MassCyberCenter
at the MassTech Collaborative

Robinson+Cole

Cybersecurity Workshops For Municipalities

Third Party Vendor Management: Map, Assess & Mitigate Risk

Webinar
October 20, 2020

Agenda

- Recent Vendor Risks to Municipalities
- Minimizing Third Party Vendor Risks:
  - MAP
    - Third Party Vendors – Who are they and What are the Risks of the Vendor to your Organization?
  - ASSESS
    - What happens if there is a Security Incident caused by a Third Party Vendor?
    - How can you properly assess the vendor?
  - MITIGATE RISK
    - What can you do to Protect Your Municipality?
    - How to Manage Third Party Vendors and Minimize Risk?
    - Cyber Liability Insurance Coverage for Third Party Vendors

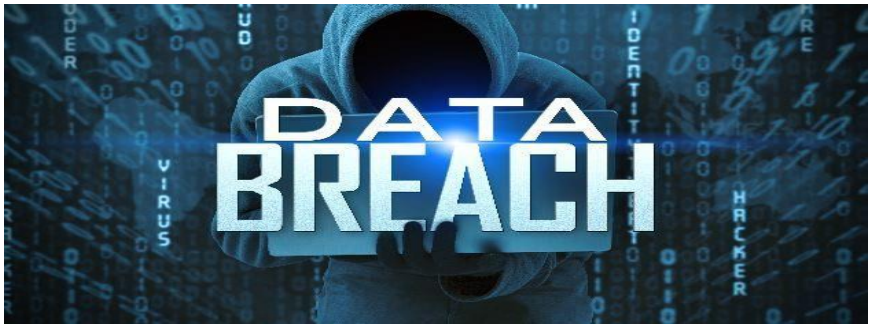
Recent Risks

What are the Third Party Vendor Risks to your Municipality?

- Data Breach
- Ransomware Attack
- Zero Day Vulnerabilities

Data Breach

- Vendors that experience a security incident that involves personal information (PI) may cause a data breach
- A data breach is a legal term that is determined by the unauthorized access, use and disclosure of PI
- All 50 states have different definitions of a reportable data breach
- If your vendor causes an incident that is a reportable data breach with your data, it is your problem



Ransomware

- **Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid (usually in bitcoin).**

- **Victims are at risk of losing their files, but may also experience financial loss due to paying the ransom, lost productivity, IT costs, legal fees, network modifications, and/or the purchase of credit monitoring services for employees/customers.**

Zero Day Vulnerabilities and Municipalities

What is a zero-day vulnerability and how could it harm a municipality?

A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw.

Vendor Security Incidents Involve Your Data so it is Your Problem!

ZD Net recently reported that according to the FBI, hackers breached the networks of two US municipalities last year by exploiting a vulnerability in Microsoft SharePoint servers to breach the two municipalities' networks.

https://www.zdnet.com/article/fbi-nation-state-actors-have-breached-two-us-municipalities/

Recent Attacks on Municipalities

Tyler Technologies Victim of Cyber-Attack

BY LINN FOSTER FREEDMAN ON OCTOBER 2, 2020
POSTED IN CYBERSECURITY

As one of the largest information technology service providers to local governments, the cyber-attack on Tyler Technologies (Tyler) in Plano, Texas is a sobering reminder of how a cyber-attack on a third-party vendor can put government data at risk.

According to reports, Tyler may have been the victim of a ransomware attack that disrupted its internal network and telephone systems. Its corporate website was deactivated and the company was working on getting it back online. Tyler sent a message to its clients indicating that it "has no reason to believe that any client data, client servers, or hosted systems were affected" and that it is working with forensic investigators and law enforcement to investigate the incident.

The company provides software to local governments for enterprise resource planning, scheduling court hearings, collecting fines, payment of bills, managing open-data programs and sharing election data.

Security experts are recommending that any customers of Tyler complete a hard reset of passwords that Tyler technicians use to access their systems.

Recent Attacks on Municipalities (con't)

Fall-Out from Blackbaud Ransomware Attack

BY LINN FOSTER FREEDMAN ON JULY 23, 2020
POSTED IN NEW + NOW

As a follow-up to last week's post on the importance of due diligence regarding high-risk vendors' security practices, Blackbaud, a global company providing financial and fundraising technology to not-for-profit entities, notified its customers late last week that it was the victim of a ransomware attack in mid-May. Blackbaud offers a number of products to its …
Continue Reading

Recent Attacks on Municipalities (con't)

Click2Gov Portal Compromised in Eight Cities

BY LINN FOSTER FREEDMAN ON SEPTEMBER 26, 2019
POSTED IN CYBERSECURITY

Many cities in the United States utilize a self-pay portal for residents to pay bills online, known as Click2Gov. Click2Gov was compromised in 2017 and 2018, when hackers were able to access over 300,000 payment cards and reportedly made more than $2 million in the heist.

It is being reported this week by security researchers that starting sometime in August, Click2Gov systems have been attacked again, compromising the systems in eight cities so far. Six of those cities – Deerfield Beach, Florida, Palm Bay, Florida, Milton, Florida, Bakersfield, California, Coral Springs, Florida, and Ames, Iowa – also were hit in the previous attack.

ASSESS

Your Municipality Has a Vendor Security Incident

What Do You Do?

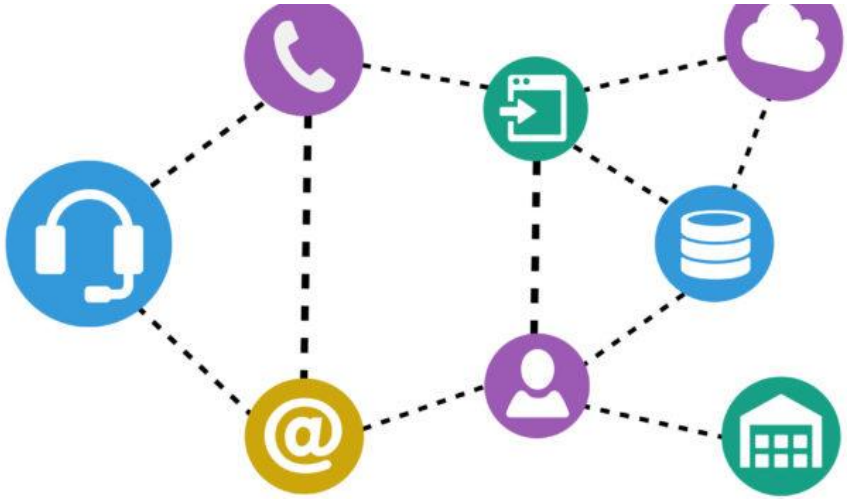
- **Be Prepared!**
- **Activate Your Incident Response Plan**
  - **If you did not attend the workshops on Incident Response Planning, now is the time to do so!**

MAP

Who are your High Risk Vendors?

Map all vendors who have access to PI

- Follow the data
- Use Accounts Payable



Who are your High Risk Vendors? (con't)

- Utility or other online payment vendors
- Retirement system administrators
- HR/payroll administrators
- Health/dental system administrators
- IT/Cloud Service Providers
- Web Hosting Services
- Legal/Accounting Services
- Any vendor who has access to your data, either with direct access to your system or if you disclose to vendor

MITIGATE

How to Protect Your Municipality?

- **Manage the Risk**
- **Mitigate the Damages from Third Party Vendors**

How to Protect Your Municipality?

Implement a Vendor Due Diligence Plan

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

How to Protect Your Municipality? (con't)

- Utilize Security Questionnaires to Assess Cyber Security Practices and Compliance with Data Security Laws
- Utilize and implement right to audit your Vendors
- Utilize written contracts with vendors that put security risks and expenses on the vendors, not the municipality
- Vendors must also have sufficient cyber liability coverage for security incidents
- Consider creating a vendor database for your agreements, questionnaires, and related documents

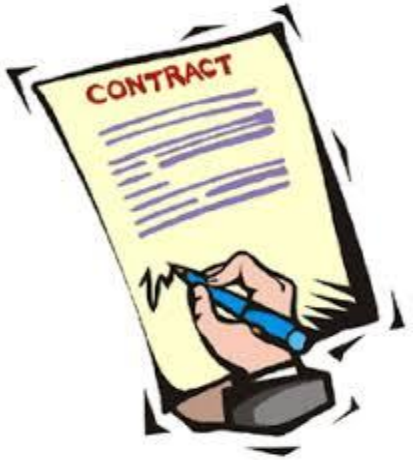
Manage the Risk and Mitigate the Damages from Third Party Vendors

- What is a Security Questionnaire and Why do you need it?
  - It is a document you provide to your vendor that should identify their controls and practices for:
    - Handling Risks
    - Security controls, including technology
    - Process controls
    - Training
  - It will tell you about the vendor's security practices and it will document your due diligence in hiring the vendor

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

- What are Audit Rights and Why do you need them?
  - Your right to audit a vendor's security practices and protocols will allow you to better understand the vendor's security practices
  - It will assist you in analyzing security incidents should they occur and obtaining access to information needed to evaluate security posture of vendor and improvements

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)



- **Look Closely at Your Written Contracts with Vendors (Vendor Agreements)**
  - **Which entity is bearing the risk?**
  - **Is the vendor attempting to shift its risk tc**
  - **What are the vendor's data security prote**
  - **What are the requirements for notification of a security incident involving your data?**
  - **Do your vendor confidentiality agreements contain data security provisions?**
  - **Who is bearing the cost of the incident and resulting costs?**
  - **Are they trying to limit their liability?**

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

Create Better Vendor Agreements:

- Don't automatically settle for the vendor's boilerplate agreement – Read it carefully -
  - Vendors will try to limit their risk and/or limit their exposure if there is a security incident to the amount of the contract--insufficient
  - How do you protect yourself?
  - Consider use of SLAs
- Negotiate for appropriate cyber security protections and provisions
  - The Municipality should not have to take on the vendor's risk

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

Some Tips for Vendor Agreements (not exhaustive):

- **Require compliance with applicable data, privacy & security laws;**
- **Require prompt patching of vulnerabilities;**
- **Require prompt reporting of potential cyber incidents;**
- **Require cooperation in investigating an incident and preserving relevant evidence;**
- **Utilize sufficient liability limits;**
- **Require incident response and mitigation expenses;**
- **Require appropriate cyber liability insurance coverage;**
- **Require use of strong passwords & multifactor authentication.**

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

Tips for Vendor Agreements (con't):

- **Address Indemnification + limitation of liability issues**
  - **Liability for causing a data breach or security incident**
  - **Reimbursement for all costs**
  - **First v. Third Party Claims**
  - **Limiting liability to the amount of the contract has no relevance to actual costs and damages**
  - **Supercap for data breach**
- **Consider cyberliability insurance for actions of 3rd parties like cloud providers**

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

Tips for Cyber Liability Insurance:

Cyberliability Insurance

- Need to cover information you have in your possession AND the data held by your service providers
- Most comprehensive general insurance liability policies DO NOT cover a data breach
  - Those general policies were not designed for when information gets into the wrong hands

Manage the Risk and Mitigate the Damages from Third Party Vendors (con't)

Tips for Cyber Liability Insurance (con't) :

Cyber liability insurance

- **Cyber liability insurance in general will cover: liability for failure to protect personal information held on computer systems or mobile devices, costs to notify individuals, investigative costs, public relations, legal fees, media coverage, mitigation, etc.**

- **Talk to broker who has experience with cyberliability policies**

- **Work with insurer to have existing relationships approved**

Cyber Liability Insurance

Questions to Ask Your Broker about Ransomware

- **Is there coverage for costs to access/restore data and for the actual payment of a ransom amount in the event of a ransomware attack?**
- **Is there coverage if there is a cyber extortion event that blocks access to the business' telephone or computer system or its data, including potential lost business and/or business interruption?**
- **Is data that is stored or backed up using cloud services covered in the event of a cyber incident, regardless of the type of attack; i.e., hacker, virus, malware, etc.?**

Cyber Liability Insurance (con't)

- **Is there coverage for damages, costs, fines, etc. resulting from social engineering fraud; e.g., an employee clicks on a link in an email that installs malware causing a virus or ransomware?**
- **If there is a data breach, is there also coverage for loss of net profits / income if the business is shut down or can't operate because of a data breach, virus, ransomware attack or other incident?**

A Final Word on Cyber Liability Insurance

Cyber Liability Insurance Must Be Combined with Good Cyber Security Practices

- **2019 Wall St. Journal article reported on a National League of Cities report that municipalities that don't follow basic cybersecurity practices could have their claims denied.**

https://www.wsj.com/articles/cities-warned-not-to-rely-on-cyber-insurance-alone-11571995801

Additional Tips & Considerations:

- Robust Back-ups
- Robust Contingent Operations and Disaster Recovery Plans
- Address any configuration issues
- Consider keeping high-risk data in-house
  - May consider adding high-risk data to cloud-based service provider's systems after a 'test period' has passed
    - Use Encryption at Rest
    - Limit access

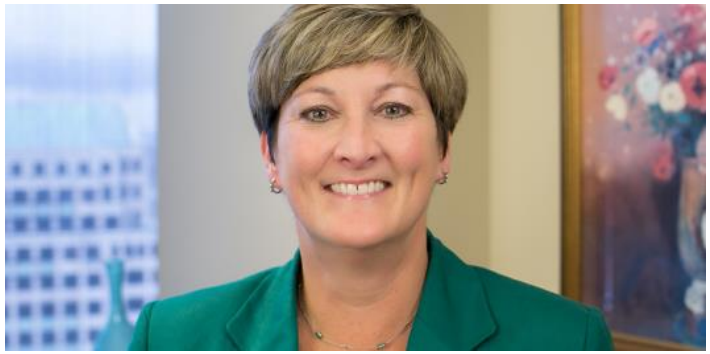
Conclusion

Know the questions to ask and the risks to your data

MassCyberCenter at the MassTech Collaborative

Robinson+Cole

Thank you! Questions?



Linn Foster Freedman
lfreedman@rc.com
Robinson + Cole

One Financial Plaza
14th floor
Providence, RI 02903
401-709-3353

https://www.dataprivacyandsecurityinsider.com/

MassCyberCenter at the MassTech Collaborative

Robinson+Cole