Cybersecurity & Education Law 2-d

Oyster Bay-East Norwich Schools

December 17, 2019

Janna Ostroff

Top 4 Cybersecurity Threats to Schools

Schools are soft targets, increasingly vulnerable to the following 4 types of attacks:

PHISHING

90% of detected attacks start with emails that trick users into revealing personal information or clicking on links that install harmful software.

“SPEAR” PHISHING

DDoS

A distributed denial of service **(DDoS)** attack occurs when multiple systems flood the bandwidth or resources of the district servers.

BREACH

The release of secure confidential information.

RANSOM -WARE

Malicious attack that encrypts district data with malware and requires a ransom to access. Software is often installed using credentials gained via targeted/spear phishing.

Managing Risk (0.01% of Detected Threats)

- https://threatmap.fortiguard.com/
- https://threatmap.bitdefender.com/
- https://www.deteque.com/live-threat-map/

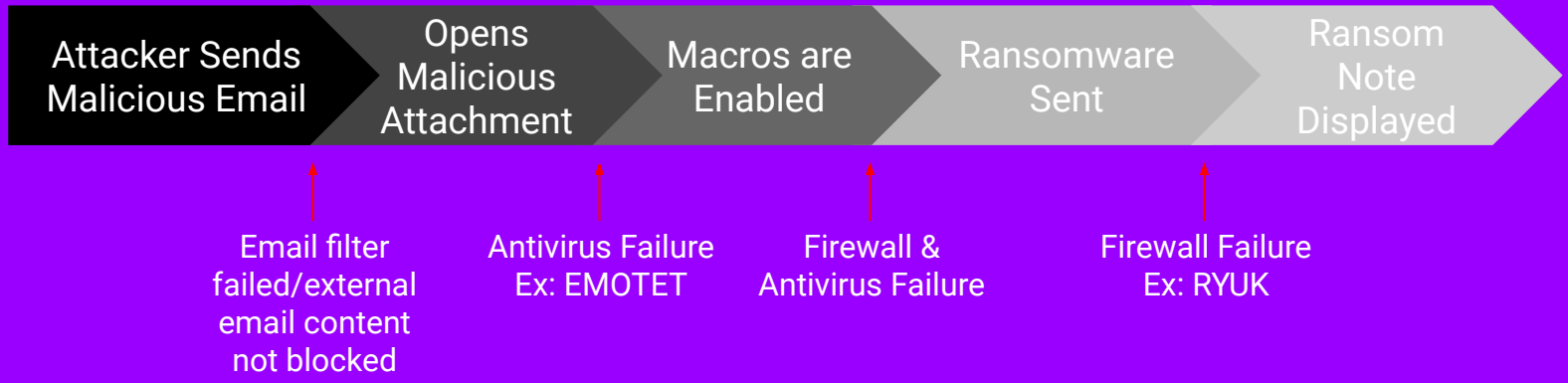
Physical Security	Digital Security
External Doors	Firewall & Email Filters
Classroom Doors	Virus Protection Software
Visitor Management	Administration
Security Guards	Technicians
ID Badges	Authentication Logins

Ransomware 2019

Rockville Center, Mt. Sinai and Mineola were among the 30+ institutions in the country reporting Bitcoin ransomware to the FBI.

Educational institutions are the second largest target in the country.

At least 5 other Long Island districts reported experiencing long-term interruptions in service due to malicious attacks this year.



Snapshot 2019

December 2nd - 9th:

Type of Attack	# Intercepted
Emotet virus attachments (6 strains/variations)	38
Malicious links embedded	4
Spear-phishing/impersonation attacks	181
“Zero-threat” attacks	41

4 Phishing Attempts Detected, Reported & Thwarted by Educated Users
- 3 (January, June & October) led granular changes in permissions
- 1 (December) traced to compromised password from home device use

3 DDos Attacks Led to Short-Term Slowed Internet Access (1-3 hours)

Ongoing District Considerations

What if a DDoS attack rendered our internet temporarily unusable? What does our day look like? What off-line systems do we need in place?

What are our subcontractors doing to protect themselves? Are the risks of sharing data with certain companies worth the potential consequence?

What if we showed up tomorrow and could not access any district documents? How quickly can we recover?

Are we doing everything we can do to insure that we are not the target of a Ransomware attack?

Education Law 2-d Part 121

http://www.counsel.nysed.gov/rules/indices-fulltext/2019/010

Goal: To protect school data using clearly communicated policies and practices

Components:

1) Data Protection

2) Communication Protocols

3) Technical Systems Management

NIST FRAMEWORK

NIST CYBERSECURITY FRAMEWORK		
	Regulations 121.5	Apply the planning, processes, and categories of information protection defined within the NIST Cybersecurity Framework to district practices and systems

2017-18 Instructional Technology Audit Comparison

- Similar in Core Function
- More Specific in Network Systems, Securities and Automated Threat Protections

NIST Cybersecurity Framework

- 5 Core Functions
  IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- 23 Categories of Institutional Action
  https://riconedpss.org/documents/NISTFrameworkCore.pdf

1. Data Protection

DATA SECURITY AND PRIVACY POLICY		
	Regulations 121.5	Adopt and post a Data Security and Privacy Policy that includes adherence to the NIST Cybersecurity Framework to protect PII

THIRD-PARTY CONTRACTS		
	Regulations 121.2, 121.3, 121.6, 121.9, 121.10	Whenever the educational agency discloses PII to a third-party contractor, ensure that the written agreement for using the product or services includes the language required by Education Law

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY		
	Regulations 121.3	Adopt and post on website a Parents Bill of Rights for Data Privacy and Security, with supplemental information about each written agreement with a third-party contractor (vendor) that involves disclosure of PII

Steps Taken

DATA SECURITY AND PRIVACY POLICY

- Board of Education Policies are in review for approval on July 1, 2020 in compliance with Educational Law 2-d.

THIRD-PARTY CONTRACTS

- Classlink was purchased to provide an inventory of approved software on a single sign-in platform.
- Protocols for software purchasing were updated to include third-party Education Law 2-d updated contracts.
- We are contracting with the BOCES Regional Information Center (RIC) Data Privacy and Security Services to access a regionally developed software vetting tool.

PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

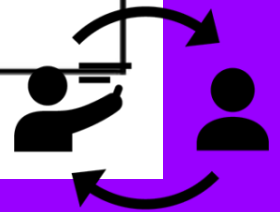
- BOCES RIC Educational Law 2-d aligned drafts will be edited and posted July 1, 2020.

2. Communication

ANNUAL EMPLOYEE TRAINING		
	Regulations 121.5 and 121.7	Deliver annual privacy and security awareness training to all employees

INCIDENT REPORTING AND NOTIFICATION		
	Regulations 121.10	Follow reporting and notification procedures when unauthorized disclosure occurs

PARENT COMPLAINT PROCEDURES		
	Regulations 121.4	Create and publish a parent complaint process



Steps Taken

ANNUAL EMPLOYEE TRAINING

- KnowBe4 was purchased to administer training and self-assess risk.
- Cybersecurity training was conducted Fall, 2019.
- Personally Identifiable Information (PII) training is planned for Spring, 2020.

INCIDENT REPORTING AND NOTIFICATION

- Protocols will be aligned with anticipated district policies, in compliance with Educational Law 2-d.

PARENT COMPLAINT PROCEDURES

- Sample posting and form are being revised for review.

3. Technical Systems Management

(Details Reserved for Live Board of Education Meeting)

VULNERABILITY **MANAGEMENT**	**Patch known vulnerabilities on all systems, but in particular those systems that house sensitive data.**
SYSTEM **BACKUPS**	**Ensure backups for critical systems are in place and audit backups for completion and functionality.**
SYSTEM **HARDENING**	**Ensure anti-virus is installed and up-to-date, enable firewalls, close unnecessary ports, and disable non-essential services.**
IDENTITY **MANAGEMENT**	**Ensure accounts have appropriate permission levels. Domain Admin accounts should never be used to access workstations.**
APPLICATION **SECURITY**	**Only use district approved softwares, audit system access, and isolate critical infrastructure.**