CYBER SECURITY AWARENESS

The 2024 Cyber Security Playbook for MHEDA Members

© 2024 USI Insurance Services. All rights reserved. All of the questions and drill down are USI IP.

TOP 8 CYBER ATTACKS – 2024

1. **Phishing Attack**
   The use of deceptive emails, texts, or websites to gain sensitive information.

2. **Ransomware**
   Malware that can encrypt data and make you pay to get them back.

3. **Denial-of-Service (Dos)**
   Loading excessive load on a machine or network so that it stops working normally.

4. **Man-in-the-Middle (MitM)**
   Engaging in covert interception and manipulation of communication between two parties without noticing it.

5. **SQL Injection**
   To get the access to the database, vulnerabilities in database queries can be exploited.

6. **Cross-Site Scripting (XSS)**
   Putting malicious code into websites that other people visit.

7. **Zero-Day Exploits**
   Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8. **Domain Name System (DNS) Spoofing**
   Sending DNS queries to malicious sites so that they can be accessed without permission.

© 2024 USI Insurance Services. All rights reserved.

Incident Type

2020

Incident Type	Count
Ransomware	1,006 (29%)
Business Email Compromise (BEC) – Total	794 (23%)
BEC – Other	607
BEC – Wire Fraud	187
Third-Party Breach	583 (17%)
Network Intrusion	450 (13%)
Other	381 (11%)
Inadvertent Disclosure	214 (7%)
Total	**3,428 (100%)**

2021

Incident Type	Count
Ransomware	1,153 (29%)
Business Email Compromise (BEC) – Total	1,059 (27%)
BEC – Other	698
BEC – Wire Fraud	361
Third-Party Breach	623 (16%)
Network Intrusion	559 (14%)
Other	367 (9%)
Inadvertent Disclosure	209 (5%)
Total	**3,970 (100%)**

2022

Incident Type	Count
Business Email Compromise (BEC) – Total	1,077 (36%)
BEC – Other	733
BEC – Wire Fraud	344
Ransomware	732 (25%)
Network Intrusion	382 (13%)
Third-Party Breach	316 (11%)
Other	245 (8%)
Inadvertent Disclosure	207 (7%)
Total	**2,959 (100%)**

2023 (through Nov.)

Incident Type	Count
Business Email Compromise (BEC) – Total	1,239 (35%)
BEC – Other	921
BEC – Wire Fraud	318
Ransomware	811 (22%)
Third-Party Breach	675 (19%)
Other	379 (10%)
Network Intrusion	302 (8%)
Inadvertent Disclosure	209 (6%)
Total	**3,615 (100%)**

© 2024 USI Insurance Services. All rights reserved.

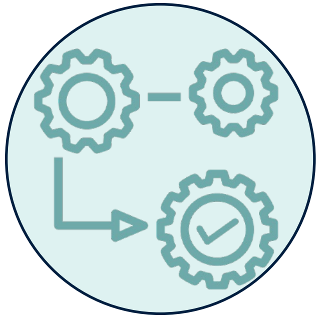
2024 Top10 Cyber Underwriting Focus Areas

The lack of these critical baseline controls *directly increases* the potential of Cyber Incidents

1 Third Party Risk Management Processes:

2 Multifactor Authentication (MFA):

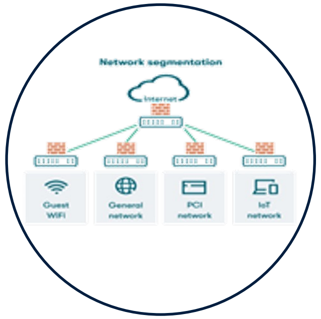
3 Patch Management Controls:



4 Endpoint Detention and Response Solutions:

5 Incident Response Plan:

6 Network Segmentation:



7 Backups:

8 Access Control:

9 Culture Training/ Phishing:

10 Email:

© 2024 USI Insurance Services. All rights reserved. All of the questions and drill down are USI IP.

2024 Top 3 Privacy Underwriting Focus Areas

The lack of these critical baseline controls *directly increases* the potential of Cyber Incidents

1 Artificial Intelligence

2 Biometrics

3 Pixels and Session Replay

© 2024 USI Insurance Services. All rights reserved. All of the questions and drill down are USI IP.

Best Practices: Pre-Incident

- **Empower** the organization’s first responders
- **Conduct risk assessment** and **implement data security improvements** prior to being asked by a regulator
- **Talk** to your IT security staff
  - Gain an appreciation of the many challenges and risk landscape
  - Not many organizations can say how many records they have; what type of data is being collected, stored, shared, protected; where all the data resides; when is it purged; etc.
- **Assess** and test the organization’s staff and operations
- **Prepare** and test your incident response plan (IRP) annually or if materially change in business practices
- **Document** your due care measures (training and enforcement) being taken
- **Insure** yourself
- **Repeat**

© 2024 USI Insurance Services. All rights reserved.

Best Practices: Legal and Administrative

- **Understand your data** – what it is, where it is, who has access to it, do you need it, etc.
- Understand **contractual obligations** to secure data and report security incidents
- Understand **legal and regulatory framework** applicable to organization and data
- Conduct a **security assessment** of your systems
- **Train** employees
- **Patch** vulnerabilities
- Operate **up-to-date software**
- Utilize **anti-virus software**
- Utilize **firewalls**
- Deploy **Endpoint Detection and Response** (EDR) solutions
- **Patch** VPN
- Enable **Multi-factor Authentication** (MFA)
- Identify and secure "**crown jewels**"
- **Backup** data
  - "3-2-1 Method" – **3** copies in **2** locations, **1** of which is offline
- Develop and test an **Incident Response Plan** (IRP)
- Develop and test a **business continuity plan**
- Develop and enforce a **vendor management program**
- Develop and manage a **patch management program**
- Purchase **cyber insurance**

© 2024 USI Insurance Services. All rights reserved.

Best Practices: Incident Response

For any actual or suspected breach, you must simultaneously inform your pre-approved "breach counsel" and notify your insurance broker:

a. **Step 1:** Invoking Breach Counsel: This is done by calling the breach hotline or phone number listed on your policy. The assigned law firm's fiduciary duty is to you the policyholder and does not provide notice to the carrier. Breach Counsel will assist in retaining experts.

b. **Step 2:** Your broker will provide written notice to the primary and excess (if applicable) cyber insurers via email on your behalf. Please provide a short description of the incident to USI to be included in the tender to the insurance company/companies. Your broker will copy you on the notice to the insurance company.

c. **Step 3:** You will receive a telephone call from the breach counsel who will further instruct you on the next steps. This may include retaining the carrier's panel providers – IT Forensics Firms, Public Relations Experts, Ransomware and Bitcoin Consultants. If warranted, breach counsel may advise on providing notification of the breach to applicable government regulators and/or the public whose information may have been compromised.

d. **Step 4:** You will receive an automated acknowledgement email from the insurance company recognizing they received USI's email. The insurer may wish to conduct an initial call with breach counsel and stakeholders.

© 2024 USI Insurance Services. All rights reserved.

Best Practices: Third Party Vendor Contract Review Considerations

- Engage legal counsel with expertise to negotiate terms, conditions, contracts and service level agreements
- No Ransomware Restrictions
- Make sure the scope of work is not only well defined…but understood by all
- Does your vendor agreement address?
  - ✓ Utilization of Artificial Intelligence
  - ✓ Compliance with data privacy standards
  - ✓ Return or destruction of PII/PHI
  - ✓ Use of Subcontractors with access to PII/PHI
  - ✓ Contractual obligation to fully disclose fact of privacy incident (including all forensics reports completed)
  - ✓ What happens during outages…what support coverage is available
  - ✓ How long may you be without access to critical business applications and most importantly how is that addressed in the contract/agreement
  - ✓ Specifically outline the formal process – change control process- to ensure that changes to a system or product are introduced in a controlled and coordinated process
  - ✓ Contractual obligation to notify of privacy incident within X hours. Who will manage the incident?

© 2024 USI Insurance Services. All rights reserved.