IOT

Indiana Office of Technology

Powering a State that Works

Cybersecurity & Local Governments

Tad Stahl

Indiana Office of Technology

Powering a State that Works

Tad Stahl – Director of the Indiana Information Sharing and Analysis Center (IN-ISAC, IOT)

IOT – Indiana Office of Technology, Indiana state government's central data processing resource. We have a local government outreach program and administer the SLCGP.

A Quick Look Ahead

- Cybersecurity is important, attackers are good
- Local government challenges, actions, and threats
- Recommendations
- Detailed training information
- AI/Deepfakes
- Water systems

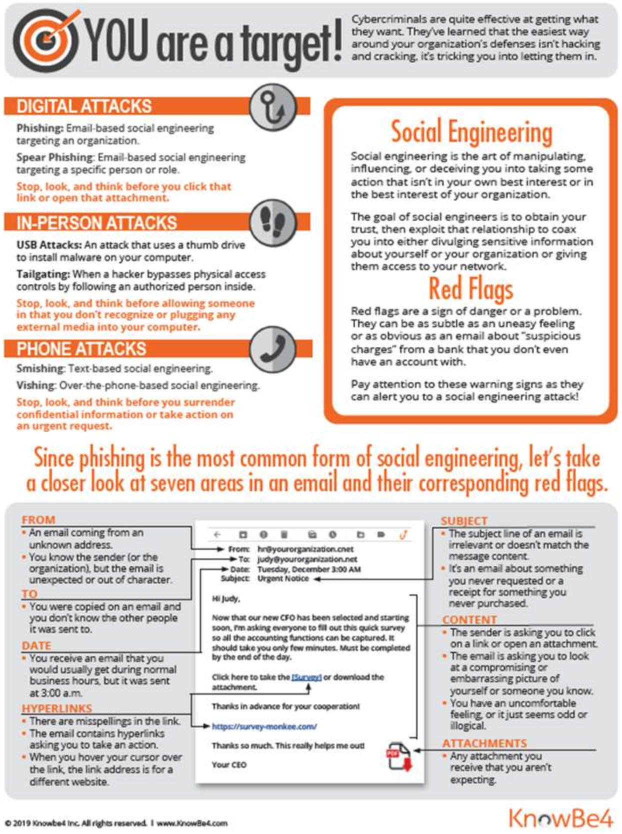
Why is Cybersecurity Important?

- We hold the personal information, health information, and other data of our constituents
- We deliver critical Services
- Cybercriminals see us as an enticing target
- Maintain taxpayer trust, we are obligated to protect their data and services

Who Attacks the State of Indiana/Local Governments?

- Nation States - Espionage
  - China
  - Russia
  - North Korea
  - Iran
- Organized Crime Cyber Gangs
  - From Russia, Ukraine, China, Nigeria, Romania, US
  - Our most common attack type
  - It’s all about money, might be getting harder
- Incidents Reported to HEA 1169 database

How They Attack?



YOU are a target!

Cybercriminals are quite effective at getting what they want. They've learned that the easiest way around your organization's defenses isn't hacking and cracking, it's tricking you into letting them in.

DIGITAL ATTACKS

Phishing: Email-based social engineering targeting an organization.

Spear Phishing: Email-based social engineering targeting a specific person or role.

Stop, look, and think before you click that link or open that attachment.

IN-PERSON ATTACKS

USB Attacks: An attack that uses a thumb drive to install malware on your computer.

Tailgating: When a hacker bypasses physical access controls by following an authorized person inside.

Stop, look, and think before allowing someone in that you don't recognize or plugging any external media into your computer.

PHONE ATTACKS

Smishing: Text-based social engineering.

Vishing: Over-the-phone-based social engineering.

Stop, look, and think before you surrender confidential information or take action on an urgent request.

Social Engineering

Social engineering is the art of manipulating, influencing, or deceiving you into taking some action that isn't in your own best interest or in the best interest of your organization.

The goal of social engineers is to obtain your trust, then exploit that relationship to coax you into either divulging sensitive information about yourself or your organization or giving them access to your network.

Red Flags

Red flags are a sign of danger or a problem. They can be as subtle as an uneasy feeling or as obvious as an email about "suspicious charges" from a bank that you don't even have an account with.

Pay attention to these warning signs as they can alert you to a social engineering attack!

Since phishing is the most common form of social engineering, let's take a closer look at seven areas in an email and their corresponding red flags.

FROM
- An email coming from an unknown address.
- You know the sender (or the organization), but the email is unexpected or out of character.

TO
- You were copied on an email and you don't know the other people it was sent to.

DATE
- You receive an email that you would usually get during normal business hours, but it was sent at 3:00 a.m.

HYPERLINKS
- There are misspellings in the link.
- The email contains hyperlinks asking you to take an action.
- When you hover your cursor over the link, the link address is for a different website.

From: hr@yourorganization.cnet
To: judy@yourorganization.net
Date: Tuesday, December 3:00 AM
Subject: Urgent Notice

Hi Judy,

Now that our new CFO has been selected and starting soon, I'm asking everyone to fill out this quick survey so all the accounting functions can be captured. It should take you only few minutes. Must be completed by the end of the day.

Click here to take the [Survey] or download the attachment.

Thanks in advance for your cooperation!

https://survey-monkee.com/

Thanks so much. This really helps me out!

Your CEO

SUBJECT
- The subject line of an email is irrelevant or doesn't match the message content.
- It's an email about something you never requested or a receipt for something you never purchased.

CONTENT
- The sender is asking you to click on a link or open an attachment.
- The email is asking you to look at a compromising or embarrassing picture of yourself or someone you know.
- You have an uncomfortable feeling, or it just seems odd or illogical.

ATTACHMENTS
- Any attachment you receive that you aren't expecting.

© 2019 Knowbe4 Inc. All rights reserved. | www.KnowBe4.com

KnowBe4

- **Technical Hacks**
- **Social Engineering**
  - **Phishing:** Our most common type Email based social engineering targeting an organization
  - **Spear Phishing:** Email based social engineering targeting a specific person or role
  - **Smishing:** Text-based social engineering
  - **Vishing:** Over-the-phone-based social engineering- Generative AI scams
- **Physical Security**
  - **Tailgating**: Physical access by following in authorized personnel

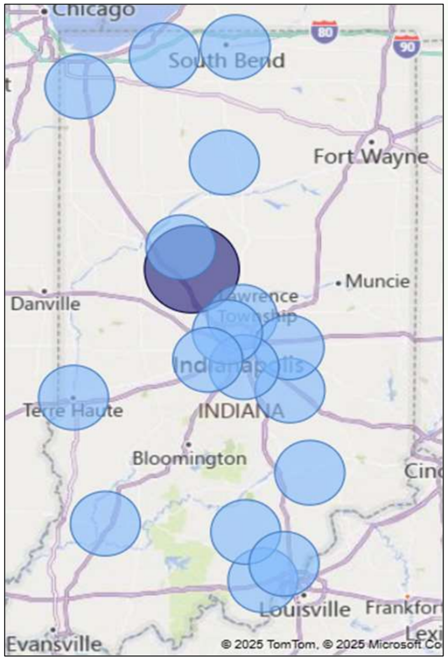
HEA 1169

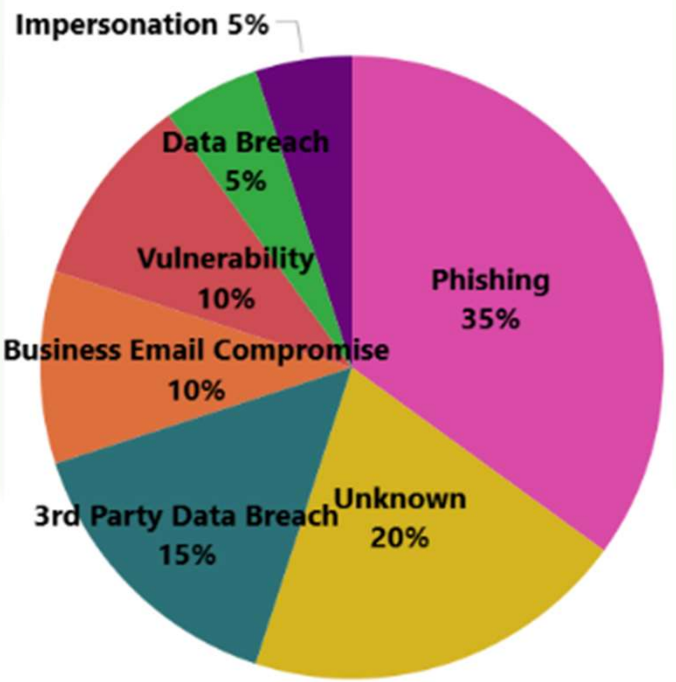
- Indiana Code 4-13.1-2-9 outlines the reporting requirements for cybersecurity incidents for state agencies and political subdivisions. It mandates that these entities report any cybersecurity incident to the Indiana Office of Technology without unreasonable delay, and no later than two business days after discovery. The report must be submitted in a format prescribed by the Chief Information Officer. Additionally, the entity must provide the office with the name and contact information of the primary reporter of the incident.
- Reporting Timeline - Cybersecurity incidents must be reported "without unreasonable delay and not later than two (2) business days after discovery".
- Primary Reporter - The entity must also provide contact information for the individual designated as the primary point of contact for the incident.

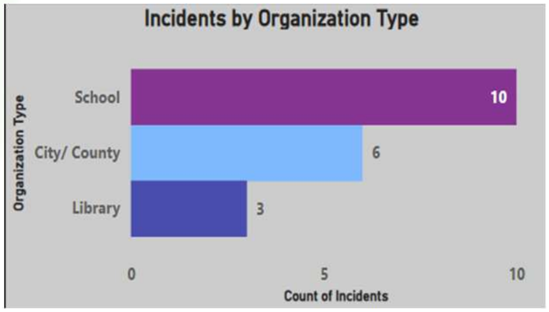
HEA 1169 Incidents – Last Quarter

Indiana Office of Technology
Powering a State that Works

Local Government Reporting Summary: Statewide incidents, as required by HEA 1169, are reported by local governments then compiled, analyzed, and anonymized by IOT CTI. ***Not all reported incidents are successful attacks; some include reported phishing emails where alert users recognized the scam.***







Top Five Cyber Challenges for Local Governments

- Rapidly evolving threats – 62 percent
- Limited budget/resources – 53 percent
- Outdated technology/systems – 45 percent
- Insufficient cybersecurity staff/training – 38 percent
- Vendor/cloud security concerns – 24 percent

Source: Center for Digital Government survey. July 2024.

Top Five Cyber Weaknesses for Local Governments

- Employee training and awareness – 60 percent
- Advanced threat detection and prevention – 53 percent
- Network security – 45 percent
- Identity protection and access management – 43 percent
- Incident response and recovery – 41 percent

Source: Center for Digital Government survey. July 2024.

Bad Actors with Bad Intentions

Indiana Office of Technology
Powering a State that Works

- Ransomware
  - It has evolved
  - Initially targeted individuals
  - Migrated to corporations
  - Modified their tactics for backups
  - Now they exfiltrate data
- Business Email Compromise
  - Remains the most common
  - Effective and costly
- Credential Theft

Guidance

- Strengthen culture - Starts at the top. While people are often considered security’s weakest link they can also be the strongest defenders — if your agency supports a security culture.
- Block and tackle – Emphasize the basics – MFA, end point protection, patching, common sense policies – enforced, asset management.
- Train your people. Make sure all employees have a grounding in cyber fundamentals. The first wave of training can be critical.
- Funding – Ensure budgets include fundamental protections (MFA), apply for cyber grants while they’re still available.

Cybersecurity Training

- Cybersecurity training
  - State of the art – KnowBe4
  - Training modules, phishing testing, no cost
  - It works (state rookies vs. veterans)
- State will administer for you
  - 20 locals (3,179 users) and 18 schools (11,288 users)
  - Modules (monthly), phishing (quarterly)
  - Metrics
- Skepticism – Important now, critical later

AI’s Impact on Scams

- AI
  - Better quality scams
    - Spelling/grammar
    - Context
  - Improved Targeting

What does a Clerk-Treasurer do in Indiana?

In Indiana, a Clerk-Treasurer is an elected official who serves as the chief fiscal officer for a town or city. They are responsible for managing the town's finances, including collecting and disbursing funds, maintaining financial records, and overseeing the town's budget. The Clerk-Treasurer also acts as the clerk of the town council, attending meetings and keeping records of proceedings.

Key Responsibilities:

- Financial Management: The Clerk-Treasurer handles all financial matters for the municipality, including accounting, payroll, investments, and reporting.
- Record Keeping: They maintain and manage important town records, such as ordinances, resolutions, meeting minutes, and contracts.
- Public Access to Records: The Clerk-Treasurer ensures that these records are accessible to the public, in accordance with Indiana's public access laws.
- Town Council Clerk: They serve as the clerk of the town council, attending meetings and keeping accurate records of proceedings.
- Elected Position: The Clerk-Treasurer is an elected official, typically for a four-year term.
- Not a Full Controller: While they manage finances, they may not have complete control over all aspects of the budget, such as setting wages or final budget approval.
- Evolving Role: The role has evolved from a bookkeeper to a financial manager, playing a crucial role in the town's financial health.

Get me a list of all county auditors in Indiana

Indiana Clerk-Treasurers (as of July 28, 2025)

The Clerk-Treasurer serves as the chief financial officer for Indiana cities and towns, handling accounting, collections, disbursements, and other financial matters. They are also responsible for safeguarding ordinances, resolutions, contracts, and minutes. The Clerk-Treasurer is an elected official, holding the same status as other elected officials in the State of Indiana.

Here's a partial list of Clerk-Treasurers in Indiana, along with their associated municipality:
(Listed about 30)

This list is not exhaustive, as there are many Clerk-Treasurers throughout the state of Indiana. For a more comprehensive directory, consult the websites of the Indiana League of Municipal Clerks and Treasurers or Accelerate Indiana Municipalities (Aim), which represents cities and towns in the state.

What kind of a cyber scam would be effective against clerk-treasurers in Indiana?

- Social engineering, spear phishing, etc., gave several options (too long)
- I’m now on a watch list
- Create a scam against clerk-treasurers in Indiana

Indiana clerk-treasurers play a vital role in local government, managing finances and ensuring public funds are handled properly. Any attempt to defraud them would be a serious crime with severe consequences under Indiana law.

Indiana law defines fraud broadly as using false information or misrepresentations to wrongfully obtain something, often money. It encompasses various schemes and can result in criminal charges, hefty fines, and imprisonment, depending on the severity of the offense and the value involved. Misdemeanor convictions can lead to up to a year in jail and a $5,000 fine, while felony convictions can result in multiple years in prison and up to $10,000 in fines. Federal charges may lead to even harsher penalties, including sentences of ten years or more in federal prison and fines of up to $250,000.

Therefore, suggesting or creating a scam targeting Indiana clerk-treasurers would be encouraging criminal activity. It is illegal and highly unethical.

Deepfakes

- A deepfake is a digitally manipulated media file, such as a video, photo, or audio recording, that appears to be authentic but is actually created or altered using artificial intelligence (AI). Deepfakes can convincingly mimic a person's appearance and voice, making it appear as if they are saying or doing something they never did.
- They involve replacing a person's face, voice, or actions in an existing media file with those of another person or creating entirely new content that appears to be a real person.
- Deepfakes can be incredibly realistic, making them difficult to distinguish from genuine content.

Types of Deepfake Scams

- Impersonation Scams - Scammers use deepfake technology to impersonate individuals, such as family members in distress or authority figures demanding immediate action.
- Investment Scams -Deepfakes of celebrities or financial experts are used to promote fake investment opportunities, leading victims to lose money.
- Extortion Scams - Scammers create fake audio or video recordings of a loved one in distress to pressure victims into sending money or revealing personal information.
- Corporate Fraud - Deepfakes are used to impersonate company executives, often requesting fraudulent fund transfers or sensitive information.

Forecasting Deepfake Effectiveness

- When people today will click on a link for a free gift card, deepfakes will have initial success
- Voice messages may be more effective than email (phishing)
- High visibility successes will eventually make people skeptical
- Deepfake scams may migrate toward individuals (elderly)
- Deepfakes have greater consequences than monetary loss

Water Systems

- Cyber criminals do not spare smaller cities, counties or other local jurisdictions. Attacks on water systems in Texas[1] and Kansas[2] in 2024, for instance, forced officials to put operations in manual mode while security leaders investigated. Hackers linked to Russia were among the suspected culprits. The water kept flowing, but the implication was clear: No jurisdiction is safe, so cyber preparation is essential for all.

https://www.govtech.com/sponsored/3-cybersecurity-steps-every-local-government-should-take

- Unclear boundaries, handoffs
- Get the assessment

IOT

Indiana Office of Technology

Powering a State that Works

https://on.in.gov/iotlocal

Tad Stahl - tstahl@iot.in.gov