

INCIDENT RESPONSE WORKSHOP

YOUR DEALERSHIP HAS BEEN HACKED
– NOW WHAT?

REG HARNISH





JOHN OLIVER
THE MITTENS OF
DISAPPROVAL
ARE ON

9PM TUESDAY





REG HARNISH
ORBITALFIRE



INCIDENT RESPONSE CRASH COURSE





ERIE COUNTY
MEDICAL CENTER

Great Lakes
Health System of WNY

UB
The University at Buffalo

Welcome

NO
PARKING
ANY
TIME



Providing Ambulatory, Wheelchair and Stretcher Services

NO
PARKING
ANY
TIME

PLEASE TAKE
TICKET WITH YOU



3
ERIE COUNTY
MEDICAL CENTER

↑ EMERGENCY

→ Main Entrance

→ Parking

→ David Miller Bldg.

ECMC

INCIDENT HIGHLIGHTS

- Incident Response activated within 3 hours
- Offline backup availability
- Minimal impact to patient care and safety
- Community and peer support
- 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**

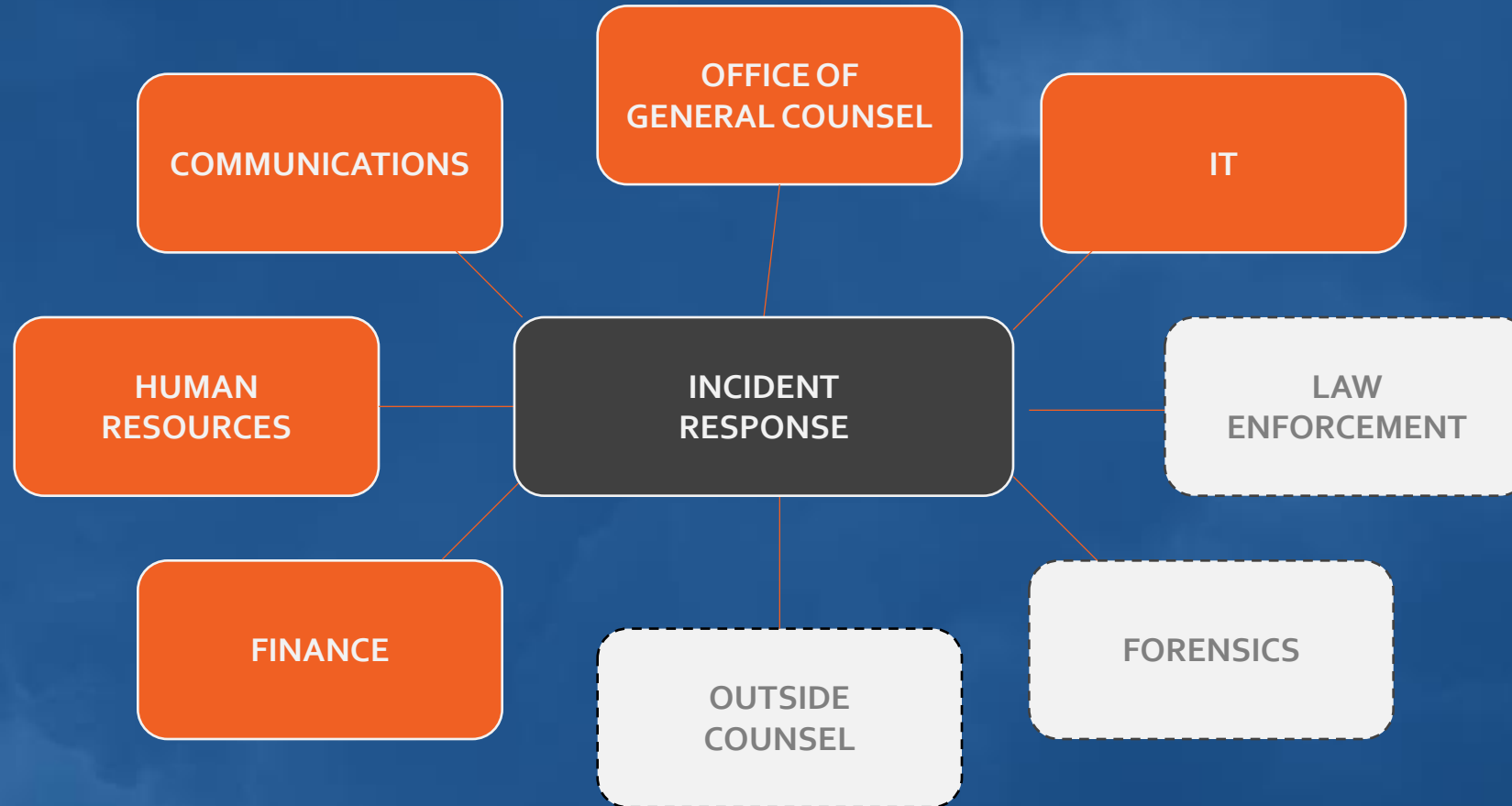


INCIDENT RESPONSE GOALS

**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



The background of the image is a high-angle, slightly tilted view of a large office space filled with cubicles. Each cubicle has a desk with a computer monitor. The monitors are all turned on, displaying a blue-tinted image, and their light illuminates the surrounding cubicle walls. The desks also have keyboards and office phones. The overall atmosphere is dark and repetitive, suggesting a large-scale surveillance or data processing environment.

**FRIDAY
07:53 AM ET
WEST POINT, NY**

The background of the image is a high-angle, perspective view of a large office cubicle farm. The cubicles are arranged in a grid-like pattern, receding into the distance. Each cubicle contains a desk with a computer monitor. Most of the monitors are illuminated with a blue light, suggesting they are on or displaying a blue screen. The overall atmosphere is dark and somewhat somber, with the blue light from the screens providing the primary illumination. The text is overlaid in the center of the image.

**FRIDAY
08:06 AM ET
WEST POINT, NY**



RANSOMWARE

Your Important Files are encrypted!!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated 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 contact your Incident Response Team members?



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 do you need to do so that your cyber insurance claim will be paid?



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?
- If yes, how will you pay the ransom?
- Will you engage with Law Enforcement? If yes, what are your expectations?
- Do you know your FTC Safeguards requirements?
- How will you continue to sell and service cars?



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?
- How can your Incident Response Team be improved?
- Did you achieve acceptable levels of DEFENSIBILITY and RESILIENCE?



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?





REG@ORBITALFIRE.COM

THANK YOU