



Presenter(s):

Professor Scott J. Shackelford, Indiana University

Chris Hart, former Chairman of the National Transportation Safety Board

Cybersecurity & Information Systems Information Analysis Center

# The Case for a National Cybersecurity Safety Board

INDIANA UNIVERSITY BLOOMINGTON

Make a difference in the fight against cyber attacks

CSIAC is sponsored by the Defense Technical Information Center (DTIC). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Defense Technical Information Center.

# Understanding the Cyber Threat to Critical Infrastructure

# What Is “Critical Infrastructure,” Who Should Defend It, and How?

1. How is it defined? Is this evolving?
2. What regulatory requirements come along with the designation?
3. What powers does the U.S. government have in protecting critical infrastructure? Are these too narrow or too broad?
4. If everything is “critical,” is anything?



# Understanding the Cyber Threat to Critical Infrastructure

## To Companies

1. Cyber attacks are **costly** – ransomware cost per incident was \$178,254 in 2020 ([Gartner](#))
2. **Widespread** – Phishing attacks increased by 11% during the pandemic ([Verizon](#))
3. **Easy** – malware is freely accessible on both the common and deep Web for as little as \$70 ([TechRepublic](#))
4. **Expanding** – Internet of (Every)thing

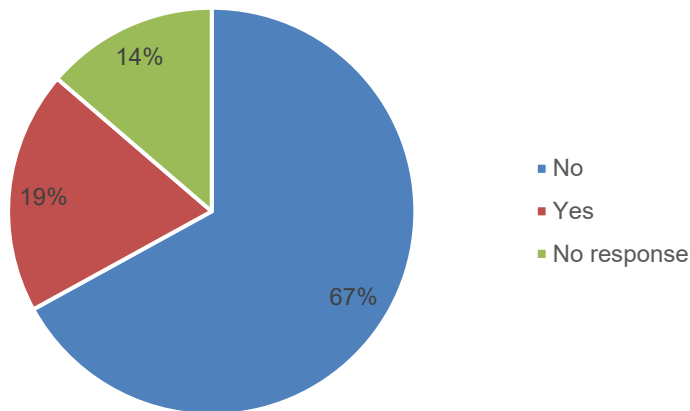
## To Countries

- Fear of “Electronic Pearl Harbor” ([overblown?](#))
- Protecting [critical national infrastructure](#)



# State of Hoosier Cybersecurity 2020 Snapshot

To your knowledge, has your organization experienced a successful cyber incident in the past three years?



- Fewer organizations in critical infrastructure sectors reported successful cyber attacks than non-critical infrastructure organizations
  - About 13% of critical infrastructure organizations reported successful attacks
  - About 28% of non-critical infrastructure organizations reported successful attacks

# Most Indiana Organizations Report Taking Steps to Prevent Cyber Incidents

- Just over 91% of organizations surveyed said they had taken some steps to prevent cyber incidents
- Slightly more critical infrastructure organizations said they had taken steps to prevent cyber incidents when compared to non-critical infrastructure organizations
  - About 94% of critical infrastructure organizations reported taking cyber incident prevention steps
  - About 88% of non-critical infrastructure organizations reported taking cyber incident preventions steps

## State of Hoosier Cybersecurity 2020

December 2020

Prepared for  
Indiana Executive Council on Cybersecurity  
By  
Kelley School of Business, Indiana University  
Indiana Business Research Center  
Anne Boustead JD, PhD (University of Arizona), Scott Shackelford JD, PhD (Indiana University)  
Special thanks to Jay Bhatia and Eric Spencer for their invaluable research support in this project. We would also like to thank the anonymous respondents who participated in our survey on behalf of their organizations, and to Stephen Vina, and Professors Asaf Labin and Angie Raymond for their helpful comments and suggestions.



# **Toward a National Cybersecurity Safety Board**

# Negligence and the NIST Cybersecurity Framework

- **2013 State of the Union Address**
  - Response to failed legislative push
  - Focus on cyber threats to nation's critical infrastructure
- **Executive Order 13636: Improving Critical Infrastructure Cybersecurity**
  - Increase information sharing
  - Ensure privacy and civil liberties protections
  - Develop a voluntary cybersecurity framework



# Proposing a National Cybersecurity Safety Board

- **Idea:** Why not create a National Transportation Safety Board (NTSB) for cyber attacks?
- **Evolution:**
  - **1991 NRC Report:** “Computers at Risk: Safe Computing in the Information Age”
  - **2014 NSF Report:** “Interdisciplinary Pathways towards a More Secure Internet”
  - 2018 [Academic Article](#) and 2019 [Wall Street Journal](#) piece
  - 2021 Belfer Center Report: “Learning from Cyber Incidents: Adapting Aviation Safety Models to Cybersecurity”
- **2021 Executive Order on Improving the Nation’s Cybersecurity**

# 2021 Executive Order on Improving the Nation's Cybersecurity

1. **Section 5 Mandate:** Establish a Review Board “co-chaired by government and private sector leads, that may convene following a significant cyber incident to analyze what happened and make concrete recommendations for improving cybersecurity.”
2. **Function:** DHS and AG work together to staff Board to investigate cyber attacks “affecting FCEB Information Systems or non-Federal systems, threat activity, vulnerabilities, mitigation activities, and agency responses.”
3. **Board Membership & Timeline:** Private sector & law enforcement, with a report due in June 2021 on Board’s scope, responsibilities, structure, “thresholds and criteria for the types of cyber incidents to be evaluated.”

# Potential Challenges

- *Political*
  - **Scope:** which cyber attacks should be investigated?
  - **Workforce:** identifying the “right” experts
  - **Industry Resistance** (and Support?)
- *Practical*
  - Information Sharing & Confidentiality
  - Defining Access to Data, Hardware & Software
  - Defining Appropriate Terminology
  - Need for Urgency
- *Related Reforms*
  - Major Cyber Incident Investigation Board (CSRB)
  - Bureau of Cyber Statistics
  - A Cyber Safety Reporting System (CSRS)



# Lessons From the NTSB

# About the NTSB

- Agency led by five members, nominated by the President, confirmed by the Senate
- Investigate transportation accidents in all modes, determine cause(s), make recommendations to prevent recurrences
- Also investigate undesirable trends (not just single accidents) and make recommendations to correct trends
- Advocate for implementation of its recommendations, which are not mandatory (but about 80% are implemented)
- Provide support as “accredited representative” for aviation accidents outside the United States

# Advantages of Independent Investigator

- Mishaps in regulated industries are usually investigated by the regulator
- Regulator's actions or omissions often play a role in mishaps
- Regulator's investigation report does not usually include its own actions or omissions as part of the cause
  - Its actions or omissions often not perceived as playing a role
  - Regulator unwilling to admit that its actions or omissions contributed to the mishap
- Independent investigation identifies actions or omissions by regulator that contributed to the mishap
  - More NTSB recommendations go to regulators than to any other single party in the industry

# History & Evolution of NTSB

- Aviation accidents were investigated by Dept. of Commerce for many years; other modes investigated other ways
- Safety for all modes (aviation, rail, highway, maritime, pipeline) was placed under one roof, Dept. of Transportation (DOT), in 1967
- NTSB was created in 1967 and placed under DOT to investigate accidents in all modes
- Due to awkwardness of NTSB recs going to its “boss,” DOT, NTSB was separated from DOT and made independent in 1974

# How Congress Made NTSB Independent

- Party balance – Only three of the five members can be of the President's party
- Insulation from political forces – Members are appointed to fixed terms rather than serving at the pleasure of the President
- Knowledge requirement – Three of the five members must have relevant background or experience
- Staggered five-year terms, one member's term expires at the end of each calendar year, so new President can only replace members whose terms have expired, provides institutional continuity
- Purpose of independence – Helps ensure that probable cause determinations and recommendations are based upon the facts, not influenced by lobbying or undue political influence



## Impetus for Extraordinary Statutory Independence

- Large percentage of the public is afraid of flying, fear of lack of control
- Most federal legislators fly frequently, e.g., to and from Washington, DC

# Separation From Litigation

- Facts are public on NTSB website to provide transparency
- NTSB's accident reports are also public, but not admissible in litigation
- Factual portion of the investigation involves all of the "parties" – airline, manufacturers, pilots, mechanics, airport, regulator – as needed for technical support, but not attorneys or passenger representatives
- To ensure independence and avoid party bias, parties are not involved in the analytical portion of the investigation, solely the NTSB
- NTSB investigators can be deposed only once and then only about the facts (not about analysis or conclusions)
  - Depositions are often unnecessary because facts are public
- Cockpit voice recorder readouts are not public, NTSB removes non-pertinent content before releasing transcript

# Accidents Are Fundamentally Different From Cyber Attacks

- Transportation accidents are almost always caused by inadvertent error
  - Objective of investigation is not to blame but to propose improvements to prevent recurrences
  - Investigation is very collaborative because everyone wants to prevent recurrences
  - Outcome of investigations is recommendations to whomever can take needed corrective actions, including regulators
  - Investigation is very transparent to demonstrate to public that conclusions and recommendations are from the facts and evidence
  - When evidence of criminal activity or intentional wrongdoing is found, e.g., 9/11, NTSB asks FBI to lead, whereupon NTSB provides technical support, investigation transparency ends

## Fundamental Differences (con't)

- Cyber attacks are intentional
  - Combines need to find perpetrator (as in criminal investigations) along with need to improve mishap defenses (as in NTSB investigations)
  - Transparency is probably undesirable, would give important hacking clues to potential perpetrators
  - Challenge is developing and implementing recommendations for improved defenses without revealing important secrets to potential perpetrators

# NTSB in Other Applications?

- E.g., healthcare, major financial mishaps
- General recommendations
  - Use exhaustive NTSB-type investigation for rare mishaps that surprise even the experts
    - Investigations are very thorough, usually take a year or more
  - For mishaps that occur frequently, use collaborative “System Think” approach to identify and address systemic issues

# Advice Based on NTSB Experience

- Problems that occur frequently indicate systemic shortcomings: suggest investigating trends rather than individual events, with focus on systemic issues
- Aviation analogy – Commercial Aviation Safety Team, voluntary gov't-industry collaborative effort to improve safety
- Problems that are rare and surprise even the safety experts indicate shortcomings that are more unique to the situation: suggest NTSB-type, in-depth investigation of the individual circumstances

# Conclusions

One size does not fit all

-- but --

Some NTSB processes, e.g., active participation by the parties for technical support, may be transferable to help cyber attack investigations identify protection gaps and develop remedial recommendations

Thank You!!!



***Questions?***

Christopher A. Hart  
Hart Solutions LLC  
chris@hartsolutionsllc.com  
202-680-4122



SECTION 2

# Global Note

# GDPR Operational Impacts & NIS Directive

1. Cybersecurity & Data Breach Requirements
2. Mandatory Data Protection Officer
3. Consent
4. Cross-Border Data Transfers
5. Profiling
6. Data Portability
7. Vendor Management
8. Pseudonymization
9. Codes of Conduct & Certifications
10. Consequences of Non-Compliance



# CYBERSECURITY

PROGRAM