

## About the Presenter



- Michael A.L. Balboni is the President & Managing Director of RedLand Strategies, a full-service consulting firm focused on homeland security, government relations, and business development
- Former Deputy Secretary of Public Safety, Homeland Security Advisor for New York State & New York State Senator

## The Exposure: Storage and Protection of Data

- Traditional concerns are not the only problems organizations are facing
- Today, security issues related to the protection and security of data are major problems faced by owners/administrators
- Proper due diligence must be conducted on selected service providers in order to prevent any security issues



**An owner/administrator's responsibility does not require a crash course in encryption.**

**But they should know the questions to ask...and ask them.**

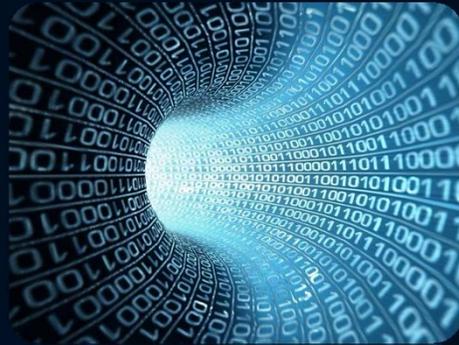
## **Cyber Law is Constantly Changing**

- Regulator compliance (FTC, SEC, HIPA, NIST)
- State statutes
- Litigation and insurance
- The bad guys (state actors, Al Qaeda, ISIS)

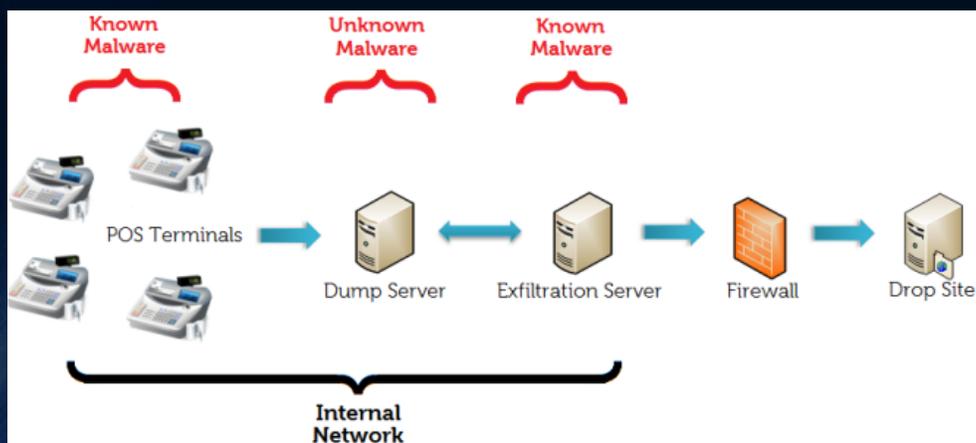


## Securing Electronic Data Has Three General Elements:

1. Managing the data
2. Securing the operating systems
3. Managing the people who interact with the data



## The Threat: Data Exfiltration



# How to Manage Data Exfiltration

## Information Security relies on Static Defense

- Intrusion Detection Systems
- Antivirus Software
- “The Kill Chain”

## “The Kill Chain”

- Can serve as a cyber security defense tool
- Assumes that attackers have an inherent advantage

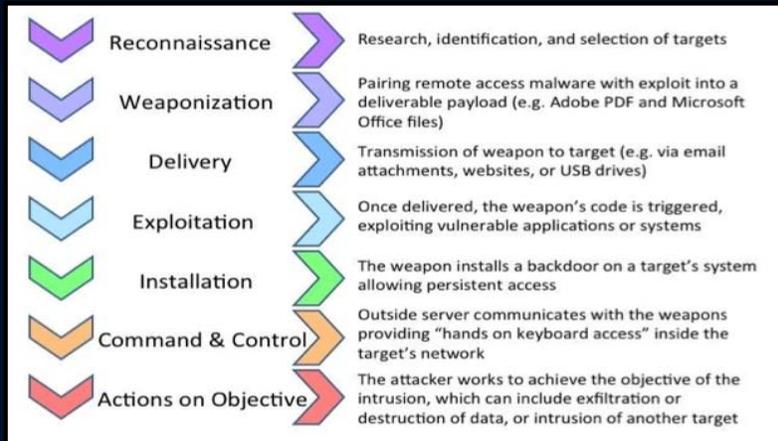


## Intrusion “Kill Chain”



This diagram lays out the process a hacker must go through to plan and execute an attack.

## Phases of the Intrusion "Kill Chain"



The defender only has to stop one of these steps in order to prevent the attack.

## The Tool Box

### Three Legs to the Cyber Security Stool

1. CEO buy-in and Employee Training
2. Internal Cyber Security Architecture
3. Threat and Use Monitoring



## Data Security & Management

Organizations must be certain that service providers are protecting data both in flight and at rest. "End to End" encryption.

### Encryption

- Are policies in place regarding encrypting sensitive data?
- Is the data stored in an encrypted state?
- NOT ALL ENCRYPTION IS EQUAL!



## Physical Security

### Physical security measures to protect sensitive data

- How secure is this facility that houses the data?
- How is printed data stored?
- Fiduciaries should request this general information.

### Data breaches can start with lost or stolen laptops

- What sort of protection is used for portable computing hardware?
- Are computers, phones, and tablets password – protected and encrypted?



## Personnel Management

### Employee Access

- What are the service providers internal audit protocols?
- Any restrictions on what material employees have access to?

### Passwords

- Are guidelines in place to enforce "strong" passwords?



## The Cloud Conundrum

- The Cloud has the promise of dramatically increased agility, information access and reduced costs. But is it safe?
- Many Cloud providers are developing security systems that are backed into their operations. One real advantage is vendor management. In this regard, certain cloud systems apply the same access protocols to all third party vendors that are utilized internally.
- Experts warn against placing all your eggs in one basket. Using multiple cloud platforms might increase costs, but doing so will provide reassurance.



## What have Courts Found Liability For?

- Failure to encrypt data
- Unnecessarily long storage periods
- Unauthorized users
- Inadequate ID verification programs
- Vulnerable storage data format for more than 30 days
- Failure to provide security for known threats
- Failure to maintain adequate access security
- Storing unnecessary data in multiple unsecured and unencrypted formats
- Failure to use readily available security measures (pen testing?)
- Failure to notify post-breach

## Seven Key Questions in Cyber Security

1. What protections systems are currently running on the system/network?

## Seven Key Questions in Cyber Security

2. Has a "core transactional analysis " been developed, which prioritizes key functions?

## Seven Key Questions in Cyber Security

3. Who owns the responsibility for the security?

## Seven Key Questions in Cyber Security

4. Have employees received training with interval refreshers regarding threats such as phishing and low level persistent threats?

## Seven Key Questions in Cyber Security

5. Are vendors required to provide their cyber security plans and protocols?

## Seven Key Questions in Cyber Security

6. Has the company performed an access point analysis for the system?

## Seven Key Questions in Cyber Security

7. Has a plan for breach response, recovery, mitigation, and notification been developed?

If so, has the plan been supported by sufficient exercise and training procedures?

