RESPONDING TO RANSOMWARE ATTACKS

2021 IMLA ANNUAL CONFERENCE PRESENTATION
SEPTEMBER 30, 2021

AMANDA CONN, GENERAL COUNSEL, WSSC WATER
MEREDITH LADD, CITY ATTORNEY, CARROLLTON, TX
PETER SIMONSEN, CHARLESWORTH CONSULTING

MODERATED BY BARBARA ADAMS, DONAHUE & ROSE, PC

INTRODUCTIONS

- AMANDA CONN, GENERAL COUNSEL, WSSC WATER
- MEREDITH LADD, CITY ATTORNEY, CARROLLTON, TX
- PETER SIMONSEN, CHARLESWORTH CONSULTING

charlesworth consulting

LEARNING OBJECTIVES

- UNDERSTAND LEGAL REQUIREMENTS FOR RESPONDING TO RANSOMWARE ATTACKS ON PUBLIC ENTITIES, INCLUDING PRIVACY NOTIFICATIONS, PUBLIC DISCLOSURES, AND RULES AND REGULATIONS GOVERNING PAYMENT OF RANSOMS.
- LEARN FROM LOCAL GOVERNMENT LAWYERS ABOUT THEIR EXPERIENCES IN RESPONDING TO RANSOMWARE ATTACKS.
- LEARN RISK MANAGEMENT AND RISK TRANSFER BASICS TO REDUCE THE RISK OF LOSS FROM RANSOMWARE ATTACKS.
- RECEIVE AN UPDATE ON POTENTIAL STATE AND FEDERAL LEGISLATION AND REGULATIONS GOVERNING RANSOMWARE ATTACKS.
- RECEIVE AN UPDATE ON THE STATE OF THE CYBER INSURANCE MARKETPLACE, ESPECIALLY RELATING TO PUBLIC ENTITIES.

charlesworth consulting

WHAT'S IT LIKE TO BE ATTACKED?

- OVERVIEW OF CITY OF CARROLLTON, TEXAS 2019 ATTACK
- OVERVIEW OF WSSC WATER 2021 ATTACK

charlesworth consulting

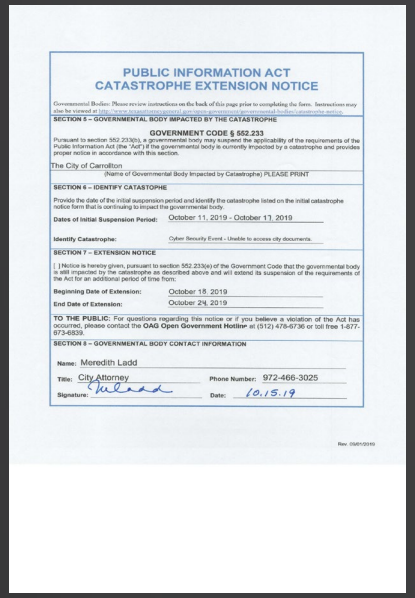
CARROLLTON
TEXAS

OCTOBER 10, 2019 – CYBERATTACK

- ACTIONS DAY OF EVENT
- I.T. STRUCTURE/ISSUES
- CITY RESPONSE TO EVENT
- TECHNICAL
- EFFECT ON PUBLIC
- LESSONS LEARNED

charlesworth consulting

CARROLLTON
TEXAS



PUBLIC INFORMATION ACT
CATASTROPHE EXTENSION NOTICE

Governmental Bodies: Please review instructions on the back of this page prior to completing the form. Instructions may also be viewed at http://www.texasattorneygeneral.gov/open-government/governmental-bodies-catastrophe-notice

SECTION 5 – GOVERNMENTAL BODY IMPACTED BY THE CATASTROPHE

GOVERNMENT CODE § 552.233

Pursuant to section 552.233(b), a governmental body may suspend the applicability of the requirements of the Public Information Act (the "Act") if the governmental body is currently impacted by a catastrophe and provides proper notice in accordance with this section.

The City of Carrollton
(Name of Governmental Body Impacted by Catastrophe) PLEASE PRINT

SECTION 6 – IDENTIFY CATASTROPHE

Provide the date of the initial suspension period and identify the catastrophe listed on the initial catastrophe notice form that is continuing to impact the governmental body.

Dates of Initial Suspension Period: October 11, 2019 - October 17, 2019

Identify Catastrophe: Cyber Security Event - Unable to access city documents.

SECTION 7 – EXTENSION NOTICE

[ ] Notice is hereby given, pursuant to section 552.233(e) of the Government Code that the governmental body is still impacted by the catastrophe as described above and will extend its suspension of the requirements of the Act for an additional period of time from:

Beginning Date of Extension: October 18, 2019

End Date of Extension: October 24, 2019

TO THE PUBLIC: For questions regarding this notice or if you believe a violation of the Act has occurred, please contact the OAG Open Government Hotline at (512) 478-6736 or toll free 1-877-673-6839.

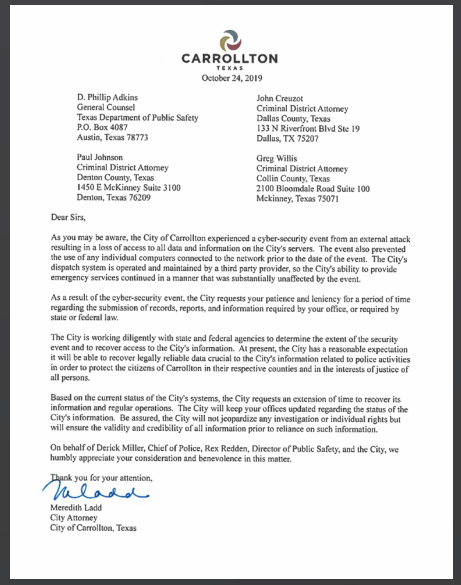
SECTION 8 – GOVERNMENTAL BODY CONTACT INFORMATION

Name: Meredith Ladd

Title: City Attorney Phone Number: 972-466-3025

Signature: Mladd Date: 10.15.19

Rev. 09/01/2019



CARROLLTON
TEXAS
October 24, 2019

D. Phillip Adkins
General Counsel
Texas Department of Public Safety
P.O. Box 4087
Austin, Texas 78773

John Creuzot
Criminal District Attorney
Dallas County, Texas
133 N Riverfront Blvd Ste 19
Dallas, TX 75207

Paul Johnson
Criminal District Attorney
Denton County, Texas
1450 E McKinney Suite 3100
Denton, Texas 76209

Greg Willis
Criminal District Attorney
Collin County, Texas
2100 Bloomdale Road Suite 100
Mckinney, Texas 75071

Dear Sirs,

As you may be aware, the City of Carrollton experienced a cyber-security event from an external attack resulting in a loss of access to all data and information on the City's servers. The event also prevented the use of any individual computers connected to the network prior to the date of the event. The City's dispatch system is operated and maintained by a third party provider, so the City's ability to provide emergency services continued in a manner that was substantially unaffected by the event.

As a result of the cyber-security event, the City requests your patience and leniency for a period of time regarding the submission of records, reports, and information required by your office, or required by state or federal law.

The City is working diligently with state and federal agencies to determine the extent of the security event and to recover access to the City's information. At present, the City has a reasonable expectation it will be able to recover legally reliable data crucial to the City's information related to police activities in order to protect the citizens of Carrollton in their respective counties and in the interests of justice of all persons.

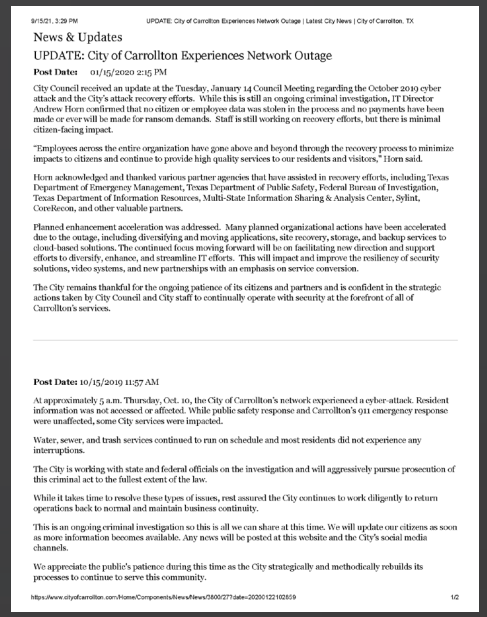
Based on the current status of the City's systems, the City requests an extension of time to recover its information and regular operations. The City will keep your offices updated regarding the status of the City's information. Be assured, the City will not jeopardize any investigation or individual rights but will ensure the validity and credibility of all information prior to reliance on such information.

On behalf of Derick Miller, Chief of Police, Rex Redden, Director of Public Safety, and the City, we humbly appreciate your consideration and benevolence in this matter.

Thank you for your attention,

Mladd

Meredith Ladd
City Attorney
City of Carrollton, Texas



9/15/21, 3:29 PM UPDATE: City of Carrollton Experiences Network Outage | Latest City News | City of Carrollton, TX

News & Updates

UPDATE: City of Carrollton Experiences Network Outage

Post Date: 01/15/2020 2:15 PM

City Council received an update at the Tuesday, January 14 Council Meeting regarding the October 2019 cyber attack and the City's attack recovery efforts. While this is still an ongoing criminal investigation, IT Director Andrew Horn confirmed that no citizen or employee data was stolen in the process and no payments have been made or ever will be made for ransom demands. Staff is still working on recovery efforts, but there is minimal citizen-facing impact.

"Employees across the entire organization have gone above and beyond through the recovery process to minimize impacts to citizens and continue to provide high quality services to our residents and visitors," Horn said.

Horn acknowledged and thanked various partner agencies that have assisted in recovery efforts, including Texas Department of Emergency Management, Texas Department of Public Safety, Federal Bureau of Investigation, Texas Department of Information Resources, Multi-State Information Sharing & Analysis Center, Sylint, CoreRecon, and other valuable partners.

Planned enhancement acceleration was addressed. Many planned organizational actions have been accelerated due to the outage, including diversifying and moving applications, site recovery, storage, and backup services to cloud-based solutions. The continued focus moving forward will be on facilitating new direction and support efforts to diversify, enhance, and streamline IT efforts. This will impact and improve the resiliency of security solutions, video systems, and new partnerships with an emphasis on service conversion.

The City remains thankful for the ongoing patience of its citizens and partners and is confident in the strategic actions taken by City Council and City staff to continually operate with security at the forefront of all of Carrollton's services.

Post Date: 10/15/2019 11:57 AM

At approximately 5 a.m. Thursday, Oct. 10, the City of Carrollton's network experienced a cyber-attack. Resident information was not accessed or affected. While public safety response and Carrollton's 911 emergency response were unaffected, some City services were impacted.

Water, sewer, and trash services continued to run on schedule and most residents did not experience any interruptions.

The City is working with state and federal officials on the investigation and will aggressively pursue prosecution of this criminal act to the fullest extent of the law.

While it takes time to resolve these types of issues, rest assured the City continues to work diligently to return operations back to normal and maintain business continuity.

This is an ongoing criminal investigation so this is all we can share at this time. We will update our citizens as soon as more information becomes available. Any news will be posted at this website and the City's social media channels.

We appreciate the public's patience during this time as the City strategically and methodically rebuilds its processes to continue to serve this community.

https://www.cityofcarrollton.com/Home/Components/News/News/3600/27?date=20200122102659 1/2

Notice

The applicability requirements of the Public Information Act (TX GOVT CODE CH. 552) to the City of Carrollton are suspended pursuant to section 552.233.

charlesworth consulting

WSSCWATER
DELIVERING THE ESSENTIAL

MAY 24, 2021 – CYBERATTACK

- NOTIFICATION OF INSURANCE COMPANY
- VENDORS PROVIDED BY IC CONVENE CALLS
  - Data breach law firm and GCO
  - IT forensic firm
  - IT key staff
- FBI AND MD ATTORNEY GENERAL NOTIFICATIONS
- JUNE 23, 2021 - PUBLIC ANNOUNCEMENT

charlesworth consulting

WSSCWATER
DELIVERING THE ESSENTIAL

WSSC Water Investigating Ransomware Cyberattack

Drinking Water and Wastewater Systems Not Impacted;
Systems Restored from Back-ups and are Fully Operational;
No Ransom Will be Paid

Contact:
Chuck Brown
Charles.Brown@wsscwater.com
301-206-8100

Laurel, Md. – June 25, 2021 – WSSC Water is investigating a ransomware attack on May 24 that impacted a portion of our network that operates non-essential business systems. The ransomware virus was successfully removed within hours and WSSC Water is fully operational. The incident does not impact water or wastewater service or quality, and those systems were never at risk. Existing cybersecurity safeguards and swift action taken by WSSC Water's IT department helped minimize the impact of this attack. WSSC Water has not and will not pay or support the criminals behind this cyberattack.

"WSSC Water continues to produce and deliver safe, clean water to 1.8 million customers in Montgomery and Prince George's counties and at no time was the quality or reliability of our drinking water in jeopardy," said WSSC Water Police and Homeland Security Director David McDonough.

The systems that operate WSSC Water's filtration and wastewater treatment plants are, by design, stand-alone networks not connected to the Internet. WSSC Water restored files from back-ups and there was no significant impact on business operations. WSSC Water maintains a partnership with the Department of Homeland Security and is regularly testing its security protocols. WSSC Water will continue to investigate this incident and take steps to protect the integrity of its systems and data.

"These attacks have become more common, especially in recent weeks, and WSSC Water has prepared for this type of event," added McDonough.

A comprehensive investigation is underway. WSSC Water has notified the FBI, Maryland Attorney General and state and local homeland security officials and will cooperate with any investigation. WSSC Water's own investigation is expected to take several weeks before all the facts are known.

While the virus was not successful, it appears the ransomware criminals did gain access to internal files. As the investigation continues, WSSC Water will notify in writing any individuals whose personal identifying information was exposed. Those individuals will be offered five years of credit monitoring with $1,000,000 in identity theft insurance at no cost to them.

All individuals are encouraged to remain vigilant and closely examine their financial statements and report anything suspicious to their bank or card issuer. Individuals can also access identitytheft.gov to report any suspicious activity and to learn how to freeze their credit.

While the investigation is ongoing, if individuals have questions or would like more information, please call 1-833-406-2411 weekdays from 9 a.m. to 9 p.m.

###

About WSSC Water: *WSSC Water is the proud provider of safe, seamless and satisfying water services, making the essential possible every day for our neighbors in Montgomery and Prince George's counties. We work to deliver our best because it's what our customers expect and deserve.*

charlesworth consulting

- **LEGAL INVESTIGATION CONTINUES**
  - Legal notifications from PI exposure
  - Credit monitoring for 5 years with $1,000,000 in identity theft insurance
  - Insurance only pays for 1 year of credit monitoring



BLOG

Florida Water Treatment Plant Hit With Cyber Attack



Steve Kardon February 9, 2021

On Friday, February 5, 2021, a hacker initiated an attack on an Oldsmar, Florida water treatment facility which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million. This attack occurred about 15 miles from the location of, and two days before the Super Bowl. If successful, the attack would have increased the amount of sodium hydroxide to an incredibly dangerous level in the water supply. Fortunately, a vigilant employee saw the intrusion attempt as it was occurring, and stopped it.

As the article noted, "Experts say municipal water and other systems have the potential to be easy targets for hackers because local governments' computer infrastructure tends to be underfunded." This is not the first attempt to gain control

charlesworth consulting

WSSCWATER
DELIVERING THE ESSENTIAL

CRITICAL INFRASTRUCTURE – SCADA SYSTEMS

(SUPERVISORY CONTROL AND DATA ACQUISITION)

- Is your critical infrastructure controlled by a SCADA system?
- Is your SCADA system connected to the internet?
- If it is connected to the internet, should it be?
- Your SCADA system can be tested by the Federal Department of Homeland Security
- WSSC's 8 plants controlled by SCADA system not connected to the internet -- each plant can operate independently
- Homeland Security has tested our system -- could not get in

charlesworth consulting

DIFFERENCES AND SIMILARITIES

- ROOT CAUSE
- DATA EXFILTRATION V ENCRYPTED DATA
- PRIVACY NOTIFICATION EXPENSE V COMPUTER HARDWARE REPLACEMENT
- INCIDENT RESPONSE
- INSURANCE COVERAGE

charlesworth consulting

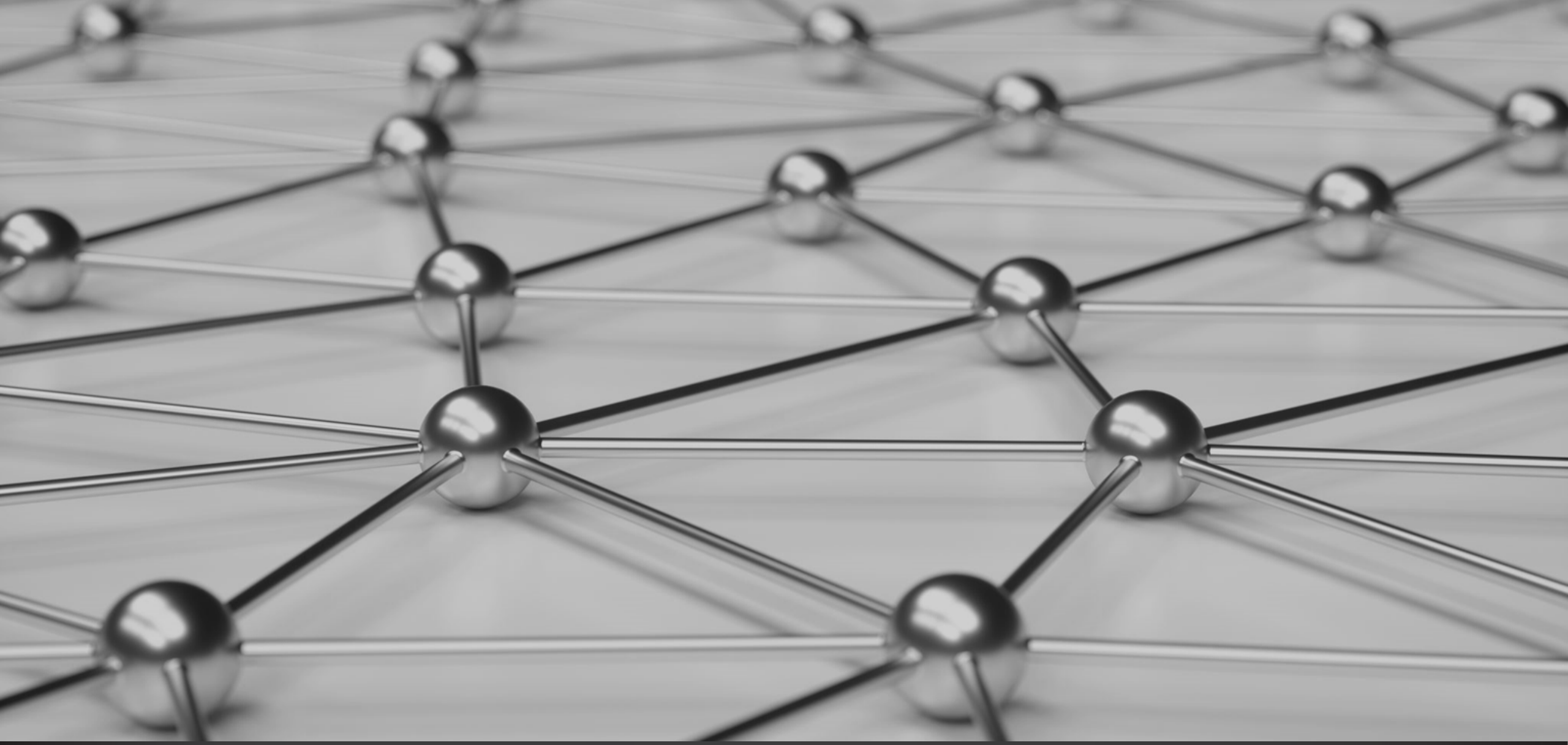
TAKEAWAYS

- HAVE SECURITY PROTOCOLS IN PLACE TO REDUCE THE RISK OF BEING ATTACKED. (EXAMPLE: MULTI-FACTOR AUTHENTICATION AND EMPLOYEE TRAINING)
- TRANSFER THE RISK OF LOSS TO VENDORS WHENEVER POSSIBLE.
- GET CYBER INSURANCE AND UNDERSTAND THE COVERAGE AND THE CYBER INCIDENT RESPONSE RESOURCES AVAILABLE.
- IF YOU CANNOT GET CYBER INSURANCE, HAVE RETAINER AGREEMENTS IN PLACE WITH A DATA BREACH LAW FIRM AND IT FORENSIC FIRM
- HAVE AN INCIDENT RESPONSE PLAN IN PLACE THAT GOES BEYOND THE IT RELATED RESPONSE AND TEST IT ANNUALLY.

charlesworth consulting

QUESTIONS AND PANEL DISCUSSION

charlesworth consulting



charlesworth
consulting