INCIDENT RESPONSE WORKSHOP

YOU'VE BEEN HACKED – NOW WHAT? WHAT?

ORBITALFIRE
CYBERSECURITY


JOHN OLIVER
THE MITTENS OF DISAPPROVAL ARE ON
9PM TUESDAY

INCIDENT RESPONSE CRASH COURSE


CBSN ON ASSIGNMENT
ECMC
ERIE COUNTY
MEDICAL CENTER
Great Lakes
Health System of WNY
Welcome
PLEASE TAKE
TICKET WITH YOU


ERIE COUNTY
MEDICAL CENTER
3
EMERGENCY
Main Entrance
Parking
David Miller Bldg.
E C M C

INCIDENT HIGHLIGHTS

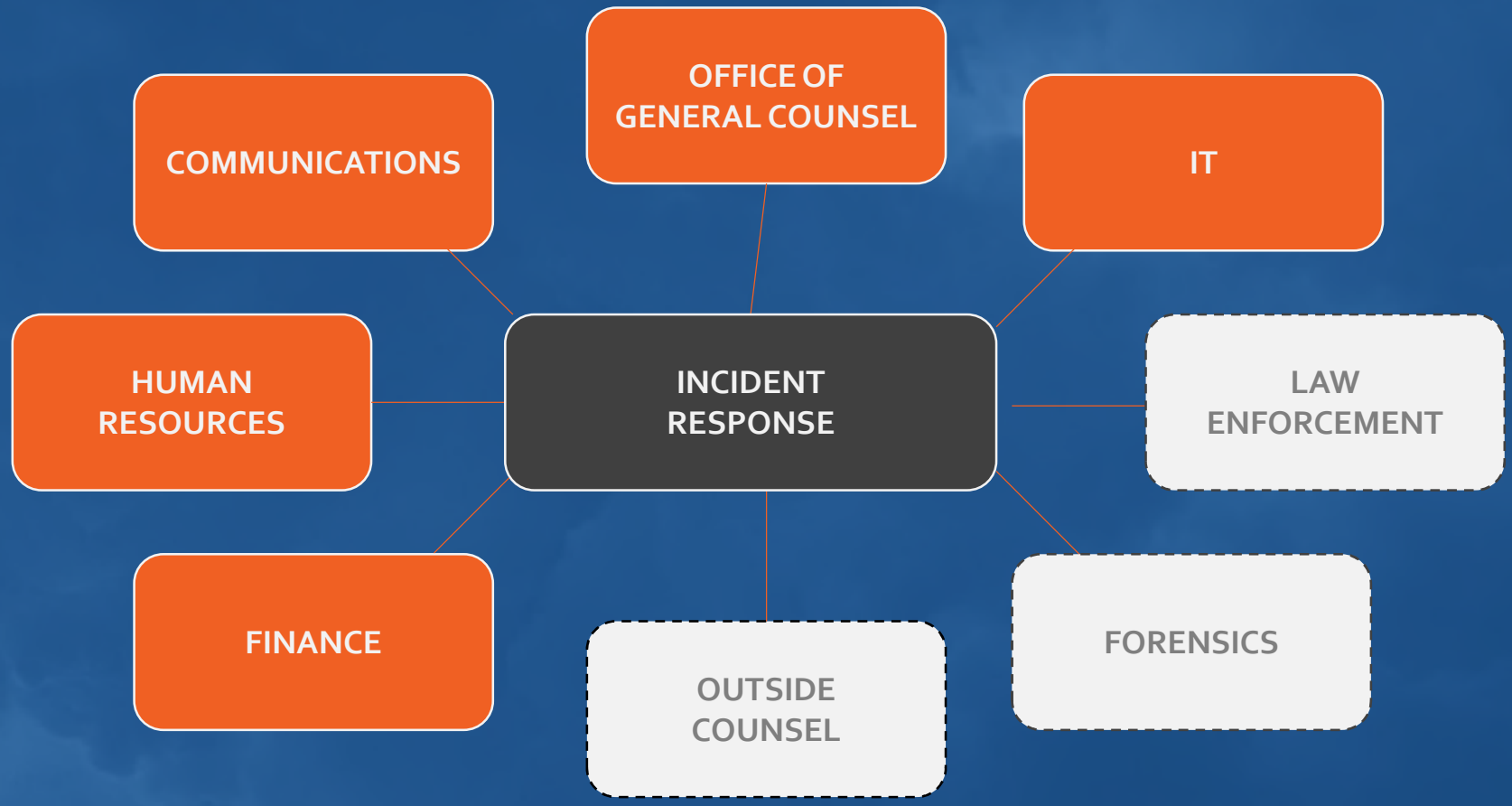
- Incident Response activated within 3 hours
- Offline backup availability
- Community and peer support
- Minimal impact to patient care and safety
- OCR verified non-breach determination
- Emergency Management Plan fluency due to recent drill

THE ABILITY TO RESPOND TO INCIDENTS HAS BECOME A CRITICAL CAPABILITY FOR ALL ORGANIZATIONS

INCIDENT RESPONSE GOALS

DEFENSIBILITY
RESILIENCE

INCIDENT RESPONSE TEAM



INCIDENT RESPONSE PROCESS

WHY DO TABLETOPS?

CONTINUOUS IMPROVEMENT

TABLETOP PEP TALK

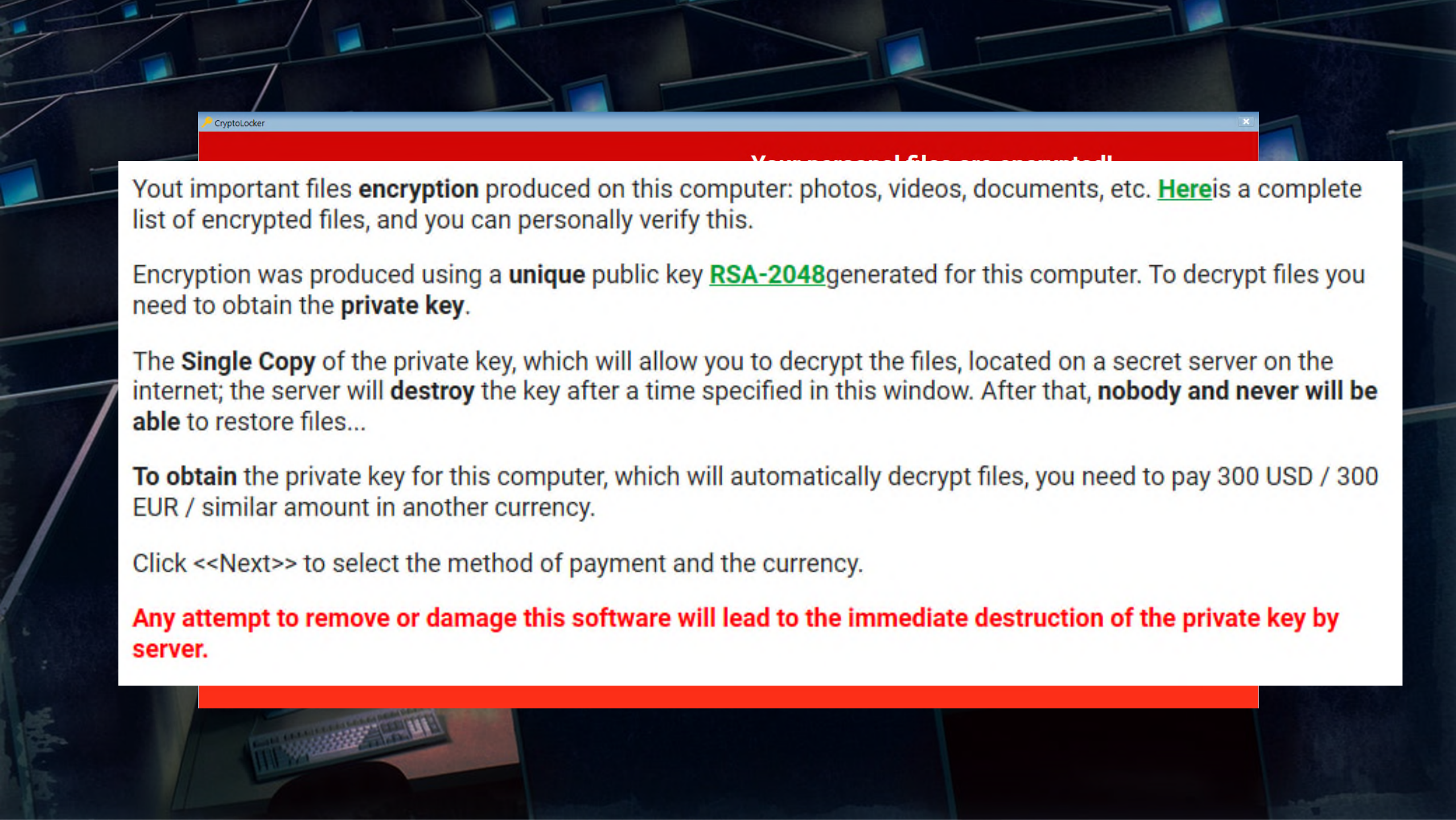
- Our primary goal today is to assess your company's preparedness and Incident Response capability
- We know that all of you are capable of personal heroics – but no one is being tested here today
- Participation is key – if you see something, say something
- We are suspending reality during this exercise – try to roll with it

WORKSHOP


FRIDAY
07:53 AM ET
WEST POINT, NY


FRIDAY
08:06 AM ET
WEST POINT, NY


RANSOMWARE


CryptoLocker
Yout important files **encryption** produced on this computer: photos, videos, documents, etc. Hereis a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a **unique** public key RSA-2048generated for this computer. To decrypt files you need to obtain the **private key**.
The **Single Copy** of the private key, which will allow you to decrypt the files, located on a secret server on the internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click <<Next>> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.


FRIDAY
08:31 AM ET
WEST POINT, NY

DETECT & ANALYZE

DISCUSSION – DETECT & ANALYZE

- What could be happening here?
- What is the first thing that you should do?
- How will your employees report the incident?
- How will you start your Incident Response process?
- How will you mobilize your Incident Response Team members?
- **How is this affecting your business?**


FRIDAY
11:22 AM ET
WEST POINT, NY


CONTAIN

DISCUSSION – CONTAIN

- How will you keep the ransomware from spreading?
- What are your legal and contractual obligations?
- How will you notify your customers?
- What information will you share with employees?
- What are your cyber insurance obligations?


FRIDAY
03:27 PM ET
WEST POINT, NY

BREAKING NEWS

JUST IN


ERADICATE

DISCUSSION – ERADICATE

- How will you respond to media inquiries?
- Will you consider paying the ransom?
- Do you have the resources to pay the ransom?
- Will you engage with Law Enforcement?
- Do you know your compliance requirements?
- **How will you continue to operate your business?**


FRIDAY
08:44 PM ET
WEST POINT, NY


RECOVER

DISCUSSION - RECOVER

- What steps will you take to prevent re-infection?
- What will you do to minimize reputational damage?
- How will affected customers be compensated?
- Will your cyber insurance cover these losses?


FRIDAY
11:44 PM ET
WEST POINT, NY


POST-
INCIDENT

DISCUSSION – POST-INCIDENT

- What do you need to close the incident?
- Could you have been better prepared? If yes, how?
- How can your Incident Response Plan be improved?
- Did you achieve acceptable levels of DEFENSIBILITY and RESILIENCE?
- **What do you wish you had done before the incident?**

FINAL THOUGHTS

DON'T DECLARE AN INCIDENT
UNLESS ABSOLUTELY NECESSARY

YOUR IT GUY
DON'T GOT THIS

"THE BEST BOXERS IN HISTORY WEREN'T THE HARDEST PUNCHERS, THEY WERE **THE ONES WHO COULD TAKE THE HARDEST PUNCH**."

- MIKE TYSON

QUESTIONS?

THANK YOU

INCIDENT RESPONSE@ORBITALFIRE.COM
(844) ORB-FIRE

Links to resources for more information on Cybersecurity Incident Response Strategies:

WATCH: A (Cyber) Preppers Guide to Incident Response: https://youtu.be/eFbQJm-Ys0I

READ: Crisis-Proof Your Organization: Build an Incident Response Plan That Works: https://orbitalfire.com/2025/01/27/incident-response-plan/