Town of Franklin

Cyber Fraud
Spear-Phishing Incident
Public Summary

Jamie Hellen, Town Administrator
Tim Rapoza, Director of Technology

December 2, 2020

Preface

- The goal of this presentation is to:
  - To help educate the public on this very real threat to every resident and business;
  - Disclose and discuss as much information of the cyber fraud spear-phishing incident, as legally allowable;
  - Respect and respond to the desire of the public to understand the “Who, What, When, Where and Hows” of this incident.

- Remains a fluid situation:
  - There is still currently an active police investigation.
  - Some questions may not be able to be answered yet, due to legal constraints or we may not have answers. We should resist speculating.
  - Tonight is an update on the situation, not a conclusion.

- Some personnel matters cannot be disclosed or discussed, per various state laws:
  - All discussion must refrain from the “reputation, character, physical condition or mental health” of any employee, but can include “professional competence.”
  - Individual liability could apply.
  - Town Charter requires Town Administrator to administer personnel matters.

What is Cybersecurity

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack - *Merriam-Webster*

A very broad term with many different interpretations

Computer or “*Computer System*”

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack - *Merriam-Webster*

What IS the “computer system ? “

Hardware

- Computers
- Network Switches
- Firewalls
- Network connections
- Fiber Optics
- Wireless Access
- Physical Access

Bits and Bytes

- Data storage
- CLOUD Storage
- User Files
- Email
- Local Applications
- Webpages
- Web Applications
- Viruses / malware

The User Base

- File Access
- Privileges
- Sharing data
- File contents
- User behavior
- User responsibility
- User Training

Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack - Merriam-Webster

Technology needs to be secured in several different areas using various *methodologies.*

Areas of Security

- Edge Security
- Internal Network
- IoT Security
- Wireless Network
- Email
- Securing Confidential data
- Disaster Recovery
- Remote Access
- Client Security
- Hardware Loss
- Physical Security
- End-User security

Methodologies in place today

- **Internet Security /** “*edge*” security: Sonicwall Firewalls
- **LAN Security /** **“***internal network”* **:**
  - Locations are V-LANed / segregated to allow only authorized access to certain areas of the network.
- **Client /** “*device*” **Security:**
  - Sophos Antivirus*
  - Sophos Intercept X - Ransomware protection*
  - Secure access on all end-user devices
    - Users cannot install software

***Important Note:** No anti-malware software will ever be 100% effective*

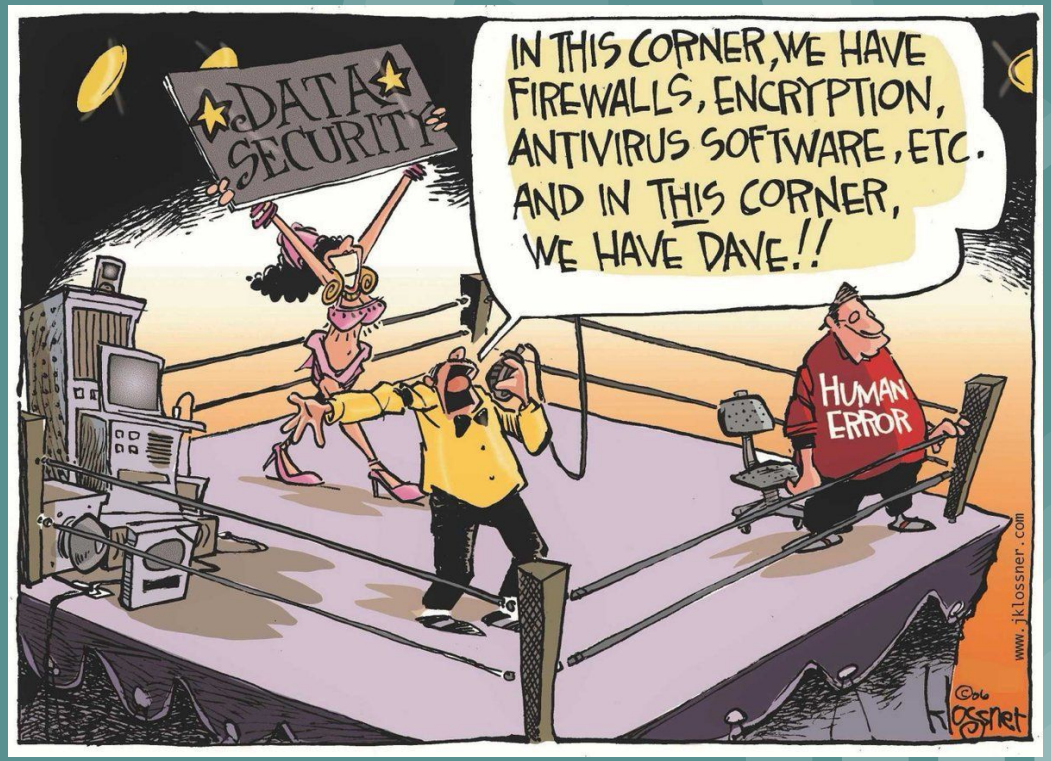
Methodologies (cont.)

- **Physical security**
  - All areas where sensitive technology is located are secured.
- **WiFi Security**
  - All personal devices are directed to a completely separate network that has no access to the internal network.
- **End user security**
  - Users are trained using the KnowBe4 Cyber-Responsibility training platform to identify and react to various online and email threats.

The Human Element - *Why are we susceptible ?*

What *"technology"* CAN'T protect against

1. Fraud
2. CLICKING!



Targeting the human element

FRAUD

- **Phishing -** *Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss.*
  - *https://www.phishing.org/what-is-phishing*
- **SPEAR-Phishing -** *Spear phishing is an email targeted at a specific individual or department within an organization that appears to be from a trusted source. It's actually cybercriminals attempting to steal confidential information. A **whopping 91% of cyberattacks** and the resulting data breach begin with a spear phishing email, according to research from security software firm Trend Micro. This conclusively shows that users really are the weak link in IT security.*
  - *https://www.knowbe4.com/spear-phishing/*

Clicking

- **Ransomware -** *Malicious files / programs similar to a computer virus but with a defined purpose. Once activated the program will employ various methods to extort money from the victim. File encryption, fear, blackmail etc ...*

Phishing / Malware statistics

- **Phishing & SPEAR-Phishing** - *https://youtu.be/_eqXZQI1tCI*
  - *Nearly 1.5 million new phishing sites are created **EACH MONTH !***
  - *Average cost of a single spear-phishing attack: $1.6 million*
  - *85% of organizations have suffered a phishing attack.*
  - *Finance Department employees are targeted due to their access to sensitive data like banking.*
  - *97% of users cannot identify a sophisticated phishing email*
  - *95% of all attacks on enterprise networks are the result of successful spear phishing*
  - *Only 3% of users report phishing emails to their management.*
  - *78% of people claim to be aware of the risks of unknown links in emails **And yet they click anyway!***
  - *30% of phishing messages are opened by targeted users, and 12% of those users click on the malicious attachment or link (see Ransomware)*
  - *81% of mobile phishing attacks were initiated outside of email using text messages or phone call.*

- **Ransomware**
  - *In 2019 , 1 in 2 organizations was targeted by ransomware and attackers have successfully encrypted the data in 73% of these attacks.*
  - *In 2020, the average ransom demand is $84,000 and 1 in 3 companies pay the ransom*

In Summary

- A technology-only based solution will never be 100% effective in guarding against an attack.
- As in OUR situation, a computer system does not necessarily need to be "*hacked*" or compromised to result in harm to data or financial loss.
- User training and diligence is an integral part - if not the most important part - of protecting ourselves from attackers.
- "The bad guys only need to be "right" once, but we need to be right 100% of the time"

What happened?

- The Town of Franklin has been the victim of a sophisticated cyber fraud spear-phishing attack.
  - Chief Lynch, Director Rapoza, Attorney Cerel & Special Counsel Kerwin confirm this fact.

- The Town Treasurer-Collector was targeted via a “spear phishing” campaign based on a fake profile.

- The fake profile used was based on a real person. In fact, the person being imitated is the Chief Financial Officer (CFO) of the vendor who is constructing the Water Treatment Plant and Wells on Grove Street.

- The Town Treasurer did not verify the request and resulted in an initial loss to the water enterprise fund of $522,965.65.

What Funds? #1

- The misdirected funds were from the Town's Water Enterprise Fund, which ***solely*** affects water rate payers. All private well properties are not affected by this incident.

- No funds from the Town's General Fund, which is borne through property taxes, were lost or misdirected, including all town departments and the School Department.

- No other town or school financial accounts have been affected.

- The misdirected payment was from our loan obligation on the new Water Treatment Plant & Wells 3 & 6 reconstruction projects being paid for through an State Revolving Fund (SRF) loan. This incident is isolated to that project, in that one division of the DPW, and nowhere else.

- The lost revenue from this incident affects solely those properties who are public water users.

What Funds? #2

- The Town of Franklins Water Department is currently building a new $13 million water treatment plant and rebuilding two wells (3 & 6) near Grove Street.
- The project is currently 75% done and scheduled to be completed in Spring (April). Construction has never stopped during COVID-19.
- Through a stable, low interest loan from the State Revolving Fund (SRF). DEP.
- Currently on time, on budget with contingency remaining. Project is under budget by approximately $420,000 in relation to the authorization of $13 million.
- For more: Grove Street Water Treatment Plant project on DPW Facebook page

Initial Response Strategy & Priorities

For the past eight weeks, the Town has spent significant time doing its due diligence to get as many facts as possible and address several themes:

1. Recover as much of the misdirected funds as possible;

2. Protect our own financial and technology systems to protect citizen information, employee information and all sensitive information;

3. Review internal and external financial procedures and protocols;

4. Hold those accountable that led to this incident; and

5. Develop a Performance Improvement Plan to begin to make our organization stronger and rebuild the public confidence in the organization.
    a. Implementation of the plan has been simultaneous to the investigations.

Findings, to date #1

- In August, the Town Treasurer was the victim of a targeted spear phishing email correspondence which caused the initial loss of $522,696.65, which otherwise would have been used as a partial payment to pay the contractor retained on the Grove Street Water Treatment Plant.

- This incident was not discovered until late September when the contractor informed Franklin it had not been paid.

- Upon learning that the contractor had not been paid and that in all likelihood the Town had been the victim of a cybercrime, the wiring bank was notified by the Treasurer and an attempt to recall the wire was undertaken.

- Franklin Police were also immediately notified.

- All financial institutions the Town does business with, including banks, were immediately notified by the Treasurer-Collector of a potential cyber attack on September 28th.

Findings, to date #2

- The fraudster using an email address very close in appearance to the email address of the CFO of the vendor contacted the Treasurer requesting that an authorization agreement form for payment be changed from check to wire transfer. They requesting the form from the Treasurer.

- The form was provided. The fraudster again posing as the CFO, asks the Treasurer as to the status of invoices being processed/authorized for payment.

- During the time period of the “spearing” in late July & August, there were 23 exchanges between the Treasurer and the fraudster which ultimately resulted in the Treasurer authorizing the wire transferring of funds to an account which was not the account of the real vendor.

- The fraud was discovered when the vendor contacted the Town to advise that it had not received payment.

- The funds were misdirected to a bank in California.

Findings, to date #3

- At approximately 4:45 PM on September 28th, the Town Administrator was notified by the Town's Finance Director of a payment that was misdirected to a third party in the amount of $522,696.65 via wire transfer.

- The Town Administrator immediately contacted the Town's insurance agent, MIIA, the Chief of Police, Technology Director and Town Attorney at 5:00 PM.

- All staff acted swiftly in the immediate recognition of the incident on September 28th.

    - These swift actions of the staff led to some of financial recovery in a very expedient manner and quick turnaround and progress on our investigations.

Findings, to date #4

- The Town's Treasurer-Collector followed town protocols at the time of discovery of the incident, including contacting law enforcement.
- The Treasurer did not follow industry best practices to independently verify that the email wire transfer request is, in fact, a request of the real vendor.
- The incident was the result of a human error, during a busy and chaotic time, as the Treasurer has acknowledged.
- The Town had insufficient, undocumented procedures regarding protocols for verification of changes in payment procedures.
- The Town began using wire transfers around 2010.

Findings, to date #5

- The Town is working with our financial auditors to develop a new “Wire Transfer Policy”.
  - This action will do much to ensure the proper checks and balances are in place for this to not happen again.

- The 2019 organization wide risk assessment did not identify this area as a risk and without recommended remediation.

- 2019 Finance Policies recently reviewed and adopted at Finance Committee & Town Council.

- Annual Financial Audits are online and have not highlighted this procedural gap.
  - The Town performs very well on its financial audits in the last decade.
  - The Town has a AA+ Bond rating; one step below a AAA.

Findings, to date #6

- The Technology Director conducted an internal audit of all electronic systems of the Town of Franklin (both municipal and school). A forensics audit was also conducted on the personal computers of the Treasurer-Collector. Only the Treasurer was contacted by the fraudster.

- We have no evidence, to date, from the forensics analysis that there was intentional, malicious, wilful or suspicious conduct by the Treasurer-Collector.

- We have evidence, to date, from the audit there were no breaches on municipal or school systems or software and they are secure.

- The Town of Franklin was not hacked, breached or compromised.

- This was not a ransomware or malware attack.

Financial Recovery #1

- The initial loss for the Water Enterprise Fund ratepayers is $522,696.65.

- $200,000 will be restored to the loss/project through the Town's Insurance carrier, MIIA.
  - $100,000 from the cyber insurance policy. Payment has been received.
  - $100,000 through crime policy. Payment has been received.
  - "Cyber Insurance" is an evolving and very risky industry. It's a relatively new market of product and uncertain from both insurers and customers. Franklin served as a pilot member of MIIA's Cyber insurance pilot task force in 2017.

- $22,696.65 of losses will be restored through employee discipline issued, to date.

- To date, the current financial loss to water ratepayers will be $300,000.

- The staff fully respect that if additional financial recovery is not available in the future, $300,000 is a lot of money for the water ratepayers of this town to absorb.

Financial Recovery #2

- The financial impact to the average property owner who pays into the Water Enterprise Fund is approximately $30 dollars.

- There is not a need to raise water rates to accomodate for the loss.

- Other options for financial recovery:
  - Police Investigation.
  - Excess contingency or savings from the project.
  - End of year surplus (if available).
  - 2019 Town Council policy to have $1 million in emergency funds in enterprise accounts.
  - At this time, litigation or claiming a surety bond on the Treasurer-Collector will not provide any financial recovery.

- The Town still has more avenues for accountability:
  - Police Investigation and federal partners.
  - Attorney General, Inspector General and Mass Cyber Center assistance.

Litigation Options #1

Third-Party lawsuits

- At the recommendation of the Town Administrator, Town Attorney and Special Counsel, the Town Council formally voted last week to not pursue litigation against any third-party involved at the current time. Why?

- Through the investigation and analysis we have completed to date, the Town has insufficient evidence or leverage to pursue litigation.

- If the Town did sue:
  - We would likely have to hire an attorney and pay a significant cost in legal fees, staff time & resources and possibly take years to proceed through the court system.
  - The Administration and Town Council would be required to invoke executive session for the duration of the litigation; this presentation would not be happening tonight.
  - If the Town did not prevail, we could be liable for potential damages and attorney's fees.

- At the end of the day, the risk analysis does not justify commencement of litigation.

Litigation Options #2

The Treasurer-Collector or Assistant Treasurer-Collector Bonds

- State law MGL requires the Town to have bonds on certain public employees, including the Town Treasurer, Town Collector, Deputy Treasurer-Collector's and Town Clerk (elected).
    - Bonds are NOT insurance.
    - The Town has $300,000 bonds on the Treasurer-Collector, Assistant Treasurer-Collector and $25,000 on the elected Town Clerk. Five bonds total.
    - The Town uses a local Franklin-based insurer for the bonds, but the bond company is nationally based.
- The bonds specify "faithfully perform the duties of his/her office"
- Bonds are present as largely surety in the event of embezzlement, collusion, or other federal or state crimes.

Litigation Options #3

The Treasurer-Collector or Assistant Treasurer-Collector Bonds

- At the recommendation of the Town Administrator, Town Attorney and Special Counsel, the Town Council formally voted last week to not pursue the bond. Why?

- I've received an estimated legal cost framework of $72,000 to $120,000 in initial legal costs to sue the bond company for the bond (if the Town filed a claim).
  - Specialized (and expensive) legal counsel would be required.
  - Case cold take years to proceed through the court system.
  - Again, staff and the Town Council would be required to invoke Executive Session.

- There is no previous Massachusetts court precedent where a community has claimed a public official bond without intentional or wilful criminal conduct as evidence.

- In other words, the risk analysis does not justify commencement of litigation.

Franklin Police Investigation

- On September 29th, detectives from the Franklin PD formally opened an investigation to this criminal act against the Town.

- Department of Homeland Security Investigative unit is assisting the Town.
  - They are also assisting the Commonwealth of Mass in their own incident, too.

- The Treasurer-Collector has been cooperative and forthright in all interviews as a part of the investigation.

- This investigation will likely take some time.
  - Cyber crime is at an all time high during the pandemic.

Performance Improvement Plan #1

- Wire Transfer Policy -
  - A new internal procedure to ensure there are checks and balances throughout the Comptroller's Office and Treasurer-Collector’s office regarding wire transfers.
  - A dual approval procedure: the policy establishes a procedure where wire transfer must now be approved by the Finance Director/Comptroller for every wire transfer account request in addition to the initial approval from the Treasurer-Collector.
  - Paused wire transfers indefinitely until further policy review.
  - Working with Town Auditor’s, Melanson & Heath, on procedure.

- “Standard Contract” revision -
  - The Town is revising its standard contract to include a Point of Contact (POC) for all contracts to ensure an authorized individual of a company is signed off on by the CEO of the service provider..
  - That individual is now the point of contact for all communication.
  - Town will require due notice from the vendor in the event of a change in POC.

Performance Improvement Plan #2

- Cybersecurity training -
  - All Municipal & School finance staff will be taking additional cybersecurity training via the KnowBe4 online training platform.
    - I thank Superintendent Ahern and Miriam Goodman for their steadfast commitment to this exercise.
  - All town staff will continue to receive training as we have done for 3 years.
  - Chief McLaughlin has also set town department heads to receive a free two-day training from the state emergency management office (and federal DHS).

- A complete financial audit from our auditors -
  - Will include a review of all internal financial procedures and any recommendations.
  - Town is also analyzing potential third party assessments of our infrastructure.

- Hiring a FTE in Technology Department to focus on cyber. Working with the Superintendent of Schools.

Personnel Accountability #1

- The Treasurer-Collector has been served with the most severe discipline in Franklin over the last two decades:
  - She will be suspended for a full month, without pay (approx $8,000);
  - Compensation will also be reduced an additional sum (approx $15,000) throughout the fiscal year;
  - Total lost wages are $22,696.65 (or 24% of annual salary);
  - Last chance agreement;
  - Mandatory performance improvement plan; and
  - Open and uniquely transparent process and embarrassing publicity.

Personnel Accountability #2

- When issuing employee discipline, the totality of an employee's record is considered.
  - We accumulate definitive facts and evidence. We evaluate every situation related to the specifics of that incident. We follow the law, contracts and consult with Labor Counsel where needed.

- When an employee makes a mistake or gets into an accident, we evaluate many criteria, including and not limited to:
  - Intentional, willful, or unintentional, unknowingly?
  - Honesty, authenticity, cooperation.
  - Personnel history, previous infractions, make same mistake twice, etc.?
  - Overall attitude, emotional intelligence, commitment and ability to improve.
  - Professional development and training history. Licensure status, if applicable.

- We have collective bargaining contracts in place for units and have an Employee Manual that governs non-union employees.

- HR Website - https://www.franklinma.gov/human-resources

Personnel Accountability #3

- In Ms. Bertone's case the following is factual:
  - No prior employee discipline.
  - She has been honest, cooperative, and assisted all lawyers, police detectives and staff.
  - Mistake was unintentional. We all learn from our mistakes to be better employees.
  - She led Town efforts in the recent bankruptcy case against Dean Foods (recouped $500,000 and still seeking more!). She has created numerous operational efficiencies in the office to save money.
  - Has fully embraced the performance improvement plan (earlier slide) and has always embraced professional development opportunities.
  - She is qualified for the position:
    - She holds the required academic and professional experience credentials
    - Recently certified Massachusetts Treasurer (got her certification the same week)

Personnel Accountability #4

- New World we are learning. Cyber crime is a modern day “pandemic” global crime enterprise.
  - ⅛ cities and towns in Massachusetts have been a victim of cyber crime.
  - Major incident this year to hospitals, colleges, universities, large businesses.
  - 2020 will show a tremendous increase in cyber crime due to the many, unique social factors we are all experiencing in 2020.
  - State Department of Revenue recently sent out a warning (October 28th) to all municipalities warning us of spear-phishing attempts on the state.

- COVID-19 year stress on all municipal employees.

- The truth is every municipal employee has risk in their jobs.
  - Every single one of us can make a mistake, which can cause poor public relations, social media frenzy, assumptions, rumors, mistruths or other residual effects such as financial loss, illness, or even fatality.
  - The most properly trained and educated employees can make human errors.

- For all of these factors and more, I am offering Ms. Bertone a second chance.

Epilogue

- Remains a fluid situation:
  - Currently, there is still an active police investigation.
  - Some questions may not be able to be answered yet, due to legal constraints or we may not have answers. We should resist speculating.
  - Tonight is an update on the situation, not a conclusion.
- Some personnel matters cannot be disclosed or discussed, per various state laws:
  - All discussion must refrain from the “reputation, character, physical condition or mental health” of any employee, but can include “professional competence.”
  - Individual liability could apply.
  - Town Charter requires Town Administrator to administer personnel matters.