YOU'VE BEEN HACKED! NOW WHAT?

ANDY ZIEGLER, CBCP

TEMPEST RISK MANAGEMENT

ANDY ZIEGLER

Andy has worked for large corporations specializing in risk management, business continuity and technology controls for 25 years. Andy helped navigate his employers through major disasters such as 9/11, Hurricanes Sandy and Katrina and many others.

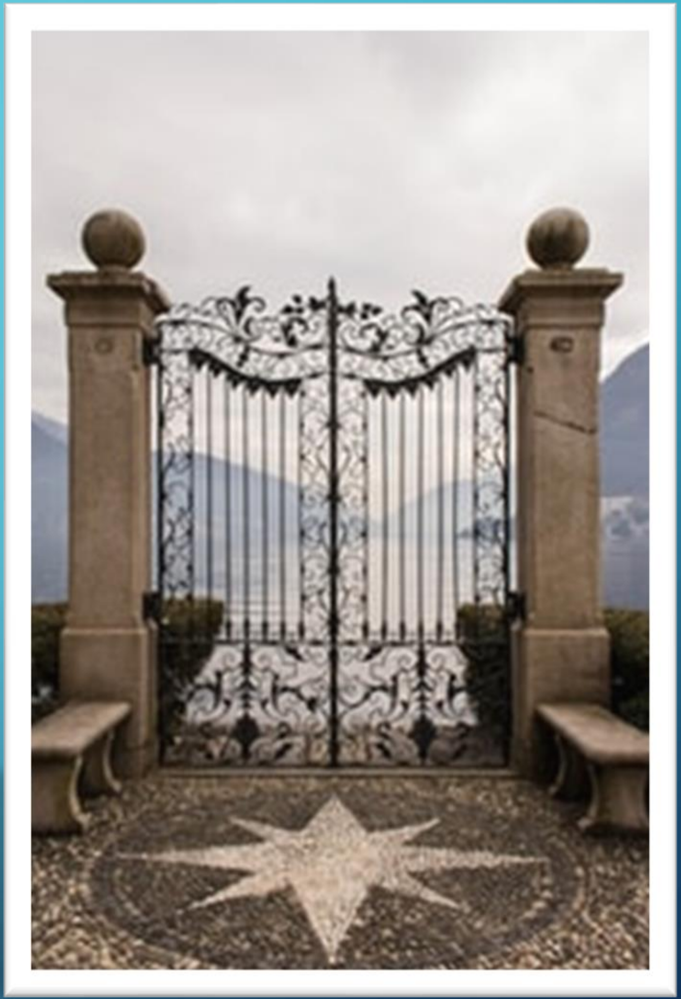
Andy is a veteran/active first responder with Talleyville Fire Company and currently serves on the Board of Directors.

Andy and his wife are located in Wilmington, Delaware with their 4 teenage children.

1. Close the gates
2. Call for help
3. Communicate
4. Plug the holes
5. Restore and Learn

CLOSE THE GATES

- Activate your Business Continuity Plan and engage your Business Continuity Team
- Identify compromised systems and isolate them
- Re-baseline access…maybe – block access and/or force a password change on all systems including
  - Internal apps and software
  - Cloud apps
- Damage assessment - Identify all lost data and notify clients/customers
  - Closely monitor all feeds and api's until root cause found
  - Immediately begin root cause investigation



CLOSE THE GATES: CONTINUED

- Assume everything is compromised, until you are sure it is not
- Identify source of the attack and block it
- Confirm the type of attack (virus, malware, remote access, ransomware, DOS (denial of service), etc)
- Engage your managed service provider or other IT company
- Prioritize the cleaning and restoration of data based on backup and component criticality
- Beware of a second attack…the first one could just be a distraction

CALL FOR HELP

- FBI
  - Ic3.gov
  - Baltimore covers DE 410-265-8080
- Your managed service provider
- Cyber insurance
  - Chubb INA Grup
  - American International Group
- Cyber recovery expert

COMMUNICATIONS

Consumers can forgive an attack. That's not your fault. They will <u>not</u> forgive keeping it secret

- Internal
  - Employees
  - Leadership
- External
  - Clients
  - Suppliers
  - Partners
  - Law Enforcement

PLUG THE HOLES: RESTORE - RECOVER

- Restore or rebuild?
- Backup/redundant system health – if the integrity of the backup is clean you can use it to restore
- Communicate eta to customers and stakeholders
- Restore critical operations first - CERTIFY

SPECIAL CASE: THIRD PARTY COMPROMISE

- If a supplier notifies you of a breach suspend all of that suppliers access
- Engage your business continuity team and prepare to engage an alternate supplier
- Check your contracts and Service Level Agreements’s with the third party
- Notify your customers of another's breach

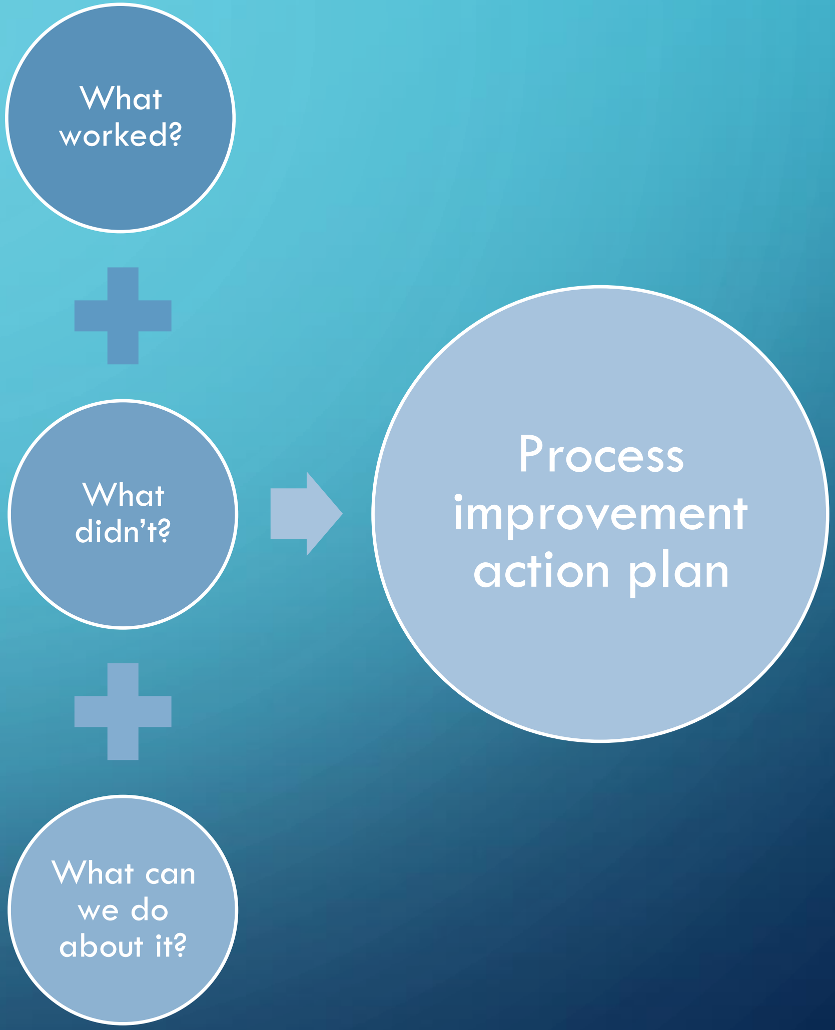
SPECIAL CASE: RANSOMWARE

- In the past, paying a ransom was considered a death knell
- Since Colonial Pipeline, not necessarily the case
- Funding to organized crime or possibly terrorist organizations
- Work with law enforcement
- Funds may be recoverable or provide law enforcement with intel

LEARN – CONDUCT A “HOT WASH”

What is a “Hot Wash”?

- Developed by the military to review lessons learned from military actions
- Identifies strengths and weaknesses in a process or organization
- Execute immediately following the event
- Includes leaders, front line managers and third parties critically involved in the incident
- FOLLOW UP ON YOUR PROCESS IMPROVEMENT PLAN



Tempest Risk Management LLC is located in Wilmington, DE and specializes in small business risk assessment and planning services, providing customized business continuity plans.

Contact us for a free 30 minute consultation

info@tempestrisk.com

THANK YOU

LinkedIn
https://www.linkedin.com/in/andrewziegler/

Website
www.tempestrisk.com

Email
andy@tempestrisk.com

Phone
302-598-8027