CENTER FOR
DEMOCRACY
& TECHNOLOGY

A SERIES ON TECHNICAL RESOURCES IN EDUCATION

Ransomware in Schools:
Best Practices for Prevention and Mitigation

In a year already full of unprecedented challenges, schools are facing another concerning problem: ransomware. Ransomware is a particular kind of cyberattack that locks legitimate users out of their own systems, typically by encrypting the data and withholding the key to decrypt it, thereby making it inaccessible. The attackers then demand a ransom, typically financial, to return access to the rightful owners. Attackers may also exfiltrate data (save a copy of the data from the system) before encrypting it, and threaten to publicly disclose that data if the victim does not pay the ransom. Attackers may or may not agree to destroy this copy as part of the exchange for payment of the ransom (though even if they claim they will do so, it is typically impossible to verify this claim).

Although schools were experiencing ransomware attacks before the pandemic (in 2019 Louisiana was forced to declare a state of emergency in response to ransomware attacks), their prevalence has increased during the pandemic. Additionally, these attacks have the potential to be particularly devastating as schools are now heavily dependent on technology for remote learning, and students are already behind on instructional time. The Clark County School District in Nevada also had to deal with the exfiltration of its data, adding all the concerns of a typical data breach (loss of trust, identity theft of students and staff, secondary breaches, etc.) to the lost access and instructional time.

Schools are appealing targets for ransomware, because they maintain large amounts of data and are often under-resourced with respect to technology and technical expertise. However, there are steps schools can take to reduce the risk of a successful attack and minimize the harm if such an attack occurs.

Prevention

Cybersecurity Best Practices

Because attackers must exploit some sort of vulnerability in order to get the ransomware onto the targeted system, standard cybersecurity practices are an important part of prevention. Best practices include: keeping systems' software up to date to ensure that they have the latest security patches and thus are vulnerable to fewer attacks; training staff on cybersecurity so they do not inadvertently undermine systems' security (such as by clicking on a malicious link or opening a malicious attachment to an email); and implementing security features such as multifactor authentication to make it easy for users to keep the system secure (particularly if users are able to use a single sign on (SSO) system to access most or all of their accounts).

Backing Up Data and Systems

A key element of being prepared for ransomware specifically is backing up systems and data. While this will not prevent the exfiltration of data (discussed below), it can help restore systems more quickly without paying the demanded ransom. However, more sophisticated ransomware will try to defeat the backup process, often by encrypting the backed up data as well or deleting it altogether. There are a few approaches to making backups that are robust enough to mitigate this risk:

- Off-site backups, which are backups that are stored in a different place or system as the primary data (such as a separate cloud instance or with a different provider), may provide more security than a backup that exists on the same system as the primary data. However, if these backups are done automatically, they may still be vulnerable if the scheduled backup happens after the ransomware infection, and thus backs up the encrypted data.
- "Air-gapping" the data backup provides stronger protection than off-site backups. Air-gapped backups are fully disconnected from the internet, serving as strong protection against that backup becoming infected with malware. However, air-gapping drives can be labor-intensive, as the process typically cannot be fully automated since disconnecting a backup physically (unplugging it) is generally the most effective approach. So, depending on an organization's resources, it may make sense to prioritize air-gapping critical data and data that will not change frequently to minimize the need for this step.
- Another backup technique is to use Write Once, Read Many (WORM) drives. These are drives that can only be written one time, permanently, and then the data cannot be changed. While these are effective against ransomware (since the original, uncorrupted data cannot be overwritten by corrupted or encrypted data), they are expensive, as every backup requires a new drive. Thus, much like air-gapped drives, it might be necessary for an organization to reserve this approach for critical data that is worth the extra cost, or relatively stable data that does not change regularly, thus giving the drive a longer lifespan.

Alternative communications

If a ransomware attack is pervasive enough, it may also impact communications systems like email or even office phone functionality ("softphones" that use the internet to make calls rather than a traditional phone provider may be vulnerable). Schools should have emergency channels of communication in place. This may mean a phone tree or call list to notify those who need to play a role in restoring the system, as well as a separate, non-soft phone line for staff to report ransomware (or other incidents) if they are unable to use normal channels.

Response

Restoring from Backups

Regardless of how an organization backs up its data, it is important to have a plan in place to restore from those backups. Additionally, organizations should routinely confirm that backups are successfully completed and practice this restoration process to ensure that it works as expected, especially as systems are updated over time. If organizations contract out their IT or otherwise do not maintain their own systems, this may mean engaging with the responsible parties to ensure they have a system for monitoring and testing data restoration. For organizations that manage their own systems, this may mean having a test bed (a separate copy of the live system to run tests and try out upgrades) that they can use to practice wiping and restoring. Test beds can be as simple as one or two computers that simulate the main functions of the system to practice restoration on a small scale.

A complicating factor in restoration is ensuring that the ransomware is fully purged from the system before it is restored from the back up—if the ransomware has not been eradicated, it may re-infect the system after restoration. Consequently, it is also important to keep a separate, air-gapped copy of the backup while restoring, in the event that the backup data is corrupted during the restoration process.

If a school does not have backups sufficient to restore their systems, they may be considering paying the ransom. However, there are legal and policy concerns to weigh before undertaking this decision, so schools should consult with their counsel and with law enforcement before taking any action.

Communication

Another important component of responding to a ransomware attack is communicating to affected parties and potentially law enforcement, usually under the guidance of legal counsel. If student or teacher data were exfiltrated, those populations should be notified. In some cases, there may be a legal requirement to do so, but there are also other reasons to communicate with the school community about an attack. Communication can help establish trust with the community, and ensure that they have accurate information from a reputable source. As part of the communication, the community should be given the information and assistance they need to protect themselves from the fallout, such as taking steps to avoid identity theft. There are also best practices to consider when communicating about an attack. Information should be timely as possible, but organizations should ensure they have accurate information before communicating, particularly about evolving incidents. Additionally, communication should be widely accessible to the community, which may mean offering the information in a variety of formats and languages.

In addition to communicating with the school community, communicating to law enforcement can be useful both for the victim organization and also as part of an information-sharing strategy to prevent other attacks and develop responses and software patches. Both local law enforcement and federal agencies may be able to assist organizations in investigating and recovering from an attack. Sharing with Information Sharing and Analysis Centers (ISACs) can also be a part of this information-building approach. Additionally, schools should have a plan for communicating with the media if necessary, and have channels in place for staff to communicate back to the organization, both to raise issues they are facing and to pass along any information requests they receive from families and the media.

Ransomware attacks can rob students of acutely needed instructional time and jeopardize financial security. Thus, it is important that schools take the necessary steps to protect themselves and, in turn, their students.

Further Reading:

- https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings
- https://www.consumer.ftc.gov/articles/0040-child-identity-theft
- https://www.ibm.com/downloads/cas/EV6NAQR4
- https://www.cisa.gov/ransomware

- https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- https://www.cisecurity.org/ms-isac/
- https://level-up.cc/curriculum/malware-protection/safer-software-updating/
- https://www.atlantech.net/blog/full-backup-vs.-incremental-backup-vs.-differential-backup-which-is-best

This is one in a series of information sheets designed to give practitioners clear, actionable guidance on how to most responsibly use technology in support of students. More info: cdt.org/student-privacy/.

Ransomware Incident Response Checklist

Preparing before an incident and responding effectively, should one occur, can greatly reduce the harm the incident causes. In addition to the steps schools should take in the event of a standard data breach attack, there are steps specific to ransomware that will help minimize the damage. The steps presented here are intended to supplement those laid out in the Data Breach Response Checklist offered by the U.S. Department of Education.

➤ Before the Incident:

□ ***Prepare a ransomware response protocol***

- ○ Assign roles and responsibilities. This should include someone responsible for overseeing restoration of systems impacted by the attack, someone to communicate with law enforcement and other partners, and a point of contact for students and families.

- ○ Put procedures in place for each role. Processes for restoration should be well documented, and a list of contacts at law enforcement agencies should be established. This may include federal agencies like the FBI, local law enforcement, and other partners like Information Sharing and Analysis Centers (ISACs).

□ ***Establish backup practices***

- ○ Set a schedule for backing up data. Information that changes regularly and is important for providing day-to-day educational services may need to be backed up more often than data that is more stable or less critical.

- ○ Critical data should also be periodically backed up to an off-site or air-gapped location, which is not connected to or accessible from the main system. This is to ensure that the most critical data is still available even if the regular backups are corrupted in a ransomware attack. Ensure that each new off-site backup is clean before erasing the last off-site backup.

- ○ Run sessions to practice restoring from backups. This will ensure that the backups are accessible to those who need them and sufficient to restore the system. Additionally, running trial sessions regularly will ensure that restoration protocols stay up to date as your systems are updated or changed. Typically, these sessions are run on a test bed (a separate copy of the live system to run tests and try out upgrades) to avoid affecting the main system during testing and practice. A testbed can be as simple as one or two computers that simulate the main functions of the system to practice restoration on a small scale.

➢ During / After the Incident:

□ ***Ensure protection of the data.***

- ○ Before you restore the system, consider contacting law enforcement. They may be able to assist, but may also request information that may help them identify attackers or assist with or prevent later attacks, and the process of restoring the system may make it impossible to obtain that information.

- ○ Also before attempting any restoration of the active system, ensure that the infected computers are isolated from any that remain unaffected (for instance, if a teacher laptop has been unaffected, ask them to disconnect it from the internet to prevent it from receiving infected updates from the main system), and that the malware has been scrubbed from the system. This will help prevent the corruption of any backups you are using to restore the system.

- ○ If the regular backups are corrupted and you need to restore critical systems from the off-site or air-gapped backup, replicate the off-site backup using a clean computer before you attempt to use the backup to restore the system. This will ensure that even if the main system has not been adequately cleaned of the ransomware and is able to corrupt the off-site backup when it is connected to the main system, there will still be a clean copy of any critical data.

□ ***Use fallback communication channels to inform staff of the incident.***

- ○ Provide them with instructions about whether or not to use school systems, how to handle any ransom demands they may receive, and provide them with a protocol for handling questions they get from students and families (what, if any, information teachers can provide to families and who families should contact for further information).

□ ***Communicate with parents and families when possible.***

- ○ In some cases there may be a legal requirement to do so, but there are also other reasons to communicate with the school community about an attack. It can help establish trust with the community, and ensure that they have accurate information from a reputable source.

- ○ Additionally, parents and families may need to take steps to protect themselves if sensitive data has been exfiltrated as part of the attack, or if attackers are using their contact information to try to launch another attack. Schools should communicate in a timely way, but ensuring the communications are accurate should be a priority, particularly for still-evolving incidents.

- ○ Communication should be widely accessible to the community, which may mean offering the information in a variety of formats and languages.