K–12 DIVE

SPONSORED

# 2 plans that can help protect your school district from a ransomware attack

Published May 16, 2022

*iStock/BongkarnThanyakij*

SPONSORED CONTENT BY yubico

Every day we hear about a new cyber attack. The targets are often public infrastructure like pipelines or companies that provide third-party services, but public agencies and school districts are just as vulnerable and have suffered many ransomware attacks in recent years that disrupt school services and cost millions of dollars.

An intrusion, often caused when a single stolen credential falls into the wrong hands, usually locks an entire district's system and is followed by a ransom demand. School district IT systems often run on limited budgets that postpone upgrades longer than they should be. The result is often a login process protected only by legacy authentication systems requiring a simple password. Some schools have found that leaving legacy authentication approaches in place for too long can have dire consequences.

So what actions can school districts take to defend against the growing ransomware threat? The first step is to develop a **mitigation plan** (stop a successful attack from happening in the first place) and an **incident response plan** (what do you do after it has happened).

## Mitigation plans

Any mitigation plan must start with a full audit of your systems – what infrastructure do you have, what authentication process is in place and where are your gaps and vulnerabilities. No action plan can be effective until an honest assessment tells you what you are currently working with. Here are a few important questions to ask during the audit:

- Where is critical data located across my systems and what is most at risk?
- Who has access to this critical data?
- What controls are in place to protect it?
- How do you recover if data is lost or encrypted?
- Are there automated systems with appropriate controls?
- Is there a system of automated reporting that alerts on flags and endpoints?
- Do you have a zero trust architecture in place? In other words, if access is given that's not expected, is there an automated way to deny access until verification is achieved?
- How do you recover the critical data if lost?
- If you're in the cloud, whether Microsoft, Amazon, or another provider, are controls set correctly and monitored?

There's a common misconception that the most common line of attack for ransomware is a malware download, usually through clicking a suspicious link in an email. But in many cases weak authentication approaches may allow attackers to gain entry to a system, pose as an authenticated user and strategically place ransomware in the most damaging places.

If your authentication systems still rely mostly on simple username and password-based logins, you should be considering a strong multi-factor authentication solution (MFA) to bolster your defenses against unwanted and unauthorized intrusion.

When you do consider an upgrade, better user experience should not be forgotten as a key consideration apart from security. There's always resistance to workplace process changes – but if the security benefits and ease-of-use is communicated clearly ahead of time, that resistance can be overcome.

## Incident response plans

We never want the worst case scenario to happen, but in case it does, a quickly referenced incident response plan can minimize the damage. This plan should be created and put in place well before any attack. It's also important to update and test it regularly, because there will be updates to infrastructure, applications and users as time goes on. Your plans should be detailed enough so that key decisions do not need to be made on the fly. The difference between a well-planned incident response plan (IRP) and "winging it" on the day you get attacked, could be the difference between a major disaster and an operational hiccup.

Here's an example of a checklist you might use for an IRP:

- Senior leadership (preferably at the VP or higher level) should be engaged and directly responsible for the plan.
- Experienced security and operational employees are given the authority to build a viable and actionable plan.
- The plan needs to be aligned and integrated with business continuity and disaster recovery plans and teams. One caveat: disaster recovery is often designed for the 10-year event, but the

IRP has to be designed for an event that's to be expected every single day.

- Incentivize delivery and maintenance for the plan through performance bonuses and clear employee evaluation goals and objectives.

## Cyber insurance

Districts are increasingly looking at cyber insurance as an option, but it's becoming increasingly too expensive. Also, coverage is not broad enough given the increased spate of cyber attacks across education and cyber insurance firms' increasingly trying to avoid more risk. Premiums aren't going to get any less expensive in a climate of increasing attacks, but you can keep premiums lower if you can prove to insurers that you have strong, phishing-resistant MFA in place. Recent guidance from the Office of Management and Budget (OMB Memo M-22-09) for the public sector states that SmartCard and FIDO/WebAuthn are the only phishing-resistant authentication standards and mobile-based authentication such as OTP, SMS and push notifications are not considered phishing-resistant. You can learn more about how to prepare your organization for a cyber insurance application here.

## How FIDO security keys such as YubiKeys, provide phishing-resistant MFA for faculty, staff and students

YubiKeys are multi-protocol hardware security keys from Yubico and offer phishing-resistant MFA and a simple tap-and-go user experience. YubiKeys can be easily handed out to employees, come in a variety of form factors and don't require a battery or Internet connectivity.

There are several ways they can be useful in your incident response plan:

- They lower IT support costs incurred through self-service help desk password resets and there is no need for mobile device and service related costs
- Every faculty member and your administrative staff can leverage a YubiKey for secure access to applications and data, with keys easily revoked as needed or reissued.
- A single key can be used across multiple devices such as desktops, laptops, mobiles, tablets and even shared workstations. It works with 700+ applications and services such as GSuite, Box, Jamf and others.
- They integrate seamlessly into existing identity and access management (IAM) solutions such as Duo, Microsoft, Okta and Ping, eliminating any rip or replace of existing systems.
- A single key supports multiple protocols including OTP and FIDO, offering phishing-resistant MFA with FIDO. It stops account takeovers which are common entry points for ransomware attacks.
- YubiKeys can be delivered straight to any user's location, which is beneficial for those working or studying from home.

Visit Yubico to learn more about how YubiKeys can help you strengthen your MFA posture against ransomware threats.