SECUREWON

Proactive Approaches to Cybersecurity for Independent Schools

Association of Independent Schools in New England

December 10th, 2024

SPEAKERS

Wayne Audette

Founder & CEO at SecureWon

Wayne, founder of SecureWon, brings over 14 years of experience in managed IT and private security to deliver tailored cybersecurity and IT solutions for independent schools, non-profits, and municipalities.

He credits SecureWon's success to its dedicated team, fostering a client-focused culture that empowers organizations to focus on their missions.

Hank Bryant

Dir. of Edu Technology & Innovation at Nashoba Brooks School

Hank brings over fourteen years of experience working with students as a teacher, in the STEAM lab, and as the Director of Educational Technology and Innovation, guiding interdisciplinary learning.

At Nashoba, Hank has designed and taught integrated curriculum, supervised the Information Services team, and played a central role in strategic initiatives with the school's leadership. He has led the development of the school's STEAM Lab, One Device Per Student Program, and cybersecurity policies, overseeing multiple budgets to support educational and technology needs.

Justin Armstrong

CISSP, HCISPP, CCSP, MS

Justin, a security leader with 23 years of IT and risk management expertise, specializes in healthcare and education.

He excels in regulatory compliance (HIPAA, GDPR) and has developed security programs for SOC 2 and ISO 27001. With experience at MEDITECH and Tausight, Justin now provides CISO services, helping organizations build secure, compliant infrastructures.

Today’s Agenda

01 Key Trends for 2025

02 Understanding Impact

03 Proactive Measures

04 Case Studies

Never Forget What We Are Protecting

Safety & School Selection

Parents listed **"Safe Environment"** as the top reason they enrolled their child in a Private School.

Safe Environment

50%

Academic Quality

47%

Class Size

31%

Source: EdChoice Survey in partnership with Morning Consult

Safety & Security
Are Top Priority

AS IT IMPACTS

PROGRAMS & FUNDRAISING

STUDENT ENROLLMENT

SCHOOL SELECTION

Goals of Security

01

Protect people, property, resources, and data

02

Ensure Continuity

03

Protect against legal and financial risks

04

Protect REPUTATION

IT & Security

HERE TO HELP

1. Ease of Use
2. Resilience
3. Lower Costs Long-term
4. Operational Excellence

Trends In Threats

6,000+ Threats Targeted Schools in 2022

Many anonymous & on social media

1,300 Gunfire Incidents on School Grounds since Sandy Hook

436 deaths & 936 injuries

Data Breaches & Ransomware

36 Million Tips About Child Exploitation in 2023

Business Email Compromise

Wire Transfers, W2s and Other Confidential Data

SECUREWON

Protecting Data Protects Students

AS DATA CAN BE USED FOR:

→ Identity Theft

→ Bullying

→ Hate speech

→ Blackmail

A LOSS IN DATA IS A LOSS OF TRUST

Data Protection Myths

Data Protection Myth #01

MYTH

"It is IT's responsibility"

TRUTH

It is everyone's responsibility

SECUREWON

Data Protection Myth #02

MYTH

"Technology can solve the problems"

TRUTH

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

— Bruce Schneier, Noted Security Expert

Data Protection Myth #03

MYTH

"Hackers only target large organizations"

TRUTH

They go after easy targets. They cast a wide net.

Data Protection Myth #04

MYTH

"GDPR does not apply here in the US"

TRUTH

GDPR does apply if you advertise in the EU to attract EU students. States continue to approve new Privacy legislation every year.

SECUREWON

Data Protection Myth #05

MYTH

"Teachers don't need training on data protection."

TRUTH

Everyone needs regular training and periodic reinforcement.

SECUREWON

Data Protection Myth #06

MYTH

"Students don't need training on data protection."

TRUTH

Students are digital natives and need help understanding the risks and how to protect themselves.

MYTHS OVERVIEW

	MYTH	TRUTH
01	"It is the responsibility of IT"	It is everyone's responsibility
02	"Technology can solve the problems"	It's not a technology problem
03	"Hackers only target large organizations"	Hackers go after easy targets
04	"GDPR does not apply here in the United States"	GDPR does apply if you advertise in the EU to attract EU students
05	"Teachers don't need training on Data Protection"	Everyone needs training and reinforcement regularly
06	"Students don't need training on Data Protection"	Students are digital natives and need help understanding the risks and how to protect themselves

Strategies

01

Culture

02

Leadership

03

Do The Basics Well

04

Resilience

05

Prepare BEFORE The Storm

Tactics

The Obligatory Sun Tzu Quote

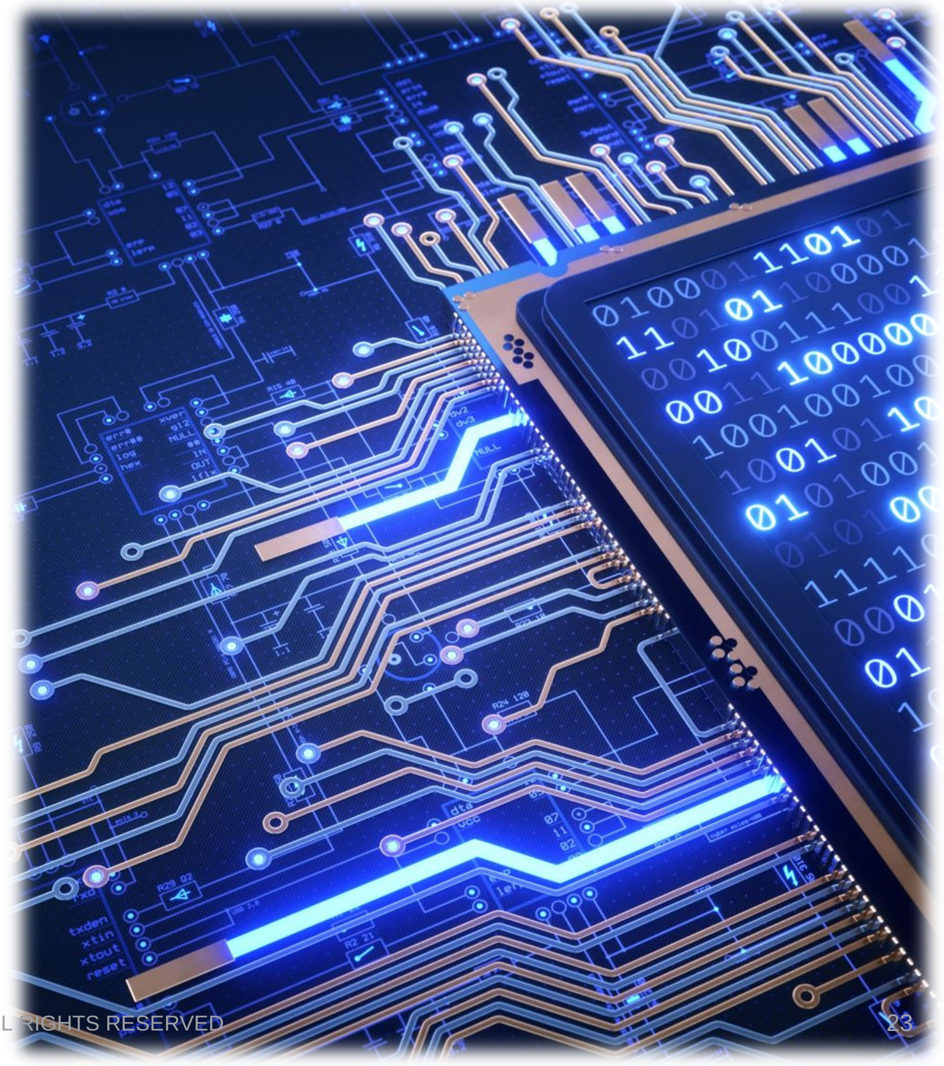
“If you know the enemy and know yourself, you need not fear the result of a hundred battles."

— Sun Tzu, "The Art of War"

Know the Enemy

Hackers Frequently Use

1. Phishing emails
2. Attachments (word docs & PDFs)
3. Malicious Links



Know Yourself

Do you know everything on your network?

1. Systems
2. Software
3. Vulnerabilities
4. AI Use
5. Free Software ("if it's for free, it's for me!")

Solutions & How They Can Help

- →Security Vulnerability Assessments
- →SIEM
- →Security Operations Center (SOC)
- →Cybersecurity as a Service (CaaS)
- →Business Continuity
- →Disaster Recovery
- →Secure Email Gateways
- →Moving to Cloud

Security Vulnerability Assessment

BENEFITS

1. Identify Vulnerable Devices & Software
2. Identify Vulnerabilities
3. Triage

THREE CHOICES

1. Take Updates
2. Add further protections
3. Retire the System

Security Incident & Event Management (SIEM)

What it does: Aggregates data from across all of your devices and networks

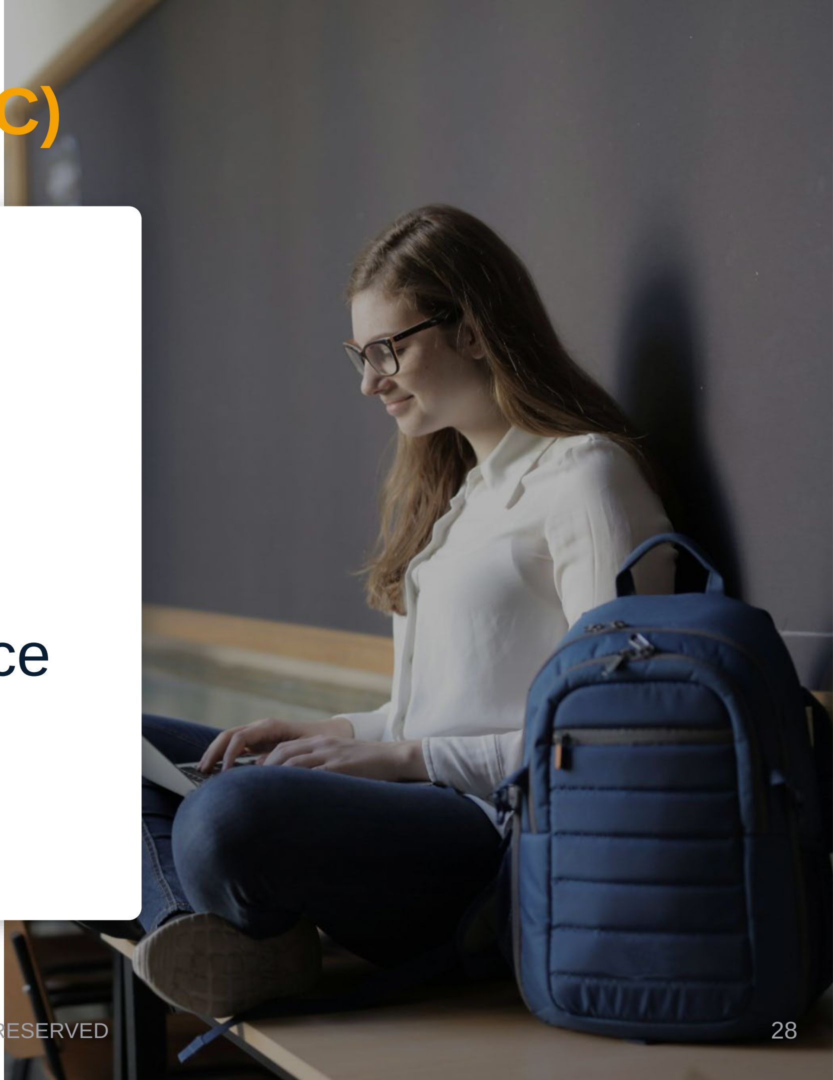
WHY IT'S IMPORTANT

1. Alerts On Suspicious Activity
2. Can Determine What Happened
3. Threat Hunting

REQUIREMENTS

1. Initial Setup
2. Storage
3. Constant Tuning
4. Experience & Well Trained Staff

Security Operations Center (SOC)



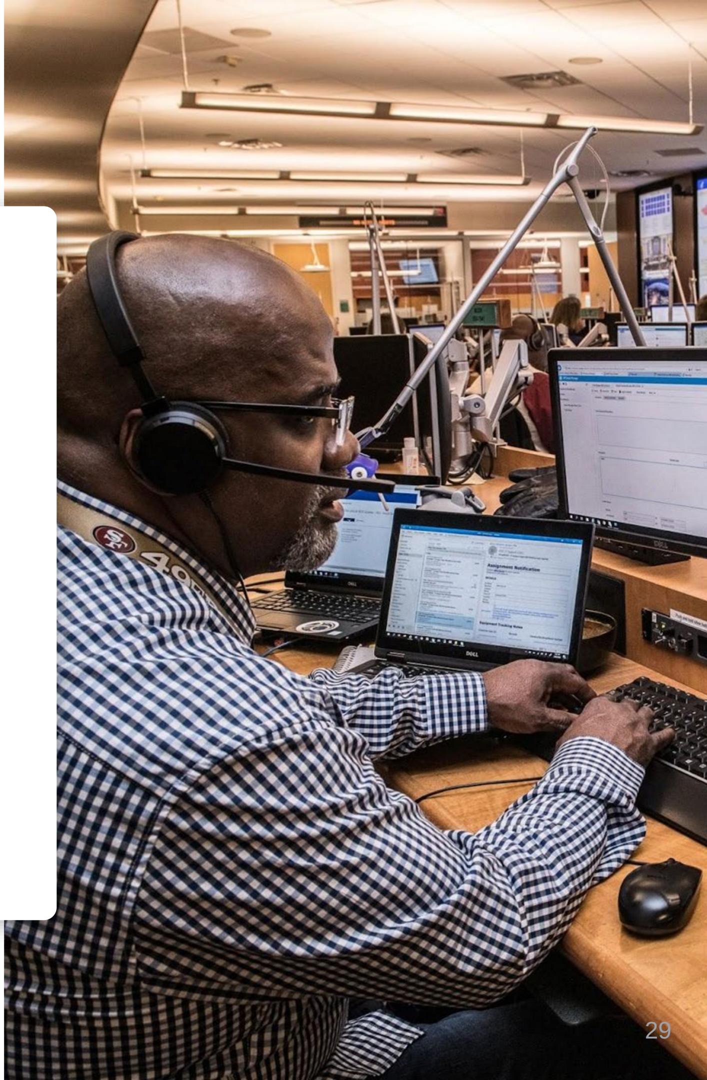
BENEFITS

1. Real Time
2. 24/7/365 Coverage
3. Staff with Real World Experience
4. Continuous Improvement

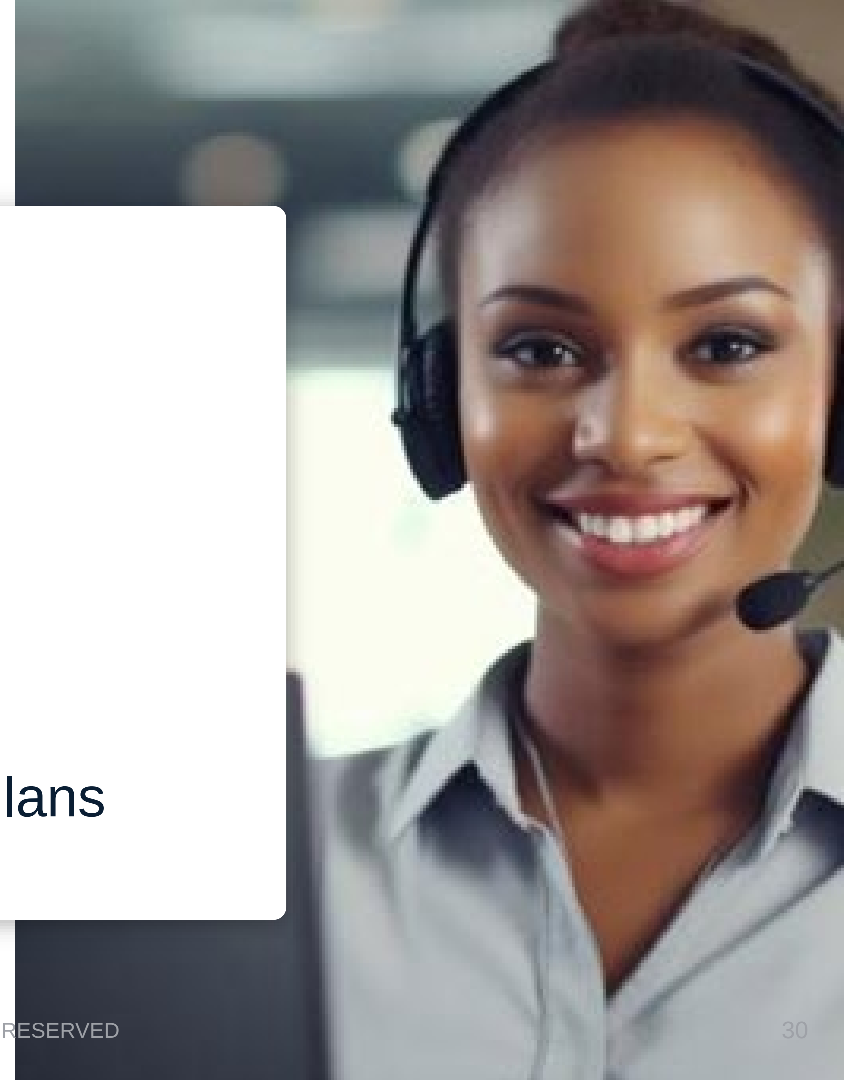
Cybersecurity as a Service (CaaS)

BENEFITS

1. Expert management of your IT Security
2. Strategy & Design for Resilience
3. Security Operations Center
4. Vulnerability Management
5. Incident Response
6. Cost Effective



Business Continuity



BENEFITS

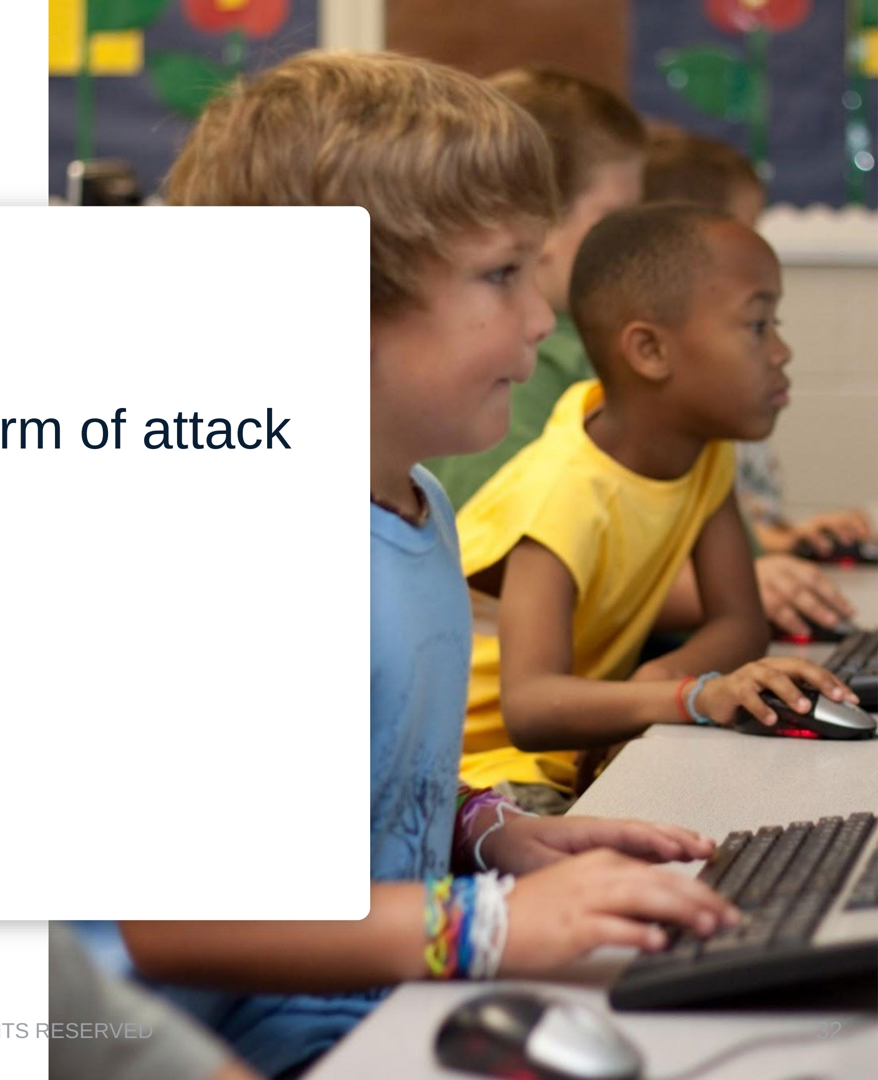
1. Plan for Resilience
2. Identify Critical Systems
3. Alternative Systems
4. BC Planning
5. Backups and Disaster Recovery Plans

Disaster Recovery

The Basics of Disaster Recovery & Backups

1. Backup critical data
2. Secure it off site
3. Verify that the backups actually work
4. Ensure that you have several people who can restore the systems

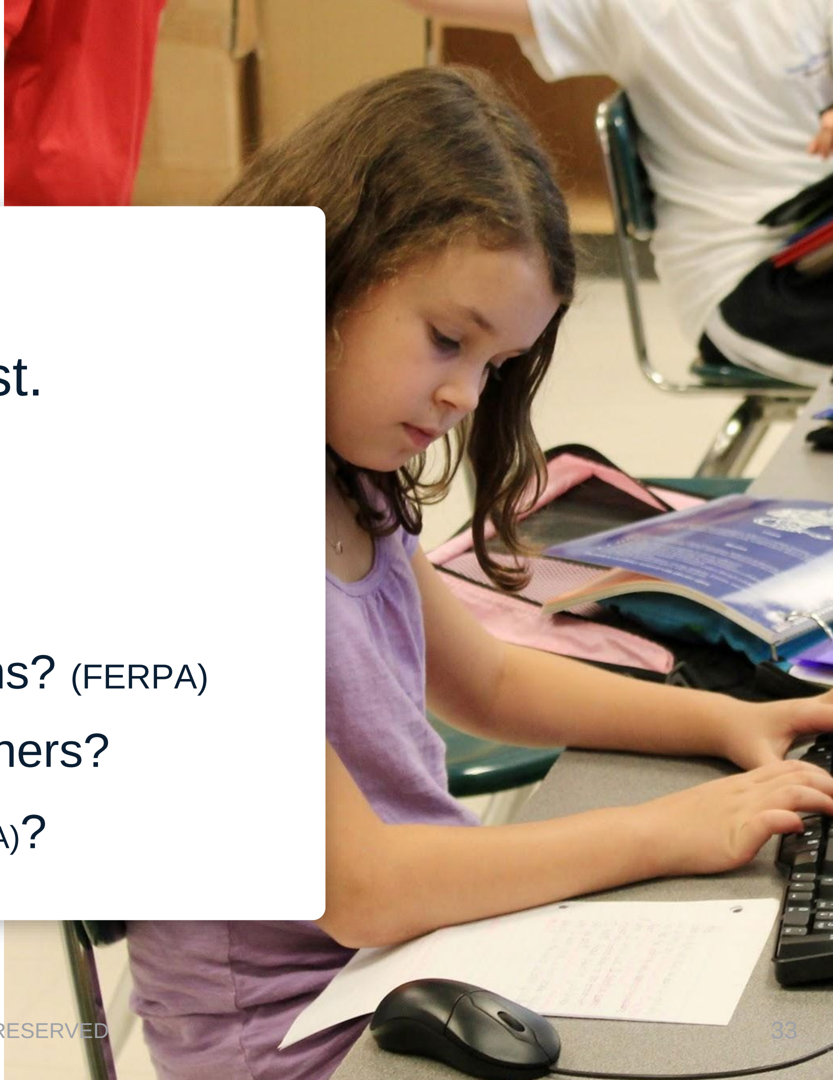
Secure Email Gateways



BENEFITS

1. Protection from most common form of attack
2. Spam Filtering
3. Phishing Protections
4. Malware Detection
5. Centralized Management

Moving to the Cloud



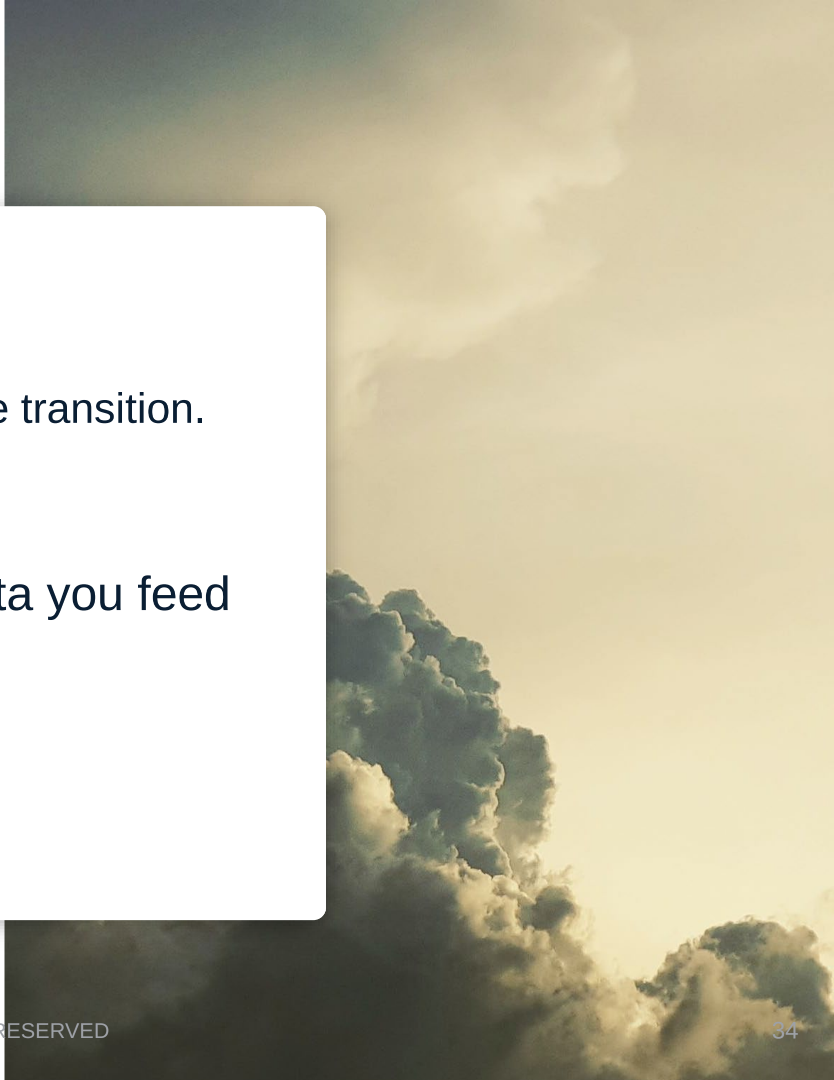
MANY ADVANTAGES

Ease of use, security, latest & greatest.

QUESTIONS TO ASK

1. How is our data protected? Backed up?
2. Does it comply with applicable regulations? (FERPA)
3. Does the provider share the data with others?
4. What is the Service Level Agreement (SLA)?

Cloud Considerations



Backups may still be needed!

Data loss can happen when there is an employee transition.

Use of AI

1. Privacy Policy? What happens to that data you feed into it?
2. Service Level Agreements
3. Inaccuracies ("hallucinations")
4. Ownership of output

STRATEGIES & TACTICS OVERVIEW

STRATEGY	
01	Culture
02	Leadership
03	Do the Basics Well
04	Resilience

TACTICS	
01	Security Vulnerability Assessments
02	SIEM
03	Security Operations Center (SOC)
04	Cybersecurity as a Service (CaaS)
05	Business Continuity & Disaster Recovery
06	Secure Email Gateways
07	Moving To The Cloud

CASE STUDY 01

OVERVIEW

A large school system in MA engaged SecureWon to perform a Physical and Cybersecurity Assessment of the municipality’s 21 physical school campuses.

SERVICES INCLUDED

1. Conduct a Physical Security Assessment to establish a security baseline for all district locations, based on leading standards.
2. Review current IT security documentation to identify areas for improvement.
3. Assess the “current” state of security operations and develop an “optimal” future state, identifying key gaps.
4. Provide actionable recommendations with a strategic implementation plan.

CASE STUDY 01

RECOMMENDATIONS

With rising school violence across major U.S. cities, we recommended that the City adopted physical security standards, training protocols, and a centralized technology platform.

Lessons point to six key recommendations:

1. **Strengthen Physical Security:** Invest in secure entrances, metal detectors, and cameras to prevent unauthorized access and enhance safety.
2. **Improve Emergency Plans:** Develop and regularly practice emergency response plans with coordinated drills to ensure readiness.
3. **Expand Mental Health Services:** Increase access to counselors, psychologists, and mental health training for early intervention.
4. **Invest in Safety Technology:** Utilize tools like threat detection software, automated alerts, and smart locks for campus security.
5. **Boost Community Engagement:** Collaborate with parents, law enforcement, and the community to support safety initiatives and encourage vigilance.
6. **Train Staff and Students:** Provide regular training in active shooter response, situational awareness, and basic first aid for emergency preparedness.

CASE STUDY 02

OVERVIEW
NASHOBA BROOKS

Located in Concord, Massachusetts, Nashoba Brooks School serves children in grades preschool-3 and girls in grades 4-8. The school focuses on developing character, confidence, and community while delivering personalized educational experiences.

THE CHALLENGE

Hank Bryant, Director of Educational Technology and Innovation at Nashoba Brooks School, manages the technology needs of 250 students and 75 staff members with a small team of two. His responsibilities also include overseeing a hands-on STEAM lab, managing schoolwide curricular integration, and teaching classes making his workload extensive and diverse.

KEY CHALLENGES INCLUDED:

1. **Limited Bandwidth:** A demanding schedule left minimal time for critical system updates, security patches, and infrastructure maintenance.
2. **Security Concerns:** Parents prioritized their children's privacy and security, placing pressure on the school to protect personal and financial data while safeguarding against malware and breaches.
3. **Subpar Support:** The school's previous IT provider offered slow response times, prompting a search for a more reliable partner.

CASE STUDY 02

THE SOLUTION

SecureWon conducted a comprehensive cybersecurity assessment and implemented a series of targeted improvements:

1. **Infrastructure Overhaul:** Recommended and executed a network switch upgrade, completed within two months, ensuring the school's network remains future-ready for at least five years.
2. **Enhanced Cybersecurity:** Developed a robust cybersecurity program, securing networks, applications, and personal data against threats.
3. **Proactive IT Support:** Provides advanced support for complex IT issues, enabling the internal team to focus on core responsibilities without adding headcount.
4. **Physical Security Enhancements:** Upgrading cameras, door security systems, and monitoring software to improve campus safety.
5. **Strategic Planning:** Partnering with the school to identify future needs and plan for growth projects

Q&A

SECUREWON

Thank you!

Next Steps

Email: info@securewon.com

Phone: 855-458-6947

Website: www.securewon.com