

CYBERSAFETY FOR SCHOOLS

How Policy, Technology, and Awareness
Can Defeat Cyberthreats In Education



Contents

Introduction	3
Why Schools Are Vulnerable To Cyberattacks	3
Incentives – What Cyberattackers Seek In Schools	3
Opportunity – How Cyberattackers Enter Schools	4
Consequences of Cyberattacks on Schools	5
Direct Financial Costs	5
Indirect Financial Costs.....	5
How Schools Can Stop Cyberattacks	6
Policy Initiatives	6
Roles & Responsibilities	7
Permitted Use	7
Standards.....	7
Lifecycle Management.....	8
Penalties	8
Technology Solutions	8
Endpoint Security.....	8
Network Security.....	9
Data Protection	9
Training and Awareness.....	10
Cybersecurity Essentials	11
Cybersecurity Communication	13
K7 Cybersecurity for Schools	14
K7 Endpoint Security.....	14
K7 Unified Threat Management.....	14
K7 Academy	14



Introduction

No school can afford to ignore the power of digital technology and how it can benefit the lives of students. Equally, no school can afford to ignore the risks that accompany such technology. Cyberattacks against American schools tripled in 2019 and had a record breaking increase again in 2020. Over 1,000 Indian schools and colleges were hit by cyberattacks between June and September 2020.

Why Schools Are Vulnerable To Cyberattacks

All cyberattacks, whether against schools or against other sectors, are carried out because the attacker or their customer stands to gain directly or indirectly from the attack. A successful cyberattack is therefore the result of the intersection of incentives and opportunity.

Incentives – What Cyberattackers Seek In Schools

- **Data** – The cyberthreat industry thrives on data just as much as the rest of the world does. Schools are highly attractive targets for data theft because they hold a wide variety of data including
 - Personal and academic information of students
 - Personal and financial information of students' parents
 - Administrative and financial records of the school
- **Disruption** – Disrupting school operations can benefit different types of threat actors in different ways:
 - **Internal Attackers**
 - Students – Students may wish to prevent an exam from occurring
 - Staff – Staff may cause disruption to divert attention from other concerns or to destroy data that could incriminate them
 - **External Attackers**
 - Ransom Demands – Threat actors launch ransomware attacks on schools because they believe that schools cannot pause academic activity indefinitely to recover from the attack and will pay the ransom quickly
 - Cyberwarfare – Nation state sponsored hackers attack schools to affect the capability of future generations



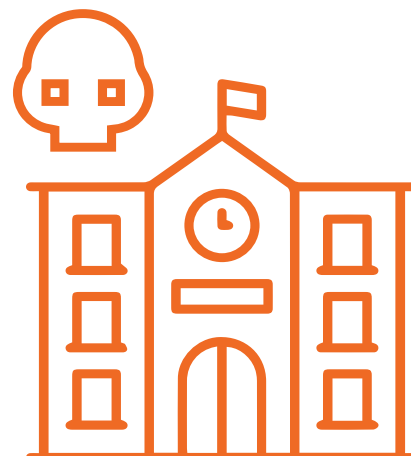
- **Fraud** – The importance given to education and the nature of a school’s activities make digitally-enabled fraud attractive for attackers, who attempt:
 - **Financial Fraud** – Both internal and external attackers may try to obtain funds fraudulently by manipulating invoices or initiating fake fund transfer requests
 - **Academic Fraud** – Academic records of students and credentials of staff can be manipulated to affect their professional opportunities , or to harm the reputation of the institution

Educational institutions may be puzzled by the demand for student data. What does the attacker gain by accessing the Personally Identifiable Information (PII) of a child? There are many ways in which such data can be used and it may not be used immediately e.g., the attacker may wait until the student turns 18 and then apply for a loan in their name (identity theft). The student may become aware of this many years later when they apply for a loan or credit card and discover that they have a bad credit rating due to the attacker’s actions, resulting in lower credit limits, higher interest rates, and the need to provide more/better loan collateral.

Opportunity – How Cyberattackers Enter Schools

The large number of students, the constant churn in users as students join and leave the institution, and the need for constant staff and student interaction imply that a large number of computing devices and storage media will interact with the school’s network, creating a number of points of entry for an attacker. Vulnerabilities arise in:

- **Classrooms** – Even if the computer that is used in a classroom is not connected to the internet, it will usually connect to the school’s network and allow access to thumb drives to transfer presentations and videos, which allow malware to spread
- **Computer Labs** – Computers in the computer lab are networked and they also need to allow students to connect their personal thumb drives to lab computers for their project work. The combination of a large number of users, a large number of personal storage devices, and the experimental nature of activities that are conducted in the computer lab create opportunities for attackers
- **Administrative Offices** – Administrative offices in schools have to interact with both internal and external stakeholders, and their computers need to connect to the internet and to the school network. Threat actors can use social engineering tactics, like phishing, to enter and spread through the school network via the devices used by the administrative office
- **Faculty Devices** – School faculty often need to use their laptops at home where they connect to personal internet. This creates an entry point for cyberattackers who can plant malware in the laptop when used at home (e.g., through a malicious website) and then wait until the laptop connects to the school network to compromise the school





Consequences of Cyberattacks on Schools

Cyberattacks are more than just an inconvenience. Schools incur direct and indirect costs following a cyberattack.

Direct Financial Costs

Direct financial costs are usually incurred immediately after the attack, and can be directly linked to the attack.

- **Operating Cost** – Altering invoice value, or similar fraudulent activity, will cause an increase in the school's operating expenses
- **Capital Expenditure** – Misappropriation of funds and underutilisation of assets (e.g., books that are available in the library are purchased again because the books' entries have been removed from the library catalogue) will result in an increase in capital expenditure
- **Opportunity Cost** – Money that is spent on recovering from the cyberattack is money that is not spent on other school projects, which can affect the growth of the institution

Indirect Financial Costs

Indirect financial costs are the costs that are incurred some time after a cyberattack, may not be directly linked to the cyberattack, and may be in the form of lost income rather than an additional cost.

- **Reputation Loss** – Cyberattackers can manipulate or delete exam results, force exams to be postponed, and put students at risk by manipulating school bus routes. Such activities can destroy your school's reputation and lead to severe financial hardship
- **Compensation** – Schools may need to pay compensation to affected parties to avoid further loss of reputation





How Schools Can Stop Cyberattacks

Schools can stop cyberattacks by following a 3-pronged approach:

The Cybersafe School



Policy Initiatives



Technology Solutions



Training and Awareness

Policy Initiatives

Every organisation, from a Fortune 500 enterprise to a neighbourhood school, should have a cybersecurity policy. The cybersecurity policy exists to define what cybersafety means in the context of that particular organisation, what is required to achieve cybersafety, and what will be required in future to remain cybersafe. The cybersecurity policy should also create powers for school officials to ensure that the policy is implemented.

The outbreak of COVID-19 has shown us that schools need to be able to switch quickly from in-person classrooms to virtual classrooms. Your school's IT policy should reflect this and promote an IT strategy that supports seamless transition to working and studying from home when required.

Your school's cybersecurity policy should discuss:

Roles & Responsibilities



Who does What and When, and who is responsible for enforcement

Permitted Use



How organisational IT assets may be used

Standards



Cybersecurity standards such as password strength and encryption technologies

Lifecycle Management



Hardware, Software, and User lifecycle management

Penalties



Penalties for non-compliance



Roles & Responsibilities

A faculty member needs access to websites that are not typically required in a school (e.g., entertainment). This requirement raises several questions:

- How, and to whom, should the request be communicated?
- Who will verify that the request is legitimate?
- Who will approve/authorise the request?
- Who is responsible for providing access (or coordinating with the school's IT vendor to get it done)?
- How long should each stage of the process take?

The cybersecurity policy should address these, and similar, questions that arise whenever the school's stakeholders are not sure how they should proceed.

Permitted Use

Before we discuss permitted use, let us first establish that no one in the organisation should enjoy completely unrestricted permissions all the time. Leaving all the doors open for a cyberattack should not be allowed and restrictions should always be applied to all users. Any and every internal or external stakeholder who has access to the school network or school data should have the least privileges required to carry out their responsibilities. Additional permissions that are required occasionally should be granted only when required and only for a short period of time. Based on the user's responsibilities, restrictions on use may be formulated as

- **Specifically Permitted** – Only specific use cases are allowed and other forms of use are not permitted. This is appropriate for most users
- **Specifically Excluded** – Everything is allowed except for some use that is not permitted. This is suitable for users at higher levels in the organisation's hierarchy

Special consideration is required for IT administrators. These roles require elevated privileges but they also pose a risk: if an attacker can plant malware through an IT administrator's account, the malware will cause a lot of damage due to the privileges enjoyed by the IT administrator. Therefore, IT administrators should use their admin accounts only for tasks that require such privileges and use accounts with restricted privileges for all other activities.

Restrictions are not limited to IT asset access. Permitted use implies permitted behaviour e.g., the school's IT equipment, services, or networks should not be used to bully or harass others.

Permitted use should also cover the school's social media channels i.e., restrictions should be placed on who can post updates, and the types of updates that can be posted

Standards

All users are encouraged to have strong passwords, but what does that mean? How many characters and what characters are permitted? How often should passwords be changed? The school's cybersecurity policy should define these standards and not leave them open to interpretation or guesswork. The [Assessing Security Requirements for Controlled Unclassified Information](#) document published by National Institutes of Standards and Technology (NIST) can be used as a starting point to determine the controls and safeguards appropriate for your school.



Lifecycle Management

Every device, application, and user has a lifecycle in the context of your organisation e.g., a device has a lifecycle from the time it is purchased to the time it is decommissioned and a user has a lifecycle from the time they join your school to the time they leave. This IT lifecycle has to be managed to keep your school cybersafe.

- **Hardware Lifecycle Management** – The manufacturer's commitment to providing frequent security updates should be confirmed before procuring hardware; security updates should be applied immediately; all hardware deployment should be recorded and monitored; lost/stolen mobile devices should be capable of being tracked and retrieved or remotely wiped; all devices should be sanitised (data should be deleted in a way that cannot be recovered) before disposal
- **Software Lifecycle Management** – Fragmentation of the IT environment should be avoided by requiring all departments to use the same software for the same task, and all software should be updated with the latest security patches available. Software that is no longer supported by the vendor (i.e., the vendor no longer provides patches for that version) should be upgraded or replaced
- **User Lifecycle Management** – All user privileges granted and removed should be recorded. Former users' data and network access privileges should be revoked as soon as they leave the school and current users should be granted access based on the [principle of least privilege](#)

Penalties

A cybersecurity policy will be ineffective if it isn't enforced. Enforcement requires penalties both for non-compliance on the part of users and non-enforcement on the part of leaders.

Framing a cybersecurity policy may seem like a daunting task, but it becomes much easier when you focus on Who, What, When, Where, Why, and How while preparing the policy. [This school's cybersecurity policy](#) can be used as a base from which you can develop a policy for your institution.

Technology Solutions

The IT infrastructure of a school includes endpoints, networks, and data, and technology solutions should be deployed to protect all three.

Endpoint Security

Every computing device (desktop, laptop, and server) that connects to your school's network is an endpoint, and every endpoint should be protected with an enterprise-grade cybersecurity solution like [K7 Endpoint Security \(K7 EPS\)](#). The solution should be easy to deploy and manage, support rapid rollout, and not impact device or network performance.

The endpoint security solution should include these features:

Device/Data Protection	Cybersecurity Management
• Malware Protection (including ransomware protection)	• Centralised and Remote Management
• Network Protection	• Hardware Asset Management
• Web Protection	• Group Based Administration
• Device Management & Control	• Security Incident Notifications
• Application Control	• Cybersecurity Reports

It is imperative that every endpoint be secured. Even one unsecured endpoint can open the doors to a cyberattack that will spread from that endpoint to your entire organisation.



Network Security

Preventing attacks on your school's network primarily involves perimeter security i.e., preventing unauthorised access and activities from the external world. An in-depth examination of network security is beyond the scope of this whitepaper but your school's network should include these security features:

- **Access Control** – Only authorised users should be able to connect to your organisation's network and they should be able to connect only with the privileges assigned to them
- **Gateway Security** – Securing the perimeter of your school's network creates a safe computing space within the perimeter
- **Segmentation** – Network segmentation effectively creates multiple internal networks e.g., the computer lab in your school and your administrative office can operate using different network segments. This reduces the possibility that a single compromised endpoint within one network segment could be used to launch an attack against the entire organisation

Network security requirements apply to both wired and wireless networks.

Data Protection

Endpoint and network security do help protect data but there is no such thing as 100% security; an attacker, especially an internal attacker, may be able to get past such security measures. It would therefore be wise to include data protection measures in your school's cyber defences.

Data Protection Measures	
Data Backup	Data Encryption

Data Backup

Having a backup of data will help your school restore data in the event data is destroyed or made inaccessible by a cyberattack. It can also serve as a point of reference if you suspect that data has been modified rather than destroyed e.g., manipulation of students' marks or teachers' credentials. Additionally, a data backup is useful in the event of hardware failure.

- **Follow the 3-2-1 rule** – Data should be backed up thrice; 2 copies should be available on-premises but stored on different media, and one backup should be available off-site. This is required to ensure that a cyberattack does not affect the data backup as well e.g., some ransomware is designed to look for and encrypt backups
- **Frame a retention policy** – Retaining old data backups is expensive and runs the risk of restoring an outdated copy of data. Evaluate your school's requirements and frame a policy to regularly delete old data backups
- **Test backup restoration** – A data backup is not of much use if the data cannot be restored quickly and easily. Perform a test restoration to verify the ease with which data can be restored

Do not limit data backups to sensitive or confidential data. Administrative data or lesson plans may not be confidential but they are essential to the smooth functioning of your school. Restoring such data from a backup will help resume normal activity quickly in the event of a cyberattack.





Data Encryption

Data encryption is necessary for sensitive information, such as personal or confidential data, to ensure that a cyberattacker cannot use or sell your school's data even if they manage to steal it. Some cyberattackers may even try to blackmail your school by threatening to release the personal information of students; such extortion attempts are not possible if the data is encrypted. Data should be encrypted both at rest (when it is stored) and in transit (when it is communicated to others). Encryption should be applied wherever it can be applied, including

- **Devices** – Sensitive data stored on a device should be encrypted. This may require that the entire device, with all data stored on it, be encrypted; this will ensure that the data is safe even if the device is stolen
- **Storage** – Data storage, such as data backups, should be encrypted; a threat actor may try to compromise the data backup to extract sensitive information as an attack on a data backup may not be noticed as quickly as an attack on data that is in use. This means that even a USB storage device, like a pen drive, should be encrypted if it is used to backup, move, or share sensitive data
- **Cloud** – Data that is stored or shared using the cloud should be encrypted. This is especially important if your school, or any individual in your school, uses 3rd party cloud-based file sharing services where you don't have much, or any, control over how your data may be accessed or used by the cloud service provider or any of their employees
 - Messenger services, and other communication tools, should also be considered cloud based data storage services in the context of institutional cybersecurity as they permit file sharing but they may not be secure. For instance, [WhatsApp data that is backed up on Google Drive isn't protected by encryption](#), which your school may need to consider when framing its communication policies
- **Website** – Your school's website should make use of HTTPS rather than HTTP to encrypt information that flows between the website's server and the user's browser; this will help prevent the interception or hijacking of communication through [Man-in-the-Middle \(MitM\)](#) attacks

Training and Awareness

Framing policies and implementing technology solutions are necessary but not sufficient to protect your school. They may also take longer to implement due to consultations with various stakeholders and budgetary concerns. Increasing awareness and training on cybersecurity for staff and students is often quicker to implement and can be very effective as well, as the user is often the weakest link in the cybersecurity chain which threat actors exploit through tactics like social engineering that target the user rather than the device or network.

Human error accounts for [22% of breaches. 91% of cyberattacks employ phishing](#) (a form of social engineering). Training and awareness programmes can mitigate such common points of entry for an attacker. They also help your school's students learn about cybersecurity which can now be considered a critical life skill.





Cybersecurity Essentials

Your school's training and awareness programmes should cover:

Password Hygiene

Many users do not practise password hygiene because they are not aware of the various ways in which threat actors can compromise passwords. Repeatedly remind the users in your organisation that passwords should be

- **Strong** – Simple and easy-to-remember passwords are tempting to use but such passwords are also easy to guess or can be discovered through techniques like [brute force cracking](#)
- **Random** – Passwords that are long and use different types of characters are described as difficult to crack, but that may not be correct if they use common phrases or the personal information of the user e.g., a long password can be created by combining the user's hometown and their car brand, but it is still relatively easy to guess even if it uses numbers in place of some alphabets. A password requires a random combination of characters to be considered safe

Equally, remind users that passwords should not be

- **Recycled** – Using old passwords again can expose the user and your school to cyberattacks because cyberattackers know that users recycle passwords and may keep trying old passwords that were previously compromised until they work again
- **Reused** – Users may not recycle passwords but may reuse the same password across different sites and services. Cyberattackers are aware of this behaviour as well, and are known to use passwords obtained from one organisation to compromise another
- **Shared** – Password sharing is another common practise that may have severe repercussions for your school. The probability of a password leaking is much higher when multiple people know it. Internal attacks also become a lot easier when a password is shared because the attacker knows they cannot be identified by the login through which the attack was launched

Password managers can be used to help users generate random passwords and remember the passwords for them. Multi-factor Authentication (e.g., receiving an OTP in addition to having a password) can also be used where additional security is required.





Phishing

Imagine the consequences if a member of the administrative staff in your school received an email that claimed to be from the principal or a trustee asking for a report with confidential information or a transfer of funds, and the staff member complied without checking if the request was genuine.

This is phishing – a form of social engineering that cyberattackers use to convince an end user to perform an action that is against their best interest or the best interest of the organisation. Some forms of phishing can be stopped by technology, but phishing is an attack on the user and not the device and can occur through email, SMS, WhatsApp, phone calls, or even through the personal social media of the user, which limits the effectiveness of technology solutions that are deployed within the school environment. The best defence against phishing is a well informed user. Computing users in your school should be trained to follow these precautions both in their personal and professional lives:

- Check the actual email ID or phone number from which a message originates to verify if the sender is genuine
- If the message includes a link, the authenticity of the link should be checked before entering any information in the linked page. Cyberattackers can create pages that mimic the look and feel of legitimate websites (such as banking websites) to lure users into entering their login credentials or providing other sensitive information
- Apps should only be installed from official app stores. The ratings and reviews of the apps should be checked before installation as official app stores may contain fake apps
- Messages that require urgent action should be scrutinised carefully as cyberattackers use urgency to get users to act quickly before their suspicions are aroused
- Any message that sounds too good to be true (such as an unbelievable offer) should be verified (e.g., visit the official website of the vendor or contact their customer support from a number mentioned on the official website to confirm if the offer is genuine)
- Do not add friends or contacts on social media if they are purely online acquaintances. If they are known to the user in real life, they should confirm that the account is theirs as attackers are known to create fake profiles of real people on social media
- When in doubt, contact the source of the message to check if the request is genuine; contact them using a verified method of communication (e.g., if a staff member receives an email asking for a transfer of funds, they should call the sender using a phone number that has been previously provided to the school)





Personal Device Protection

Your school can install updates on official devices, but students and staff use their personal devices for academic and extra-curricular activities and such personal devices need to be protected as well to prevent malware spreading from them to the school. Personal device protection includes

- **Updates** – Encourage staff and students to keep their personal devices updated with the latest patches, and to choose devices where the vendors have a track record of providing timely updates. Personal devices, in this context, include home Wi-Fi routers and connected devices like fitness trackers and smart speakers whose patches are provided as firmware updates. [Even cameras are vulnerable](#) to cyberthreats, indicating that no personal device is safe and all personal devices have to be updated diligently
- **Antivirus** – All personal computing devices (desktops, laptops, mobile phones, and tablets) should be protected by antivirus such as [K7's home user antivirus](#). The antivirus should also be kept updated with the malware definition updates that are released every day by antivirus vendors. Antivirus for mobile devices should include device tracking to enable the retrieval of lost or stolen devices

Cybersecurity Communication

Training and awareness cannot be a one-time event. Even if training seminars cannot be conducted frequently, students and staff can be reminded to be cyber cautious through messages circulated via notice boards, social media, email, or any other channel that your school uses to communicate with staff, students, and the parents of students. Constant reiteration is required for effectiveness.





K7 Cybersecurity for Schools

K7 Security combines 30 years' expertise in cybersecurity with a state-of-the-art threat research lab to deliver multi-layered, rapidly updated enterprise cybersecurity solutions that protect critical data and devices in small and large organisations around the world.

K7 Endpoint Security

The international award-winning [cybersecurity solution for desktops, laptops, and servers](#) offers more than just protection against malware:

- **Manageability** – Complete centralised and granular control over hardware, applications, and web access
- **Cost-savings** – Lean definition updates and world-renowned low-impact protection that does not impair device performance ensure that bandwidth or hardware upgrade will not be required
- **Rapid Rollout** – Compact installers, optimised out-of-the-box configuration, and customisable endpoint installers ensure quick deployment that will not disrupt school operations

K7 Unified Threat Management

This [range of high-performance security devices](#) provide gateway security to protect the school's network, and include:

- **AAA Framework** – Authentication, Authorisation, and Accounting for intelligent access management
- **SPI Firewall** – The Stateful Packet Inspection Firewall with integrated Intrusion Detection System/Intrusion Prevention System (IDS/IPS) and Denial-of-Service (DoS) attack protection keeps hackers at bay
- **VPN** – SSL/IPSec Virtual Private Network for secure communication

K7 Academy

The K7 Academy offers training by cybersecurity experts backed by K7's 30-year expertise in cybersecurity. Awareness and training programmes are customised to the needs of your organisation and include

- Staff and student training which covers the fundamentals of cyber hygiene, awareness on phishing attacks and how to spot them, and securing home IT infrastructure
- IT staff cybersecurity training to ensure that your IT team have the knowledge and skills required to create a safe computing environment in your school





Copyright © 2021 K7 Computing Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7computing.com