GAT Labs for education

Cyber Incident Response Plan for School Admins

Table of Contents

Getting Started: School Cybersecurity Challenges

Nowadays, digital resources and electronic devices are essential to the modern classroom. School cloud storage is a goldmine of students' sensitive data: names, addresses, contact details, Social Security numbers, health information, and much more.

That's why educational centres are today put in the crosshairs of cybercriminals. Frequent school cyberattacks make K12 admins ask themselves not if their schools could be a target but when an incident will happen.

You can't make your school immune to a cyberattack, but you can do your best to defend student data. Actions you take before, during and after an incident will impact your school's cybersecurity. All of them should form part of the Cyber Incident Response Plan, a fine-tuned and reliable tool against digital dangers.

Why Does Your School Need a Cyber Incident Response Plan?

Incident response planning covering cybersecurity threats in your school:

- Streamline effective and quick emergency management in the event of a cybersecurity incident in your school by designing key roles and responsibilities
- Reduce short- and long-term damages caused by cybersecurity incidents and help prevent them in the future
- Support your school in terms of complying with data security, student privacy and incident responding regulations

How to Create a Cyber Incident Response Plan Step-by-Step

These are general guidelines for preparing a plan in case of a cybersecurity emergency at school. Adjust its content to fit your institution's size, location, stored data, e-learning tools, and specific needs.

Working on the comprehensive and efficient CIRP will require the collaboration of different departments across your school. You may also want to consult external IT service providers and cybersecurity experts.

The plan should be coordinated with the general emergency procedures of your school and national or federal regulations on cybersecurity responding.

1. Planification & Preparation

Cyber Recovery Team

Indicate who will form the emergency team and take action to respond to a cyber incident. Assign each member their specific roles and responsibilities in case of emergency.

They might cover data management, IT recovery, security analysis, public relations, internal communication, legal issues, etc. Involving people with different backgrounds will smooth the decision-making process in an emergency.

Risk Assessment

a. Identify Critical Resources

Register all data assets you store in the school domain, networks, drives and devices. They include, for example, student and staff information, classroom data and resources, and educational and organisational software.

Indicate critical, sensitive data and services that should be prioritised to ensure safety and provide fast recovery during a cybersecurity incident.

b. Identify Possible Threats

Although each school has a specific digital environment, we can identify and monitor the most common cyber threats to educational institutions that may threaten your data. Consider what threats may happen in your school, and remember the cyber incidents that occurred in other schools to learn from their experience.

b. Identify Possible Threats

Although each school has a specific digital environment, we can identify and monitor the most common cyber threats to educational institutions that may threaten your data. Consider what threats may happen in your school, and remember the cyber incidents that occurred in other schools to learn from their experience.

Malware infections.
Usually caused by a user who accidentally downloads malicious software via an attachment or visits a compromised website. Once a virus infects a device, it scans for system vulnerabilities.

Data breaches and leaks.
They happen when sensitive data is disclosed to unauthorised individuals or exposed in public. They can be unconsciously (data leak) or caused by a cyberattack (data breach)

Stolen or lost devices.
School devices such as laptops, Chromebooks, iPads, etc., give access to sensitive data of the owner and the entire school.

Phishing.
It's a sophisticated method of social engineering. Email scams aim to install malicious software on devices to control them.

Ransomware.
This happens when a hacker takes over the computer system and blocks access to school data. The perpetrator releases it after receiving a ransom.

Unauthorised access or intrusion attempts.
They occur when individuals gain access to data, networks, devices, etc., without permission.

Cyberbullying.
In this case, both perpetrators and victims could be students from the same school, which makes this an internal threat.

Other cybersecurity incidents specific to the school environment

School Cyber Risk Assessment Table

This risk assessment table provides a comprehensive and visual overview of the likelihood and impact of a school's cyber risks. Green risks may not require any action, while orange risks probably do. Red risks, on the other hand, require immediate action. Assess all threats to your school and consider them in your cybersecurity plan accordingly.

Impact

How severe would the outcome be if the risk ocured?

Probability

What is the probability the risk will happen?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very High 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very High 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very High 15
2 Unlikely	Very Low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very Low 1	Very Low 2	Low 3	Medium 4	Medium 5

c. Risk Monitoring

Current and efficient monitoring of your domain is crucial for a fast response during a cyber incident. Monitor all school systems, networks, and devices to detect suspicious activities immediately, such as file activity, settings changes, or unauthorised access.

No human can manually monitor all digital facilities in real-time. Employ monitoring capabilities and automate cybersecurity threat detection using advanced Classroom monitoring, content, and web filtering tools.

Bonus: GAT Shield, Your Cyber Threats Detection Tool

If you're seeking a highly trusted tool to monitor online risks in your school, look at **GAT Shield.** This powerful solution provides granular monitoring of all users' activity on every site and at every moment in your Google Workspace for Education domain. The most complex web filtering grants you complete visibility and control over Chrome-based cloud users.

GAT Shield allows you to set up real-time alerting, create your own rules, and blacklist sites for given users. Additionally, it enables you to monitor sites visited, keyword searches, etc. This Data Loss Prevention tool is the safest real-time option in the education market.

d. Efficient Communication

When a cyber incident surges, each minute is priceless. Firstly, you need to establish effective communication channels to avoid wasting time and resources and manage the emergency successfully.

CIRP must indicate who should be informed about the incident in the first stage. Usually, it's the IT department or a stated member of the Cyber Response Team. A student, teacher or staff member who identifies an incident must report this, including time, location and other important information.

To streamline communication, maintain direct contact with individuals responsible for crucial school infrastructure internally and externally. You may have contracted vendors for IT services such as cloud storage, the wi-fi network, firewall and virus protection, content filtering, etc.

The Plan should specify how and when the school needs to inform about the cyber emergency third parties providing affected services and data, the insurance company, the local police office, etc.

2. Cybersecurity Emergency Procedures

During the Incident

a. Incident Detection

Automated, real-time risk monitoring enables you to detect a cyber incident rapidly. Remember to record the incident from the beginning; you will need solid evidence for cybercrime. Take your methods for handling and safeguarding proofs for further investigation and reporting.

b. Incident Analysis

- Assess Incident Nature

In this stage, the Cyber Response Team deeply investigates the cyber incident that is occurring in the school. They determine what caused it, when and where it started, what user or service is involved, and how the incident happened.

Incident classification is essential to understand what challenge is facing your school.

- Assess Incident Impact

Your next steps depend on the severity of the cyber incident. Incident Triage helps evaluate the incident's severity and impact on school infrastructure, users, data, resources, and services.

The cybersecurity event may have no or minor, medium or high impact, and cause data breaches of different scopes; its restoration may need only school or third-party resources.

After this analysis, you can prioritise and resolve the cyber threat.

c. Incident Response

Your mission now is to react accordingly to the cybersecurity emergency, contain the threat, and stop its escalation. The way to achieve this depends on the character and scope of the cyber incident.

Act quickly to prevent its consequences from spreading and to prevent further damage to your school system. You must have the appropriate privileges and knowledge to temporarily disable some functions, connections, or user permissions in your domain if needed.

After the Incident

a. Recovery

Once the cyber threat emergency has been managed and controlled, it's time to eliminate the cause of the incident. School recovery may mean removing malicious software, restoring affected data, and restarting the entire school system.

This process should last as fast as possible to prevent the long-term deprivation of students, teachers, and other staff members of essential functions, resources, and data. At the same time, make sure the recovered systems are working correctly before enabling them for all users. Thoroughly cleaning affected systems and data is vital for avoiding any risk of the following cyber incident.

b. Conclusions

As the Cyber Recovery Team, discuss the lessons you learned from the incident and update school cybersecurity policies and procedures accordingly. Additionally, remember to review the emergency communication policy, considering the conclusions after managing the last incident.

Report the school incident to the parents' council, your school district, the federal law enforcement office, and any other school-related body that should be aware of it.

3. Post-Incident Maintenance

Reviewing

Review and update your Cyber Incident Response Plan regularly to stay prepared and efficient in an emergency. Continuously learn from your and other schools' experiences dealing with cybersecurity challenges.

To avoid vulnerabilities, keep all digital infrastructure, such as devices, software, data storage, and networks, up to date. Also, stay current with current digital threats and new techniques of cyber attacks in education and beyond.

Cyber Training

Education and exercises in emergency scenarios are crucial for raising cybersecurity awareness and improving skills among students and teachers. The simulated tests should include all people involved in the crisis management of an actual cyber incident.

Closing Thoughts

The Cyber Incident Response Plan is your powerful instrument to build a safe and secure digital environment in your school. It supports you, admin, in the event of a cyber incident and guides you step-by-step in managing the emergency effectively and reducing damages. Protect student data – your school's treasure – successfully and maintain peace of mind.

Download our Cyber Incident Response Plan Checklist to keep every detail of your CIRP under control.

Dive Deeper Into GAT Labs For Education

EXPLORE MORE

Want To Know More?

Schedule a Demo

GAT Labs for education