Dellicker STRATEGIES

Cyber Threats to Schools & Municipalities

SERVICES

Dellicker Strategies has solutions & services to help public organizations get their cybersecurity under control.

ESSENTIALS PACKAGE

- Security awareness training
- Network vulnerability scanning
- Cybersecurity program development & launch

SUSTAINMENT PACKAGE

- Essentials Package plus:
- Program Dashboard
- Additional training capabilities
- Technical and program support

COMPREHENSIVE PACKAGE

- Sustainment Package plus:
- Penetration testing or
- Customized services for continuous cybersecurity program improvement

Dellicker's cybersecurity delivery partners include KnowBe4 & ETHOS Technology

Contact us for a free cybersecurity assessment:
info@dellicker.com

SOFTWARE VULNERABILITY EXPLOITATION

Schools and municipalities need to understand software vulnerabilities to reduce their exposure to cyberattacks and protect sensitive information.

What is software vulnerability exploitation?

Software vulnerability exploitation occurs when attackers take advantage of weaknesses in software to gain unauthorized access. These weaknesses can allow attackers to access information, execute commands, or enter a network.

Who are the perpetrators?

Cybercriminals, criminal organizations, hacktivists, and nation-state groups may exploit software vulnerabilities. Their goals can include financial gain, information theft, disruption, or gaining access to an organization's systems.

How prevalent is vulnerability exploitation?

Vulnerability exploitation is a major cybersecurity threat across industries and was involved in 31% of breaches in Verizon's 2026 report. Because schools and municipalities are also potential targets, New Jersey schools are required to conduct regular security assessments.

How dangerous is it?

A single software weakness can give an attacker access to an organization's sensitive information and critical systems. This can put sensitive student, staff, and financial information at risk, potentially causing significant damage.

What can we do to protect our schools and municipalities?

Organizations should keep software updated, identify and prioritize important vulnerabilities, replace outdated software, and limit access to systems that cannot be fixed immediately.

Sources:
https://www.cisa.gov/sites/default/files/2026-08/aa25-022a-threat-actors-chained-vulnerabilities-in-ivanti-cloud-service-applications_2.pdf
https://www.verizon.com/business/resources/T343/reports/2026-dbir-data-breach-investigations-report.pdf
https://www.fbi.gov/investigate/cyber/ten-actions-to-improve-cyber-resiliency

Contact Dellicker Strategies:

8766 Bittners Ct., Lehigh Valley, PA 18053 | P: 484-788-1221 | E: info@dellicker.com | www.dellicker.com