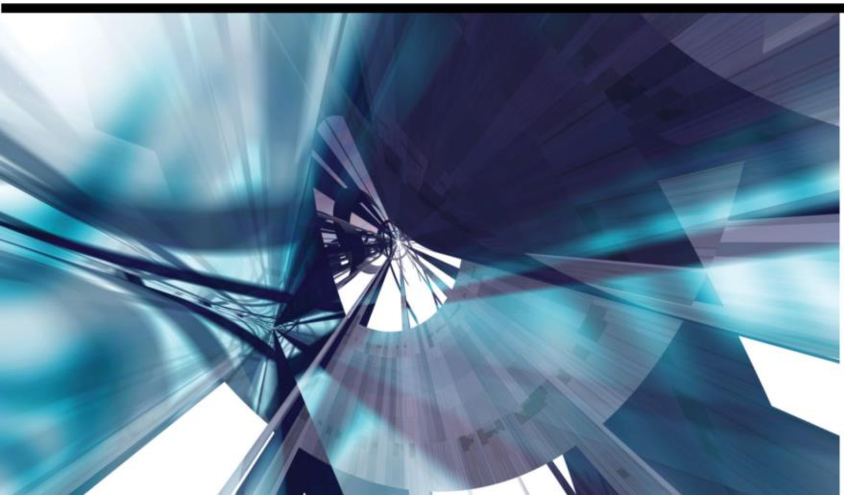
PEOPLE I PROPERTY I REPUTATION

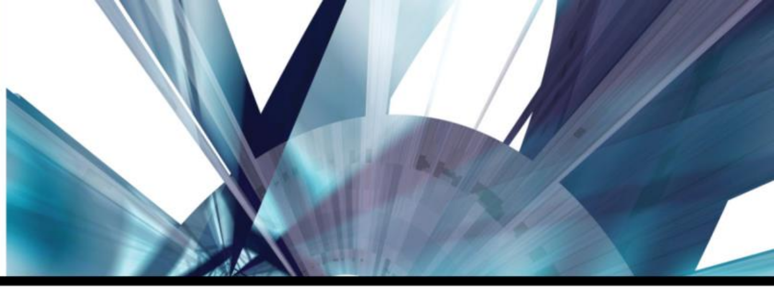
ASSET PROTECTION



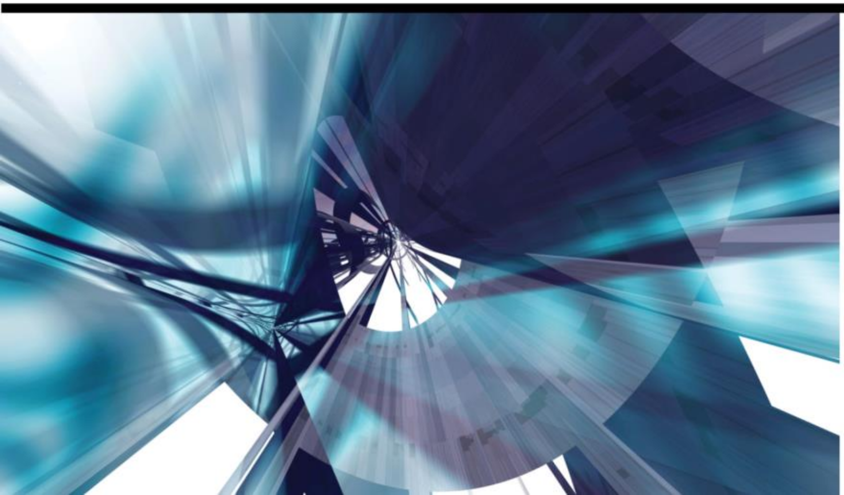
FMI®

THE VOICE OF FOOD RETAIL

PEOPLE I PROPERTY I REPUTATION



THE BREACH, THE FALLOUT, AND YOUR RESPONSE: A TABLETOP EXERCISE



FMI®

THE VOICE OF FOOD RETAIL

The Need for an Incident Response Capability

“In the wake of recent high profile targeted attacks in the retail sector, a company’s ability to quickly identify and classify an incident, and execute a response plan, is critical to not only protecting corporate assets and customer data, but the brand, reputation and bottom line of the company.”

Arbor Networks president Matthew Moynahan

Agenda

- Kick-Off Session: Goals and Objectives
- Setting the Stage: A Threat Briefing
- Incident Response Framework Introduction
- Scenario Walkthrough
- Hot Wash and Final Thoughts

Goals and Objectives

1. Review cyber threat environment for the retail sector.
2. Introduce FMI’s Incident Response Framework.
3. Apply the Incident Response Framework through a focused tabletop exercise (TTX).

Food and Retail Sector Risks

Leading FMI Companies' Understand the Cyber Reality

Third Party

If third parties or our associates *are able to penetrate our network security or otherwise misappropriate our customers' personal information or credit or debit card information, or if we give third parties or our associates' improper access to our* ***customers' personal information or credit card information we could be subject to liability.***

Food Lion, 2012 Annual Report

Technology Dependent

The efficient operation of the Company's ***businesses is dependent on computer hardware*** *and software systems. Information systems are vulnerable to security breach by computer hackers and cyber terrorists.*

SUPERVALU, 2013 SEC 10-k

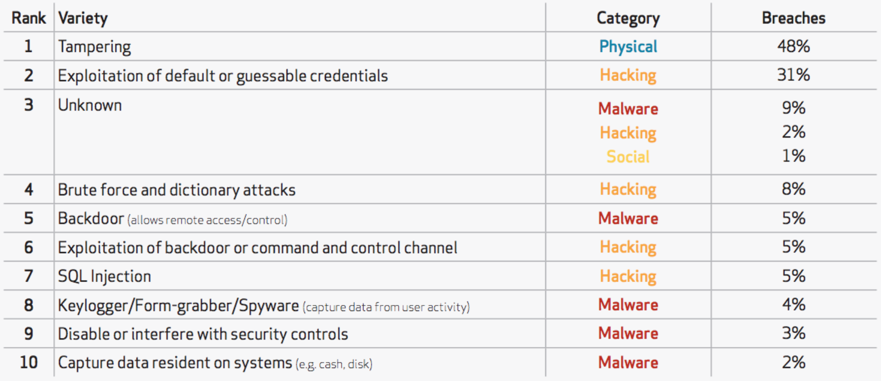
Business & Innovation

Risks include ***disruption in the availability of our online shopping sites on the internet, cyber attacks on our information systems, disruption in our supply chain,*** *including availability and transport of goods from domestic and foreign suppliers, trade restrictions, changes in tariff and freight rates.*

Wal-Mart, 2014 SEC 10-k

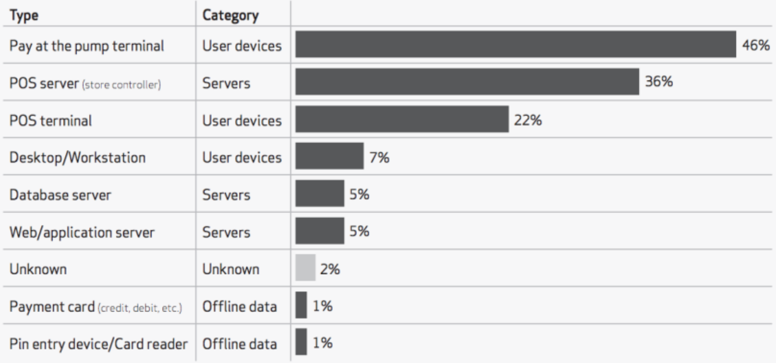
Cyber Threat Reality for Retail

Table 2. Threat action varieties by percent of breaches in the Retail Trade industry



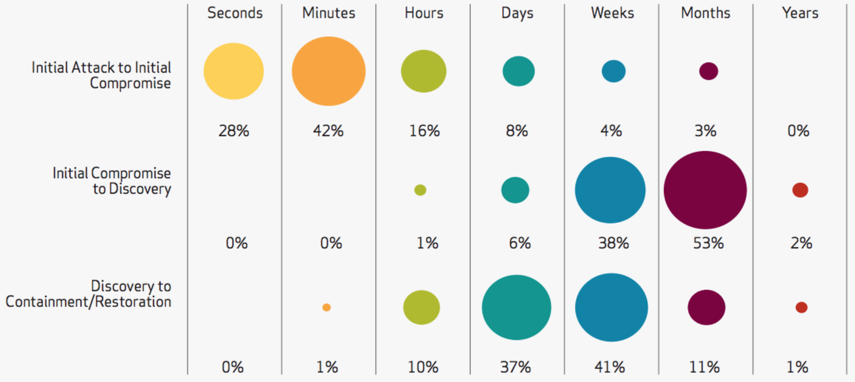
Rank	Variety	Category	Breaches
1	Tampering	Physical	48%
2	Exploitation of default or guessable credentials	Hacking	31%
3	Unknown	Malware Hacking Social	9% 2% 1%
4	Brute force and dictionary attacks	Hacking	8%
5	Backdoor (allows remote access/control)	Malware	5%
6	Exploitation of backdoor or command and control channel	Hacking	5%
7	SQL Injection	Hacking	5%
8	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	4%
9	Disable or interfere with security controls	Malware	3%
10	Capture data resident on systems (e.g. cash, disk)	Malware	2%

Figure 3. Compromised assets by percent of breaches in the Retail Trade industry*



*Assets involved in less than 1% of breaches are not shown

Figure 4. Timespan of events by percent of breaches in the Retail Trade industry



DBIR INDUSTRY SNAPSHOT:
RETAIL TRADE

A study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting & Information Security Service, Police Central e-Crime Unit, and United States Secret Service.

verizon

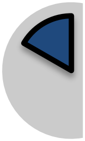
In this industry, with its large number of automated and opportunistic attacks, perpetrators have often been and gone before anyone realizes there's a problem.

In over two-thirds of cases, mere minutes—or even seconds—elapse before the victim's systems are infiltrated.

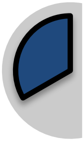
A high number of targets mixed with weak defenses creates a concoction irresistible to criminals.

FMI Members Are Committed!

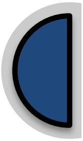
FMI members are taking the threat of cyber incidents seriously!



60% FMI members of the PCI Security Standards Council



79% An Employee or Team dedicated to Cyber Security



92% Initial Cyber Security Policy in place

The Food Industry is on the right path to securing its data, as evident by the following efforts:

- PCI Compliance
- Documenting How to Report an Incident, see FMI's Incident Response Framework
- Assigning dedicated resources to information security

Preparation, Response, and Recovery

Pre Breach
Incident Response
Post Breach

Thorough and effective incident response capabilities can minimize the damage to your company from a data breach.

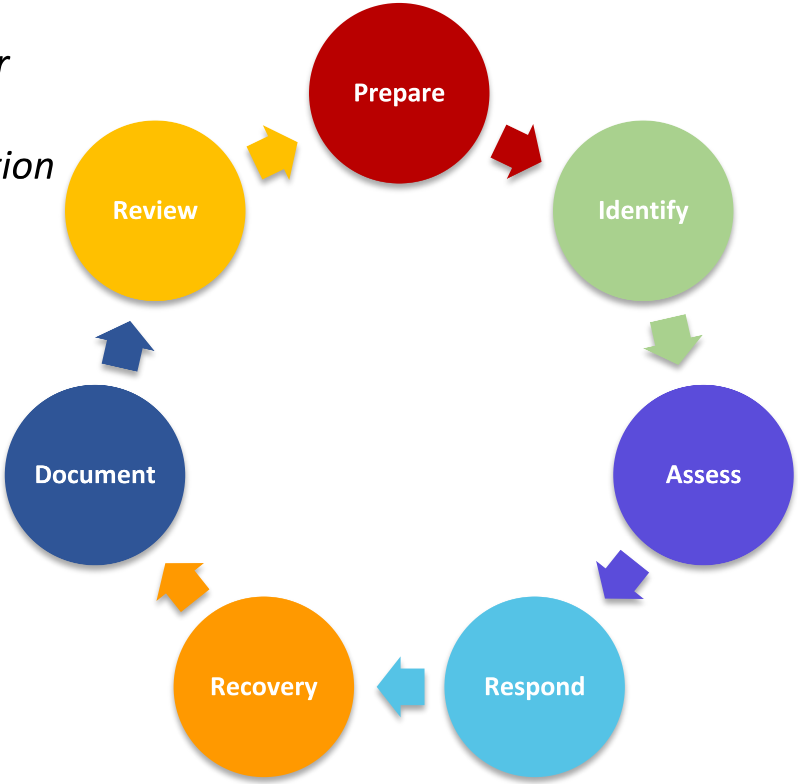
The FMI Incident Response Framework

Purpose of the Framework

The purpose of an incident response structure is to maintain awareness of incidents occurring on the your network, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore Information Technology (IT) services.

Overview of Structure

1. Prepare
2. Identify
3. Assess
4. Respond and Recovery
5. Document
6. Review



The FMI Incident Response Framework

Assembling the Incident Response Team (IRT)

Internal support

- Executive Management
- Corporate Communications
- Incident Response Manager* and Technical Staff
- Legal Counsel
- Compliance Staff
- Insurance Company

External support

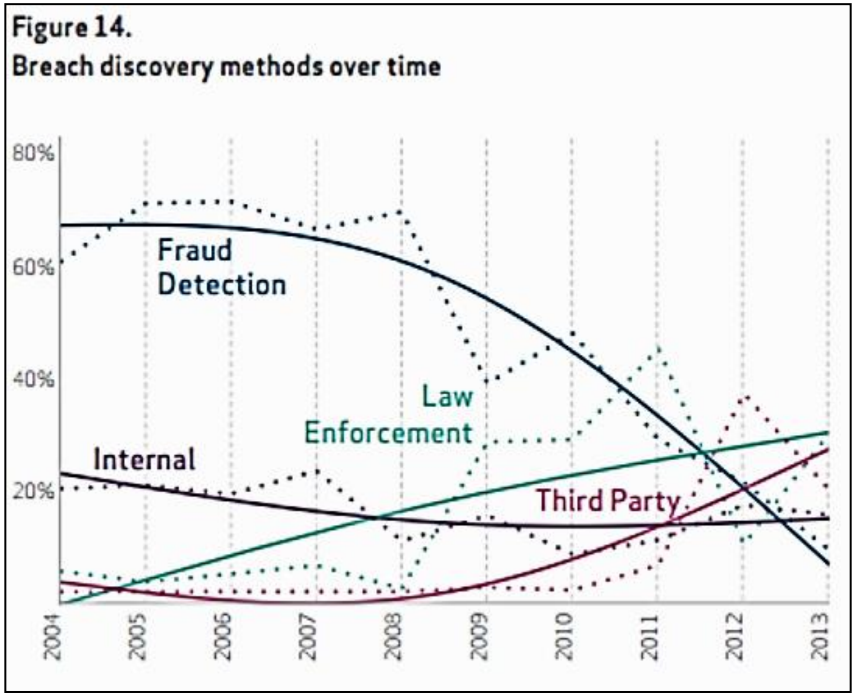
- Crisis PR
- Cyber Liability Insurance
- Legal Counsel
- Investigations and Forensics from Law Enforcement or Contractors

The FMI Incident Response Framework

- **Step 1: Preparation**
  - Well prepared teams to understand latest in cyber attacks and abnormal computer activity.
  - Preparation teams should implement risk-based security controls.
  - Education and awareness across the enterprise.
- **Step 2: Identify**
  - Does the incident threaten the confidentiality (C), integrity (I), or availability (A) of company (or third party) data?
- **Step 3: Assess**
  - What are the symptoms?
  - What may be the cause?
  - What is being impacted?
  - How widespread is it?
  - What part of the system or network is impacted?
  - Could this impact your business partners?

Incident Response Framework

- **Step 4: Respond**
  - Brief Corporate Leadership
  - Initial Response
- **Step 5: Recovery**
  - Changing all passwords associated with the incident that may have been compromised.
  - Conducting a vulnerability scan of the compromise machine/system before reconnecting to the network.
  - Recovery of data from backups.
  - Continued monitoring of the impacted system(s).
  - Documenting recovery procedures and change management information for any configuration changes.
  - Engaging third party experts for forensic examination and recovery of data.



2014 Verizon Data Breach Investigations Report

The FMI Incident Response Framework

- **Step 6: Document**
  - Best Practices from DHS Industrial Controls Systems Cyber Emergency Response Team (ICS-CERT):
    - Keep detailed notes
    - Capture live system data
    - Capture forensic images
    - Avoid running antivirus post-incident
    - Avoid making changes to the operating system, hardware or software
- **Step 7: Review**
  - Was the problem discovered in proper fashion?
  - Was the response appropriate?
  - Was enough information obtained?
  - Were steps properly executed?
  - What was the business impact?
  - Is the organization still vulnerable to a similar incident?

Incident Response Framework

- Questions?
- Comments?

Ready. Set. Go!

Table Top Exercises (TTX)

A tabletop exercise typically consists of a scenario, objectives, roles, and injects.

- Scenario: The backstory for the TTX to include an overview of the current environment and any assumptions that must be made.
- Objectives: The purpose of the table top exercise (e.g., test component X of our plan).
- Roles: The key roles that are involved in the TTX, the roles required are related to the objectives established.
- Injects: A pre-planned set of actions that guide the table top towards achieving the objectives.

SCENARIO 2:
PAYMENT CARD COMPROMISE

Scenario 2: Payment Card Compromise

- Scenario: A nation state actor is attacking the retail sector to gain payment card data to sell on the black market.
- Objectives:
  - Understand the role of the US Secret Service.
  - Craft talking points and public statements for post-breach crisis communications.
  - Understand and monitor your company’s social media page for reputational risk.

Scenario 2

- **Inject #1: (Directed to IT and Management)**
  - The United States Secret Service (USSS) reaches out to your organization’s management/ operations and informs them that they have seen activity that leads them to believe that your customers’ data is currently being used on the black market.
  - Based on similar incidents, the USSS suggests that your organization’s IT infrastructure has been breached for some time.

Scenario 2

- **Inject #2: (Directed to IT)**
  – Your internal IT Team or 3rd Party Security Service provider begins investigating and discovers that there is a high likelihood that an external party has utilized a compromised Web site to "taste" credit card numbers for validity.

Scenario 2

- **Inject #3: (Directed to IT and Communications)**
  - – A security vendor releases a statement about the attack and breach effecting your company.

Scenario 2

- **Inject #4: (Directed to Communications)**
  - A day later, explicit demands are sent to your company via Twitter.
  - These demands include corporate information and customer data.
  - They have tagged national cable news channels in their tweets.

Scenario 2

- **Inject #5: (Directed to Communications and Management)**
  - The local and national media have begun calling and requesting quotes from executives and further information from your front office.

Scenario 2

- **Inject #6: (Directed to Communications and Management)**
    - Your CEO requests that the internal Incident Response Team in coordination with corporate leadership provide the public with a statement regarding the breach.

Hot Wash

- Strengths of your organization?
- Do you have the internal support and subject matters necessary to respond to a breach?
- Who would you communicate with during an incident?
- Areas for improvement?
- Did the Incident Response Plan help you work through the incident?

Final Thoughts

- Best Practices
  - FMI Incident Response Framework
  - Creating a "Neighborhood Watch Program"
  - Testing the Incident Response Capability
- Final comments and remarks.

Thanks!!

Contact Information

Theresa Payton

CEO and Chief Advisor

Vince Crisler

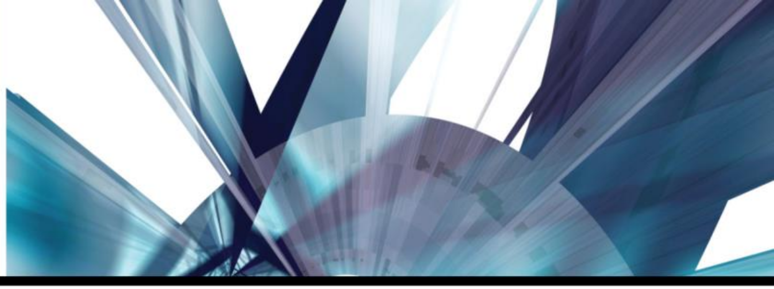
Partner

☎ (877) 487-8160

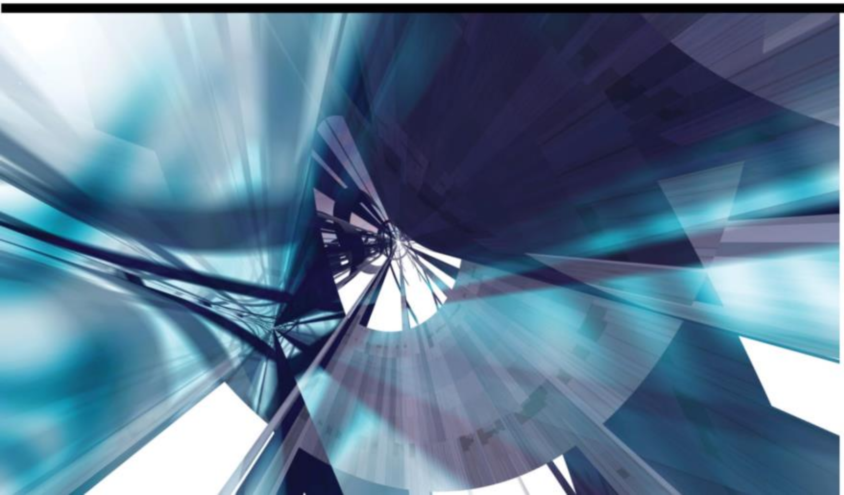
🌐 http://www.fortalicesolutions.com

✉ watchmen@fortalicesolutions.com

🐦 @fortalicellc



APPENDIX



Incident Response Framework

What is an incident?

•“A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

– An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

– Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

– An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

– A user provides or exposes sensitive information to others through peer-to-peer file sharing services”.

Incident Response Framework

- Authorities and Role of the IRT
  - Coordination with key partners in law enforcement.
  - Coordination with financial institutions (if payment information has been compromised).
  - Coordination with health care providers (if pharmaceutical information has been compromised).
  - Vendor/Supplier Management (if they are the source of the incident and/or impacted by the incident).
  - Intrusion Detection.
  - Advisory Distribution.
  - Education and Awareness.
  - Information Sharing.
  - Triage Management.