MILLER JOHNSON Attorneys

# An Employer's Low-Tech Guide to Preventing Cyber Attacks

- *Jason Crow, CIPP/US*
- *Jeff Muth*


The materials and information have been prepared for informational purposes only. This is not legal advice, nor intended to create or constitute a lawyer-client relationship. Before acting on the basis of any information or material, readers who have specific questions or problems should consult their lawyer.

MILLER JOHNSON Attorneys



© 2022 Miller Johnson. All rights reserved.

MILLER JOHNSON Attorneys

# What are the 3 pillars of any cybersecurity risk management program?



1. Implement a WISP.
2. Train Employees to that WISP.
3. Insure the WISP.



© 2022 Miller Johnson. All rights reserved.

© 2022 Miller Johnson. All rights reserved.

1. Implement a WISP.
2. Train Employees to that WISP.
3. Insure the WISP.

7

# 1. Implement a WISP

8

© 2022 Miller Johnson. All rights reserved.

*The People of the State of Michigan enact:*

CHAPTER 5A

DATA SECURITY

Sec. 555. (1) Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program, based on the licensee's risk assessment, that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system.

(2) A licensee's information security program must be designed to do all of the following:

*The People of the State of Michigan enact:*

CHAPTER 5A

DATA SECURITY

(a) Protect the security and confidentiality of nonpublic information and the security of the information system.

(b) Protect against any threats or hazards to the security or integrity of nonpublic information and the information system.

(c) Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer.

(d) Maintain policies and procedures for the secure disposal on a periodic basis of any nonpublic information that is no longer necessary for business operations or for other legitimate business purposes.

(3) A licensee shall do all of the following:

(a) Designate 1 or more employees, an affiliate, or an outside vendor to act on behalf of the licensee that is responsible for the information security program.

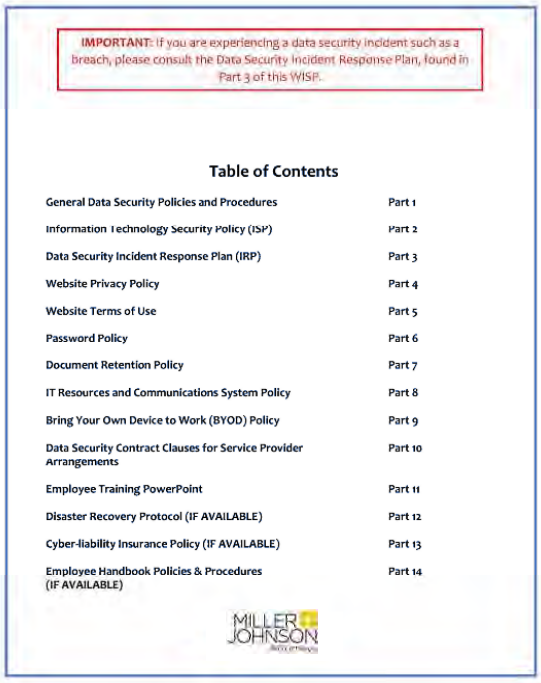
(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers.

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information.

(d) Assess the sufficiency of policies, procedures, information systems, and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including all of the following:

(*i*) Employee training and management.

© 2022 Miller Johnson. All rights reserved.



IMPORTANT: If you are experiencing a data security incident such as a breach, please consult the Data Security Incident Response Plan, found in Part 3 of this WISP.

**Table of Contents**


| | |
|---|---|
| General Data Security Policies and Procedures | Part 1 |
| Information Technology Security Policy (ISP) | Part 2 |
| Data Security Incident Response Plan (IRP) | Part 3 |
| Website Privacy Policy | Part 4 |
| Website Terms of Use | Part 5 |
| Password Policy | Part 6 |
| Document Retention Policy | Part 7 |
| IT Resources and Communications System Policy | Part 8 |
| Bring Your Own Device to Work (BYOD) Policy | Part 9 |
| Data Security Contract Clauses for Service Provider Arrangements | Part 10 |
| Employee Training PowerPoint | Part 11 |
| Disaster Recovery Protocol (IF AVAILABLE) | Part 12 |
| Cyber-liability Insurance Policy (IF AVAILABLE) | Part 13 |
| Employee Handbook Policies & Procedures (IF AVAILABLE) | Part 14 |


# Company WISP

1. General Data Security Policies and Procedures.
2. IT Security Policy.
3. Data Security Incident Response Plan.
4. Website Privacy Policy & Terms of Use.



© 2022 Miller Johnson. All rights reserved.

## Company WISP

5. Password Policy/MFA.
6. Document Retention Policy.
7. Acceptable Use Policy.
8. BYOD Policy.

13

## Company WISP

5. Password Policy/MFA

- Security.org/how-secure-is-my-password.
- 10 characters
- MFA

14

© 2022 Miller Johnson. All rights reserved.

## Company WISP

9. Vendor Management Policy.
10. Remote Work Policy.
11. Employee Training PowerPoint/KnowBe4.
12. Disaster Recovery Protocol.

15

## Company WISP

13. Employee Handbook.
14. Cyber-liability Insurance.

16

© 2022 Miller Johnson. All rights reserved.

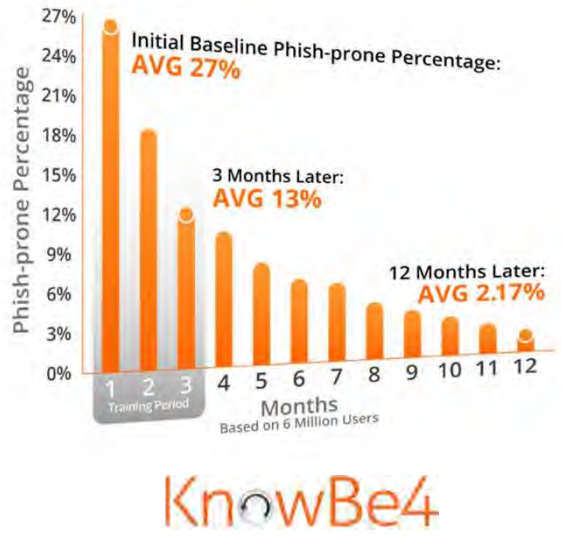
1. Implement a WISP.
2. Train Employees to that WISP.
3. Insure the WISP.



# 2. Train Employees to WISP



© 2022 Miller Johnson. All rights reserved.



© 2022 Miller Johnson. All rights reserved.

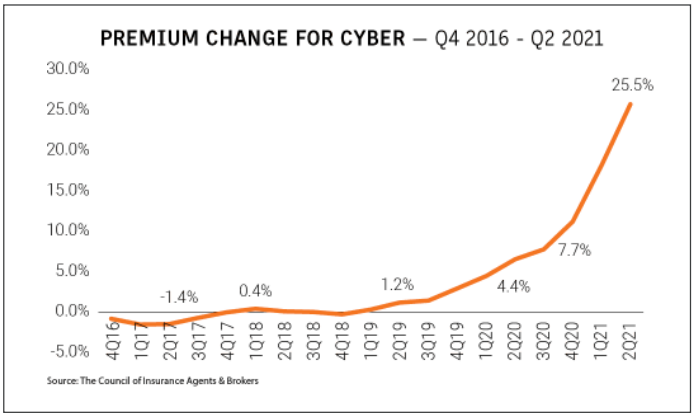
YOUR HR/IT TEAM

1. Implement a WISP.
2. Train Employees to that WISP.
3. Insure the WISP.



© 2022 Miller Johnson. All rights reserved.

## Cyber premiums soar 25.5% in Q2: CIAB



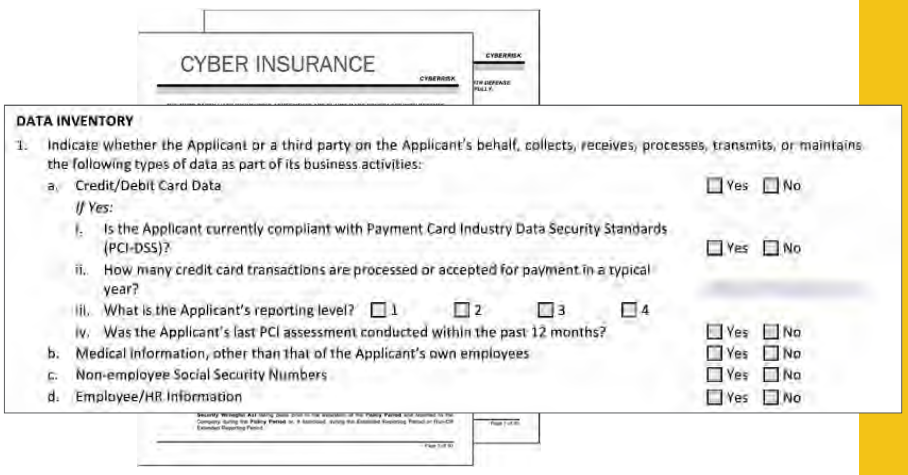

**Source:** The Council of Insurance Agents & Brokers' Q2 Commercial P/C Market Survey https://www.businessinsurance.com, August 24, 2021

- 1. First Party Coverage
  - Crisis Management Event Expenses
  - Security Breach Remediation and Notification Expenses
  - Computer Program and Electronic Data Restoration Expenses
  - Computer Fraud
  - Funds Transfer Fraud
  - E-Commerce Extortion
  - Business Interruption and Additional Expenses

© 2022 Miller Johnson. All rights reserved.

- 2. Third Party Coverage
  - Network and Information Security Liability
  - Communications and Media Liability
  - Regulatory Defense Expenses

## Underwriting Questionnaire



CYBER INSURANCE

**DATA INVENTORY**

1. Indicate whether the Applicant or a third party on the Applicant's behalf, collects, receives, processes, transmits, or maintains the following types of data as part of its business activities:
   - a. Credit/Debit Card Data ☐ Yes ☐ No
     *If Yes:*
     - i. Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)? ☐ Yes ☐ No
     - ii. How many credit card transactions are processed or accepted for payment in a typical year?
     - iii. What is the Applicant's reporting level? ☐ 1 ☐ 2 ☐ 3 ☐ 4
     - iv. Was the Applicant's last PCI assessment conducted within the past 12 months? ☐ Yes ☐ No
   - b. Medical information, other than that of the Applicant's own employees ☐ Yes ☐ No
   - c. Non-employee Social Security Numbers ☐ Yes ☐ No
   - d. Employee/HR information ☐ Yes ☐ No

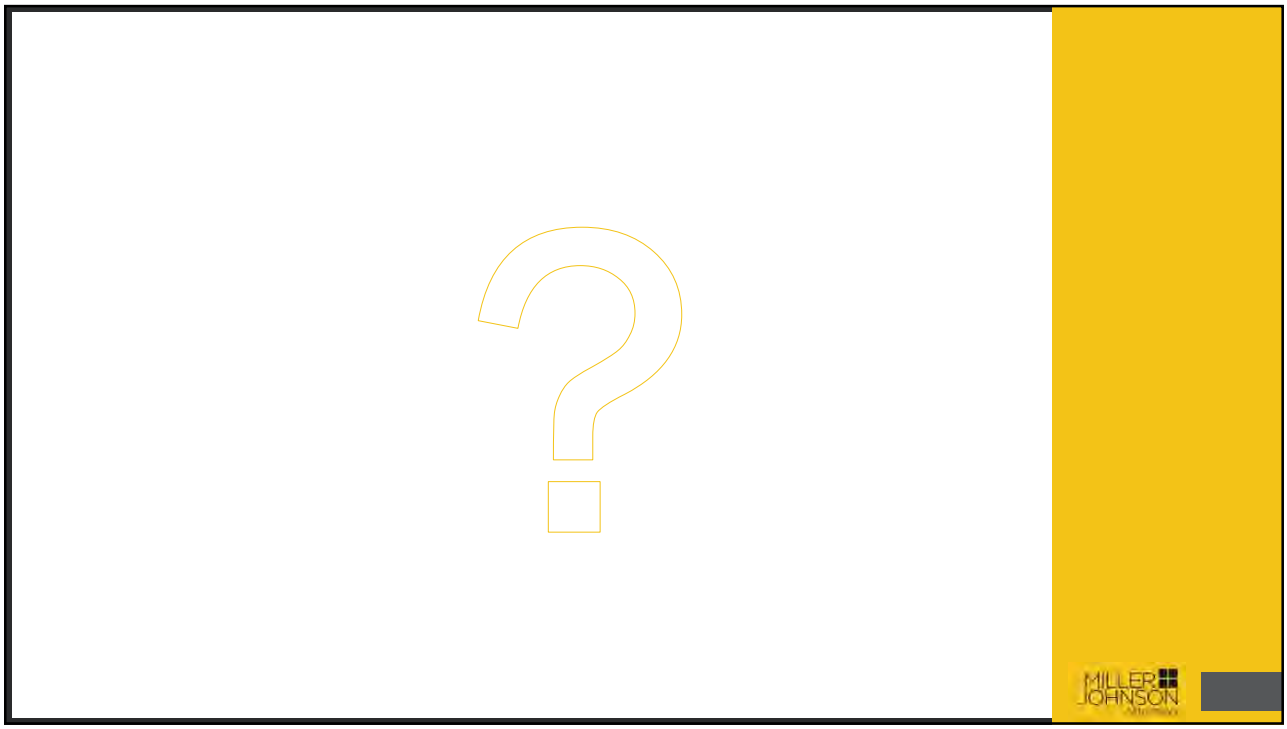
© 2022 Miller Johnson. All rights reserved.

## Recap: what are the 3 pillars of any cybersecurity risk management program?

1. Implement a WISP.
2. Train Employees to that WISP.
3. Insure the WISP.



© 2022 Miller Johnson. All rights reserved.



© 2022 Miller Johnson. All rights reserved.

MILLER JOHNSON Attorneys

MILLER JOHNSON Attorneys

**Jason Crow, CIPP/US**

616.831.1745

crowj@millerjohnson.com

**Jeff Muth**

616.831.1706

muthjg@millerjohnson.com



**DETROIT**
409 E. Jefferson Ave
Fifth Floor
Detroit, MI 48226

**GRAND RAPIDS**
45 Ottawa Ave SW
Suite 1100
Grand Rapids, MI 49503

**KALAMAZOO**
100 W Michigan Ave
Suite 200
Kalamazoo, MI 49007

**millerjohnson.com**


© 2022 Miller Johnson. All rights reserved.