COMMVAULT

10 STEPS

EVERY SCHOOL AND COLLEGE SHOULD TAKE TO PREPARE FOR A CYBER ATTACK

Microsoft

10 STEPS

EVERY SCHOOL AND COLLEGE SHOULD TAKE TO PREPARE FOR A CYBER ATTACK

Have you done the basics? Cyber defense starts with these core strategies

During the four-week period from Aug. 14 to Sept. 12, 2021, schools and colleges were the target of more than 5.8 million malware attacks worldwide, or 63% of all such attacks. Including the costs of downtime, repairs, and lost opportunities, the average ransomware attack cost educational institutions $2.73 million in 2020—and 44% of educational institutions were targeted by such attacks.[1]

Cybersecurity is no longer something educational institutions can take lightly. Cyber crime affects schools and colleges of all sizes. Because it's hard to predict how technology will be exploited, K-12 and college leaders must assume that anything connected to their network is a potential target and prepare to be as resilient as possible.

The average ransomware attack cost educational institutions $2.73 million in 2020—and 44% of schools and colleges were targeted by such attacks.

Here are **10 essential steps** you should take to protect your institution from a cyber attack

PROTECT

1 Assess risks and form a plan

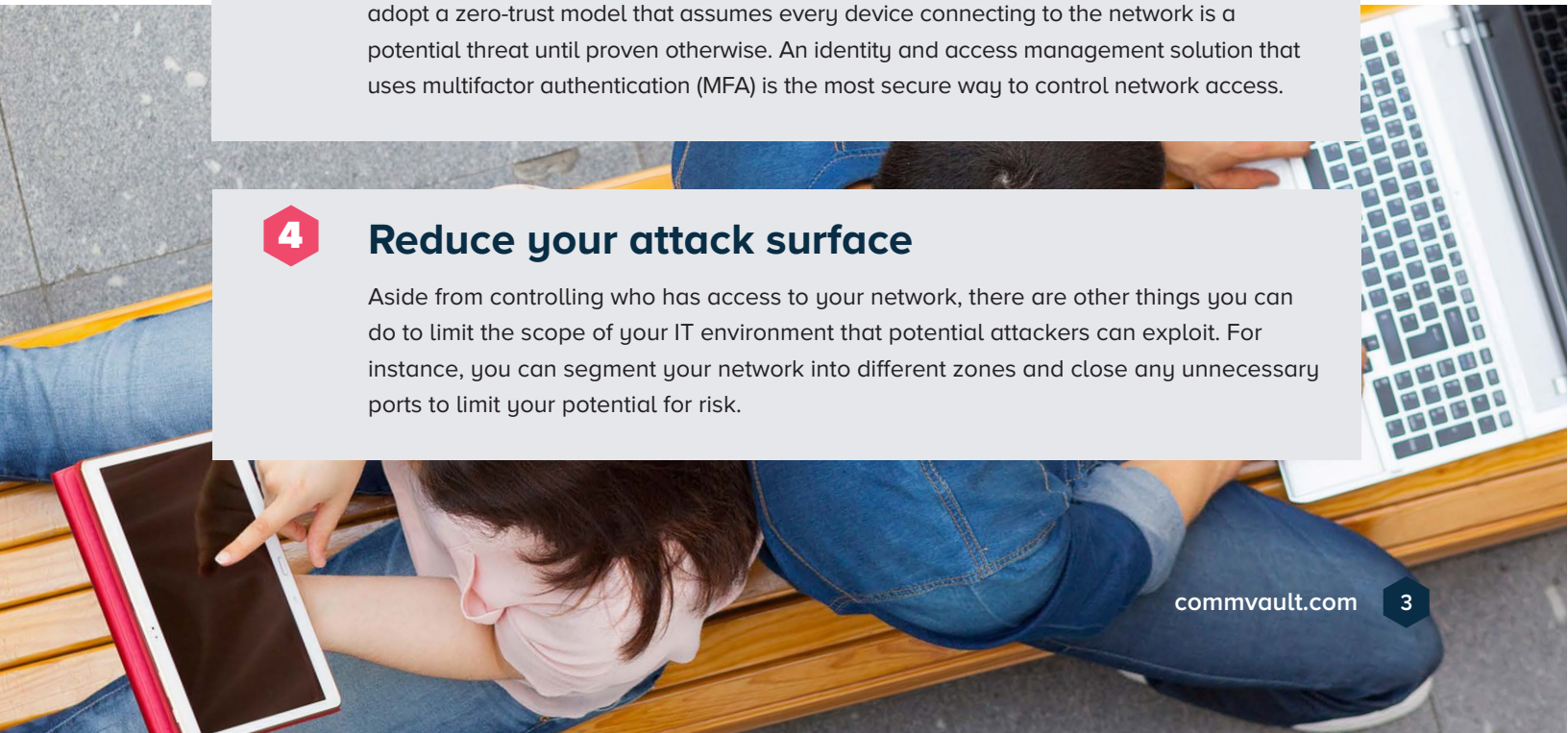
Your plan should address not only how you'll protect your systems from attacks, but also how you'll respond and recover in the event of a security breach. Make sure you understand who's responsible for what tasks and set data recovery priorities.

2 Educate users

Students and staff must learn cybersecurity best practices, such as how to create strong passwords and update them regularly. They also need to know how to identify potential phishing scams and what to do if they receive a suspicious-looking email. These conversations should happen throughout the school year, not just once at the beginning of the term.

3 Control access

In addition to using a firewall and antivirus/anti-malware software, institutions should adopt a zero-trust model that assumes every device connecting to the network is a potential threat until proven otherwise. An identity and access management solution that uses multifactor authentication (MFA) is the most secure way to control network access.



4 Reduce your attack surface

Aside from controlling who has access to your network, there are other things you can do to limit the scope of your IT environment that potential attackers can exploit. For instance, you can segment your network into different zones and close any unnecessary ports to limit your potential for risk.

PROTECT

5 Regularly back up data

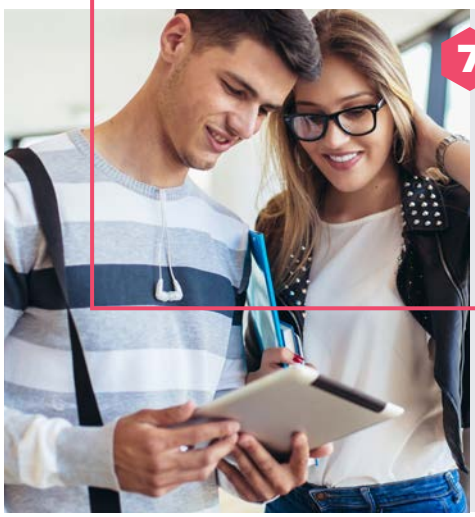
Keep immutable, offsite backups for high-priority data and/or highly sensitive information, as well as critical system configuration files. Test your backup systems regularly, and practice restoring your data so you're prepared to do this as needed.

Test your backup systems regularly, and practice restoring your data

6 Practice basic security hygiene

Keep all IT systems up to date so they have the latest protection, install security patches as these are released, test defenses to make sure they're working correctly, routinely audit systems to see where vulnerabilities might exist, and review sensitive data to see what can be archived or deleted.

DETECT



7 Monitor your IT environment

You should be scanning your network for vulnerabilities so you can detect and respond to attacks in real time, before they can do much damage. Monitoring your IT environment requires full visibility into all connected devices and the applications they're using, ideally through a single interface. Establish baseline behaviors for your IT environment, and watch for signs of anomalies with a combination of machine learning technology and trained security staff.

RESPOND

8 Identify, contain, and eradicate threats

When a breach is discovered, the first step is to identify the source and contain the threat so that it doesn't spread and cause further damage. Then, all traces of the threat must be eliminated. A trusted third party can help you respond to an incident swiftly and effectively.

9 Restore systems to their original state

You can minimize the disruption to your operations if an incident does occur by quickly recovering your data. If you're a victim of ransomware, paying your attacker can't guarantee a return to business as usual. The only safe strategy is to invest in a solution that fully restores your data from backup systems.

10 Learn from the incident

Once you've recovered from an attack, hold a debriefing meeting with all IT security team members and discuss what you learned from the incident. Determine what worked well in your response plan and where there might have been gaps. The lessons you learn from both real and mock events will help strengthen your defenses against future attacks.

A CRITICAL NEED

Cybersecurity is too important to be left to chance. Schools and colleges can build robust cyber defense and recovery systems into their operating budget like any other utility through a security-as-a-service model. To learn how Commvault and Microsoft can help, contact your Commvault sales representative today: microsoft@commvault.com

Learn more: https://www.commvault.com/supported-technologies/microsoft/edu-solutions

[1] Kshetri, Nir. "The average ransomware attack cost educational institutions $2.73 million." Nextgov, Sept. 17, 2021. https://www.nextgov.com/ideas/2021/09/cybercriminals-use-pandemic-attack-schools-and-colleges/185429/