Bismarck Public Schools

Cyber Security Services Overview

Information Technology Committee – 10/21/2021

About Bismarck Public Schools Technology Services

- 13,468 students and 2,247 employees on the first day of the 2021-2022 school year
- 16 grade schools (+2), 3 middle schools, 3 senior high schools, an alternative high school, a Career Academy and Technical Center, and an early childhood education program (BECEP)
- Classroom and administrative technology
  - Staff are issued laptops and students are issued Chromebooks (1:1)
  - Projectors, printers, document cameras, audio reinforcement systems
- Infrastructure and support technology
  - Building control systems (HVAC, intercoms, lighting)
  - Network (switches, access points, routers, firewalls, telephony, and security cameras)
  - Servers and systems (physical and virtual, software as a service and cloud)
  - Data integrations

bps

Bismarck Public Schools History of Technology Services

Timeline	Classroom	Network & Security
1990's Mainframe computing Servers at each site	• Scheduled use of library or lab devices for content and topic research • Film strip, transparency, and overheads in classroom • Limited printing	• One connection in school on one device • Wiring of schools
2000's Internet & Wide Area Networking Centralize server connectivity Personal computing System integrations Data sharing	• Employees receive desktop for administrative and attendance work • Desktop computer lab use increases • Mobile computer labs carts • Checkout projectors, scanners	• Wireless deployed • Basic antivirus services • Internet filtering (privacy online, AUP) • Basic firewalls • Data practices like password on files, https and secured Wi-Fi • Backups
2010's Web-based applications Mobile computing	• Research integrated into daily activities just in time • Reduce computer labs and move towards 1:1 • Pod printing, network projection, building automation systems, security cameras	• Segmentation in network (Guest, Employee, Student) • Sophisticated firewalls • Web applications (Java, ASP, HTML, Flash, Shockwave) • Authentication methods • Data integration with systems • Security Buzzwords - Malware, virus, phishing • Data confidentiality
2020's Hybrid computing (On-Premise, SaaS, Cloud)	• Technology in all aspects of life • District issued equipment and bring your own device	• Content online (Software as a Service, Cloud) • Apps and Extensions • Where data it lives, who has access, what will they do with it • Bad actors (malware, zero day, ransomware, data breaches)

Security Buzzwords and Framework

- Buzzwords and vocabulary
  - Virus, Malware, ransomware, worm, zero day, spoofing, phishing, work, Trojan horse, bots,
  - Brute force, DDoS, command-and-control, honeypot, bit locking
  - Whitelists, blacklists
  - Breach, Exploit, Vulnerability
  - Encryption, certificates, patch, updates, multi-factor authentication, zero trust
  - Intrusion detection system (IDS), Security Information and Event Management (SIEM)
  - Security Incident Response, penetration testing, and red teams
- Security Framework
  - Prevention, Monitoring, and behavior changes and analysis
  - Protection (network, agent, and user based)
  - Remediation
  - Information Sharing

Bismarck Public Schools

Cyber Security Services Overview

Leveraging security services at BPS

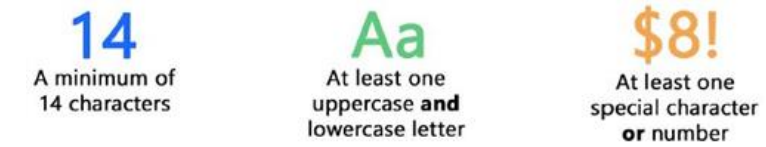
- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- NDIT/K12 managed security services
- Shared resources and partnerships

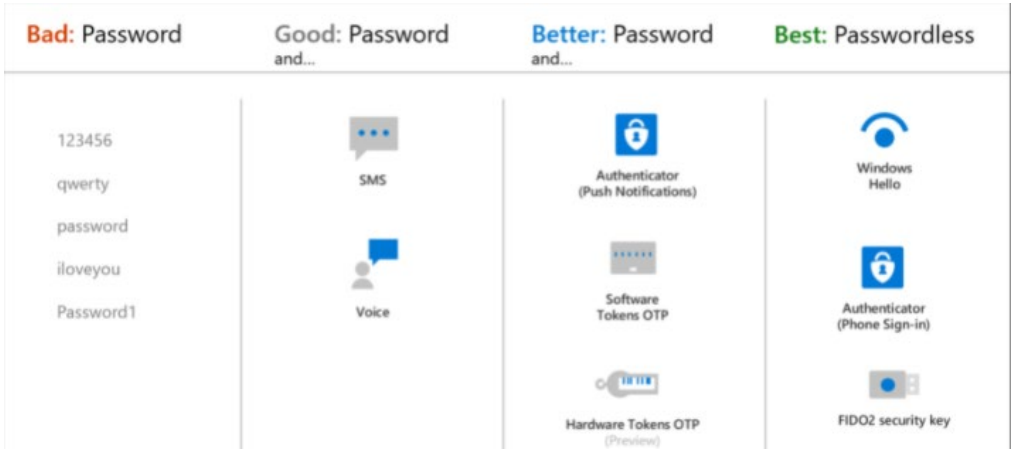
bps

Leveraging security services at BPS

- **Staff, Students and other stakeholder awareness**
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- NDIT/K12 managed security services
- Shared resources and partnerships

- Customers are part of the solution
- Provide user awareness and training for best security practices (social engineering, careful clicking, ask is this real, handling sensitive information)
- How to choose a password and password length and expiration
- Multi-Factor Authentication
  - Employees, challenges for Students: 9-12 Students, K-8??





Leveraging security services at BPS

- Staff, Students and other stakeholder awareness
- **Policies, Standards, and Safeguards**
- Internal Systems & Network protection
- NDIT/K12 managed security services
- Shared resources and partnerships

- Acceptable Use Policies for Employees and Students
- Families sign off on the responsible use policy
    - 1:1 device or bring your own device
- Digital etiquette courses offered
- Educators mindful and aware about what data is shared, where it is stored, and who has access to it

Leveraging security services at BPS

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- **Internal Systems & Network protection**
- NDIT/K12 managed security services
- Shared resources and partnerships

Best practices

- Inventory of hardware and software
- Patching and updating of computers, network, and systems
- Logging of access to provide audit trail
- Utilize rights and permissions to protect sensitive data
- Utilize privileged access accounts for applicable systems
- Monitor devices, systems and networks for anomalies
- Backup and restoration of critical data and configuration of systems
- Segmentation (Guest, Employee, Student, and other stakeholder access)
- Firewalls and VPN services to provide zero trust methodology in network and servers
- Incident response plans

Leveraging security services with NDIT at BPS

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- **NDIT/K12 managed security services**
- Shared resources and partnerships

Layered approach

- STAGEnet – perimeter network protection
- Agent and User based – Systems, application, and user protection
- Monitoring & Remediation
- Information sharing

NDIT/K12 managed security services

STAGEnet | Agent and User Based | Monitoring and Remediation | Information Sharing

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- **NDIT/K12 managed security services**
- Shared resources and partnerships

STAGEnet – perimeter network protection

- Security operations performed close to source (customers)
- Provides Internet protection and protection between different State entities and sites
- Firewall technology utilizes next generation firewall (NGFW) capabilities
  - Real time antivirus scanning of network traffic
  - Malware detection and mitigation of network traffic
  - Dynamic vulnerability protection to known vulnerabilities
  - Protection against Distributed Denial of Service (DDoS)

Other protection layers utilizing NGFW and other products

- Phishing protection to known malicious links
- Automatic blacklisting of sites based on partner threat feeds and user behavior
- Customizable URL content filtering
- DNS threat blocking
- Internet of Things (IooT device/detection

Other services offered to all users:

- DNS/DHCP services

NDIT/K12 managed security services

STAGEnet | **Agent and User Based** | Monitoring and Remediation | Information Sharing

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- **NDIT/K12 managed security services**
- Shared resources and partnerships

Agent and User based – Systems, application, and user protection

Endpoint Protection

- Palo Cortex XDR analyzes and protects against viruses, malware, Trojans, and other bad actors
- Windows, macOS, and Chromebook devices
- Security Based Access Controlled (SBAC) Console
- $172 per endpoint per year – State currently absorbs the cost

Systems Monitoring

- Nessus Tenable scanning shows patch and update levels of operating systems and applications
- Windows and macOS devices
- Chromebooks are scanned using unauthenticated scans
- Software vulnerability scanning capabilities
- $137 per endpoint per year – State currently absorbs the cost

End User Awareness and Training

- KnowBe4 Training offers real world end user CyberSecurity training
- Phishing email campaigns
- $33 per endpoint per year – State currently absorbs the cost

NDIT/K12 managed security services

STAGEnet | Agent and User Based | **Monitoring and Remediation** | Information Sharing

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- **NDIT/K12 managed security services**
- Shared resources and partnerships

Monitoring and Remediation

- Continuous Monitoring and Incident Response - Staffed Cyber Operations Center
  - Access to over 40+ security team members at NDIT to consult, advise, or assist with security related events
  - Digital Forensics, Malware Analysis, and Reverse Engineering upon request
  - Endpoint Log Storage and Monitoring
- Threat Hunting by Palo Alto Networks Unit 42 Hunt Team

NDIT/K12 managed security services

STAGEnet | Agent and User Based | Monitoring and Remediation | **Information Sharing**

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- **NDIT/K12 managed security services**
- Shared resources and partnerships

Information Sharing

- Multi-State Information Sharing & Analysis Center (MS-ISAC)
  - Improves the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber threat prevention, protection, response, and recovery.
- Cybersecurity and Infrastructure Security Agency (CISA)
  - CISA builds the national capacity to defend against cyber attacks and works with the federal government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.
- Dark Web Monitoring for sites that have been breached
- Cyber Maturity Assessments (CMA) for multiple State Agencies, K12, Higher Ed, Cities and Counties

Leveraging security services at BPS

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- NDIT/K12 managed security services
- **Shared resources and partnerships**

Shared resources and partnerships

- Costs of doing nothing or minimal security is not an option
- Security technologies evolve fast requiring constant awareness and investment
- Quality and timely security services require dedicated human and capital resources
- Local resources are stretched and shared resource approach has been valuable
  - Large school districts may have limited security resources because of necessity, smaller districts may not
- Partnership with the ND Insurance Reserve Fund to provide Cyber Insurance

bps

Bismarck Public Schools

Cyber Security Services Overview

Leveraging security services at BPS

- Staff, Students and other stakeholder awareness
- Policies, Standards, and Safeguards
- Internal Systems & Network protection
- NDIT/K12 managed security services
- Shared resources and partnerships

bps