff result in consistent quality configurations on new computers (i.e., images), the timely rollout of security patches across the enterprise, and the effective targeted deployment of software updates (such as new assessments or instructional software). The automation of these processes has facilitated support for an ever-increasing number of computers.

# Security Operations

## Fresno Unified School District

This section addresses:

- *Network Security*
- *Application Security*
- *Physical Security*
- *Cloud Security*

### Authenticating Identity, Authorizing Access

Authentication is the process in which a system verifies the identity of a user. Authorization is the process in which the system verifies if the identified user has access or levels of access to a system. All systems rely on authentication and authorization; however, implementation may vary. In a local environment, authentication can be handled by a system such as Microsoft's Active Directory and authorization by Active Directory group membership.

A cloud service can use the infrastructure already in place with a federated trust such as Active Directory Federation Service (ADFS), which allows secure online transactions among partner organizations. In this approach, authentication occurs using your own directory service, eliminating the need to create new log-in credentials for the cloud service or share password information with a third party. An additional benefit of federated authorization is timely changes to the directory; for example, a fired employee with a disabled account will no longer be able to log into the service.

Accounts for educational institutions are unique in that there are multiple groups of users—including certificated staff, uncertificated staff, and students—each with its own set of needs and challenges. Well written acceptable-use policies help define what is suitable for each group to use and access; responsible-use policies take this one step further, moving beyond the black-and-white nature of an acceptable-use policy to include and encourage positive digital citizenship as well as accountability for actions online. To reduce risks associated with account compromise and following the principle of least privilege, each account should be assigned the minimal security rights needed for the user.

The organization's Help Desk provides a vital role in account management and front-line security defense. Help Desk staff assist users with issues related to account access and can also inform users of good practices. Employee account self-service portals can reduce the burden on the Help Desk and improve time-to-account reset for employees while using multifactor authentication. Either way, account resets and Help Desk requests should be logged to monitor for potential abuse or attacks.

Most user accounts are compromised by clicking on a link in an email, perusing the web, or careless password management. To minimize the harm of a compromised account, a separate privileged account can be created for administrative functions as well as for functions that a user won't often need to access. There are users both inside and outside of the IT department who need a greater level of access. For example, the payroll manager may need to approve checks for the pay period, a system administer may need to modify a report, and Help Desk staff will need to reset a user's password. These functions could be done using an administrative account in lieu of granting access to the user's regular account.

### *Groups and Roles.*

Managing accounts can be labor intensive, but the task can be automated. Users can be more efficiently managed by assigning individual accounts to a group or role, and then granting access for all assigned individuals based on that group or role. Security can be adjusted for the group rather than individual users. Products such as Microsoft Active Directory use group membership at the network level, and most student information systems allow for role-based security.

Security roles or groups may be defined by factors such as job title, department, functional group, or job function. Identity management can streamline this process further and generate accounts for new employees, assign predefined security roles, and update systems as necessary. A single system of record (such as the human resources system) defines new employees and changes in department or job title.

Successful permission management requires stakeholders to collaborate on the design of identity provisioning and permissions. If users feel the rules are tedious, draconian, or not based in the reality of job functions, they will find a way to subvert the system and negate any gains made. As noted previously, Fresno Unified created its multi-departmental Security Review Committee (SRC) to create the initial security roles for the student information system. The intent was to give all stakeholders a voice and ensure that decisions were made based on knowledge and input from different areas.

Account directories need to be reviewed on a regular schedule to highlight potential issues with identity management automation, disable inactive administrator or service accounts, and identify accounts that have unusual account activity or inactivity. A filterable report with job title, separation date, and date of last log-on can identify accounts that may need attention. It is highly unlikely that a teacher's account would be inactive, whereas a bus driver who does not need regular access to email may have little account activity.

*Physical Security.*

Keep in mind that "access control" includes physical access to technology as well as user account management. Data centers and control rooms need be locked and monitored, including for climate control and potential flooding. As buildings and classrooms get "smarter" with more technological devices and enhancements, security becomes an issue there as well. IT, facilities, and campus safety departments have traditionally worked in silos; however, collaboration among them can enhance student safety and protect assets.

Use of technology systems, such as video monitoring and DVRs, benefits from such collaboration. Video surveillance is a powerful tool for campus safety. Moving DVRs away from school sites and into physically secured central locations can prevent equipment tampering and damage as well as provide access for outside agencies, such as local police. Such projects require data-sharing agreements among the organizations.

## Incident Response

With respect to information security, it's not a matter of if but when there will be an attack or other incident. When a security incident does occur, an Incident Response Plan will enable an organization to focus on containment rather than identifying the people and processes that need to occur. A successful incident management program combines people, processes, and technology.

According to the SANS Institute, a security incident has one or more of the following indicators: violation of security policy, attempts to gain unauthorized access, denial of resources, unauthorized use, or changes without the owner's knowledge or consent. Incident management begins with clearly defining responsibilities and processes for addressing each of these indicators before any incident occurs. An incident response team with defined roles enables effective, efficient handling of the situation. Any single team member has limited capacity during a crisis and cannot manage multiple responsibilities concurrently.

In terms of process, addressing any incident follows a path of triage, remedy or mitigation, recovery, reporting, and review. The triage phase includes ascertaining the scope of the incident and which systems and users are affected. Mitigating the incident while preserving evidence for further analysis is a paramount activity. Recovery may include restoring from a backup, eradicating a virus, or containing a vulnerability. Reporting can be a delicate matter and may include external stakeholders or the media. A review or postmortem provides the organization with insight on the effectiveness of the response, guidance on preventing future incidents, and any breakdowns in processes.

Keep in mind that communications protocols are an important part of the Incident Response Plan. Decisions about how to report on incidents of various types should be made in advance, with draft communications prepared so that, when an incident occurs, administrators do not need to be distracted or take time away from resolving the incident to review language for timely communications to stakeholders, authorities, or the media. Note also that incidents that result in compromising privacy requirements under FERPA, HIPAA, or other regulations require reporting to the appropriate agencies.

## Preventive Measures Against Attacks

### *Background, impact, and rationale.*

A variety of preventive measures are available to address different sorts of threats. For example, preventive measures against the threat of unauthorized access by hackers, crackers, or employees or partners (unintentional or intentional) include solutions that protect and monitor sensitive information and privileged use. Preventive measures can also mitigate against the threat of destruction, interruption, and theft, including unintentional destruction of assets, systems failure affecting access to information and services, malicious code or network attacks that disrupt access to information and services, and environmental factors and people that damage IT assets.

A network monitoring system should be in place to log the status of IT services and track availability and changes to IT assets. This information can be used for forensic investigation during incident response or for correlation analysis to discover behavioral anomalies. Vulnerability assessment is both a process and a technology that assesses applications and their underlying stack for vulnerabilities, remediates those vulnerabilities, and provides ongoing monitoring of these applications.

Employ integrity protections to ensure access to and availability of critical IT assets are controlled and monitored. Such protections can include secure content management platforms, network and host-based firewalls, data loss protection tools, active network intrusion detection systems, and filtering services using sandboxing and machine learning. Active network intrusion detection systems or "next-gen" security platforms can actively inspect, identify, and disrupt intrusions through decryption of traffic and correlation of user-application-host behavior based upon machine learning. A layered defense of the data center can use both next-gen security platforms and traditional firewalls that protect application services and server ports. Security Event and Incident Management systems correlate security expertise and multiple sources of information including logs from directory servers, logs from network equipment, remote sensors, and logs from security appliances.

At a minimum, school districts should employ content and email filtering and inspection to reduce the likelihood that users will fall prey to nefarious actionable code in websites or email messages and attachments. Prevention requires building capacity of the IT department as well as awareness among the user community.

### *Best Practices:*

- *Socialize IT staff to the importance of configuration and change management as well as asset tracking*
- *Consider implementing a data center configuration management or Runbook tool to track high priority IT assets, their current configuration, and all changes made to these assets*
- *Standardize IT assets and configurations wherever possible*
- *Automate provisioning of IT assets, including initial configuration, changes, patches, and software updates*

## Disaster Recovery and Business Continuity Process

### *Background, impact, and rationale.*

Disruptions to the everyday work of organizations happen: an internet outage caused by a squirrel or a denial of service attack; a power outage caused by a backhoe or utility speculation; a data center outage caused by a malfunctioning HVAC unit or self- propagating malware. What varies for organizations is the frequency, probability, and impact of disruptions, and the readiness to prepare for, respond to, and recover from such disruptions. Disaster recovery focuses on preparation and recovery from disruptive events, while the business continuity process seeks to ensure the ongoing operation of the organization's work, regardless of disruptions (although capacity may be limited depending upon the nature of the disruption).

Disaster recovery considers what services must be restored and which critical IT assets recovered after the disruption, how to recover from the disruption to normal operations, and why the investment in the planning, testing, and actual recovery is necessary. Disaster recovery planning should consider the probability and impact of disruptions. A mature practice will extend to IT resiliency: Do all critical functions have at least two persons who can perform them? What happens if those persons are unable to perform their functions? What can be done to manage the risks of possible disruptions? Assuming the payroll data are recovered and the payroll software is working following the disruption, who will continue to process payroll? Where will they work, and what will they need to perform their work? Further, will there still be employees for whom to process payroll?

A disaster recovery plan begs questions of business continuity. The business continuity plan extends beyond IT to all critical functions within the organization. The organizational impact is assessed for each substantial risk to determine how to manage the risk as well as recover from and respond to disruptions to the organization's normal, critical operations.

## *Best Practices:*

- *Develop an initial disaster recovery plan, test its execution according to the documented plan, and update and improve the plan annually*
- *Implement steps to increase IT resilience to reduce risks associated with disruptions*
- *Participate in developing, reviewing, and updating the organization's business continuity plan*

# Security Awareness

## Miami-Dade County Public Schools

**This section addresses:**

• *Network Security* • *Content Security* • *End-Point Security*

## Communication: A Key Component

Regular communications ensure an enterprise stays abreast of current events and the evolving threat landscape. Sparse or infrequent communications allow information to become stale, doing little to reinforce secure or responsible online behavior. However, organizations must be careful to temper messages so they don't become overwhelming; users tend to tune out if they get hit with too much information or receive messages too frequently.

Responsible digital citizenship should be emphasized to help users form secure cyber habits. A user who is conscientious about her or his browsing routines at school is more likely to be so at home, and vice versa. Simply letting users know how easy it is to fall prey to exploits or hackers is often enough to pique their interest. Once you have their attention, the next step is getting them to understand that threats and vulnerabilities are ever present--just because they haven't seen or heard anything for some time, doesn't mean that they can return to unsafe practices. This is the digital equivalent to changing your eating habits, rather than going on a diet.

One often overlooked facet of security awareness is regulatory compliance. In the education sector, we are bound by a multitude of local, state, and federal mandates and regulations. These mandates and regulations may not necessarily be straightforward in terms of allowing users to adhere to them without deviating from their "normal" online behaviors. Without providing guidelines or policies and procedures for users, it may be unreasonable to expect them to achieve full compliance. Guidelines, policies, and procedures must exist to cover a wide array of scenarios, and users must be told that these documents exist. They should be written in a user-friendly style that makes them understandable to the layperson while being comprehensive enough to cover all areas of concern. It does very little if an organization documents everything in a format that most users doesn't understand.

Initiatives such as bring your own devices (BYOD), one-to-one computing, and take-home devices can often introduce wrinkles into a security plan by making it more difficult to control networked resources. Physically or logically segmenting these devices from the business or general instructional network is paramount to helping control the environment. As such, users should be given clear and explicit instructions

on how to ensure that they are connected to the appropriate network. A contract or acceptable use policy is a must; not only should it be informative as a user resource, but it should also serve as the foundation for data protection--not only for the user but also for enterprise assets.

Informing users of potential or imminent threats and teaching them how to be responsible digital citizens may help to avoid unfavorable situations, but it likely won't eliminate them altogether. Despite best-effort approaches to addressing the threat landscape, users can still intentionally or unwittingly circumvent established measures and place themselves in harm's way. While backing up data doesn't often appear at the top of "security awareness" documents, providing information to users about how, when, why, and where to back up data is crucial in helping users and the organization recover from the inevitable cyber incident. In addition, by providing clear information to users and making data available on more than one front, situations can avoid being exacerbated by insecure data storage and resulting data loss.

Several years ago, the district centralized the management of school-based technicians to make technical support more efficient. One of the more positive results of this reorganization is our ability to control the network environment and to disseminate pertinent information to our technicians. Meetings (both in person and online), conference calls, and email communications occur regularly to keep technicians "in the loop." The technicians, in turn, are aware of imminent threats and concerns and have the ability not only to mitigate them, but also to pass information along to end users.

We also observe National Cyber Security Awareness Month districtwide in October. Tips and tricks to help keep users safe when using connected devices are posted on student and employee portal pages, along with videos tailored to the various age demographics to engage our users with useful information.

## *Local Note:*

*Managing network security within a school district is an interesting proposition. Network resources are just as likely to be targeted by "hackers" from outside of the network as by students sitting in a classroom. The wide range of technical abilities also provides a fertile ground for unwitting victims. A layered approach to security and security awareness is necessary for mitigating concerns.*

*At Miami-Dade County Public Schools, we have various methods for communicating concerns to our users. For example, our "Weekly Briefings" system conveys information about topics of concern, ranging from notifications of new systems or procedures to alerts regarding cyber-security threats. For concerns that require more immediacy, email is used.*

## Security Testing

*Background, impact, and rationale.*

An organization should pay attention to vulnerability assessment testing in its environment. Often, vulnerabilities are introduced unwittingly and go undetected until well after they have been exploited. For organizations staffed or equipped to perform internal vulnerability assessments, these should be performed frequently to determine whether weaknesses exist within the infrastructure or systems. The goal is to find and repair vulnerabilities before they are exploited and a breach occurs.

Frequent and ongoing internal vulnerability assessments should be accompanied by periodic penetration testing (pen testing) performed by a trusted outside entity to uncover any vulnerabilities undetected by internal scans. New vulnerabilities are found in software and hardware (firmware) on a regular basis; passing a pen test this month doesn't mean an organization will still be vulnerability-free next month. Pen testing may be the only option for organizations that do not have the staff or expertise to perform internal assessments, and may also serve to augment internal efforts with different tools or methods of evaluation.

Utilities such as port scanners and service enumerators are helpful in providing a good initial overview of what may be an easy target. That gives us a starting point to protect our assets. Protecting high-value targets directly does not guarantee that they will not be compromised, however. When a hacker is unable to compromise a high-value target, she or he will often use any device that can be easily compromised as a jump-off point to enter your network and look for other targets. New vulnerabilities and exploits are released regularly, so regular assessments are necessary to remain in step.

### *Local Note:*

*A pen test is often like seeing the doctor for an annual checkup. It is generally cost prohibitive for school districts to enter into an engagement more frequently for this type of testing. At Miami-Dade, we began ramping up our internal assessment efforts to keep our network healthy between checkups.*

*In performing internal assessments, we initially identified high-value targets, such as SQL databases, financial servers, and other servers that held sensitive data but were essentially "set-it-and-forget-it" boxes that nobody interacted with directly on a frequent basis.*

# Software Development Security

## Baltimore City Public Schools

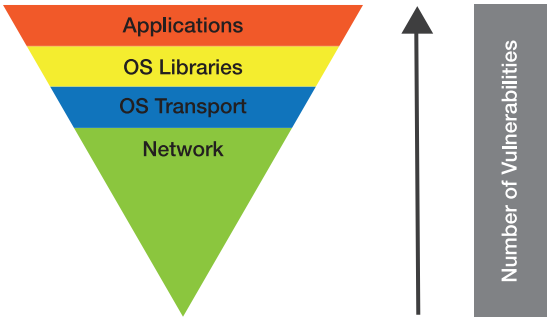
**This section addresses:**

- *Application Security*

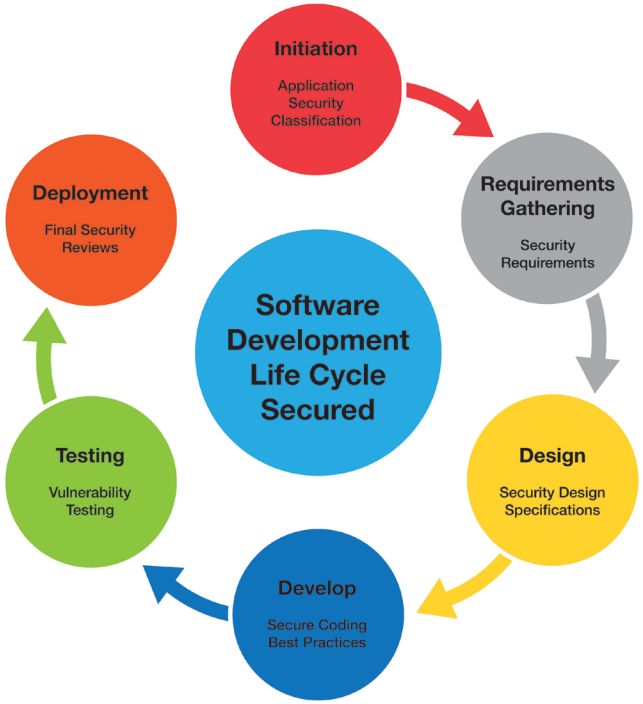
In recent years, school districts have been the target of sophisticated cyberattacks. Application software vulnerabilities continue to be among the top targets for exploitation by hackers, and these deficiencies have become one of the top information security concerns facing school districts today. The need for security is an integral part of application development, requiring consistent application of methodologies that adhere to agreed-upon security policies, objectives, and principles. It does not happen by itself, and the fact that many applications are outsourced adds to the complexity of ensuring that application development includes a strong integration of security components.

## A Lifecycle Approach

In conventional system development, software security is an afterthought and typically reactive in nature, incorporated sometimes in the development phase or when a vulnerability is discovered. But integrating software security at a later stage is cost prohibitive and time consuming. A more effective and cost-efficient way to protect information and information systems is to integrate security into every step of the development lifecycle: "The cost of removing an application security vulnerability during the design phase ranges from 30-60 times less than if removed during production" (as noted by NIST, IBM, and the Gartner Group).




Most organizations use some type of lifecycle framework to build applications. They are several standard models in use to fit individual circumstances and organizational needs. A typical process includes phases for initiation, requirements gathering, design, development, testing, and deployment ("Securing the software development lifecycle," 2015; "Security and resilience in the software development life cycle," n.d.). Ensuring that security is embedded into every phase will result in the most secure end-product possible.




## *Initiation.*

During this phase, staff assign an initial categorization of the proposed application (e.g., low, moderate, or high) based on the potential impact a security breach could have on organizations or individuals (e.g., loss of confidentiality, integrity, or availability). Some of the parameters that can drive the application security categorization include data sensitivity (sensitive or not sensitive) and technology used (web based or not web based). Security categorization assists organizations in making the appropriate selection of security controls for their information systems.

## *Requirements gathering.*

During this phase, a more in-depth assessment should be done. In addition to the preliminary assessment of the initiation phase, staff should map out and document security requirements and identify and review any organizational security and privacy policies and compliance laws that could affect implementation of the product.

### *Design.*

During this phase, staff identify security design specifications and requirements along with any potential system vulnerabilities using threat modeling and system design and architecture reviews.

### *Development.*

Here the development team goes over best practices and guidelines in secure coding. Code analyzer tools can be used to perform source code scanning to identify vulnerabilities and provide timely feedback to the developers. Peer reviews should be sought to mitigate or minimize vulnerabilities.

### *Testing.*

This is a critical phase to detect any software vulnerabilities not detected earlier. Comprehensive security test cases should be created using business processes and assumptions. The test plans should include unit testing, integration testing, stress testing, and user-acceptance testing. Dynamic analysis is an effective way of performing security testing. This approach consists of using automated tools to test for security vulnerabilities to identify vulnerabilities.

### *Deployment.*

During this phase, the system is installed and evaluated in the organization's operational environment, and server and network configuration reviews are performed--along with final security reviews to ensure all security risks identified in the prior phases have been fixed or a mitigation protocol exists. The software system should be continually monitored for performance in accordance with security requirements and periodically assessed to determine how it can be made more effective, secure, and efficient.

## Benefits

There are several benefits of incorporating security as part of the system development lifecycle:

- Early identification and mitigation of security vulnerabilities and problems with the configuration of systems, resulting in lower costs to implement security controls
- Identification of shared security services and reuse of security strategies and tools that will reduce development costs and improve the system's overall security posture through the application of proven methods and techniques
- Facilitation of informed decision making through the timely application of a comprehensive risk-management process
- Documentation of important security decisions made during the development process to inform management about security considerations during all phases of development
- Improved interoperability and integration of systems that would be difficult to achieve if security was considered separately at various system levels

# Communication and Network Security: Designing and Protecting Network Security

## Seminole County Public Schools

**This section addresses:**

• *Network Security* • *Content Security* • *End-Point Security*

Network security is at the top of the list of concerns for IT professionals, regardless of the industry. In public education, network security concerns move from the perimeter of the network inward to include segmenting, logging, monitoring, and encrypting as well as improving overall security through improved communication among all stakeholders.

## Challenge

The primary mission of a public-school district focuses on teaching and learning. School district IT teams must therefore position themselves to make the case that continued improvements and strengthening of the organization's networks directly support this mission. As leaders in this space, it is incumbent on IT professionals to develop a formalized strategy for maintaining a secure network, soliciting recurring funding sources to invest in needed network security tools, identifying and closing gaps in network vulnerabilities, and educating all individuals within the organization—students, staff, and faculty—on appropriate behaviors when using the network.

The challenge is to develop an agile strategy that maximizes limited resources to ensure appropriate measures are in place, while also creating an IT culture where network security is part of an ongoing journey rather than a destination. Ongoing assessments of network security must be part of the primary responsibility of any IT unit, whether large or small and regardless of industry. In public education, IT professionals bear what is arguably an even greater responsibility, considering that a secure network with appropriate stakeholder communication is part of preparing our next generation of digital citizens.

## Solution Overview

Possibly the best place to begin identifying network security needs is to assess the current state of the network. Awareness of current trends, available security tools, and services on the market can all be enhanced by a three-pronged approach:

1. Investing in professional development focused on network security and cybersecurity

2. Building relationships with local resources (e.g., law enforcement), with the goal of creating a collaborative team of security experts

3. Leveraging strong vendor relationships to maintain awareness of network security and cybersecurity trends in the market space

These strategies must lead to diligence in creating a network and cybersecurity strategy that includes an education component targeting all individuals in the organization. Like traditional emergency procedures, the mature network and cybersecurity strategy should include components ranging from identification of appropriate individuals to serve on a cybersecurity committee, hardware and services, incident response procedures, and an end-user education component.

## Solution Details

A strategic framework for looking at network security and vulnerabilities begins outside the network perimeter and moves inside to the network. Concurrently, a program for educating users on network use and data privacy best practices, such as creating strong passwords and the risks of malware and phishing, should be designed or procured, implemented, and moved to a sustained maintenance level.

A layered approach known as "defense in depth" is vital to network security. This architecture includes firewalls, intrusion detection and prevention systems, and content inspection systems including anti-virus, anti-malware, anti-spam, and URL filtering. These defenses should exist at the client, server, and perimeter (gateway) levels of the network. Layered security protections complement one another by catching what an individual component might miss.

Zoning through network segmentation is also essential for a solid security strategy. Computer systems providing mail, web, FTP, and other services for the internet should be in a "de-militarized zone" separate from the internal network's computer systems. In addition, user workstations should be in different security zones than servers. A network access control solution may also be implemented to keep guest mobile device traffic separate from all other internal networks.

Security information and event management (SIEM) solutions that provide the network security team with monitoring ability along with event-logging and alerting applications contribute to the overall health of the network and facilitate troubleshooting and identifying intrusion attempts. A deeper dive into network security will take into consideration strategic solutions that provide for data loss prevention (DLP) and encryption.

Penetration tests along with third-party assessments are valuable tools for identifying strengths and weaknesses in the perimeter of the network.

These tools and approaches are critical, but without doubt the most critical resource in the network security equation is the IT security team. Individuals who are passionate about their profession and connected to the teaching and learning mission of the organization are the heart of any strong security program in K-12 public education, and their contributions are vital. Investing in their professional learning must be deliberate and ongoing.

## Working Toward Learning Continuity

Strong practices and policies focused on network security and user education allow for what is often called "business continuity." In education, this is what allows us to make efficient use of every minute for teaching the individual child. Providing a stable, reliable, and safe network in public education means our teachers and learners can go about the business of being lifelong learners. Multiple examples exist showing the concrete costs incurred when an organization's security and data are breached. While maintaining a continuous improvement mindset in this area of network security will never offer complete protection, it establishes a posture that mitigates risk to a point that allows for "learning continuity" through appropriate responses ready for implementation in the event of a breach.

When it comes to network security and communication, the approach outlined is aligned in some degree to industry standards. As the world of cybersecurity changes almost on a minute-by-minute basis, so do standards and solutions that attempt to mitigate known and emerging risks. The constant in this equation, and oftentimes both the most challenging and the most rewarding component, is the technology user. Taking advantage of opportunities to educate our network guests in appropriate uses of technology and how to recognize if something suspicious is a real threat provides the greatest return on investment in both organizational and societal terms.

# It's Really a Revolution, Not an Evolution

## Broward County Public Schools

**This section addresses:**

***• Network Security • Content Security • Cloud/Data Center Security***

The Broward County Public Schools' Information and Technology (I&T) Department is committed to its vision of "Technology, enabling learning for all—any time, any place." We know the district's network is truly the foundational enabler for solutions that improve student achievement and operational efficiencies. As instructional applications, network connectivity, communications systems, and administrative services increase in complexity, it is the I&T Department's goal to keep things as simple as possible. Mixing simplicity with technical elegance is the ultimate balance the I&T Department would like to achieve.

As the I&T Department's responsibilities have expanded, Broward County engages its vendors and service providers for additional expert guidance and support. For example, we engage our Internet service provider, Education Networks of America (ENA), for their expertise in network design and ongoing support. We also reach out to our vendors for research and design services for projects that are specific to Broward's needs.

The biggest network security issues the I&T Department currently focuses on include:

- Identity Management
- DDoS Attacks and Social Engineering
- Network Health

### Identity Management

Users want easier access, but it also must be secure. Providing secure access, authentication, and provisioning for 271,000 students and 31,000 staff members to both control and allow access to appropriate resources is a daily challenge. Single sign-on for student and business applications is essential for the district to implement. With our personalized learning approach, students now have 15 or more applications available to them, which is just one of the reasons why single sign-on is so important. Password protection is one of the biggest internal network security breach threats faced. The human factor is difficult to manage, but education is an effective mitigation strategy when it comes to password protection.

## DDoS Attacks and Social Engineering

Distributed Denial of Service (DDoS) attacks are the biggest external network security threat. In the past, it took a highly tech-savvy person to hack a network and bring it down. Today, a non-technical person can easily purchase a hacking service to bring down a network for the equivalent of a few days of lunch money. Unfortunately, this is becoming a common occurrence in education, especially during test days. This can also fall into the category of social engineering, which is defined as a non-technical method of intrusion, used by hackers, that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. Like identity management, network security threats from DDoS attacks or other forms of social engineering results from the human factor. We are addressing these concerns with network designs that are redundant and resilient to mitigate the effects of attacks.

## Network Health

Two of the best strategies for maintaining network health include building a strong perimeter defense and diligently monitoring the network. The I&T Department is proactive in finding and implementing best-of-breed solutions. The team also engages service providers for firewall, quality of service, traffic management, and intrusion prevention services. In addition to having great tools, we emphasize the importance of having staff and/or service providers in place who are engaged in monitoring the network. Monitoring the system or network logs is a critical part of a school system's network security strategy. Having a diligent network monitoring team, whether it is composed of internal staff members or through a service provider, is a crucial component of a mitigation plan.

## Network Security Recommendations

Based on our experiences, we have several recommendations for school districts who want to stay on top of network security in a hyperconnected world.

1. Have the right technology infrastructure in place
2. Strike a balance between complexity and simplicity
3. Develop and implement identity management strategies and solutions for personalization and security management
4. Educate all your stakeholders and users on the importance of network security
5. Be diligent in monitoring the network or utilize a service provider who is
6. Implement strong perimeter defense services and solutions
7. Be proactive—research emerging technologies and implement best-of-breed solutions for perimeter defense and intrusion prevention

8. Engage service providers and vendors who not only have a deep understanding of the solution they are providing but also have experience and knowledge of the unique needs of the K-12 environment

9. Designate security manager to work with service providers and focus on all aspects of network security

10. Conduct an end-to-end network security assessment to identify gaps or areas of improvement

# Conclusion

In today's hyperconnected world, school districts need to adopt a holistic approach when creating security strategies. Security considerations must be embedded into virtually every aspect of school district operations and applications to be effective. From forming strategic partnerships with service providers, to effectively leveraging applications and resources, to developing impactful stakeholder communications and enforceable policies, to planning for the worst, district technology leaders must take proactive and defensive steps to protect their organizations.

While each of the school district briefs addresses a different aspect of security, there are several common themes that run through the best practices and information shared, as noted below.

- *Identify risks and vulnerabilities*
  It is important to be ever vigilant. Monitoring networks and other systems is critical, as are regular security audits and vulnerability testing. This can be accomplished using internal personnel and resources in addition to engaging service providers and external tools and resources.

- *Architect for resilience and diversity*
  It is not a matter of "if", but "when" your school district will be targeted or compromised. Designing resilience and diversity will help you address a security breach and recover more quickly.

- *Develop disaster recovery and business continuity plans*
  Not only is it important to develop disaster recovery and business continuity plans, but it is also important to test and update them on a regular basis. Disaster recovery and business continuity plans determine how a district will recover from and respond to disruptions and expeditiously return to steady-state operations.

- *Design for Failure*
  When designing your infrastructure, assume that components will fail or become compromised, and then build layers of resiliency around the concept of failure. This leads to developing multiple checkpoints and barriers for intruders and well as a robust infrastructure overall. Consider expanding security resilience into the design of processes, the organizational culture, and the executive suite.

- *Collaborate*
  Creating a culture of collaboration is important for implementing successful security strategies. Protection of critical information assets require collaboration internally across district departments, beyond district boundaries with external partners, and to users of information assets.

- *Communicate and train*
  Social engineering is becoming the most common and frequent form of vulnerability in organizations. Communicating and training all education community stakeholders ensure the school system stays abreast of current events and the evolving threat landscape. Proactive communication and training are the best ways to combat social engineering threats.

- *Establish clear policies and procedures*
  Establishing clear policies and procedures is essential for maintaining security in a school system. They also set the stage for proper executive sponsorship and responsibility to maintain ongoing ownership and relevance. Policies should be considered "living documents" that evolve to accommodate the needs of dynamically changing school systems.

The information shared in this white paper is not exhaustive, but designed to provide insight into key considerations for today's K-12 environments. The most important takeaway is what Seminole County Public Schools labeled "defense in depth". While their brief was primarily addressing network security, this "defense in depth" approach can and should be applied to each of the security layers discussed in the white paper. In looking to the future, we know that security attacks are not going away and are, unfortunately, becoming more prevalent. New tools and resources, such as enhanced visibility management and data analytics, are being introduced to help identify, mitigate, and eliminate these threats. The more we share information and needs with our internal and external communities, the better we will become in defending and protecting our organizations.


## *A Special Thanks to Contributing School Districts and Sector Partners*

*The Council of the Great City Schools Security Committee, led by Dr. Kenneth J. Thompson, Chief Information Technology Officer for Baltimore City Public Schools, would like to thank the contributing school districts and private sector partners for their participation in developing this white paper. Their insights and recommendations regarding security strategies will be very beneficial to school districts nationwide.*

***Baltimore City Public Schools*** is the third largest school system in Maryland with over 180 schools serving more than 82,000 students. Dr. Kenneth J. Thompson is the Chief Information Technology Officer leading the Information Technology Office. Mr. Shashikanth Buddula, Director Applications, also contributed to the Baltimore City Public Schools brief.

***Broward County Public Schools*** is the second largest school system in Florida with over 235 schools serving more than 271,000 students. Mr. Tony Hunter is the Chief Information Office leading the Information & Technology Department.

***Fresno Unified School District*** is the fourth largest school system in California with over 100 schools serving more than 73,000 students. Mr. Kurt Madden is the Chief Technology Officer leading the Information Technology Department. Dr. Philip Neufeld, Executive Director for Information Technology, authored and Ashley Aouate, Information Security Specialist, contributed to the Fresno Unified School District brief.

***Miami-Dade County Public Schools*** is the largest school system in Florida with over 392 schools serving more than 345,000 students. Ms. Debbie Karcher is the Chief Information Officer leading the Information Technology Services Department.

***Orange County Public Schools*** is the fourth largest school system in Florida with over 188 schools serving more than 203,000 students. Mr. Jim Pullam is the Chief Information Officer leading the Information Technology Services Department.

***Seminole County Public Schools*** is the twelfth largest school system in Florida with over schools serving more than 67,000 students. Mr. Tim Harper is the Chief Information Officer leading the Information Services Department. Mr. Tom Condo, Supervisor, DevOps Division, also contributed to the Seminole County Public Schools brief.

***Education Networks of America ® (ENA)*** is the leading provider of Infrastructure as a Service (IaaS) solutions to K–12 schools, high education institutions, and libraries. Since 1996, we have worked with our customers to ensure they have the robust and reliable high-capacity broadband, Wi-Fi/LAN, communication, and cloud solutions they require to meet the present and emerging technology needs of the communities they serve. Today, ENA manages numerous system-wide and statewide contracts, including 16 of the largest school systems in the country, successfully delivering IaaS solutions to more than 8.0 million users across the nation. For more information, please visit www.ena.com, call 866- 615-1101, or email info@ena.com.

***Worldgate*** is a management and technology consulting firm specializing in solutions to support the information technology needs of our K-12 and State and Local Government clients. We have a deep understanding of the very specific needs of these Public Sector clients and have successfully supported our clients through varied enterprise software implementations by truly understanding their needs and aligning with their unique cultures. For more information, please visit http://worldgatellc.com, call 571-349-0493, or email info@worldgatellc.com.


Council of the Great City Schools
1331 Pennsylvania Avenue, NW
Suite 1100N
Washington, DC 20004