

ALYSSA PUGH

The ISO's Guide to Managing Ransomware



1

Disclaimer

A FEW THINGS FIRST

This presentation is for information only.

Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.

Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.

Unauthorized release of this information is prohibited.

Original material is copyright © 2022 Tandem.



2



Alyssa Pugh

CISM, SECURITY+
TANDEM GRC CONTENT MANAGER



3

Agenda

HERE'S THE PLAN

- The Problem with Ransomware
- Managing the Risk of Ransomware
- Communicating about Ransomware
- Questions & Answers



4



The Problem with Ransomware

(IT'S A BIT OF A PROBLEM)

5

Ransomware Definition

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA)

“Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid.”

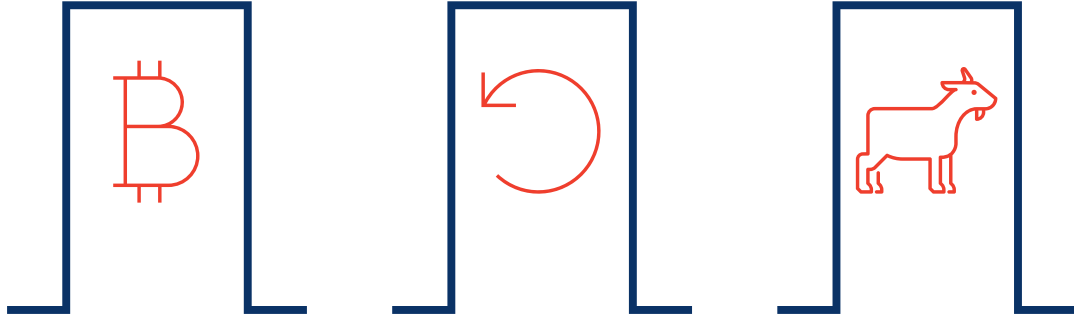
<https://us-cert.cisa.gov/ncas/tips/ST19-001>



6

Let's Make a Deal

(HINT: IT'S NOT AS FUN AS THE GAME SHOW)



7

A collage of news articles related to cybersecurity incidents. On the left is a CISA article titled "Kaseya Ransomware Attacks MSPs and their Customers". In the center is a Bloomberg article titled "NBA's Houston Rockets Face Cyber-Attack by Ransomware Group". On the right is a New York Times article titled "Cyberattack Forces a Shutdown of a Top U.S. Pipeline". The collage also includes a "KEYS CONFERENCE" logo in the top right corner and a list of URLs at the bottom.

8

Hackers' Statement

COLONIAL PIPELINE

"We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined government and look for other our motives. **Our goal is to make money and not creating problems for society.** From today, we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future."

<https://www.theverge.com/2021/5/10/22428996/colonial-pipeline-ransomware-attack-apology-investigation>



9

HIGHER
or
LOWER



10

Average downtime due to ransomware.

~~7 DAYS~~
21 DAYS

HIGHER
or
LOWER

<https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>




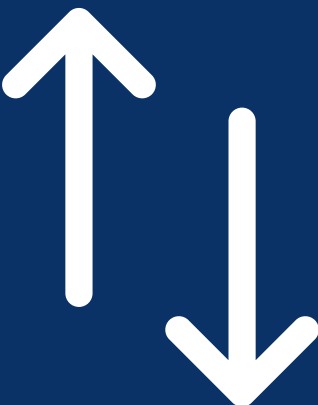
11

Cryptocurrency value paid to ransomware attackers since the start of 2020.

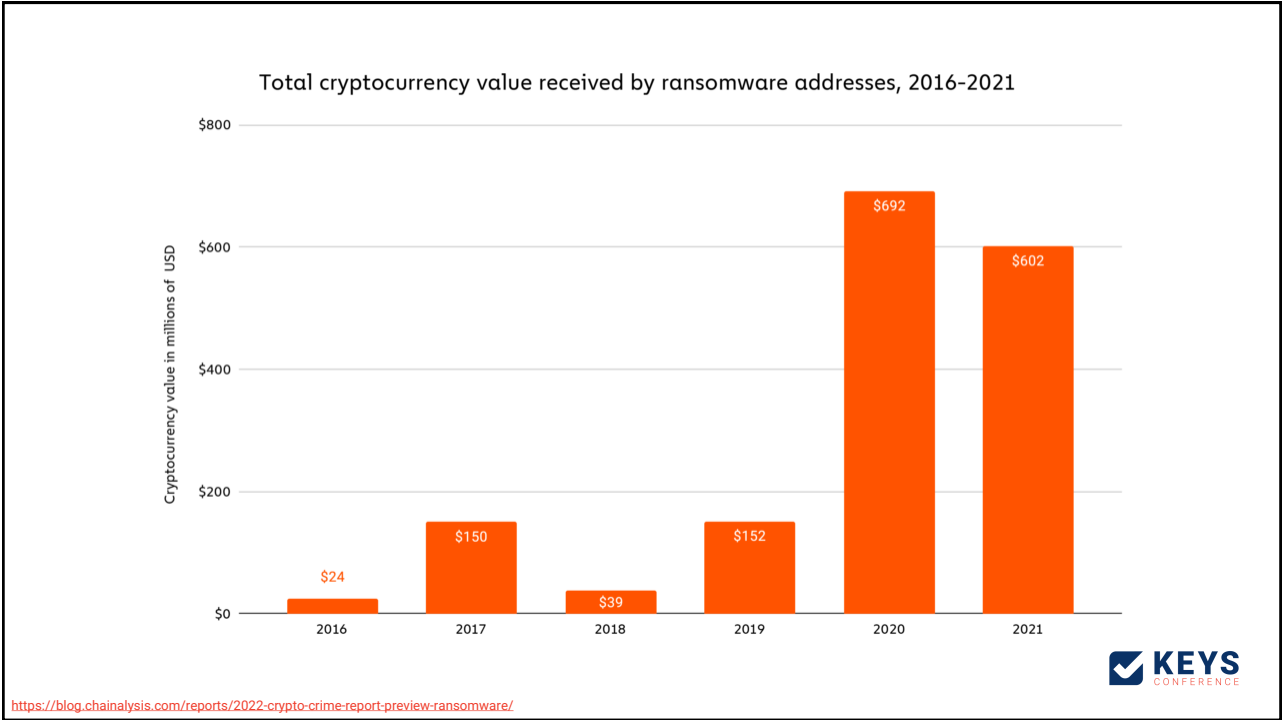
~~\$650 MILLION~~
\$1.3 BILLION

HIGHER
or
LOWER

<https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/>



12



13

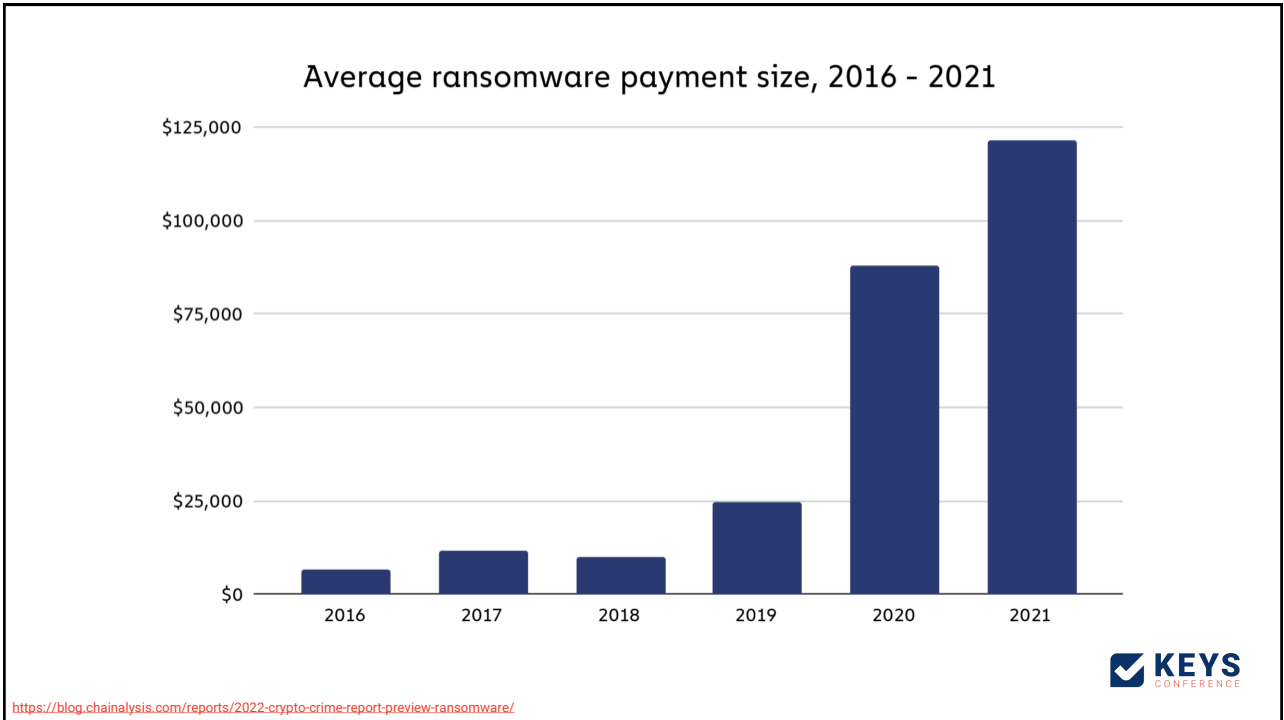
Average 2021 ransomware payment size.

~~\$25,000~~
\$118,000

HIGHER
or
LOWER

<https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/>

14



15

2021 Trends Show Increased Globalized Threat of Ransomware

SUMMARY

In 2021, cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. The Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the top U.S. critical infrastructure sectors, including the Defense Industrial Base, Emergency Services, Food and Agriculture, Government Facilities, and Information Technology Sectors. The Australian Cyber Security Centre (ACSC) observed continued ransomware targeting of Australian critical infrastructure entities, including in the Healthcare and Medical, Financial Services and Markets, Higher Education and Research, and Energy Sectors. The United Kingdom's National Cyber Security Centre (NCSC-UK) recognizes ransomware as the biggest cyber threat facing the United Kingdom. Education is one of the top UK sectors targeted by ransomware actors, but the NCSC-UK has also seen attacks targeting businesses, charities, the legal profession, and public services in the Local Government and Health Sectors.

Immediate Actions You Can Take Now to Protect Against Ransomware:

- [Update](#) your operating system and software.
- Implement user training and phishing exercises to raise awareness about the risks of [suspicious links and attachments](#).
- If you use [Remote Desktop Protocol \(RDP\)](#), secure and monitor it.
- Make an [offline backup](#) of your data.
- Use [multifactor authentication \(MFA\)](#).

U.S. organizations: to report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at cyber@fbi.gov, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at cyber@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISA.ServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nasa.gov. Australian organizations should report incidents to the Australian Signals Directorate's (ASD's) ACSC via cyber.gov.au or call 1300 292 371 (1300 CYBER 1). UK organizations should report a significant cyber security incident: csa.gov.uk/ncsc/aa22-040a (monitored 24 hrs) or for urgent assistance, call 0300 200 973.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see [cisa.gov/tlp](https://www.cisa.gov/tlp).

CISA ALERT (AA22-040A)

In the first half of 2021, cybersecurity authorities in the United States and Australia observed ransomware threat actors targeting “big game” organizations—i.e., perceived high-value organizations and/or those that provide critical services—in several high-profile incidents. However, ransomware groups suffered disruptions from U.S. authorities in mid-2021. Subsequently, the FBI observed some ransomware threat actors redirecting ransomware efforts away from “big-game” and toward mid-sized victims to reduce scrutiny.

<https://www.cisa.gov/uscert/ncas/alerts/aa22-040a>

KEYS
CONFERENCE

16

THE TAKEAWAY

The problem with ransomware is three-fold:

1. Ransomware is one of few threats which can compromise the confidentiality, integrity, and availability of your systems and data *simultaneously*.
2. Ransomware is expensive (and at times impossible) to fully remediate.
3. Ransomware actors are shifting their focus towards organizations, like yours.



17



Managing the Risk of Ransomware

WHAT ARE YOU GOING TO DO ABOUT IT?

18

Risk = **Likelihood** + **Potential Impact**
of an event's occurrence of the event's consequences



19

Effective risk management focuses
on reducing the **likelihood** and
potential damage of ransomware.



20

Reducing Likelihood



21

Know How It Gets In

REDUCING LIKELIHOOD



Phishing



Vulnerabilities



22

Phishing

REDUCING LIKELIHOOD

Respond with Answers

Click a Link

Call a Number for Assistance

Forward the Email

Open an Attachment




23

Phishing

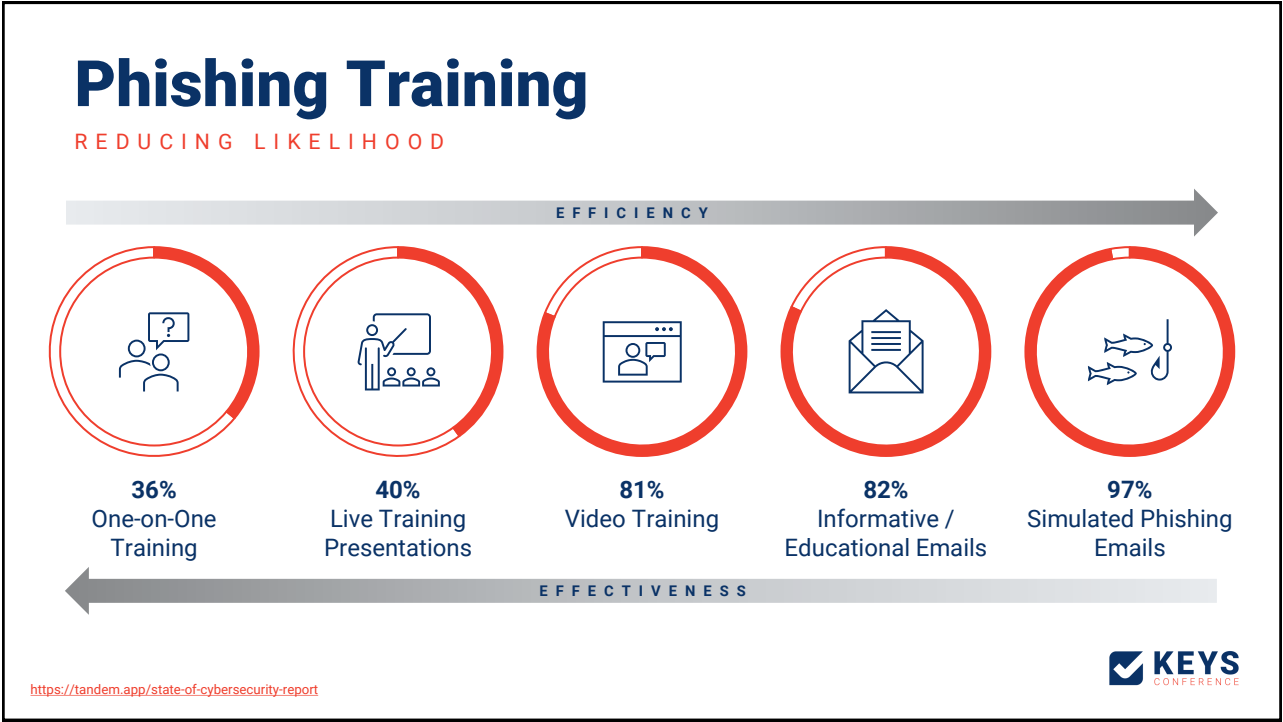
REDUCING LIKELIHOOD

Direct Malware Installation

Compromised Credentials



24



25



26

Vulnerabilities

REDUCING LIKELIHOOD

Shadow IT

Unpatched Systems

Remote Systems

Lack of Monitoring

Missing Controls



27

Vulnerabilities

REDUCING LIKELIHOOD

- 1 Know what you have.
(IT Asset Management)
- 2 Know how it gets updated.
(Patch & Vulnerability Management)
- 3 Know your controls work.
(Assurance & Testing)



28

THE TAKEAWAY

As ISOs, the best protection we have against ransomware attacks starts with the basics.



29

Reducing Potential Damage



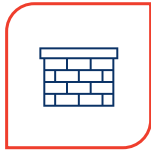
30

Controls

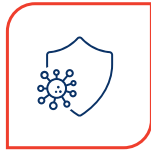
REDUCING POTENTIAL DAMAGE



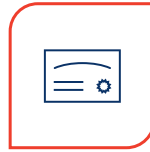
Access Controls



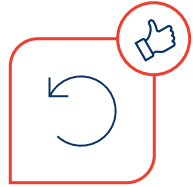
Network Segmentation / Air Gapping



Behavior-Based Anti-Malware



Cyber Insurance*



Data Backups

* <https://static.rusi.org/247-op-cyber-insurance.pdf>



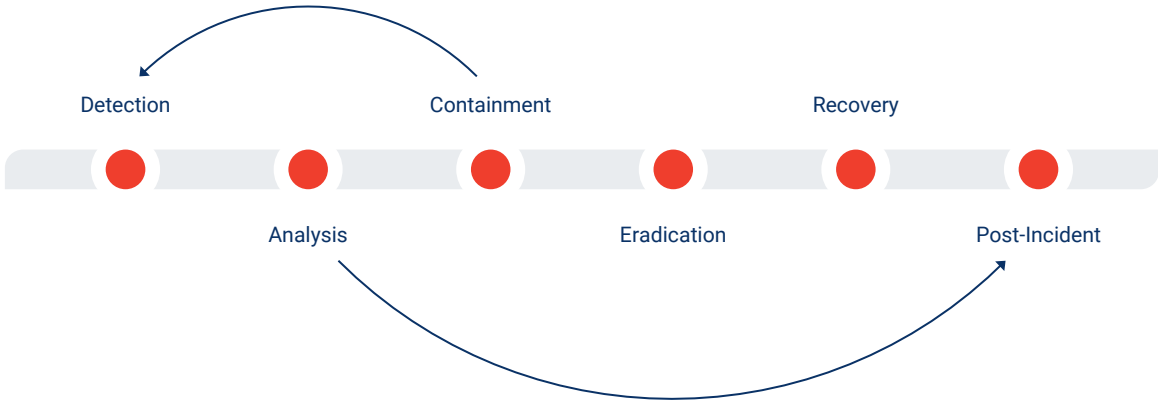
HAPPY WORLD BACKUP DAY!

<https://worldbackupday.com>

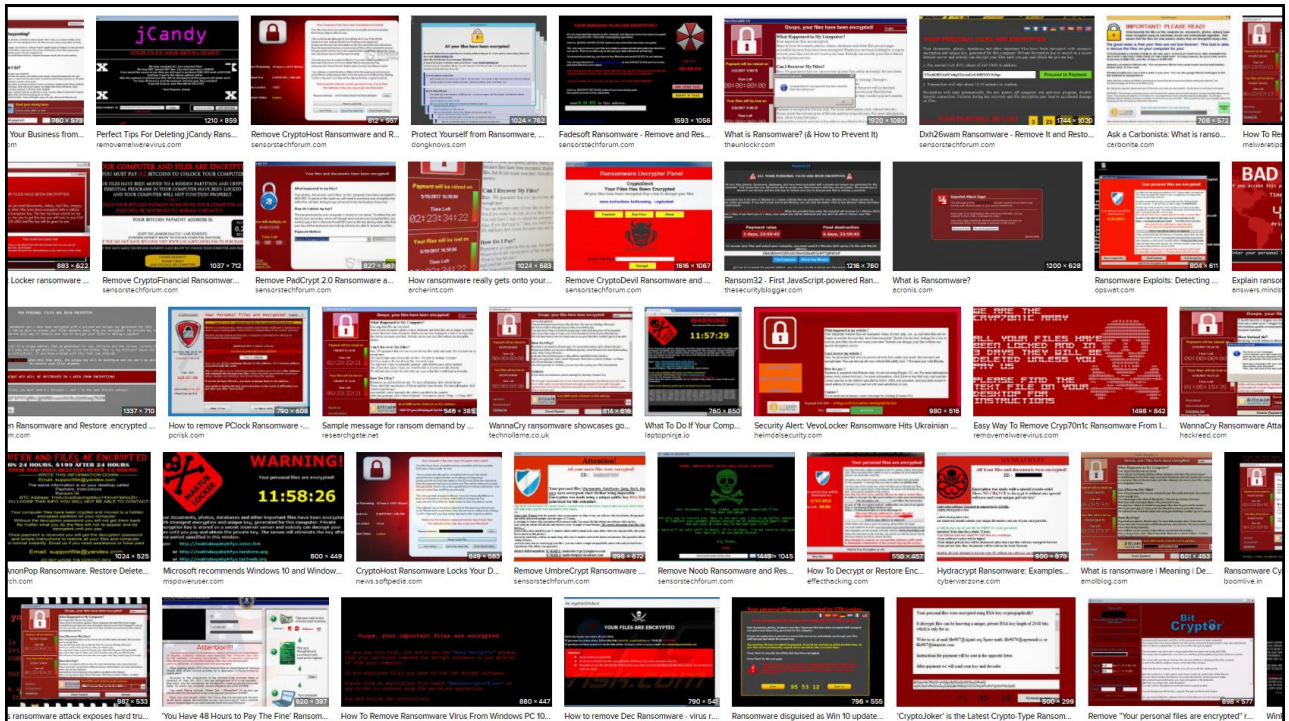


Incident Response Plan

REDUCING POTENTIAL DAMAGE



33



34

Report Ransomware

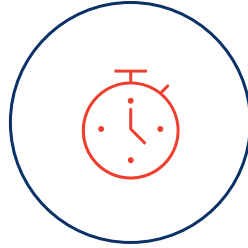
REDUCING POTENTIAL DAMAGE



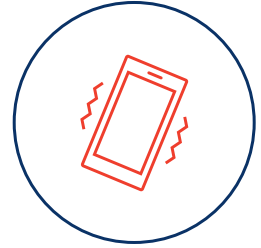
WHO
needs to be notified?



WHAT
needs to be done?



WHEN
does it need reported?



HOW
is best to report?



35

Analysis

REDUCING POTENTIAL DAMAGE

1

System Logs

2

Access Events

3

RDP Network Connections

4

Encrypted Data

5

Decryption Key



36

Containment

REDUCING POTENTIAL DAMAGE



Isolate
Affected
Systems



Check
Backup
Data



Create an
Image of
the System



Reset
Compromised
Passwords



37

Next Steps

REDUCING POTENTIAL DAMAGE

Eradicate

1

2

Recover

Postmortem

3



38

Ransomware Incident Checklist

RESOURCE DOWNLOAD

Ransomware Incident Checklist

[Tandem.App/Ransomware-KEYS](https://tandem.app/Ransomware-KEYS)

KEYS CONFERENCE

CONTAINMENT

- ☐ Determine a containment strategy.
- ☐ Isolate systems which may be compromised.
- ☐ Ensure backup data is secured from compromise.

ANALYSIS

- ☐ Include other handlers, as needed.
- ☐ Research the malicious code's type and behavior.
- ☐ Collect and review system logs, identify access events, and check for RDP network connections.
- ☐ Review sessions and open files lists to determine the user or system accessing the files.
- ☐ Determine what data was encrypted.
- ☐ Review properties of encrypted files to identify owners.
- ☐ Determine if there is a known decryption key.
- ☐ Determine how long the malware has been installed.
- ☐ Determine the incident's scope, origins, and occurrence patterns.
- ☐ Document applicable categories and subcategories for the incident.
- ☐ Determine the severity of the incident.
- ☐ Notify affected personnel and third parties (e.g., law enforcement, regulators, etc.).

DETECTION

- ☐ Designate a Lead Incident Handler.
- ☐ Document how the incident was detected.

PREPAREDNESS

- ☐ Consider creating an image of the affected system.

Learn more

Visit Tandem App for more incident management resources. Tandem, LLC Copyright © 2021

Tandem

39

KEYS CONFERENCE

Communicating about Ransomware

WITH SENIOR MANAGEMENT

40

THE TAKEAWAY

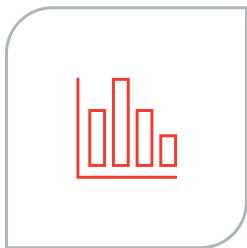
Ransomware resources are difficult to justify because the business value occurs when ransomware doesn't.



41

Three Tips

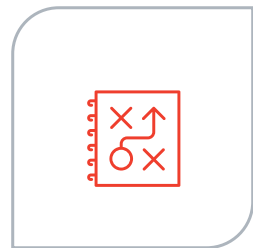
COMMUNICATING ABOUT RANSOMWARE



Be Objective



Be Precise



Be Clear



42

Session Recap

TAKEAWAYS

- Renew your focus on mitigating the risk of ransomware.
- Implement controls to reduce likelihood and potential damage, such as:
 - Security Awareness Training
 - IT Asset Management
 - Patch & Vulnerability Management
 - Assurance & Testing
 - Access Controls
 - Network Segmentation
 - Behavior-Based Anti-Malware
 - Cyber Insurance
 - Air-Gapped Data Backups
 - Incident Response Plan
- Communicate objectively, precisely, and clearly with management.
- Have fun.



43



44

A white bar chart icon with three bars of increasing height, centered within a white rounded square, which is itself centered within a large orange circle. The background is a dark blue gradient.

KEYS
CONFERENCE

DON'T FORGET!

**Fill out the
survey to get
your sticker!**

45



KEYS
CONFERENCE

THANKS FOR JOINING!

**The ISO's Guide to
Managing Ransomware**

Alyssa Pugh

CISM, SECURITY+

TANDEM GRC CONTENT MANAGER

46

Upcoming Sessions

TANDEM

So You're an Admin...

Cory Faust, Tandem

RISK & COMPLIANCE

CoNetrix Technology Engineers: A Panel Discussion

Rob Garrison, Brad Copeland, & Mike Richline, CoNetrix Technology

CYBERSECURITY

Better Your Communication Between Technical & Non-Technical People

Brad Landis & Brian Whipple, Tandem

