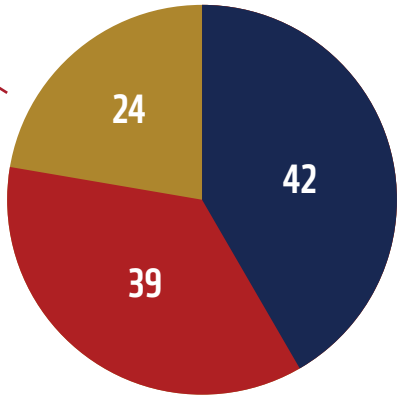
CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

CYBERATTACKS IN INDIANA: QUICK RESPONSE GUIDE

105 total breaches reported over the last 12 months

94% of malware continues via email



42 State, County and Municipalities Government

39 K-12 and Higher Education

24 County / Local Healthcare (not privately owned)

**Source: HIPPA Breach reporting, public news, Indiana Attorney General Breach reporting from July 2018 – July 2019; 2019 Verizon Data Breach Report*

REPORT A CYBER CRIME

When an organization's experiencing a cyber attack, follow these steps to report the cyber crime.

STEP 1 - CONTACT LAW ENFORCEMENT

- FBI Internet Crime Complaint Center (IC3) Alert authorities of suspected criminal or civil violations.
- **Indiana State Police (ISP)** Cybercrime & Investigative Technologies specialize in conducting cyber crime investigations.
- If there is an immediate threat to public health or safety, call 911.

STEP 2 - ADDITIONAL REPORTING SUCH AS:

- **Indiana Attorney General** requires organizations report any security breach resulted in exposure of personal information. For more information, click here.
- **Regulators:** Regulated organizations may need to report cyber crimes to other state or federal agencies.
- **Secretary of State:** If necessary, contact the SOS offices regarding any related cyber incidents at electionsecurity@sos.in.gov.
- **Federal Government:** This fact sheet explains how to report cyber crimes to many federal agencies.

STEP 3 - UTILIZE ADDTIONAL RESOURCES

Utilize additional resources about tips regarding avoiding ransomware, National Governors Association Response Planning Memo, National Emergency Readiness Team information, Department of Homeland Security's National Cybersecurity and Communications Integration Center, and more for 24/7 cyber situational awareness, incident response, and management center at www.in.gov/cybersecurity/3807.htm.

STEP 4 - INFORMATION SHARING

It's important to share cyber crime information with other organizations to protect critical infrastructure, the State of Indiana, and our nation. Learn more at www.in.gov/cybersecurity/3819.htm.

CYBERATTACKS IN INDIANA: QUICK RESPONSE GUIDE

THREE STEPS TO RESILIENCY AGAINST RANSOMWARE NOW

STEP 1 - BACK UP YOUR SYSTEM - NOW AND DAILY

Immediately and regularly back up all critical agency and system configuration information on a separate device and store the back-ups offline, verifying their integrity and restoration process. If recovering after an attack, restore a stronger system than you lost, fully patched and updated to the latest version.

STEP 2 - REINFORCE BASIC CYBERSECURITY AWARENESS AND EDUCATION

Ransomware attacks often require the human element to succeed. Refresh employee training on recognizing cyber threats, phishing and suspicious links – the most common vectors for ransomware attacks. Remind employees of how to report incidents to appropriate information technology staff in a timely manner, which should include out-of-band communication paths.

STEP 3- REVISIT AND REFINE CYBER INCIDENT RESPONSE PLANS

Agencies must have a clear plan to address attacks when they occur, including when internal capabilities are overwhelmed. Make sure response plans include how to request assistance from external cyber first responders, such as state agencies, CISA and the MS-ISAC, in the event of an attack.

EMERGENCY MANAGER RESOURCES

To find cybersecurity toolkit, planning templates, guides, resources, and more for emergency managers, visit https://www.in.gov/cybersecurity/3818.htm.