KEAN

World-Class Education

Ransomware Incident Preparations With Ethical Considerations and Command System Framework Proposal

Presented by:
Stan Mierzwa, M.S.; CISSP
Kean University Department of Criminal Justice & Center for Cybersecurity

June 9-10, 2022
* 15 minute presentation

Thank you!

To kick it off – Many thanks to CAE Community for this opportunity to speak and present on this topic!

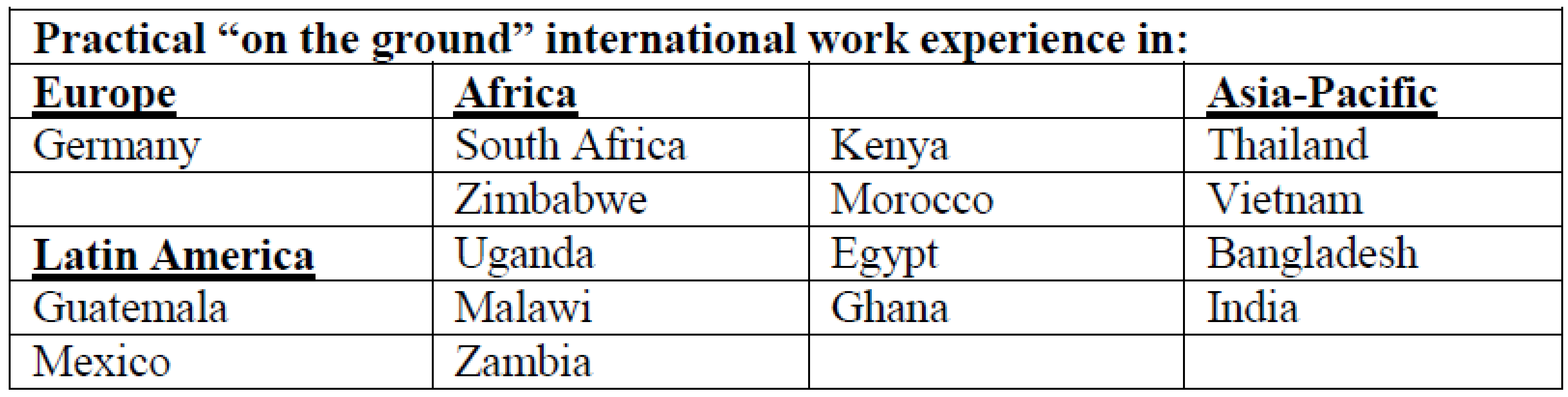
KEAN

Outline

1. Speakers Background
2. Project Team Background
3. Kean Center for Cybersecurity
4. Ransomware: Role of Ethics
5. Constraints
6. Incident Command System (ICS)
7. Non-Technical RecoveryTasks
8. Discussion/Limitations
9. Questions & Thank you!

Speaker Background

- Center for Cybersecurity, Kean University
- Over 25 years IT experience.
  - **Industry:** Sr. Programmer Analyst – UPS.
  - **Academic/Non-Profit:** Director, IT – large NGO, Cyber Lecturer.
  - **State Agency:** Application Security Lead – State of NY, MTA Police. FBI Infragard.
  - **Board Member:** CTO – Non-Profit - Vennue.
  - Pursuing Ph.D.
- International work experience.



Practical “on the ground” international work experience in:			
Europe	**Africa**		**Asia-Pacific**
Germany	South Africa	Kenya	Thailand
	Zimbabwe	Morocco	Vietnam
Latin America	Uganda	Egypt	Bangladesh
Guatemala	Malawi	Ghana	India
Mexico	Zambia		

Outline

2

Project Team Background

Project Team Background

- Stan Mierzwa
  - Center for Cybersecurity, Kean University.
- Dr. James. J. Drylie
  - Former law enforcement. School of Criminal Justice, Kean University.
- Cochi Ho
  - Former FBI Agent and NJ InfraGard Board member.
- Dennis Bogdan
  - Former law enforcement. School of Criminal Justice, Kean University.
- Kenneth Watson
  - Current law enforcement. Faculty at Montclair State University.

Outline

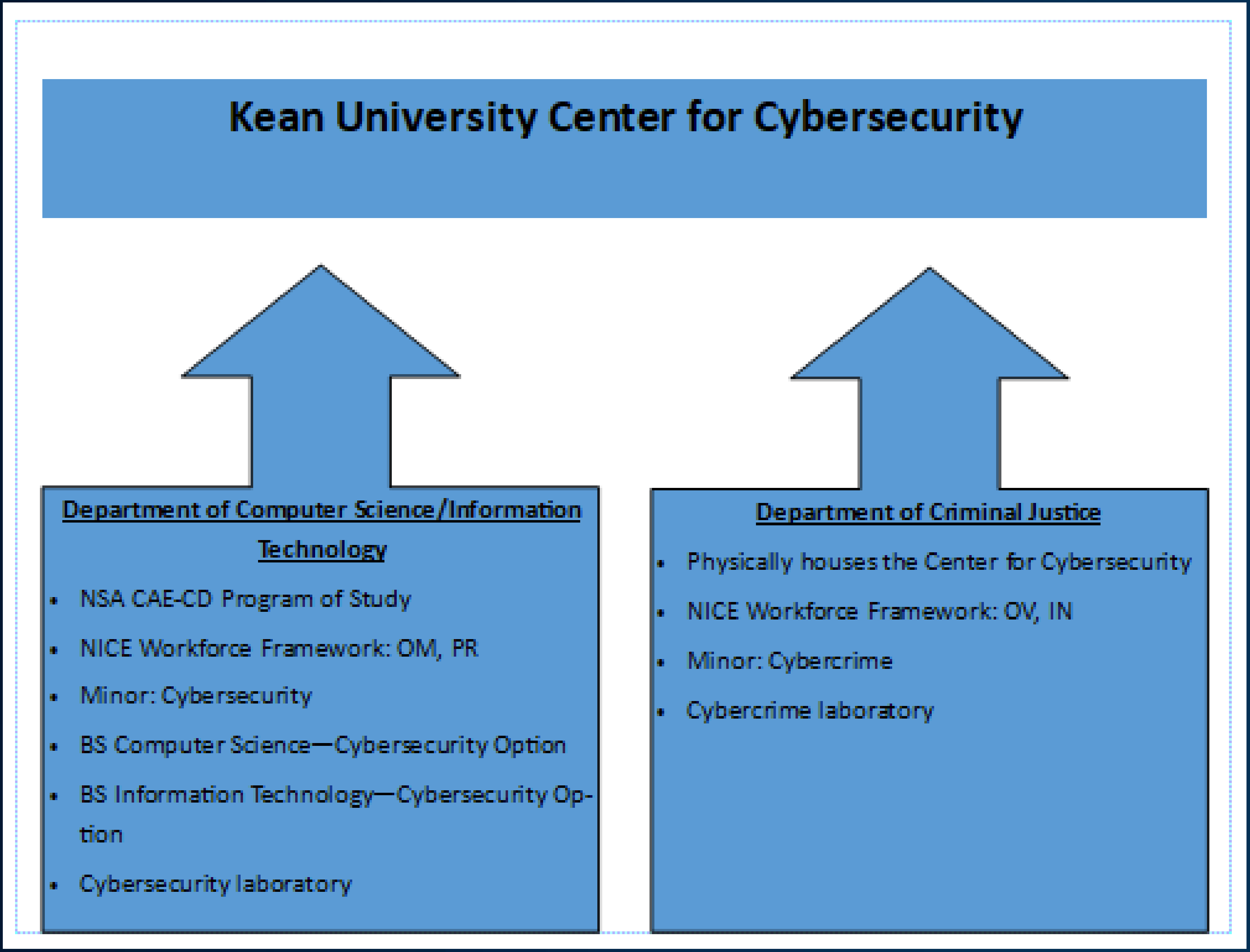
3 Kean Center for Cybersecurity

KEAN
Center for
Cybersecurity
kean.edu/cybersecurity
5732C207
7061746
System Protected

HYNES HALL
KEAN
KEAN UNIVERSITY
BUSINESS &
PUBLIC MANAGEMENT

Cross-Discipline Collaboration (Computer Science/Information Technology and Criminal Justice)

https://www.kean.edu/academics/center-cybersecurity



Kean University Center for Cybersecurity

Department of Computer Science/Information Technology

- NSA CAE-CD Program of Study
- NICE Workforce Framework: OM, PR
- Minor: Cybersecurity
- BS Computer Science—Cybersecurity Option
- BS Information Technology—Cybersecurity Option
- Cybersecurity laboratory

Department of Criminal Justice

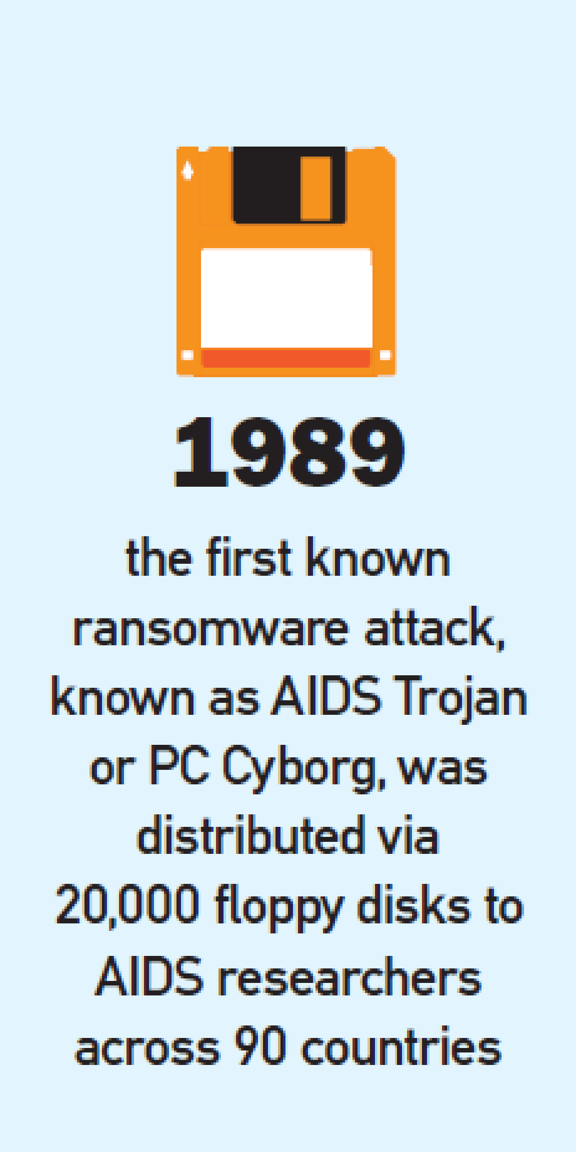
- Physically houses the Center for Cybersecurity
- NICE Workforce Framework: OV, IN
- Minor: Cybercrime
- Cybercrime laboratory

Outline

4

Ransomware: Role of Ethics

Ransomware Isn’t Really New



1989

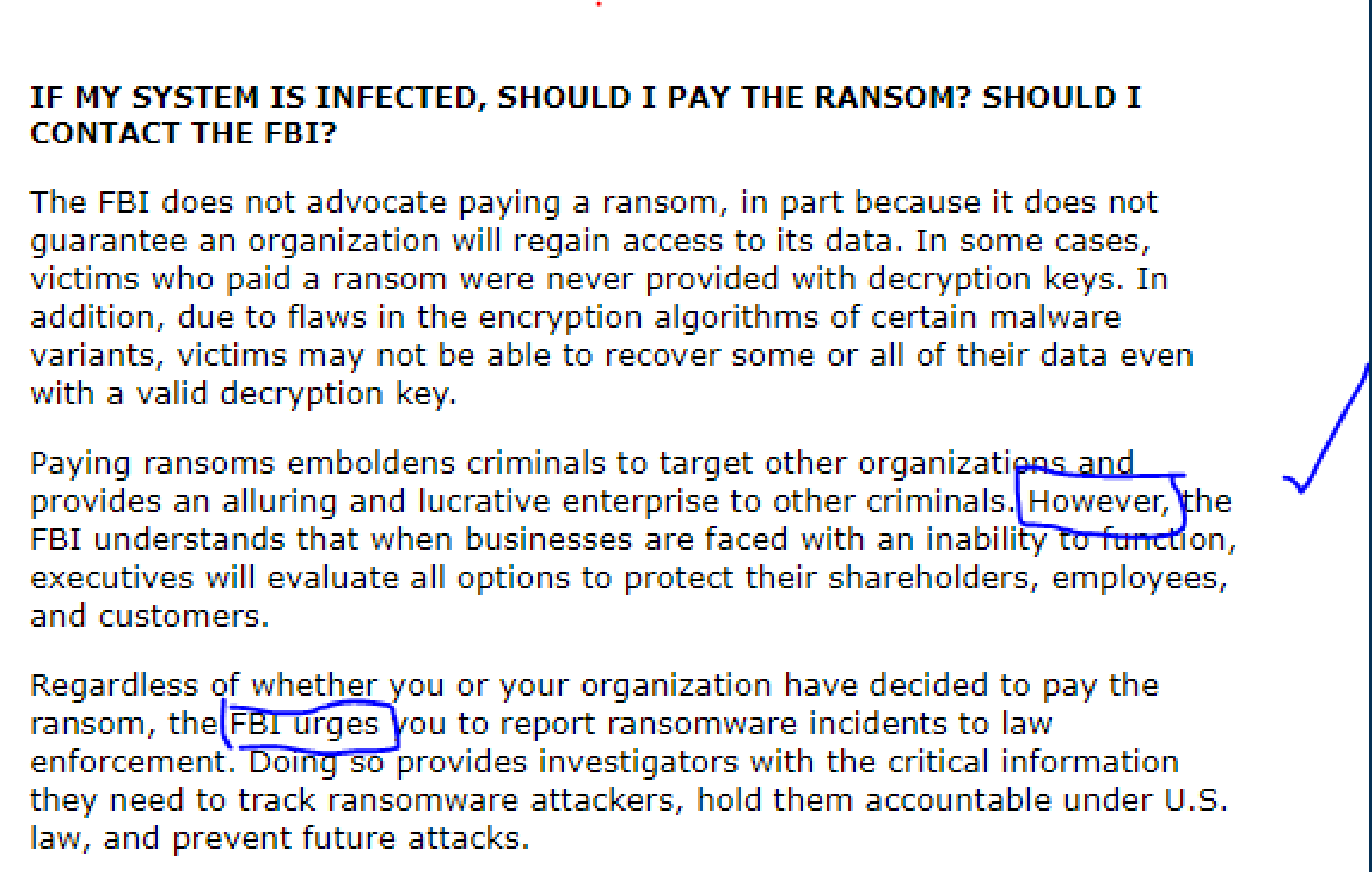
the first known ransomware attack, known as AIDS Trojan or PC Cyborg, was distributed via 20,000 floppy disks to AIDS researchers across 90 countries

Source: Tuttle, 2017

Ethics and Ransomware

- Greater accountability and decision-making – ethics will add value as a reminder.
- Cybersecurity social responsibility.
  - Leadership & Board.
    - Key stakeholders (customers, employees).
  - Avoid negligence.
- This specific effort involved combining several research interests:
  - Ethics – NEDSI Submitted Conference Paper
  - Incident Command System – JLAE Paper

Ransom - Ethics



IF MY SYSTEM IS INFECTED, SHOULD I PAY THE RANSOM? SHOULD I CONTACT THE FBI?

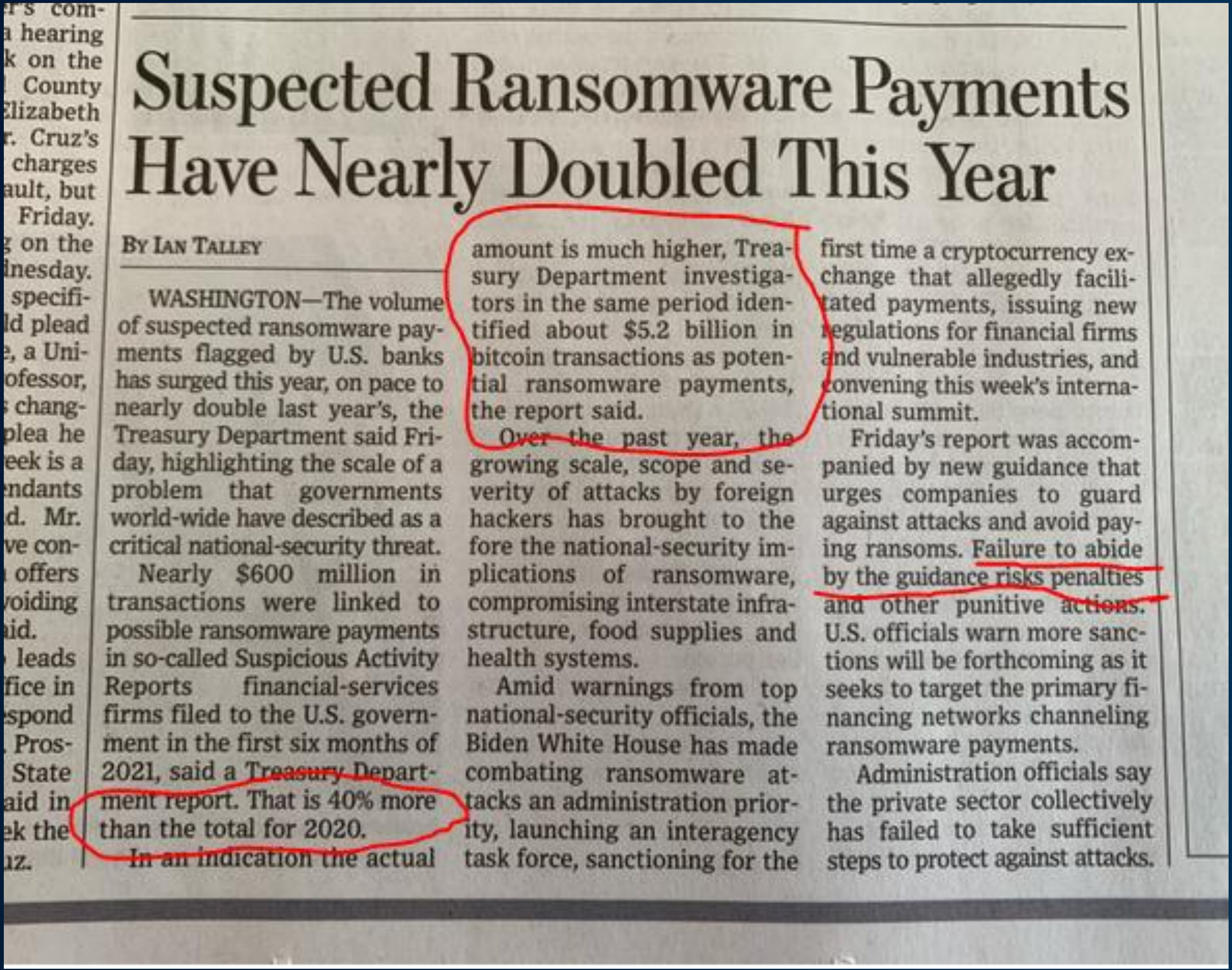
The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to law enforcement. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

Source: https://www.ic3.gov/Media/Y2019/PSA191002

Ransomware Constraints



r's com-
a hearing
k on the
County
Elizabeth
r. Cruz's
charges
ault, but
Friday.
g on the
dnesday.
specifi-
ld plead
e, a Uni-
ofessor,
chang-
plea he
eek is a
ndants
d. Mr.
ve con-
offers
oiding
aid.
leads
fice in
spond
Pros-
State
aid in
ek the
uz.

Suspected Ransomware Payments Have Nearly Doubled This Year

By Ian Talley

WASHINGTON—The volume of suspected ransomware payments flagged by U.S. banks has surged this year, on pace to nearly double last year's, the Treasury Department said Friday, highlighting the scale of a problem that governments world-wide have described as a critical national-security threat.

Nearly $600 million in transactions were linked to possible ransomware payments in so-called Suspicious Activity Reports financial-services firms filed to the U.S. government in the first six months of 2021, said a Treasury Department report. That is 40% more than the total for 2020.

In an indication the actual amount is much higher, Treasury Department investigators in the same period identified about $5.2 billion in bitcoin transactions as potential ransomware payments, the report said.

Over the past year, the growing scale, scope and severity of attacks by foreign hackers has brought to the fore the national-security implications of ransomware, compromising interstate infrastructure, food supplies and health systems.

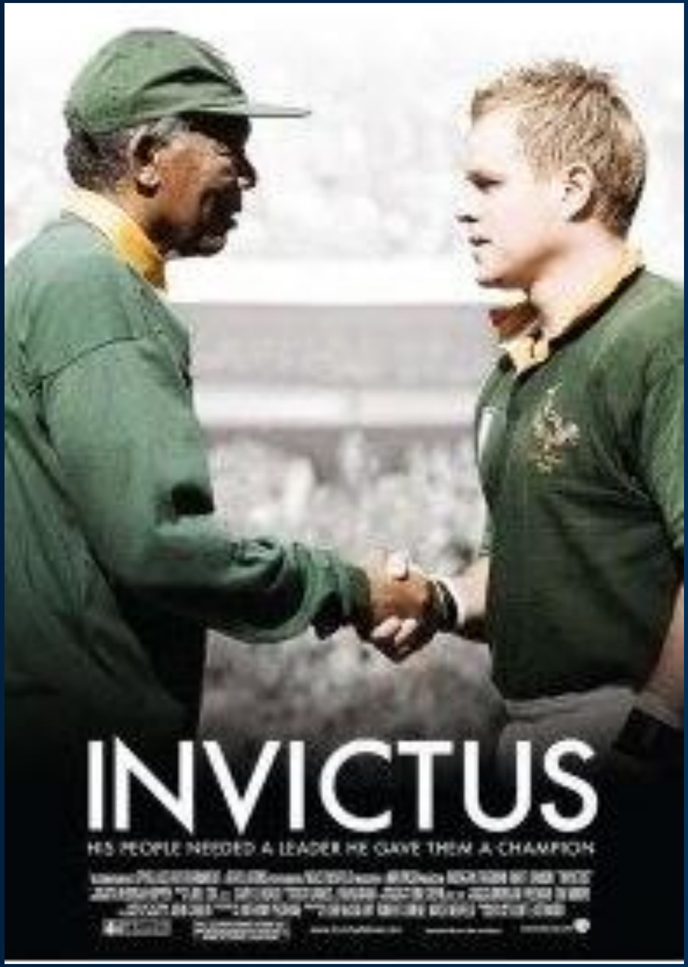
Amid warnings from top national-security officials, the Biden White House has made combating ransomware attacks an administration priority, launching an interagency task force, sanctioning for the first time a cryptocurrency exchange that allegedly facilitated payments, issuing new regulations for financial firms and vulnerable industries, and convening this week's international summit.

Friday's report was accompanied by new guidance that urges companies to guard against attacks and avoid paying ransoms. Failure to abide by the guidance risks penalties and other punitive actions. U.S. officials warn more sanctions will be forthcoming as it seeks to target the primary financing networks channeling ransomware payments.

Administration officials say the private sector collectively has failed to take sufficient steps to protect against attacks.

Source: Talley, I. (10/17/2021). Wall Street Journal

Change: Focus on Ethics?



- Something has to change if we are going to make a dent in the increasing cyberattacks – can greater ethics assist?

IEEE Code of Ethics - Excerpt

- To avoid real or perceived conflicts of interest….. And to disclose them to affected parties when they do exist.
- To avoid unlawful conduct in professional activities, and to reject bribery in all its forms.
- To improve understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies.

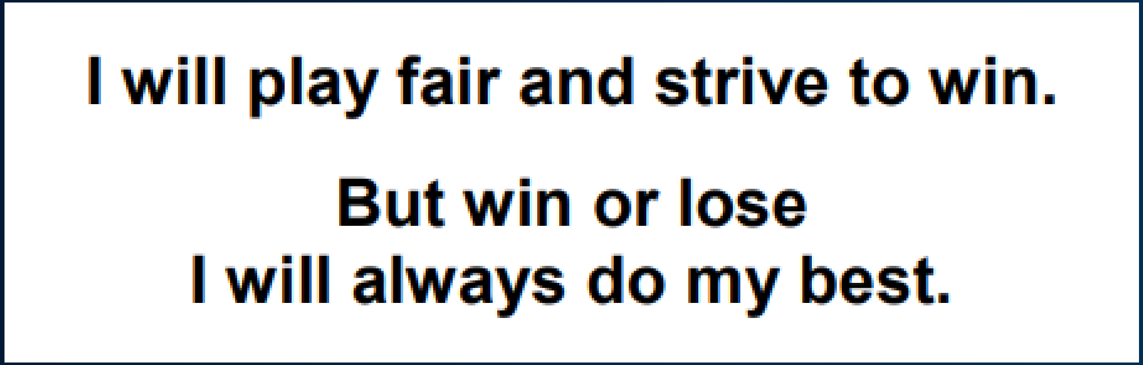
Source: https://www.ieee.org/about/corporate/governance/p7-8.html

Oath Example

- Modern Hippocratic Oath.
  - Uphold ethical standards.
- “I will remember that I remain a member of society, with special obligations to all my fellow human beings, those sound of mine and body as well as the infirm” (NOVA & Lasagna, L., 1964)
- How to consider a humble approach with cybersecurity?

Little League Baseball Pledge

The Little League Pledge



I will play fair and strive to win.

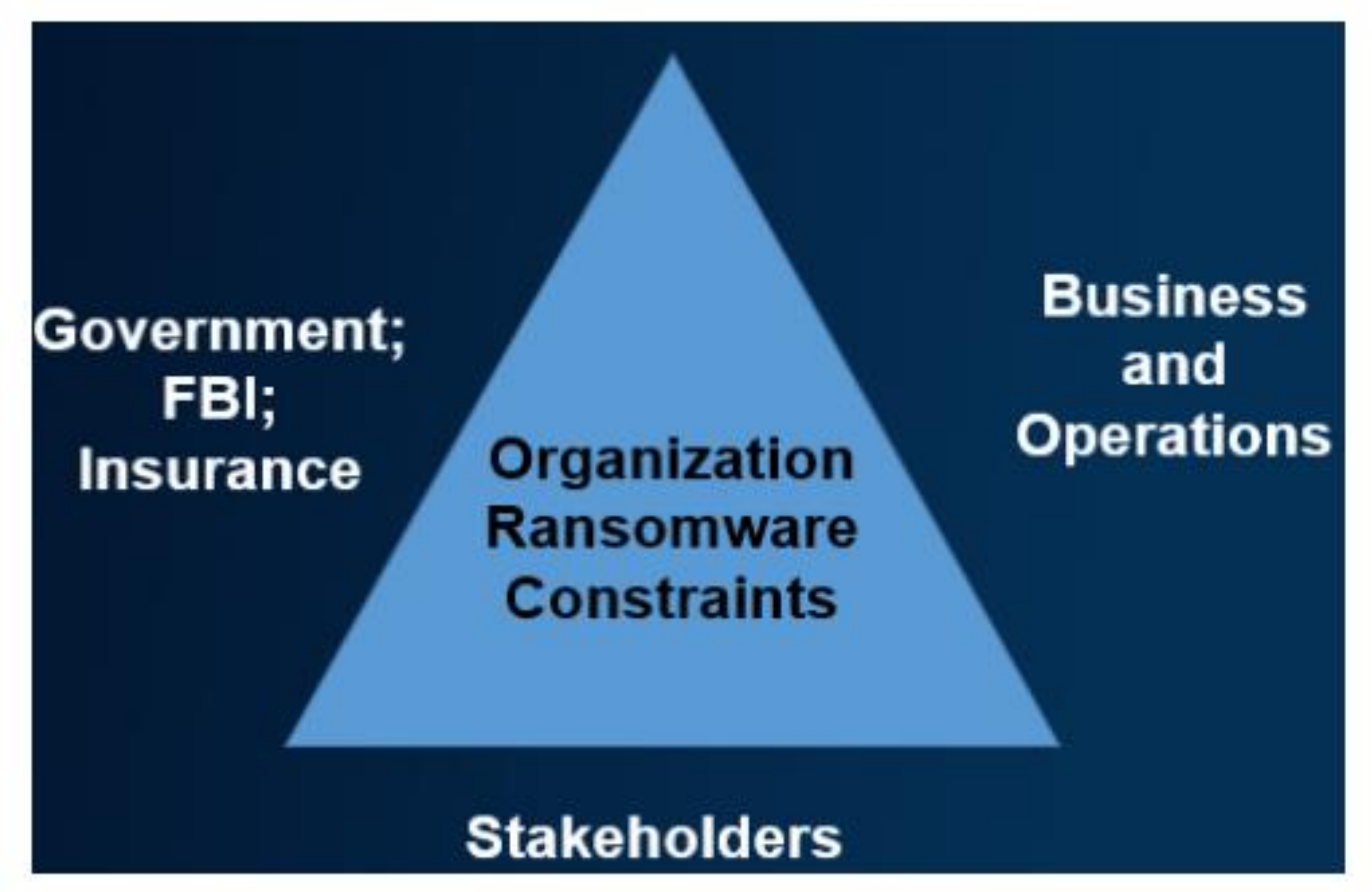
But win or lose
I will always do my best.

Outline

5

Constraints

Complex Ransomware Constraints Arise



Cybersecurity Defense

- Increasing cybersecurity attacks – especially during the COVID-19 pandemic! i.e. Scams – stimulus checks, fake CDC emails. Our Kean Center for Cybersecurity Resource Page.
- New and more technologies to complement health systems.
- World Economic Forum – cyber attacks 1 of the 5 top global risks.

Outline

6

Incident Command System

Ransomware Recovery Org. Preparation

- Dilemma: Pay the ransom, or something bad will happen (Bennett & Genung, 2021).
- Response must be well planned and tested.
- Time to decide on response plan is NOT during the crisis – intensity of situation can distort judgement (Bennett & Genung, 2021).
- **Creation of a ransomware policy brief – outlining general steps to be taken.**
  - When to contact law enforcement.
  - Determination of timeframe before committing to paying ransom.
  - Verification and testing of BCP/DR plan.
  - Remaining defensive – not allowing re-occurrence.
  - Keeping in mind the ethical considerations of the said company. (Public, Shareholders, Customers, Employees, etc.).

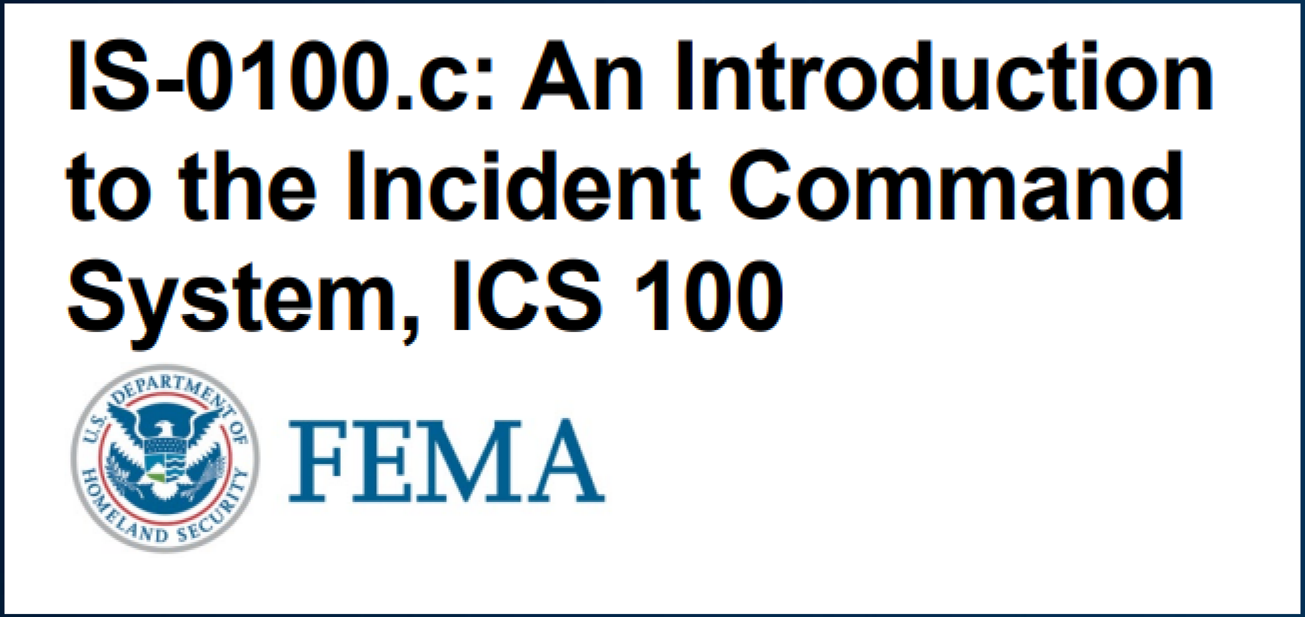
Ransomware Organization Preparation – Cont.

- **Costs (budget) to consider – it may not end with the ransom (Tuttle, 2021)**
  - Downtime and lost productivity.
  - Business disruption and loss of data.
  - Forensic investigation.
  - Reputation.
  - Additional employee training.
  - Potential for hiring attorneys.
  - Identify the forensics team, under privilege – through legal (Tuttle, 2017)
  - Be prepared to work around the clock to address the incident.
- **Contacting the FBI and law enforcement**
  - Prepare with known contacts – rather than scrambling to determine who to specifically contact.
  - Report to FBI, often aware of emerging threats not yet made public (Tuttle, 2017).

Ransomware Organization Preparation – Cont.

- **Board and Executive Leadership**
  - Bring up the risk topic and provide education.
  - Determine ethical considerations of when to pay/not pay.
  - Keep the topic, potential for incident, and steps that will be followed transparent.
  - Partner the CISO and Enterprise Risk Management teams.
- **Insurance**
  - Proactively determine if changes are required to cyber insurance policy.
  - Determine guidelines for insurance coverage from agent.
  - Mindful of notice clause under policy (Tuttle, 2017).
- **Operational**
  - Perform a table-top exercise for ransomware incident.
  - Follow standardized approach for response (Incident Command System (ICS) & National Incident Management System (NIMS) from FEMA).
  - Cyber risk self-assessments (internal and external).
  - Post incident review (adjust backup, email filters, more education)

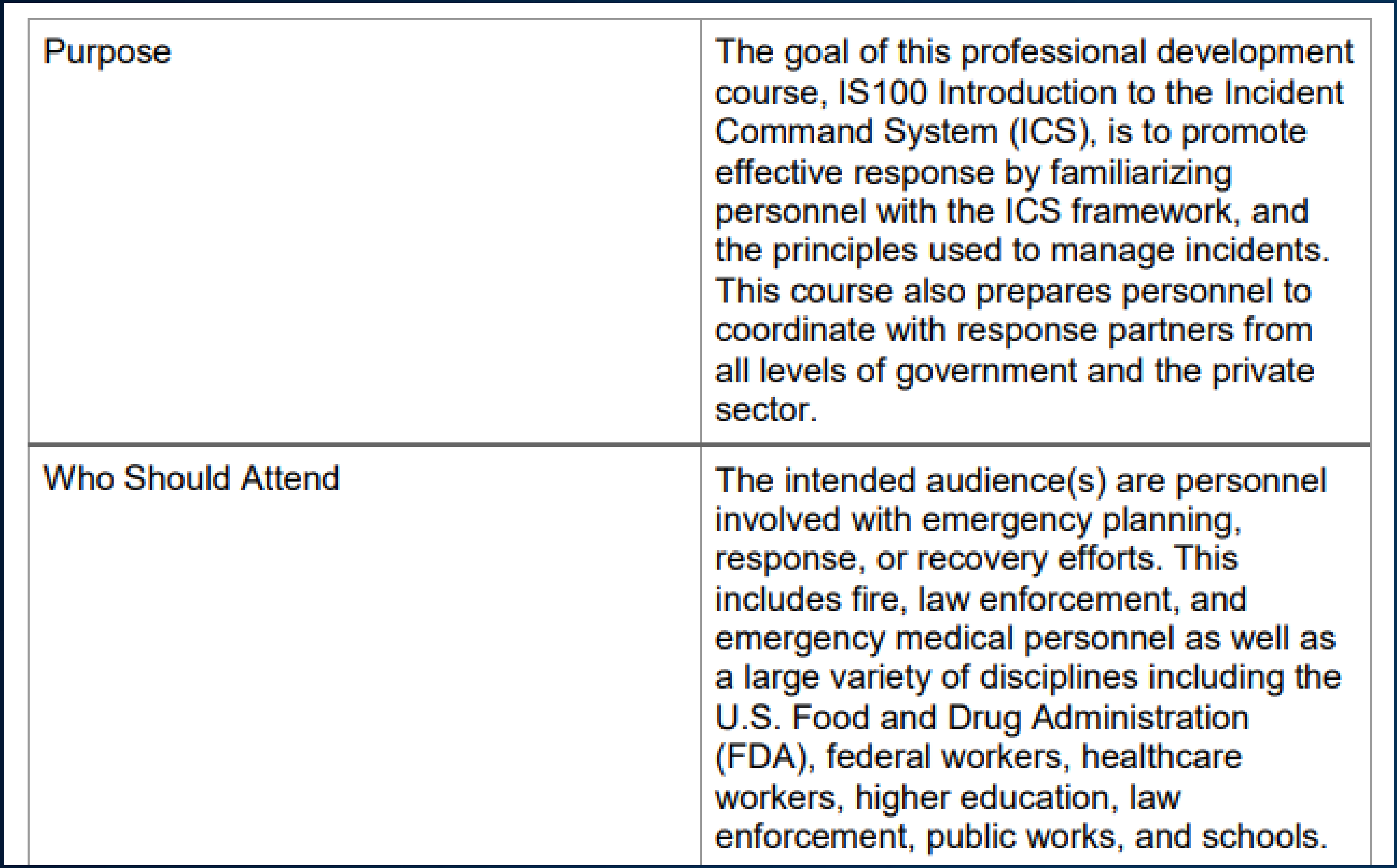
FEMA ICS-100



IS-0100.c: An Introduction to the Incident Command System, ICS 100

U.S. DEPARTMENT OF HOMELAND SECURITY
FEMA

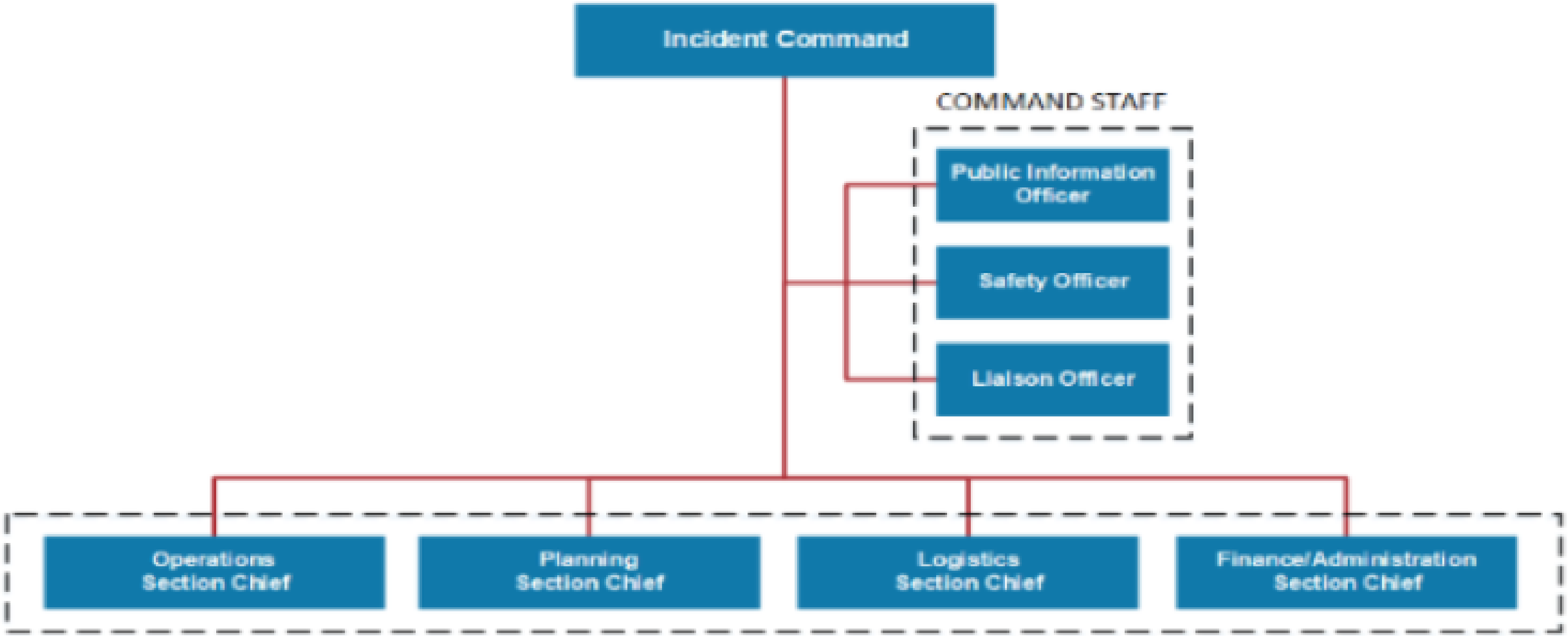
FEMA ICS-100



Purpose	The goal of this professional development course, IS100 Introduction to the Incident Command System (ICS), is to promote effective response by familiarizing personnel with the ICS framework, and the principles used to manage incidents. This course also prepares personnel to coordinate with response partners from all levels of government and the private sector.
Who Should Attend	The intended audience(s) are personnel involved with emergency planning, response, or recovery efforts. This includes fire, law enforcement, and emergency medical personnel as well as a large variety of disciplines including the U.S. Food and Drug Administration (FDA), federal workers, healthcare workers, higher education, law enforcement, public works, and schools.

FEMA ICS-100

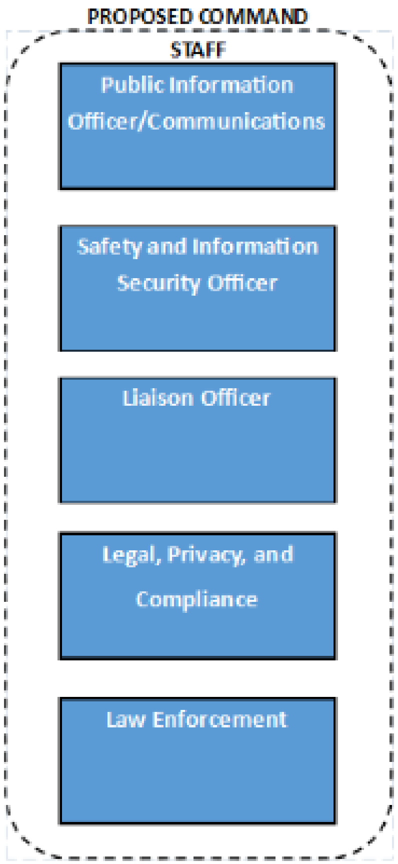
FIGURE 2
STANDARD INCIDENT COMMAND SYSTEM (ICS) ORGANIZATION STRUCTURE



Source: FEMA: IS-0110.C: An Introduction to the Incident Command System

FEMA ICS-100

FIGURE 3
PROPOSED AMENDMENT OR INCLUSION OF COMMAND STAFF GROUPS FOR ICS



PROPOSED COMMAND STAFF

Public Information Officer/Communications

Safety and Information Security Officer

Liaison Officer

Legal, Privacy, and Compliance

Law Enforcement

Outline

7

Non-Technical Recovery Tasks

Complementary Checklist for ICS - 1

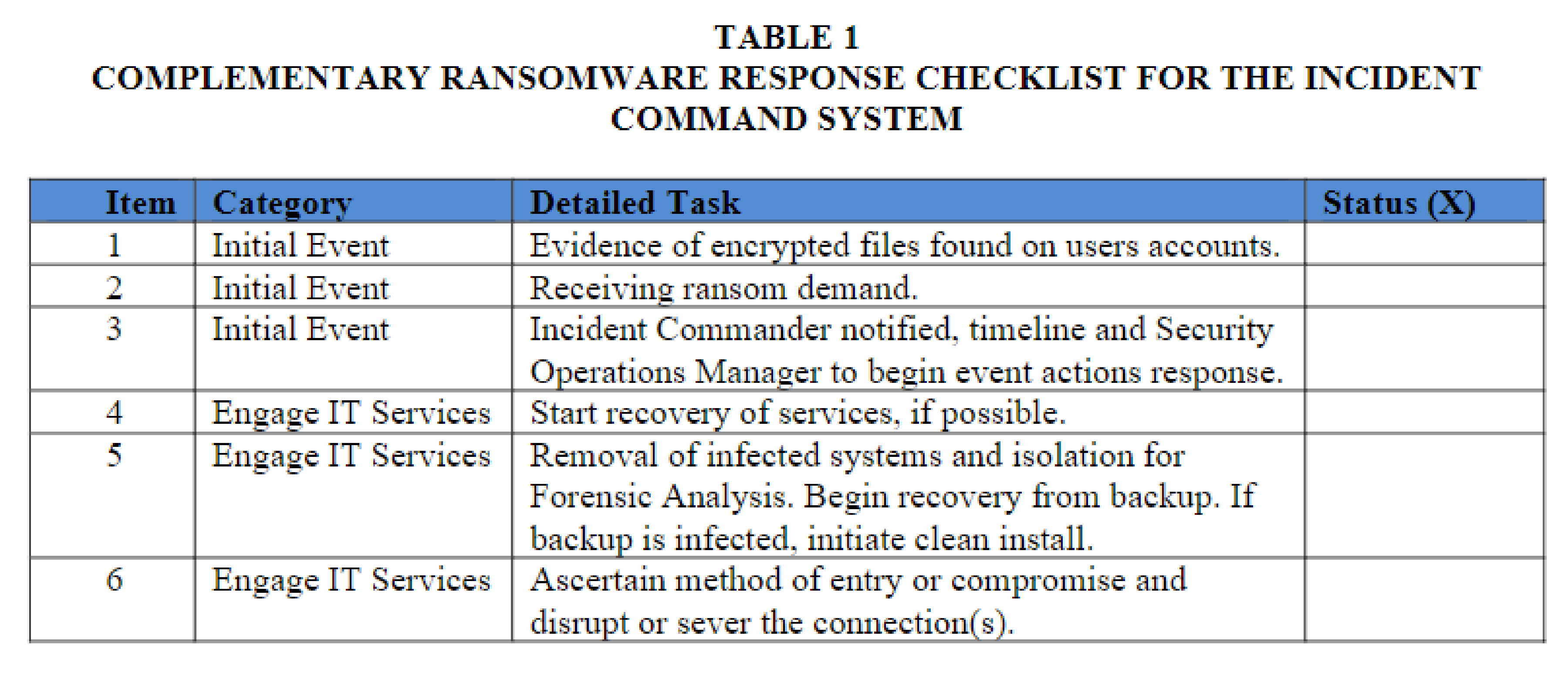
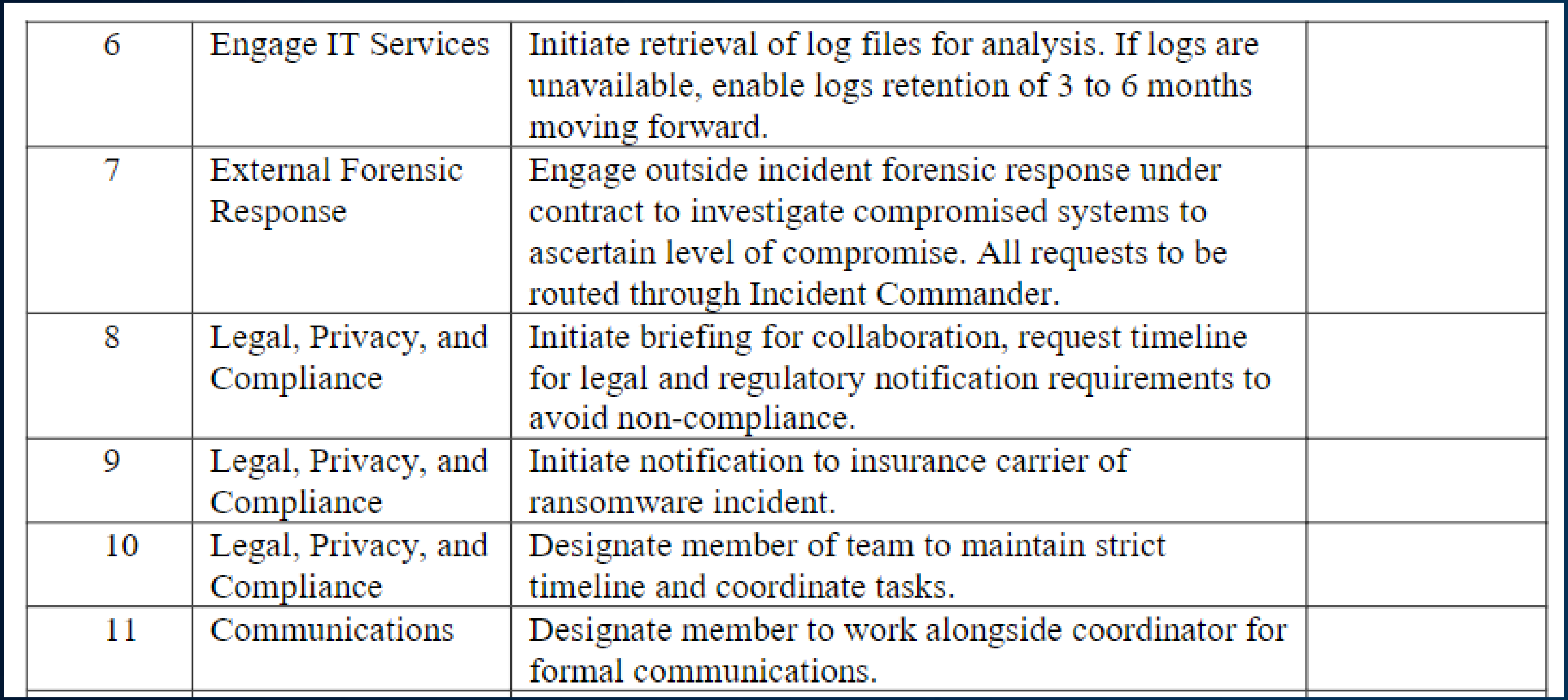


TABLE 1
COMPLEMENTARY RANSOMWARE RESPONSE CHECKLIST FOR THE INCIDENT COMMAND SYSTEM

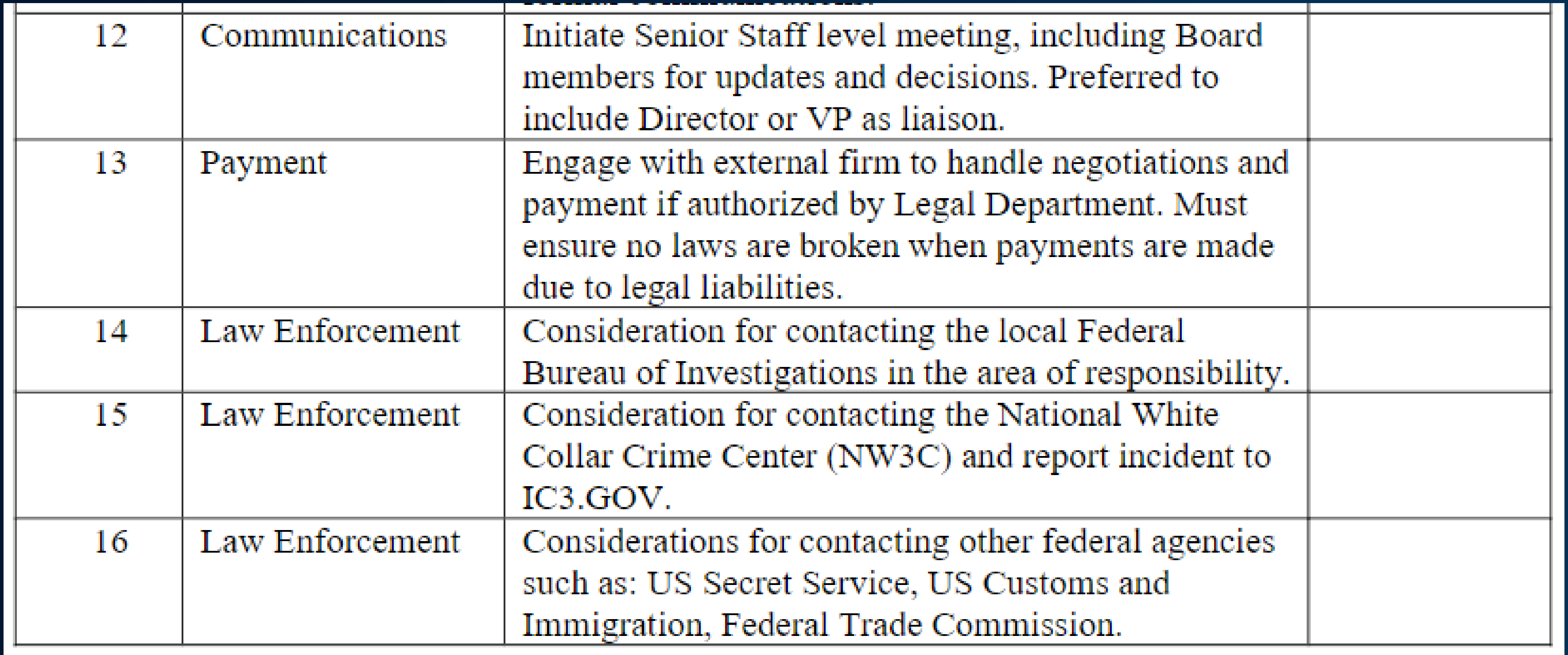
Item	Category	Detailed Task	Status (X)
1	Initial Event	Evidence of encrypted files found on users accounts.	
2	Initial Event	Receiving ransom demand.	
3	Initial Event	Incident Commander notified, timeline and Security Operations Manager to begin event actions response.	
4	Engage IT Services	Start recovery of services, if possible.	
5	Engage IT Services	Removal of infected systems and isolation for Forensic Analysis. Begin recovery from backup. If backup is infected, initiate clean install.	
6	Engage IT Services	Ascertain method of entry or compromise and disrupt or sever the connection(s).	

Complementary Checklist for ICS - 2



6	Engage IT Services	Initiate retrieval of log files for analysis. If logs are unavailable, enable logs retention of 3 to 6 months moving forward.	
7	External Forensic Response	Engage outside incident forensic response under contract to investigate compromised systems to ascertain level of compromise. All requests to be routed through Incident Commander.	
8	Legal, Privacy, and Compliance	Initiate briefing for collaboration, request timeline for legal and regulatory notification requirements to avoid non-compliance.	
9	Legal, Privacy, and Compliance	Initiate notification to insurance carrier of ransomware incident.	
10	Legal, Privacy, and Compliance	Designate member of team to maintain strict timeline and coordinate tasks.	
11	Communications	Designate member to work alongside coordinator for formal communications.	

Complementary Checklist for ICS - 3



12	Communications	Initiate Senior Staff level meeting, including Board members for updates and decisions. Preferred to include Director or VP as liaison.	
13	Payment	Engage with external firm to handle negotiations and payment if authorized by Legal Department. Must ensure no laws are broken when payments are made due to legal liabilities.	
14	Law Enforcement	Consideration for contacting the local Federal Bureau of Investigations in the area of responsibility.	
15	Law Enforcement	Consideration for contacting the National White Collar Crime Center (NW3C) and report incident to IC3.GOV.	
16	Law Enforcement	Considerations for contacting other federal agencies such as: US Secret Service, US Customs and Immigration, Federal Trade Commission.	

Future Potential

- Provide Incident Command System (ICS) training more broadly:
  - Introduce to faculty and students.
    - Potentially through the CAE community.
  - Reinforce how ICS can be utilized with ransomware events.
- Provide more awareness and focus on the responsibility of cybersecurity ethics.
- Contact FEMA to determine if the proposed amendment can be leveraged or integrated into ICS-100 or other.

Outline

8 Discussion/Limitations

9 Thank you!

Limitations

- Commentary and thought leadership papers.
  - Did not test on actual ransomware scenarios.
  - Formal training program not yet created.
  - Rapid literature reviews.

References

- Aud der Heide, E. (1989). Disaster Response: Principles of Preparation and Coordination. Mosby, Baltimore, MD.
- Bennett, S. & Genung, J. (2021). All in One: Certified Chief Information Security officer Exam Guide. *McGraw Hill. New York*. p167-168.
- Chen, P-H., Bodak, R. & Gandhi, N.S. (2021). Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *Journal of Digital Imaging. 34*:731-740.
- Federal Emergency Management Institute. (2021). Emergency Management Institute – National Incident Management System (NIMS). As retrieved from: https://training.fema.gov/is/courseoverview.aspx?code=IS-200.c
- Federal Emergency Management Institute. (2021). Emergency Management Institute – Independent Study Course Brochure. As retrieved from: https://training.fema.gov/is/docs/fema_emi_independent-study-brochure_10-01-2021.pdf
- FEMA IS-100.c. (2021). An Introduction to the Incident Command System, ICS 100. As retrieved from: https://emilms.fema.gov/is_0100c/curriculum/1.html
- FEMA Incident Command System. (2020). Unit Seven Incident Command System. *FEMA Training*. As retrieved from: https://training.fema.gov/emiweb/downloads/301unt07.pdf
- IC3.GOV. (2016). Ransomware Victims Urged to Report Infections to Federal Law Enforcement. *Public Service Announcement I-091516-PSA. Federal Bureau of Investigation*. As retrieved from: https://www.ic3.gov/Media/Y2016/PSA160915
- IC3.GOV. (2019). High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations. *Public Service Announcement I-100219-PSA. Federal Bureau of Investigation*. As retrieved from: https://www.ic3.gov/Media/Y2019/PSA191002
- IC3.GOV. (2021). Internet Crime Report 2020. As retrieved from: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
- Jensen, J. & Thompson, S. (2006). The Incident Command System: A Literature Review. *Disasters. 40*(I). 158-182.
- KnowBe4. (2021). AIDS Trojan or PC Cyborg Ransomware. As retrieved from: https://www.knowbe4.com/aids-trojan
- Lean Production. (2021). Theory of Constraints (TOC). As retrieved from: https://www.leanproduction.com/theory-of-constraints/
- Lederer, E.M. (2020). UN Reports Sharp Increase in Cybercrime during the Pandemic. *AP News.*
- Mierzwa, S., RamaRao, S. & Jackson. T. (2021). Global Ethical and Societal Issues and Considerations with Cybersecurity in Digital Health: A rapid review. Northeast Decision Sciences Institute Conference Proceedings. As retrieved from: https://nedsi.decisionsciences.org/wp-content/uploads/2021/06/NEDSI-2021-Proceedings.pdf
- Mierzwa, S., Spath-Caviglia, L. & Christov, I. (2021). Commentary or Perspective: Opportunities to Leverage Global Public Health Innovative Research Technology in Combatting Cybercrime. *Journal of Leadership, Accountability and Ethics. 18*(4). DOI: https://doi.org/10.33423/jlae.v18i4.4608
- National Safety Inc. (2009). The Basics of Incident Command. National Safety Inc. As retrieved from: https://www.nationalsafetyinc.com/Assets/Downloadables/The%20Basics%20of%20Incident%20Command.pdf
- O'Kane, P., Sezer, S. & Carlin, D. (2018). Evolution of Ransomware. *The Institution of Engineering and Technology Journals.* DOI: 10.1049/iet-net.2017.0207.
- Shea, J. & Flinton, B. (2021). Preparing for Ransomware. *The Business Journal – Central New York. 35*(27).
- Talley, I. (2021). Suspected Ransomware Payments Have Doubled This Year. *Wall Street Journal*. Oct. 17, 2021.
- Tuttle, H. (2017). Ransomware Ready: How to Prepare for the Day You Get Locked Out*. Risk Management. 64*(7).
- Tuttle, H. & Jacobson, A. (2019). Enemy of the State: Ransomware Surges Against State and Local Governments in 2019. *Risk Management. 66*(11). 30-35.
- Kobzar, S. (2013). Transforming research into an engaging policy story: how to write a policy brief. Migration Policy Centre, CARIM-East. As retrieved from: http://diana-n.iue.it:8080/handle/1814/62781

References

- Ahmad, T. (2020). Coronavirus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Retrieved from: http://dx.doi.org/10.2139/ssrn.3658830.
- Benatar, S. (2020). More eyes on COVID-19: Perspectives from Ethics: The most powerful health-promotion forces in COVID-19 are social. *South African Journal of Science. Vol. 16. No. 7/8.*
- Burton, J. & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach, *Journal of Cyber Policy*, DOI: 10.1080/23738871.2020.1856903
- Center for Internet Security. (2020). “Know the Rules of Cyber Ethics”. As retrieved from: https://www.cisecurity.org/daily-tip/know-the-rules-of-cyber-ethics/
- Cannon, D. L., O’Hara, B.T. and Keele, Allen. 2016*. CISA Certified Information Systems Auditor Study Guide, Fourth Edition.* Sybex. Indianapolis, Indiana.
- Forbes. (2020). Top 10 Most Popular Cybersecurity Certifications in 2020. As retrieved from: https://www.forbes.com/sites/louiscolumbus/2020/06/16/top-10-most-popular-cybersecurity-certifications-in-2020/#241f07f43f51
- Grimes, R. (2017). “Hacking the Hacker: Learn from the Experts Who Take Down Hackers”, *Wiley & Sons, Inc*. Indianapolis, Indiana.
- Hall, B. R. (2014). A Synthesized Definition of Computer Ethics. *SIGCAS Computers & Society*. Vol 44. No. 3.
- Harkins, M. W. (2016). Managing Risk and Information Security: Protect to Enable. Second Edition. *Apress Open*.
- Harvard Catalyst. (2016). The Harvard Clinical and Translational Science Center. Information Risks & IRB Strategies for Technologies Used in Research: A Guide for Researchers, IT, and IRBs
- Coles-Kemp, L., Ashenden, D. & O’Hara, K. (2017). Why Should I? Cybersecurity, the Security of the State and the Insecurity of the Citizen. *Politics and Governance. 6*(2). 41-48.
- Mikalauskas, E. (2020). 5 Cybersecurity Scandals That Could’ve Been Easily Prevented. DZone Security Zone. As retrieved from: https://dzone.com/articles/5-cybersecurity-scandals-that-couldve-been-easily
- Shackelford, S. (2019). Should Cybersecurity Be a Human Right? Exploring the Shared Responsibility of Cyber Peace. *Stanford Journal of International Law. 2*. 155-184.
- Bennett, S. & Genung, J. (2021). All In One: Certified Chief Information Security Officer Exam Guide. McGraw Hill.
- Tuttle, H. (2017). Ransomware Ready: How to Prepare for the Day You Get Locked Out. *Risk Management. 64*(7).

References

- Mierzwa, S., RamaRao, S., Yun, J. A. & Jeong, B. G. (2020). Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health. *International Journal of Cybersecurity Intelligence & Cybercrime.*
- Narayanan, S., Ganesan, A., Joshi, K., Oates, T., Joshi, A. & Finin, T. (2018). Early Detection of Cybersecurity Threats Using Collaborative Cognition. *IEEE Explore 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).*
- Koenig, T. H., Rustad, M. L. (2018). Global Information Technology Ethics and the Law. *West Academic Publishing.* St. Paul, Minnesota.
- Ruotsalainen, P. & Blobel, B. (2020). Health Information Systems in the Digital Health Ecosystem-Problems and Solutions for Ethics, Trust and Privacy*. International Journal of Environmental Research and Public Health.*
- Tidy, J. (2020). How hackers extorted $1.14m from University of California, San Franciso. BBC News. As retrieved from: https://www.bbc.com/news/technology-53214783
- United States Department of Homeland Security. 2019. CISA Cybersecurity Talen Identification and Assessment. As retrieved from: https://niccs.cisa.gov/sites/default/files/documents/pdf/cybersecurity%20talent%20identification%20and%20assessment.pdf?trackDocs=cybersecurity%20talent%20identification%20and%20assessment.pdf
- Well, T. & Murugesan, S. (2020). IT Risk and Resilience – Cybersecurity Response to COVID-19. *IT Professional. Vol 22. No. 3.*
- World Economic Forum. (2020). The Global Risks Report 2020. As retrieved from: http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
- Wykes, T., Lipshitz, J. & Schueller, S.M. Towards the Design of Ethical Standards Related to Digital Mental Health and all Its Applications. *Curr Treat Options Psych* **6,** 232–242 (2019). https://doi.org/10.1007/s40501-019-00180-0

Thank you!!
Have a productive and fun conference!

KEAN

World-Class Education