Cyber Risk High for Schools, Cities, SMBs

STACK Cybersecurity Urges High-Risk Sectors to Conduct Cybersecurity Risk Assessments as Iranian Attacks Hit U.S. Soil

STACK Cybersecurity achieves SOC 2 Type 2 Cert

DETROIT, MI, UNITED STATES, April 6, 2026 /EINPresswire.com/ -- STACK Cybersecurity is issuing an urgent call for schools, local governments, health systems, and businesses to conduct a Cybersecurity Risk Assessment (CSRA) as Iranian-linked threat actors accelerate attacks on American targets, including a county government in Indiana.

St. Joseph County, Indiana, officials acknowledge the Iranian-backed hacking group Handala breached county systems and claimed to have taken sensitive data from multiple county departments. The attack is the latest in a growing wave of Iranian cyber operations targeting everyday American institutions, not just large corporations or federal agencies. This is the same hacking group that infiltrated FBI Director Kash Patel's personal email account.

> If Handala can breach a county government in Indiana, they may already be in your systems right now."
>
> *Tracey Birkenhauer*

Michigan has already felt this threat up close. On March 11, Stryker Corporation, the Michigan-based medical technology company, disclosed a cyberattack that disrupted its global internal networks and left thousands of employees unable to access corporate systems. Handala claimed responsibility and said it permanently destroyed data on more than 200,000 devices across 79 countries. The attack destroyed data permanently rather than holding it for ransom, a tactic that leaves victims with no recovery path.

What makes these incidents especially alarming is not just their severity but their timing. In a recent intrusion attributed to Handala, initial access is believed to have been established well before the destructive phase, with network access dating back several months. By the time an attack becomes visible, the adversary may have been quietly inside the network for weeks.

Iran and its supporters are leveraging cyber capabilities to compensate for military disadvantages.

"If Handala can breach a county government in Indiana, they may already be in your systems right now," said Tracey Birkenhauer, Chief Impact Officer at STACK Cybersecurity. "Schools, municipalities, and smaller businesses are prime targets. A Cybersecurity Risk Assessment is how you find out where you're exposed before someone else does."

The threat extends beyond Handala. A separate group of Iranian cyber actors, known by aliases including Pioneer Kitten and Lemon Sandstorm, has conducted a high volume of network intrusion attempts against U.S. entities since 2017, with confirmed victims including schools, municipal governments, financial institutions, and health care facilities.

Iran is going after the weakest links, not the strongest ones. Supply chains supporting the economy and the defense industrial base, along with critical infrastructure including ports, rail lines, water treatment plants, and hospitals, are squarely in the crosshairs. Iranian actors have also targeted data centers using both cyberattacks and conventional weapons, reflecting how deeply those facilities are now woven into commerce, communications, and national security.

The timing of this threat surge couldn't be much worse from a federal response standpoint. The Cybersecurity and Infrastructure Security Agency (CISA) has been stretched thin following staffing reductions and a lapse in federal funding that halted active management of agency resources and canceled cybersecurity assessments and training engagements. Local and midsize entities cannot count on the federal backstop that may have once existed.

Fitch Ratings has warned that historically, municipal and local entities haven't benefited from the same level of cybersecurity investment as larger enterprises, making them both more attractive and more accessible targets. An Iranian national has already pleaded guilty to ransomware attacks that crippled Baltimore and other U.S. municipalities, causing tens of millions in damages.

A CSRA gives any entity, regardless of size or sector, a clear picture of where vulnerabilities exist, which systems are exposed, and what steps can most quickly reduce risk. STACK Cybersecurity conducts assessments and builds prioritized remediation plans based on each client's environment, budget, and threat profile.

Any school district, local government, health provider, or business that has not had a CSRA within the past 12 months should schedule one immediately. To learn more or get started, visit stackcybersecurity.com, email info@stackcyber.com, or call 734-744-5300.

Tracey Birkenhauer
STACK Cybersecurity
+1 734-744-5300
email us here