Incident Response Best Practices: Bruise Now, So You Don't Bleed Later

Ross Lemke
Director
Privacy Technical Assistance Center (PTAC)

United States Department of Education
Student Privacy Policy Office
Privacy Technical Assistance Center

Why is Incident Response Important?

Education: THE Most Targeted Sector

- 30% increase in cyberattacks on schools
- ~650k students impacted in 2021 alone
- Targeted more than healthcare and government

FORBES > LEADERSHIP > EDUCATION

The Top Target For Ransomware? It's Now K-12 Schools

Frederick Hess Senior Contributor

I write about policy and practice in K-12 and higher education.

Follow

Schools Are the Most Targeted Industry by Ransomware Gangs

Posted on September 20, 2023 by Dissent

Waqas reports that based on research by Sophos, the education sector is the most vulnerable and targeted by ransomware attacks.

KEY FINDINGS

- 80% of lower education providers and 79% of higher education institutions reported ransomware attacks in the last year.
- Education is the most targeted industry by cybercriminals, primarily motivated by the high percentage of schools choosing to pay the ransom.
- The recovery costs from ransomware attacks have remained steady at around $1.59 million in 2023 and 2022 for lower education providers, while recovery costs in higher education have decreased significantly from the $1.42 million reported last year to just over $1 million in 2023.
- Education providers lack the funds that large corporations have to invest in robust cybersecurity measures and even staff training, leading to many loopholes sophisticated hacker groups can exploit.
- The Biden-Harris Administration has announced a $200 million initiative over three years to bolster cyber defences in K-12 schools.

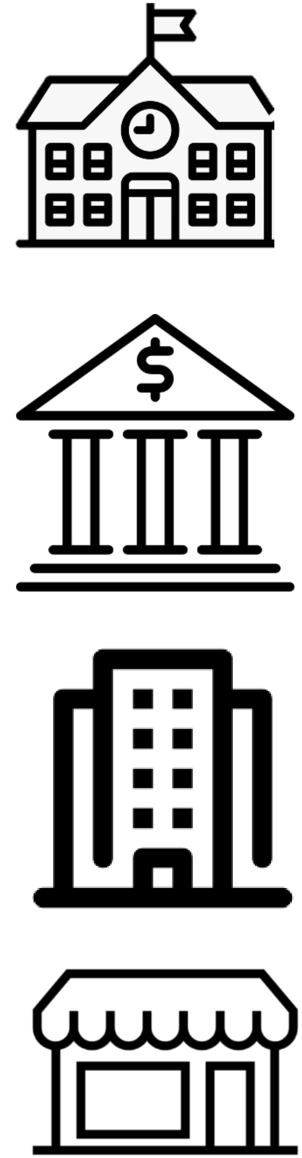
Read more at HackRead.

Cliff’s Notes: You’re Gonna Get Hit

- Education == Retail and Finance
- **Employees** and **Staff** are going to be the way in
- If it isn’t Ransomware, its going to be DDoS
- Spend **Time** and **Resources** on **training**
- Response plans and processes better be tailored to meet these threats

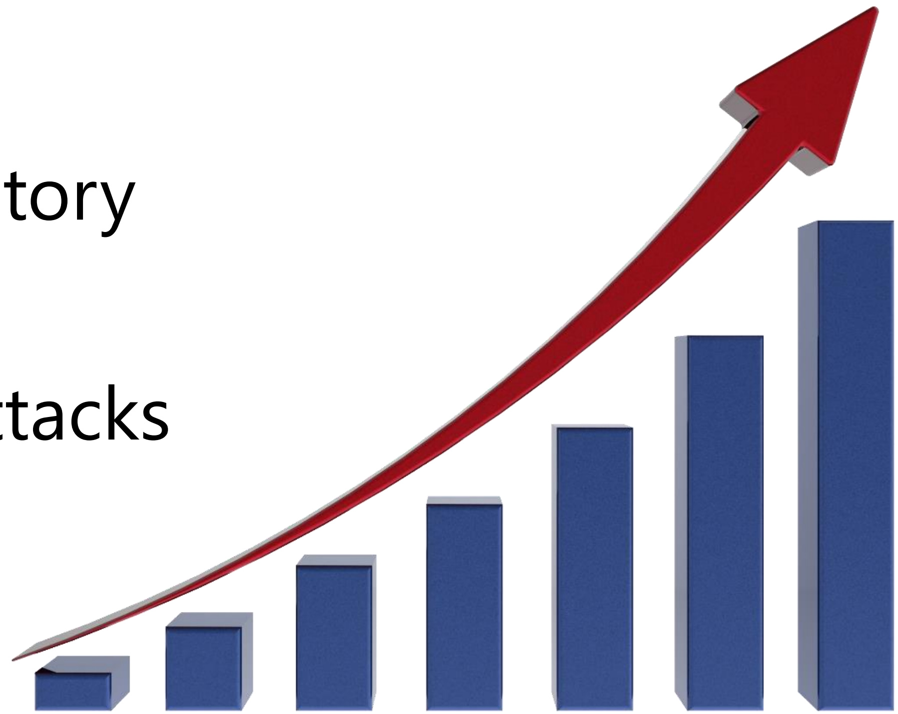
Schools are not JUST Schools

- More than just student data
- Health, family, financial data
- Employee data
- Sensitive Research data
- Other agencies' data
- Payment / Commerce data



Data Breach Impacts to Education

- Billions of dollars in costs
- Downtime from days to weeks
- Legal liabilities & regulatory penalties
- Further targeting and attacks
- Reputational harm



Many Laws May Apply

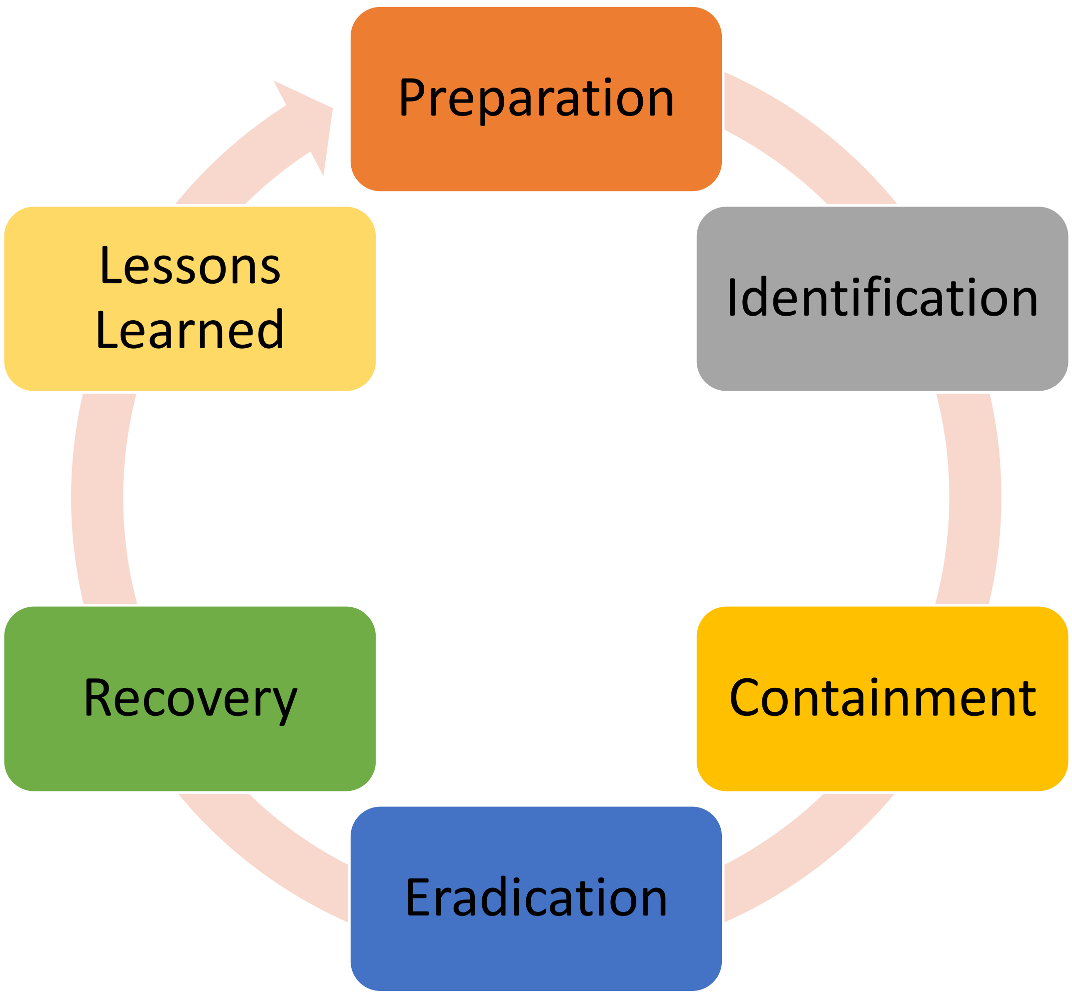
- FERPA
- IDEA
- Higher Education Act (HEA)
- GLBA implications & other applicable financial laws
- State Laws

Incident Response: What's Inside the Box?

Key phases typically include:

1. **Preparation**: Defining the response team, roles and responsibilities, developing communication plans, and resourcing
2. **Identification**: Detecting and determining the nature of the incident.
3. **Containment**: Containing the incident, mitigating further damage
4. **Eradication**: This involves removing the threat from the affected systems
5. **Recovery**: Restoring and returning systems and networks to normal operations
6. **Lessons Learned**: Post-mortem analysis and lessons learned for process improvement

The Process


Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

Rule #1: Have a Plan

Failure to plan is planning to Fail…

You Need an Incident Response Plan

Incident Response Plans

"An Incident Response Plan is a written document, formally approved by the senior leadership team, that helps your organization before, during, and after a confirmed or suspected security incident." -CISA

- *Defines the Purpose / Mission*
- *Identifies Roles & Responsibilities*
- *Sets organizational priorities*
- *Determines response thresholds*
- *Outlines response processes*
- *Creates standards for documentation & metrics*
- *Establishes compliance & review timelines*

Putting a Plan Together

- Determine the “Musts”
- Define your Stakeholders
- Obtain leadership buy-in
- Understand what you have
- Evaluate the threat
- Perform a risk-assessment

Perform Annual Risk Assessments

"The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact."

-National Institute of Standards and Technology (NIST)

What is a Risk Assessment?

Formal organizational process involving leadership, IT, and organizational stakeholders

Four stages:

- **Identification** – *finding, documenting, and categorizing risks*
- **Analysis –** *ascertaining the nature of the risks and determining their potential impact and effects*
- **Evaluation –** *applying organizational risk tolerance and existing controls to the risk to determine significance*
- **Control –** identifying and applying mitigating controls to reduce the risk based on analysis

Continuous Re-Assessment

- Incident response plans are tailored to threats
- Threats change over time
- Risk-assessments drive understanding of the threat
- Periodically perform risk assessments and leverage the results to enhance incident response
- Tie these processes together with training and awareness to supercharge your preparedness and resilience

Incident Response Teams

There are two key success factors to good Incident Response Team performance.

The right Team

&

Somebody in-charge

Incident Response Team

Incident Response Teams are groups tasked with the response, management, and recovery of security and privacy incidents.

CORE

- Leadership
- Legal
- Communications / PA
- IT

AD-HOC

- Vendors / Partners
- Law Enforcement
- Facilities
- State Agencies

Incident Response Team Responsibilities

- Assess, analyze, and manage incidents from initial reporting to out-brief
- Speed recovery, ensure threat data flow, contain the incident
- Coordinate with stakeholders, decisionmakers, regulatory bodies, and communicate
- Documentation & reporting of response actions
- Post-incident analysis, prevention, education, and training

Who's in Charge Here?
The Role of the Incident Manager

Acts as the coordinator and focal point for the response efforts

Key Responsibilities Include:

- Incident Coordination & Mgmt
- Communication
- Decision Making
- Strategy & Planning
- Resource Allocation
- Post-Incident Review
- Compliance Considerations
- Process Improvement
- Training & Awareness

Let's Talk IR Secret Sauce

Secrets to *less Painful Incident Response:

- Not Owned by IT
- **Includes Legal Counsel & Public Affairs**
- Starts with Validation
- Continuous review & testing
- Incorporates lessons learned

Privacy & IT Security Training

- Annual threat awareness training for all employees, faculty, administrators, students
- Focusing on cyber-hygiene, social engineering awareness, and threat reporting
- Great time to revisit AUP and employee expectations for security

Leadership Involvement

- Formal policy & plan
- Publicized and socialized throughout the organization
- Supported by reporting & feedback mechanisms
- Policy should assign roles and responsibilities, including leadership presence on IRT
- Absolutely NOT just an IT thing!

Legal Eagles

Legal Counsel is a huge benefit in incident response. This could be your local counsel, outside counsel *(or even cyber-insurance company).*

- Often confusing legal requirements
- Need to protect organizational interests
- Interfacing with Law Enforcement & State entities

Communications is KEY

Think about including Public Affairs / Communications representatives in your IRT. Message is the often the hardest part of a response

- Ransomware & DDoS require some 'splaining
- Need concise, clear, consistent messaging both internally and externally
- Frees up critical response resources
- Consistency of messaging conveys reassurance that the response is under control

Would you like to play a game?

Threats evolve, so should your Incident Response plan!

- *Periodic risk assessments*
- *Annual IR exercise*
- *Involve third-parties, vendors, and partners*
- *Use as an opportunity to talk to law enforcement, cyber-insurance reps, contractors, etc.*

Tabletop Exercises

Simulated incident response based on carefully selected scenarios, where the IRT sits down and walks through a response.

- Build IRT cohesiveness and confidence
- Establish lines of communication
- Identify problem areas and streamline the IRP
- Ensure process and plans are extensible to the widest spectrum of incidents

Data Breach Resources

Downloadable Data Breach Training Kits

https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings

New Expansion Pack Available!

Feedback Loops

"The most neglected part of the incident response plan is the part where you remember all the mistakes you made and fix them for next time"

-**Me**

Feedback Loops

Every organization should document their process and capture important data for process improvement:

- *What worked well?*
- *What didn't work at all?*
- *Did we miss something?*
- *What can we do better?*

Final Food for Thought

- You should have an incident response plan in place and train to it
- Data privacy & security awareness training for all employees, as well as contractors, researchers, and other 3rd parties
- Clearly understand the legal requirements for compliance with all applicable federal, state and local laws
- Consider calling PTAC, we can help!!!

PTAC Resources

- **Data Breach Response Checklist**
  https://studentprivacy.ed.gov/resources/data-breach-response-checklist
- **Downloadable Data Breach Training Kits**
  https://studentprivacy.ed.gov/resources/data-breach-response-training-kit
- **PTAC Student Privacy Training**
  - ***Videos*** - https://studentprivacy.ed.gov/content/videos
  - ***Online Training Modules*** - https://studentprivacy.ed.gov/content/online-training-modules

CONTACT INFORMATION

United States Department of Education,
Privacy Technical Assistance Center

(855) 249-3072
(202) 260-3887

privacyTA@ed.gov

https://studentprivacy.ed.gov

(855) 249-3073