Osseo City Council
AGENDA

WORK SESSION
Monday, January 24, 2022
6:00 p.m., Virtual Meeting

MAYOR DUANE POPPE COUNCILMEMBERS: JULIANA HULTSTROM, HAROLD E. JOHNSON, LARRY STELMACH, ALICIA VICKERMAN

1. **Call to Order**

2. **Roll Call** (quorum is 3)

3. **Approval of Agenda** (requires unanimous additions)

4. **Discussion Items**

   A. **Email and Internet Security Training – Element Technologies**

5. **Adjournment**

The City of Osseo's mission is to provide high-quality public services in a cost-effective, responsible, innovative, and professional manner given changing needs and available resources.

4 A

City of Osseo City Council
Work Session Meeting Item

Agenda Item: **Email and Internet Security Training – Element Technologies**

Meeting Date: January 24, 2022
Prepared by: Riley Grams, City Administrator

Attachments: Element Cybersecurity Information

Background:

Late last year, the Risk Management Committee asked that Staff coordinate an email and internet security training session with our IT consultant, Element Technologies. Element does provide this type of education and training to their clients as needed. Several Element employees who are a part of their Security Team will be available on Monday evening to provide training tailored towards phishing attacks, other prevalent threats, social engineering, and overall best practices to help mitigate the risk of exposure to malware, viruses, and other harmful attacks that would compromise the City's IT systems.

Staff members from Element Technologies will provide the Council with a relevant and pertinent cybersecurity training presentation at the work session meeting on Monday night.

Recommendation/Action Requested:
Staff recommends the City Council discuss the item and direct Staff accordingly.

HOME

COMPANY

SERVICES

NEWS

CONTACT US

LINKEDIN

CYBERSECURITY

We keep a close eye on your network. Through proven tools and industry best practices, we provide ongoing monitoring to assess your risks and secure your data. Every assessment is reviewed by a senior member of our team with Certified Information Systems Security Professionals (CISSP) credentials

Security Audits

We conduct a comprehensive risk assessment to identify and quantify the risks to your organizations information assets. We will identify technical vulnerabilities and determine how best to mitigate those risks to keep your information safe

Managed Cybersecurity Service

We use a number of industry leading tools and reporting to protect your network and provide security monitoring and remediation. Our quarterly reports outline the health of your organization through proactive threat detection and analysis.

Cybersecurity Awareness Program

User / employee awareness of threats and scams is the most important component of maintaining a strong layer of security. We deliver a three-phase approach to security education through training, phishing tests and continued education on the latest security trends to help strengthen your company's defenses.

CYBERSECURITY 101 - BACK TO THE BASICS

Too often in cybersecurity, business leaders are forced into the 'what' decisions before ever getting an opportunity to understand the 'why' behind them. The purchasing conversations with IT start with requests like "We need to upgrade our AV to a next-gen EDR solution.", "Our firewalls need to be application aware and allow for DPI-SSL with full throughput.", or "We need to move from VPN to a zero-trust solution." (*Note: if you are interested in what all this techno-babble means, check out the glossary at the end of the article*)

While the above requests are all important parts of cybersecurity, an understanding that the many diverse pieces should come together to provide a layered and complete security solution is more important overall. Decision makers often either look at the financial impact and say yes to some pieces and no to others, they implement just enough to be compliant with regulators, or, in rare cases, they say yes to everything. Any of these responses can result in security holes, increased risk, or unnecessary spending. As business leaders, we need to begin by building a foundational understanding of what we are trying to accomplish. For this reason, we are going to go back to the basics in this article.

WHAT IS CYBERSECURITY?

Cybersecurity can take many forms, and the purposes of those forms vary. However, the basic definition of the word remains: *Cybersecurity encompasses the measures taken to protect a computer—or entire network—from unauthorized access or attack.*

This definition offers the first step toward understanding how massive the process of securing a network against cyberattacks really is. Shielding computer systems and networks requires everything from the people (cybersecurity experts and end users alike), to the processes, techniques, and technology put into place as forms of protection. Without properly implemented layers of security (sometimes called defense-in-depth), cyberattacks are easily executed and can greatly damage an organization's reputation and lead to significant financial loss.

WHY IS CYBERSECURITY IMPORTANT?

Each and every day, businesses rely more and more on the internet. The field of technology is an easy example of this, but the financial, legal, and medical fields are quickly moving to cloud-based solutions and remote workforces. Cybersecurity serves as a wall of protection for the organizations in these fields, assessing the threats, risks, and vulnerabilities in their systems in order to keep their networks safe.

Cybercrime is, by its nature, far more abstract than the threats we see in our everyday lives; A cybersecurity threat may never present itself until after the damage is done. Unfortunately, that does not mean the threat is any less real. The importance of cybersecurity cannot be overemphasized. Every day at Element we work with victims of cybercrime. Phishing attacks, stolen credentials (or devices), and ransomware are just a few examples of how their lives have been turned upside down.

A dynamic cybersecurity practice keeps personal information and intellectual property from falling into the hands of attackers. User authentication, password security, multifactor authentication, and protection against phishing and keystroke logging are just a few of the first steps to building the layers of security necessary for excellent defense.

Of particular note, the legal, financial, and medical fields are prime examples of industries that risk the greatest loss if they fall prey to a cyberattack, because these organizations hold an exceptional amount of data on individuals, businesses, and governments.

CYBERSECURITY FOR LAW FIRMS AND HEALTHCARE

While cyberattacks on law firms and financial firms are not a new occurrence, they are becoming increasingly prevalent because these organizations have access to files and information on many other industries. Law firms in particular keep records of crucial documents that could be accessed through a data breach: Case files, attorney-client documents, and patient records, for a start.

Similarly, cyberattacks on healthcare facilities pose a grave danger, because each successful attack exposes patient medical records. These records may contain information that dates back over many years, and though exposure of a medical record may sound trivial at first thought, this kind of document contains a patient's name, date of birth, social security number, and billing information. This is information that can cause unprecedented amounts of damage if it is exposed to unauthorized malicious parties.

So, how do organizations protect themselves, if there are this many threats out there, and even more layers to cybersecurity? Security Awareness Training is a good place to start.

WHAT IS SECURITY AWARENESS TRAINING?

It is not strange to know that employees are mostly focused on Continuing Professional Development (a process for continuously developing the knowledge they have within their industries) that they forget to learn about the industry that makes cyber connectivity and enhanced workplace productivity possible (read: the IT industry).

Security Awareness Training brings this need-to-learn-activity to the fore by educating employees on the types of cyber attacks, the processes and techniques for computer security in order to protect against cyber attack. A standard Security Awareness Training program covers materials on these areas: social engineering, encryption, dictionary attacks, user disclosure, phishing and smishing, malware, clean disk policy, password protection and authentication methods, compliance, BYOD vs COPE, Business Email Compromise and other computer security areas that helps the employees identify potential attacks and/or scams. Oftentimes, this training simulates attacks like phishing attacks, malware attacks, ransomware attacks and the likes to ensure that employees have a feel of what potential attacks could look like and how to not fall prey.

These trainings are highly recommended for the employees of law firms and healthcare providers while the employers focus on risk assessments and the introduction of cybersecurity procedures in their organizations to identify cyber threats and prevent cyber attacks.

WHAT IS HIPAA?

An acronym for Health Insurance Portability and Accountability Act (HIPAA), it was passed into law by President Bill Clinton in 1996. Best known as HIPAA, it covers 5 clearly defined rules about data privacy and security of medical information:

- Privacy Rule;
- Security Rule;
- Transactions Rule;
- Identifiers Rule;
- Enforcement Rule.

Because HIPAA covers the protection of data and privacy of the medical industry from a legal perspective, it connects these two industries on how medical information ought to be treated and complied with.

WHAT IS A HIPAA SECURITY AUDIT?

In line with the above, a HIPAA Security Audit involves the legal inspection and assessment of medical providers' databases to ensure that they are aligned with the clearly defined rules of the HIPAA act, especially HIPAA Title II which manages Protected Health Information (PHI) of patients. This audit is usually carried out to make certain that healthcare providers are not running foul of the rules set out by HIPAA.

Breaching HIPAA rules leads to non-compliance financial costs that run into millions of dollars. When it comes to the privacy and security of patients' Medicare information, it is best to err on the path of conscious, constantly-evolving cybersecurity processes.

GLOSSARY:

AV: Anti-Virus.

EDR: Endpoint Detection and Response—A solution that gives security teams a centralized platform for continuously monitoring endpoints in order to respond to incidents as they arise.

DPI-SSL: Deep Packet Inspection of Secure Socket Layer traffic — a type of data processing that inspects encrypted traffic in detail being sent in and out of the network. Encrypted traffic if often ignored during inspection by firewalls meaning that the IT/Security team has no idea what is being sent in or out over the Internet.

VPN: Virtual Private Network—a network that is constructed using public wires—usually the internet—to connect remote users or regional offices to a company's private, internal network.

- **IT Services**
- Audits & Assessments
- Managed Services
- **Cloud**
- Online Backups
- Email Security
- Hosting & Colocation
- **Enterprise Content Management**
- NetDocuments
- ECM - BPM
- **About Us**
- Blog
- Upcoming Events
- Contact Us
- Testimonials

- Hardware & Software
- **Advisory**
- Business Planning
- Security Compliance
- Tech Evolution

- **Cybersecurity**
- Security Audits
- Managed Cybersecurity
- Awareness Training
- Dark Web Scan

- ECM - Products
- Education & Training
- Element University

- Careers