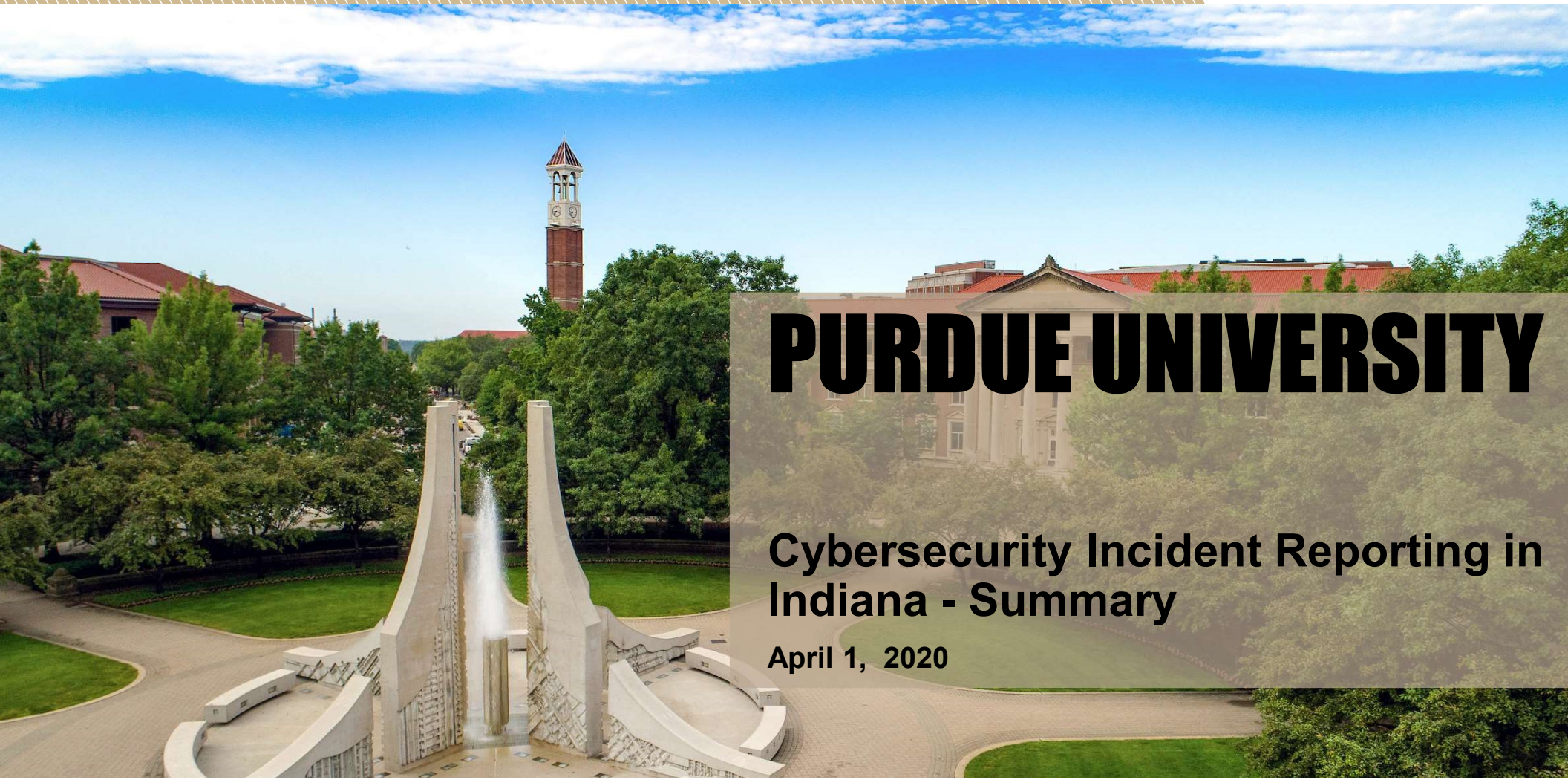
PURDUE UNIVERSITY | cyberTAP



PURDUE UNIVERSITY

Cybersecurity Incident Reporting in Indiana - Summary

April 1, 2020

DISCLAIMER

These slides are not legal advice and should not be relied on in place of advice from a qualified attorney familiar with laws and regulations relating to cybersecurity, incident reporting, and computer crime.

PURDUE UNIVERSITY | cyberTAP

OUTLINE

- About Us
- Security Incident Definitions, Regulations and Applicability
- What Constitutes a Reportable Cybersecurity Incident in Indiana?
- Reporting an Incident

About cyberTAP

PURDUE – CYBER TECHNICAL ASSISTANCE PROGRAM

Mission

cyberTAP exists to help its clients improve their cybersecurity posture through tailored professional services and education

CYBERTAP CONTACTS

PURDUE UNIVERSITY | cyberTAP

Mat Trampski
Director
mtrampsk@purdue.edu
765-494-1049

Carly Turow
Assistant Director – Program Execution
cturow@purdue.edu
317-201-5034

Karen Leaman
Admin Assistant
leamank@purdue.edu
765-494-9188

George Bailey
Assistant Director – Cyber Services
baileyga@purdue.edu
765-494-7538

Michael Johnson
Assistant Director – Business & Tech Services
johnso84@purdue.edu
765-494-6576

Cybersecurity Incident Definitions Regulations & Applicability

DEFINITIONS:

- ***Cybersecurity Incident***
  - An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon.

    -- Indiana Office of Technology

DEFINITIONS:

- ***Security Breach Incident***
  - An unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information
    - *Indiana Attorney General's Office*
  - A Security Breach Incident is largely a sub-category of a Cybersecurity Incident, except that a Security Breach Incident includes non-electronic (paper) data.

REGULATIONS

- IN Code 4-1-11 “Notice of Security Breach”
- IN Code 24-4.9-2-2 “Breach of the Security of Data”

APPLICABILITY

- State government agencies
- Local government
- IN businesses

What Constitutes a Reportable Cybersecurity Incident?

UNAUTHORIZED ACCESS

FEDERAL	STATE	LOCAL
18 U.S.C.§1030 Computer Fraud & Abuse Act	IC 35-43-1-4; 35-43-2-3 Property Offenses; Computer Trespass	Various Property Offenses; Facilitation of other Offenses

EFFECT:

Unauthorized access into any non-public computer system is a crime at federal, state, and local levels of law enforcement. Public computers are those that any citizen is authorized to use – not those owned by the government.

"SECURITY BREACH INCIDENT" – IN BUSINESSES & STATE AGENCIES*

"…unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of **personal information**…" - Indiana Code article 24-4.9

Set 1: One of the Following
• First Name & Last Name • First Initial & Last Name

Set 2: One of the Following
• Social Security Number • Driver's license Number or Identification Card Number • Account Number, Credit Card Number, Debit Card Number, Security Code, Access Code, or Password of an individual's financial account

* These requirements do not mention IN local governments explicitly but are your best guidance.

"SECURITY BREACH INCIDENT": EXCEPTIONS

"…unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of **personal information**…" - Indiana Code article 24-4.9

Exceptions to the Rule
• The last four (4) digits of an individual's Social Security Number, Driver's License Number or Identification Card Number • Publicly available information that is lawfully made available to the public from records of a federal agency or local agency • Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure • Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key that has not been compromised

Reporting a Cybersecurity Incident

REPORTING: IN THE CONTEXT OF CYBERSECURITY INCIDENT RESPONSE

1) Understand your reporting requirements – before you need to meet them!
    a. TIME IS OF THE ESSENCE
    b. FOLLOW YOUR CYBERSECURITY INCIDENT RESPONSE POLICY
2) Stop the incident.
    a. Determine the scope of the attack and disconnect affected systems
    b. Identify the resources necessary to stop, recover and **document** the attack. Documentation efforts should be informed by your legal reporting responsibilities, keys to learning from the incident, and in some cases, in support of forensic analysis. **Consult your legal counsel, Privacy Officer, and insurance carrier before reporting to any other organization or government agency not assisting in stopping the incident!**
    c. Connect with those resources and bring them to bear
3) Meet reporting obligations for your organization, including to individuals and the public. Consider PR aspects of reporting. It's usually better for the public to hear it from you directly and quickly.
4) Provide information to other stakeholders
    - Law enforcement agencies or clearinghouses to which you are not required to report, Your "community of practice" – trade associations, local business groups, academic institutions

REPORTING: RECOMMENDATIONS – "CYBERSECURITY INCIDENT"

If your organization experiences a security incident, but can prove that no regulated data was breached:

1. **Consult your legal counsel, Privacy Officer, and insurance carrier before reporting to any other organization or government agency!**
2. …you **should** report the incident to:
   a. FBI Internet Crime Complaint Center (IC3)
   b. ISP's Cybercrime & Investigative Technologies Section
   c. Indiana Attorney General's office

REPORTING: SPECIFIC OBLIGATIONS & RECOMMENDATIONS – SECURITY BREACH INCIDENT

If your organization experiences a security breach incident as shown on slide 8…

1) …you **must (per Indiana Code article 24-4.9)** report the incident to the Attorney General's office, the data owner (if not your org), and exposed individuals in writing or via e-mail within a reasonable timeframe (think in terms of <60 days). You must also assist law enforcement, where applicable.
2) …if the security breach incident is the result of an unauthorized intrusion (cyberattack):
    a. …you **should also** report the incident to:
        - FBI Internet Crime Complaint Center (IC3)
        - ISP's Cybercrime & Investigative Technologies Section
3) **Consult your legal counsel, Privacy Officer, and insurance carrier before reporting to any other organization or government agency!**

REPORTING: OTHER CONSIDERATIONS

1) **Additional Reporting**: If your organization experiences a security breach incident, the type of data breached may obligate your organization to report to other organizations not previously noted.
   - Examples of such obligations include, but are not limited to:
     - Reporting loss of personal health information (PHI) to the United States Department of Health and Human Services
     - Reporting breaches of credit card information to the Payment Card Industry (PCI)
2) **Cyber-insurance**: If your organization has cyber-insurance, those policies may require specific reporting criteria to be met before policy provisions can be activated.
3) **Public Relations**: Your organization should have a plan for addressing the public and answering questions about the security incident and should execute that plan as part of its incident reporting activities.

SPECIAL THANKS FOR EXTERNAL LEGAL REVIEW OF THE CONTENT OF THIS PRESENTATION TO:

- Valita Fredland, Vice President and Senior General Counsel, Community Health Network and member of the Board of Directors of the Indiana Security and Privacy Network (INSPN)

- Purdue University Office of Legal Counsel


PURDUE
UNIVERSITY
cyberTAP