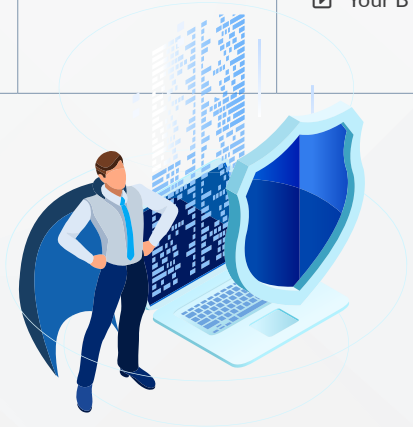
TOP 10 TIPS TO PROTECT YOUR SCHOOL FROM RANSOMWARE

Kaseya

Over the past several years, educational institutions, especially K-12 schools, have become hot targets for ransomware attacks. Their relatively simple IT and security infrastructure makes it easy for cybercriminals to execute their nefarious schemes. Moreover, by demanding a small ransom, most cybercriminals get what they want without drawing much attention to themselves.

In this environment, safeguarding the data and personal information of your students, teachers, administrators and all stakeholders is paramount. To help you build a robust cybersecurity strategy to keep your school safe from ransomware and other threatening cyberattacks, we've created a handy 10-point checklist so you can carry out all the necessary checks.

✓		
	1. Perform a security assessment	Identify: ☐ Your critical assets ☐ External vulnerabilities that could be potential security gaps that would allow hackers access to your network and information ☐ System protocol leakage - outbound protocols that shouldn't be allowed ☐ Lack of web browser controls ☐ Wireless network security issues ☐ Network share permissions
	2. Set up a secure VPN connection for students, teachers and administrators to access resources safely and remotely	Here are a few guidelines: ☐ Use a strong encryption method for VPN ☐ Consider Layer Two Tunneling Protocol (L2TP) over Internet Protocol security (IPsec) ☐ Consider OpenVPN over Point-to-Point Tunneling Protocol (PPTP) ☐ Use an endpoint management tool to deploy, configure and monitor VPN clients on remote endpoints ☐ Automate the process of redeploying the VPN client if it goes down
	3. Have a Bring Your Own Device (BYOD) policy that specifies security requirements	Your BYOD policy should have the following provisions to ensure maximum endpoint security: ☐ Chart out the minimum required security controls for devices ☐ Provide components, such as SSL certificates, for device authentication ☐ Enforce strong password policies ☐ Control and monitor the installation of apps ☐ Define policies to be followed when individuals leave school. Outline procedures for data erasure and the restriction of access to resources ☐ Your BYOD policy should require an agent to be installed on the endpoint for managing the device



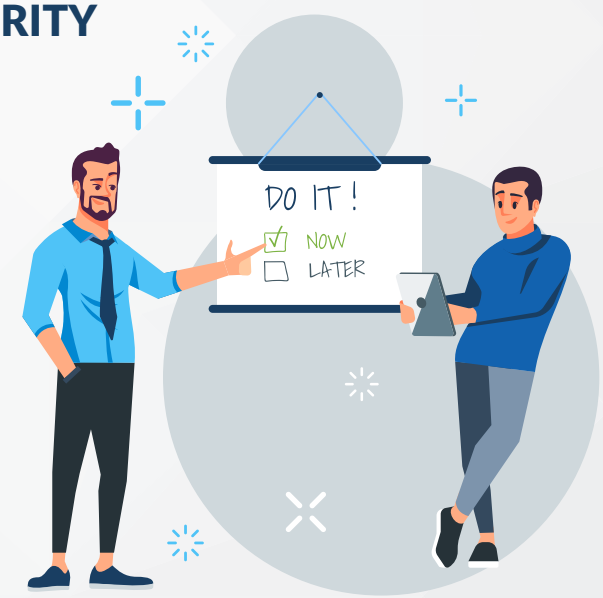
Kaseya

✓		
	4. Automate software patch management and vulnerability management	Install, deploy and update software on each endpoint automatically using an endpoint management solution. Timely patching helps keep software and operating systems up to date and addresses known vulnerabilities, thus strengthening cybersecurity. A best-in-class RMM effortlessly automates the complete patching lifecycle. From sourcing patches to installing them based on specified policies and priorities, it should do everything for you. ☐ Have real-time visibility into the patch status of your on-and-off network devices ☐ Have visibility into the software vulnerabilities that impact your IT environment ☐ Set up auto-remediation of vulnerabilities through proactive scanning and automated patching
	5. Back up systems and SaaS application data with integrated backup and disaster recovery solutions	Implement a robust backup solution that: ☐ Integrates with your endpoint management solution for seamless backup management ☐ Automates testing for guaranteed recovery ☐ Ensures clean, instant recoveries Back up your SaaS data for speedy restoration in case of malware, phishing or user errors.
	6. Implement multifactor authentication (MFA) and single sign-on (SSO)	SSO and MFA increase authentication security by: ☐ Reducing the need to remember user credentials ☐ Requiring additional information, beyond passwords, to log in to the user's account. For example, with two-factor authentication, you would get a one-time passcode ☐ Letting users log in securely to multiple applications with one set of credentials
	7. Educate your students and staff, and monitor your exposure to the dark web	Monitor the dark web to take proactive steps to prevent a security breach ☐ Scan the dark web for stolen credentials ☐ Set up alerts if any institutional data or student/teacher personal data is found on the dark web ☐ Change the passwords as needed and implement strong password policies ☐ Educate students, administrators and all stakeholders with simulated phishing emails and security awareness training videos
	8. Detect and respond to insider threats and monitor for all unknowns	The moment of compromise is not the moment you learn of the compromise. It's often weeks beforehand. Attackers won't detonate their ransomware bomb until they're confident they can lock out a significant portion of the network. Early warning can easily prevent the attack itself. Due to end-user propensity for clicking infected links, ransomware is no longer an "if" but rather a "when" scenario. A best-in-class RMM can do all of this for you. If you don't have an RMM that can do this out of the box, make sure to manually enhance your organization's security by taking these steps to respond to these threats: ☐ Monitor unauthorized logins and restrict privileged user access ☐ Track unusual or odd-hour login behavior ☐ Set alerts when wireless connections are added to the network ☐ Set alerts for foreign RMM agents being installed ☐ Monitor for any ransomware-style notes left ☐ Automatically isolate potentially infected endpoints when one or more of the above conditions are met

✓		
	9. Deploy an antivirus/anti-malware and endpoint detection and response (EDR) combined solution	Go beyond traditional antivirus and anti-malware and implement an EDR solution to combat cyberattacks. EDR solutions record system activities and events taking place on endpoints and provide security teams with the visibility they need to uncover and remediate incidents. A sophisticated EDR solution identifies and removes cyberthreats from your environment by: ☐ Constantly monitoring your environment for security incidents and anomalies ☐ Providing real-time threat detection and automated remediation ☐ Delivering fast incident triage, investigation and response ☐ Offering pre- and post-compromise attack visibility (Root Cause Analysis)
	10. Implement and practice your incident response plan	All institutions must be prepared for major security incidents that could drastically affect their operations. Plan and practice a step-by-step incident response strategy that incorporates the following: ☐ Define the roles and responsibilities of each member of your incident response team ☐ Have a business continuity plan ☐ Identify the tools, technologies and resources that must be in place ☐ Define all critical network and data recovery processes ☐ Identify and remediate the root cause of the incident – apply patches, update systems, remove malware, etc. ☐ Have a communications plan for both internal and external stakeholders

FOR COMPREHENSIVE LAYERED SECURITY OF YOUR DEVICES AND DATA

CLAIM YOUR FREE TRIAL NOW



About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

02062024