# Have we been breached? A Data Security Incident Simulation

Taylor Gast
Foster Swift Collins & Smith, PC
TGast@fosterswift.com

Josh Gembala ASK ess@justask.net







#### Old Haven Township

You are a municipal administrator for the township.

Late on a Friday afternoon receptionist Bobby Williams interrupts your planning meeting telling you there is an emergency. Bobby takes you to their computer and shows you a PDF document named PayUp.

Pop: 30,0000 IT Budget: \$372,000 Personnel 35% Services 25% Software 25% Infrastructure 15%

# What do you do?

- ☐ Do nothing this is obviously a scam.
- ☐ Contact Corey Smith your IT Administrator
- ☐ Have Bobby email you the PDF so you can check it out on your pc.



# What do you do?

- ☐ Retrieve the Word document from SharePoint.
- ☐ Wait till Bobby comes in Tuesday and ask what it is.
- ☐ Forward the email to Kelly in Planning.
- ☐ Contact Corey Smith your IT Administrator



Baltimore transfers \$6 million to pay for ransomware attack; city considers insurance against hacks

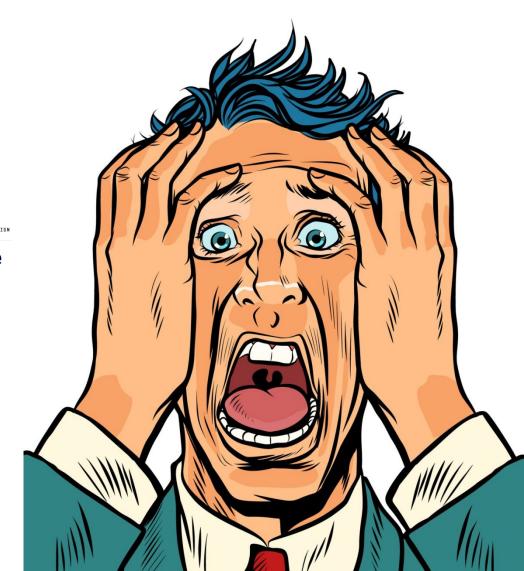
Another Hacked Florida City Pays a Ransom, This Time for \$460,000

WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION

Atlanta Spent \$2.6M to Recover From a \$52,000 Ransomware Scare

22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

August 20, 2019 · 10:16 AM ET



# Breach Response: Summarizing Key Considerations

- Do you have a plan?
  - Must be a living document
  - Is it practiced?
- Who's on your team?
  - Who's making decisions?
- When to get a lawyer involved?
  - Is it an incident, or a breach?

- Ransomware: do you pay?
- Law enforcement involvement
- Insurance considerations
- Communication plan
- Contractual notification obligations



### Updating Best Practices: "Reasonable Security"

#### The evolving "Reasonable Security" standard

- 1. Identify an employee who is responsible for the entity's information security initiative.
- 2. Annually review internal and external security risks and implement any measures necessary to mitigate or eliminate them.
- 3. Evaluate and test the efficacy of security measures.
- 4. Adopt and enforce written policies or guidelines aimed at implementing an enhanced information security program.
- 5. Offer regular training programs on cybersecurity issues, including at least annual training on security awareness for all employees.
- 6. Keep top-level leadership (or a relevant subcommittee) updated about the information security program.
- 7. Ensure that third parties with access to your data are employing sufficient cybersecurity measures



#### Updating Best Practices: Technical Measures

- Data mapping
- Encryption
- Multi-factor authentication
- Limit access
- Administrative privileges

- Patch and update
- Penetration testing and vulnerability assessments
- Network monitoring
- Data retention and minimization



#### Questions?

Taylor Gast

Foster Swift Collins & Smith

TGast@fosterswift.com

Foster Swift Cybersecurity Hotline:

517.FS1.TASK (517.371.8275)

Josh Gembala

**ASK** 

ess@justask.net

517.676.6633

