FORSYTH COUNTY SCHOOLS

CYBERSECURITY
THE DETAILS MATTER

TABLE OF CONTENTS

THE DETAILS MATTER

We often hear that funding is a major barrier to having an effective security program, so we wanted to show that need not be the case. With that said, however, it **IS** important to note that some initiatives will have cost associated with them

To help you implement these important changes, and to encourage buy-in, we would highly recommend that you commission a cybersecurity committee. Many of the following items will be difficult- if not impossible- to enable without the support of the dedicated committee. The basic concept of the committee is to get buy-in and input from the entire organization, rather than just the technology department.

The following sections will be laid-out in three logical designations: baseline, intermediate, and advanced cybersecurity goals. Please understand that this is NOT an immutable list. Indeed, there are several discussion points which could easily be in a different category. Feel free to take these topics and adjust them to your organization.

CYBERSECURITY "TRUTHS"

- Nothing is unhackable. One must spend their time, efforts, and money wisely to protect from common attacks.
- People are fallible. No matter the amount of training or remedial instruction, people can and will make mistakes.
- Products will fail. Don't rely too much on products you buy, nothing is perfect. Be prepared for that.
- Communication is key. If stakeholders feel they are being misled or poorly informed, your efforts are likely to be unfruitful.

CYBERSECURITY GOALS

Baseline

- Limiting User Rights
- Systems Management
- Account Lifestyle
- Network Isolation

Intermediate

- User Training
- Federated Accounts
- Datecenter Isolation
- Network Analysis
- Cybersecurity Personnel

Advanced

- Comprehensive Security Actions & Enhanced Data Analysis
- Data Classification and Protection
- Handling Student Accounts

Learn to crawl before learning to walk

BASELINE

Limiting User Rights

The largest threat vector for your environment comes from your users. One of the easiest and most effective steps you can take to reduce your attack surface is to remove administrative rights from users on their computers. The cybersecurity committee will help you find the concerns of the district and give you an appropriate timeline to roll this out.

For those users who may need occasional elevated access to computers- such as technicians- it would be best practice to provide a separate account to be used for those times. For instance, no general user has elevated access in our system... everyone uses their district-issued account for basic job functions, such as email, printing, etc. and those accounts are very restrictive. However, we also provide a 'special administrator' account to those people who need it for their job requirements. That 'SA' account does not have email assigned to it, nor can it get to many websites. This naturally "isolates" the account should it become compromised.

Limiting User Rights Continued

Additionally, all these accounts should be network-authenticated. The use of local computer accounts should be discouraged, or outright banned, by policy. If local accounts are needed for troubleshooting, then they should have randomized passwords to limit the possibility of lateral movement should a workstation be compromised.

Users should not have access to anything more than what is necessary to do their job 'principal of least privilege'. Most importantly, one should require multifactor authentication (MFA) for all non-student accounts. The combination of MFA and removing administrative rights are two of the most successful cybersecurity measures that you can implement.

One final item to consider is the separation of user accounts from service accounts. The service accounts should be isolated from one another and purposed for a single service so to limit the possibility of lateral movement in the event an account is compromised.

Systems Management

The first part of any management system's plan should be operating system patching followed then by patching applications. It is important to communicate your patching schedule with stakeholders. For instance, we publish a patching schedule a year in advanced and send out a reminder email a few days ahead of time.

Operating System Patching

Client and server operating systems generally have security patches released monthly and your patching cadence should align with that schedule, too. It is important to test patches before applying them to production systems to mitigate the risk of unintended consequences.

Application Patching

Generally, application patches can fall into two broad categories; update/feature enhancements and security patches. Patching security flaws is where your organization should focus its security concerns on. You should have a process defined to evaluate the risk, acquire patch(es), test patch(es), and then deploy the patch(es).

Internet of Things

You now have to worry about the risks associated with nontraditional networked devices such as:

- HVAC controls
- Lighting systems
- Door access switches

It's important to have a close working relationship with the departments that operate these so that effective management can occur with little friction.

Unsupported/Abandoned Applications

The lack of security patches for an application does not necessarily indicate a lack of vulnerabilities; indeed, many applications may lack patches because they are no longer supported by the developer. You should have a process for evaluating and retiring legacy systems if the risk is too great to assume.

Endpoint Protection & Response

Implementation of endpoint detection and response (EDR) software. There are some excellent options on the market, and some might already be a part of your existing licensing or available from state department of education resources. No device should be allowed on the trusted network without a basic EDR installation.

- **Servers**
- **Workstations**
- **Network Hardware**
- **Printers**
- **Any device that connects to your network**

Firewall

Operating System firewalls have come a long way and should be heavily considered to be a core element to any security program in your organization.

Comprehensive Back up System

If data becomes corrupt/encrypted/lost, one must have the ability to recover that data in a clear and efficient manner. While there is not one, best solution- your enterprise and budget will largely impact what you can do- whichever product is selected should be chosen with security in mind.

Account Lifecycle

An account lifecycle management system helps reduce the likelihood of human error by automating account processes creation, editing, retiring, and tying them to a "source of truth" (SOT).

For our organization, we have designated our Human Resource Information System as the SOT for staff accounts and our Student Management System for student accounts. We have tasks setup to take the information from these systems and create/modify accounts to match their job role, location and to provision resources for the account type.

Though you may opt for a different SOT, the goal should be to automate as much of the account management process as possible. Manually creating accounts should be an exception for creation of guest/temporary accounts and service accounts.

Network
Isolation

One of the easiest ways to secure your infrastructure is by segmenting off your various networks and placing security logic at the ingress/egress points. This could be as simple as creating a VLAN or applying basic access control lists (ACLs) to as complex as hosting all networks on your firewall and inspecting/routing all traffic through it. At a minimum you should separate trusted and untrusted devices.

In our district we have all BYOT devices on a wholly separate network with no access to internal resources without coming through the firewall. We even have dedicated DNS and DHCP servers for this untrusted zone to logically airgap the network.

A growing concern is the proliferation of 'Internet of Things' (IoT) devices. Placing these devices in a network with no access to anything other than what is required for them to function can go a long way to secure your network.

Also don't overlook physical security. If possible, make sure access to network closets is restricted only to those who require it. Other measures can include:

- disconnecting unused switch ports.
- placing locking plugs into unused wall plates.
- using color-coded cabling for quick visual identification of unauthorized devices.
- logically naming ports on network switch if one is performing a network audit.
- use of IoT- scanning devices.

INTERMEDIATE

User Training

Without proper and regular training, nothing else you do will yield meaningful results. Training is the most time-intensive facet of cyber readiness. One must make it a TOP priority to train ALL employees because threat vectors will eventually target the path of least resistance: untrained or undertrained staff.

Basic cybersecurity training should be done at onboarding for new staff and a refresher should be done for all employees at the beginning of a new school year. Random phishing campaigns- coupled with an online training component are a great way to train users.

Federated Accounts

Most organizations rely on multiple systems for daily operation. This collection of systems may require you to manage multiple accounts for each person and requires all users to remember their credentials for each system. Federated accounts can simplify things while making your organization more secure. If your organization is using a modern authentication system then it is highly likely that you already have the tools needed to enable a federated system.

Datecenter Isolation

Datacenter isolation is placing all critical assets in a logical zone of protection. It can be as simple as creating a network dedicated solely for servers, routers, firewalls, and other core networking infrastructure or as complex as defining strict application and user access policies so granular that ONLY necessary traffic can pass.

At FCS, we have macro networks with access control lists placed on the gateway on each network. Those ACLs work in conjunction with server-based firewalls to limit access to most services other than those hosted by the server/device. Additionally, we BLOCK all access to the management interfaces in the datacenter from ALL networks other than the one hosting the Network Operations Center.

Network Analysis

Odds are that you're already collecting all the data you would need to troubleshoot, diagnose, and remediate any issue on your network. Indeed, every system has the capability to collect the data and in most cases send that information to a centralized logging system. Unfortunately, the background "noise" can drown out legitimate alerts. This is where advanced analysis tools can help. Using a combination of pre-built templated and artificial intelligence, these systems can help pinpoint the issues in your environment.

This can be an expensive endeavor. It is important to size the system properly so that it has enough capacity to handle your data without overbuying capability. We use tools like Splunk and LogRhythm to ingest our logs and supply reports/alerts for issues of concern.

Cybersecurity Personnel

It is difficult to have an effective cybersecurity program without the right personnel to oversee and manage those systems no matter how much cybersecurity services/software you have available.

Present the need for at least one person dedicated to cyber operations in your department to your cybersecurity committee. This person should be dedicated to cybersecurity operations. To fill this position it might be best to look internally for the right person. You want someone that has attention to detail, is a good problem solver and has an interest in puzzles and then train them up on technical skills.

ADVANCED

Comprehensive Security Actions & Enhanced Analysis

When making automated actions based off of the information you have been collecting from the myriad of network and system logs, you will want to take the time to ensure the log-backed actions are properly calibrated. An example is "impossible travel" alerts for user accounts. You will have to answers questions like: is the account truly compromised or is the user actually traveling or using a VPN? The only way to know if the alert is legitimate is to ensure that you're analyzing all your logs. Any system that logs a user's authentication information can be used for analysis. The key is to make sure that these systems are synchronized and can be correlated with each other.

It is important to filter these alerts through an automated system, preferably something with machine learning (ML) capabilities. This will enhance the efficacy of the alerts and ensure that only the alerts that matter get attention. Additionally, every new system purchased by your organization should be capable of "dumping" its logs to this analytic system.

Data Classification & Protection

Every organization has information that it needs to keep confidential. Your staff needs to be informed on how to handle this type of information. The best way to handle sensitive information is to classify it. Make classifications easy to understand. FCS has four major classification categories:

- Restricted
- Confidential
- For Internal Use Only
- Public

This seems easy enough to follow, but in reality it is one of the most difficult programs to implement. The difficulty stems from lack of cohesion between applications, interruption to well-engrained workflows, low interest in learning the new information, and a large "back catalog" of content needing to be classified.

Handling Student Accounts

Staff accounts are not the only accounts in the user environment. For every staff account there could be ten or more student accounts. Even though student accounts don't have as much access, that doesn't stop threat actors from using them to create mischief within that limited-rights universe. At FCS we have a highly diverse district, with students coming from nearly every country on Earth. Many students travel to other countries throughout the school year so we have to work to protect those accounts and ensure they have access to their classwork even when traveling. FCS is still working on making final decisions on how to handle this but we have narrowed the list of options to a handful:

- Allow students to enable MFA for their account
- Access coursework only through their FCS provided portal
- Use an FCS provided VPN

We feel it is important to restrict foreign access via student accounts unless they've enrolled in one of the choices listed above.

CONTACT

770-887-2461

cyber.forsythk12.org

tech@forsyth.k12.ga.us

1140 Dahlonega Highway
Cumming, GA 30040