Incident Response Playbook: Cyberattack Mitigation for Rural K-12 Public School District

Phase 1. Preparation

Team Formation:

Establish an Incident Response Team (IRT) with clear roles including IT staff, cybersecurity experts, school administrators, legal counsel, and communication officers.

Tool and Access Preparation:

Detail the process for engaging escalation and external vendors, including contact lists, and criteria for when to involve experts, and coordination protocols.

Ensure the IRT has access to necessary tools and systems for analysis and recovery.

Patch Deployment

- SCCM, Ansible, WSUS, Puppet

SIEM (Security Information and Event Management)

- Splunk, LogRhythm, IBM QRadar, Azure Sentinel

EDR (Endpoint Detection and Response)

- CrowdStrike, SentinelOne, Carbon Black, Symantec

Network Analysis & Monitoring

- Wireshark, SolarWinds, Nagios, Nmap, NetFlow

Firewall

- Cisco ASA, Check Point, pfSense, Barracuda

IPS (Intrusion Prevention System)

- Cisco Firepower (NGIPS), Palo Alto (NGFW), FortiGate, Snort

IDS (Intrusion Detection Systems)

- Suricata, Bro/Zeek, OSSEC, Security Onion

Security Orchestration, Automation, and Response (SOAR)

- Splunk Phantom, Cisco SecureX, IBM Resilient

Vulnerability Scanners

- Nessus, Qualys, Rapid7, OpenVAS, Burp

Forensics

- Volatility, The Sleuth Kit, EnCase, Autopsy

Collect, analyze, and utilize real-time threat intelligence platforms (TIPs - open source, commercial, industry partnerships)

- AlienVault OTX, IBM X-Force, Crowdstrike Falcon Intelligence, Recorded Future, ThreatConnect, MISP (Malware Information Sharing Platform)

Automate and integrate the ingestion of threat feeds into security information and event management (SIEM) systems, defensive measures, and incident response strategies.

Regularly review and update relevant threat profiles and indicators of compromise (IoCs)

A-Poc Blue Team Tools ~ Github

Secure Infrastructure:

Ensure all systems are updated with the latest security patches and have robust antivirus and anti-malware solutions installed.

Implement an email filtering solutions to detect and block potentially malicious emails and phishing attempts.

Implement data loss protection (DLP) measures that comply with the Family Educational Rights and Privacy Act (FERPA) requirements, ensuring that student information is securely stored and transmitted.

Implement and maintain regular backup routines for all critical data, with backups stored securely off-site or in a cloud environment.

Regularly validate that backups have completed and that data can be successfully restored from them.

Awareness and Training:

Conduct regular training sessions for all staff and students on cybersecurity best practices, including recognizing and reporting phishing attempts and malicious emails.

Include FERPA training as part of the regular security awareness program for staff and the IRT, emphasizing the importance of protecting student education records.

Ensure all team members understand the legal obligations under FERPA in the context of cybersecurity threats.

Highlight that protecting student data is not just a cybersecurity issue but a legal requirement.

Communication Plan:

Develop a communication plan to inform stakeholders (staff, students, students' parents, media) while maintaining privacy and security.

Ensure all members understand the importance of protecting student information during the investigation and response processes.

Phase 2: Identification

Incident Detection:

Utilize antivirus alerts, network monitoring tools, and reports from users to identify potential security incidents and identify which systems are infected.

Configure email and network monitoring tools to automatically flag unusual activities, such as the rapid spread of emails or file changes, indicative of a virus.

Confirm the nature of the incident and the initial attack vector (malicious email attachment).

Incident Confirmation:

Assign a team member to quickly confirm if the alert indicates a real incident or a false positive.

When identifying potential incidents, consider any unauthorized access to student information as a critical trigger for FERPA violation alerts.

Scope Assessment:

Determine the extent of the infection, identifying all impacted machines and systems.

Assess whether sensitive data, including student and staff personally identifiable information (PII), has been compromised.

When assessing the scope of the cyberattack, specifically identify whether student data has been accessed or compromised.

This includes grades, schedules, and personally identifiable information (PII) protected under FERPA.

System and Network Monitoring:

Enhance monitoring to identify all impacted systems, including servers and endpoints at the elementary school and other schools.

Incident Documentation:

Document all findings, actions taken, and evidence of the attack and its spread.

When documenting the incident, include specific checklist items to identify any and all potential FERPA violations or risks to student data privacy.

Phase 3: Containment

Immediate Actions:

Disconnect infected machines from the network to prevent further spread.

This includes individual computers and, if necessary, entire network segments.

Isolate critical network segments and block malicious IP addresses, especially those connecting to central IT and other schools within the district.

Change passwords and security credentials to prevent unauthorized access.

When taking steps to contain the breach, prioritize actions that protect student records from unauthorized access, in line with FERPA guidelines.

Conduct forensic analysis, including the collection of logs, disk images, and memory snapshots

Capture and analyze network traffic, memory, and disk images to identify the scope of an intrusion, the methods used by the attacker, and any data exfiltration.

Email Quarantine:

Implement rules to intercept and quarantine emails similar to the initial malicious attachment.

If necessary, temporarily suspend email services to halt the spread and communicate through alternative channels.

Long-Term Containment:

Change all network passwords and credentials, especially for those with administrative access.

Implement stricter network segmentation to limit the spread of future infections.

Implement multi-factor authentication (MFA) and access control lists (ACLs) where appropriate.

Phase 4: Eradication

Remove Threats:

Use antivirus and anti-malware tools to clean infected machines.

Manually remove any malware if automatic tools are insufficient.

In severe cases, a complete wipe and reinstall the operating system.

System Updates:

Ensure that all systems are updated to the latest security patches to prevent re-infection.

Update antivirus and antimalware definitions to the latest versions.

Phase 5: Recovery

Restore Systems & Services:

Use backups to restore machines and data to their state before the incident.

Verify the integrity and accessibility of the restored data.

Ensure that all restored data complies with FERPA's privacy requirements, ensuring no unauthorized modifications or disclosures have occurred.

Gradually restore cleaned systems to the network after confirming they are no longer compromised

Bring email and other critical services back online with increased monitoring for suspicious activities.

Ensure that steps taken to contain the breach, eradicate the virus, and recover any lost data comply with FERPA regulations.

This includes secure handling and restoration of student records and maintaining the confidentiality of the information throughout the process

Monitoring:

Implement enhanced monitoring and continuously monitor the network for signs of malicious activity and conduct tests to ensure the integrity of the systems.

Phase 6: Lessons Learned

Review, Document, and Analyze:

Convene a meeting with the IRT to discuss the incident, what was done to resolve it, how it was handled, and areas for improvement.

Document the attack's details (indicator of compromise [IoC], tactics-techniques-procedures [TTP]), how the attack succeeded, what failure allowed the attack to be successful, how it was mitigated/remediated, and steps taken to prevent a similar incident.

Document every step of the response, including the initial breach, response actions, lessons learned, and any changes implemented to prevent future incidents.

Policy Update:

Update policies, procedures, and security measures based on the lessons learned from the incident.

Update security policies and response strategies based on the lessons learned.

Revise the incident response plan (IRP) and security policies based on the lessons learned.

Incorporate a review of FERPA compliance in the post-incident analysis.

Determine if any changes to policies or procedures are necessary to better protect student data in the future.

Training Update:

Incorporate the experience into future awareness and training sessions to prevent similar incidents.

Determine what can be improved in the response process, including technical defenses, training, and awareness programs for staff and students.

Communication:

Communicate transparently yet sensitively with all stakeholders, including staff, students, parents, and possibly the wider community, about what happened and what steps are being taken to prevent cybersecurity and privacy future incidents.

Ensure that any communication about the breach is cautious does not inadvertently disclose protected student information or compromise security.

When communicating about the incident to stakeholders, be mindful of FERPA regulations and notification requirements.

Keep staff and stakeholders informed throughout the process, using predefined communication channels.

Offer counseling and support to any students or staff members affected, reinforcing the district's commitment to a safe and inclusive environment ~ Psychological First Aid (PFA) Training

Implement a process for collecting and analyzing feedback post-incident, including surveys or debriefing sessions, to inform playbook updates.

Legal and Regulatory Compliance:

Work with legal counsel to report the incident to relevant authorities if required.

Ensure compliance with data protection laws, such as reporting breaches involving personal data.

In the documentation and review of the incident, include an analysis of how well FERPA-protected data was safeguarded and whether any breaches of FERPA occurred.

Report the incident to relevant authorities as required by FERPA guidelines when student data is involved.

Be aware of and comply with local and national laws regarding cybersecurity incidents, especially those involving hate speech and the protection of minors.

Phase 7: Prevention

Regular Audits:

Conduct regular security audits, vulnerability assessments, and penetration tests to identify and rectify potential weaknesses.

Perform tabletop exercises where incident response playbooks can be used to evaluated different scenarios and responses.

Conduct behavioral analysis for anomaly detection,

Conduct annual or bi-annual simulations (red vs blue), including objectives, scenarios, and evaluation criteria to measure the effectiveness of the IRT.

Engage in continuous monitoring and proactive threat hunting.

Community Engagement:

Work with local law enforcement/cybercrime units, cybersecurity organizations, and other educational institutions to share information and strategies for preventing cyberattacks.

Seek assistance in tracing the source of the attack and holding the perpetrators accountable

Resilience Planning:

Develop and regularly update a comprehensive cyber resilience plan to ensure the district's preparedness for future incidents.

Develop further incident response playbooks (IRP), business continuity plans (BCP), and disaster recovery plans (DRP).

Establish a review cycle to incorporate changes in data protection laws, focusing on compliance with FERPA and other relevant legislation.

Use cybersecurity training platforms like Cyber Ranges, TCM Security, Immersive Labs for realistic scenario training

Regularly review and update the playbook to align with IT policies, conducting joint reviews with IT policy managers to ensure coherence and compliance.

Specify intervals (bi-annually) and conditions (e.g., after a major incident) under which the playbook should be updated.

Aligning explicitly with recognized cybersecurity frameworks (NIST Cybersecurity Framework) to ensure comprehensive coverage of security controls and best practices.

Define playbooks for common scenarios (phishing, malware, DDoS)

Integrate advanced threat detection capabilities with a focus on user and entity behavior analytics (UEBA) to identify unusual activities indicative of cyber threats.

Cybersecurity Insurance:

Consider purchasing cybersecurity insurance to cover the costs associated with cyberattacks, including recovery and legal fees.