CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

REPORT A CYBER CRIME

When an organization's experiencing a cyberattack, follow these steps to report the cybercrime.

- If there is an immediate threat to public health or safety, call 911.

Step 1: What's In Your Plan?

- Communicate with your management per your organization's policies.
- Take out your Cyber Incident Response Plan to see what immediate steps you need to take next. This will be critical to your response and recovery.
- If you have cyber insurance that requires you to call them first, then contact them as soon as possible.

Step 2: Contact Law Enforcement

Law enforcement performs an essential role in achieving the nation's and state's cybersecurity objectives by investigating, apprehending, and prosecuting those responsible for a wide range of cybercrimes.

If you are a victim of a cybercrime, contact a law enforcement agency right away**.**

Agencies include:

- **FBI - Internet Crime Complaint Center (IC3)**The FBI Internet Crime Complaint Center's (IC3) mission is to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cybercrime. The IC3 gives the victims of cybercrime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. Go to: https://www.ic3.gov.
  - FBI Cyber - The FBI is the lead federal agency for investigating cyberattacks and intrusions. To learn more about what you can do to protect yourself against various forms of cybercrimes, FBI Cyber offers a great deal of information and resources including:
    - Partnering with the FBI
    - Benefits of Reporting a Cyber Incident to the FBI

- **Indianapolis Cyber Fraud Task Force**
  Cyber incidents financially related can be reported to the Indianapolis Cyber Fraud Task Force at: ind-cftf@usss.dhs.gov or call (317) 635-6420.

- **Indiana State Police (ISP)**ISP's Cybercrime & Investigative Technologies Section has detectives who specialize in conducting cybercrime investigations. Call (317) 232-8248 or visit https://www.in.gov/isp/3234.htm.

- **Immediate Threat to Public Safety**
  If there is an immediate threat to public health or safety, the public should always call 911.

Step 3: Additional Reporting

- **Local Government Reporting Requirement**
  - All local government/public-sector entities are required to report incidents such as ransomware, software vulnerability exploitations, denial-of-service attacks and more to the Indiana Office of Technology IN-ISAC within 48 hours of the incident. To learn more, click here.
  - Local governments across Indiana are partnering with the Indiana Office of Technology as a resource for free cybersecurity training, web hosting and access to cost-saving technology and equipment. We are working together to make technology secure for all of Indiana.
  - **Many of our services are free, easy to access and implement,** and they help reduce the burdens that come with the massive responsibility local governments face. This enables them to deliver government services more effectively and efficiently, saving time and money for the higher priority projects.
  - To learn more, visit the Indiana Office of Technology's Local Government Services website page at: https://www.in.gov/iot/local-government-services/.

- **Indiana Attorney General**
  - Indiana's security breach notification statute requires organizations to provide Indiana residents with the right to know when a security breach has resulted in the exposure of their personal information. For more information and to report a security breach, click here.
- **CISA**
  - CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870. To learn more, visit www.cisa.gov/report.

- **Regulators**
  - If you are an organization that is regulated, you may be required to report cybercrimes to other state or federal agencies.
- **Other Federal Government Agencies**
  - This fact sheet, Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government, further explains when what, and how to report a cybercrime to a number of federal agencies.

Step 4: Know Your Resources

- Join an Information Sharing and Analysis Center (ISAC)
- CISA Stop Ransomware Resources at: https://www.cisa.gov/stopransomware/
- **CISA Central**
  CISA Central (https://www.cisa.gov/central) is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications or physical origin. CISA Central is the simplest, most centralized way for critical infrastructure partners and stakeholders to engage with CISA and is the easiest way for all critical infrastructure stakeholders to request assistance and get the information you need to understand the constantly evolving risk landscape.
- **CISA Shields Up**
  CISA's Shields Up site provides the latest guidance and information to help organizations increase their resilience to cyberattacks and protect people and property. This robust catalog of free resources is especially helpful today, as the cybersecurity threats facing the world have increased exponentially.

- **CISA Threats and Advisories**
  CISA offers the latest cybersecurity news, advisories, alerts, tools, and resources for defending against ever-evolving cyber threats and attacks.
- **National Institute of Standards and Technology (NIST)**
  NIST's Computer Security Incident Handling Guide assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively.
- **Ready.gov**
  Ready.gov (https://www.ready.gov/cybersecurity) is a national public service campaign designed to educate and empower the American people to prepare for, respond to, and mitigate emergencies, including cybersecurity.

Step 5: Information Sharing

- If you are a victim of a cybercrime, it is important to share such information with other organizations in order to protect critical infrastructure, the state of Indiana, and our nation. Learn more about cyber sharing.

CYBERSECURITY ATTACKS IN INDIANA: QUICK RESPONSE GUIDE

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/government/emergency-response-and-recovery/