Secure Cyber Defense, LLC

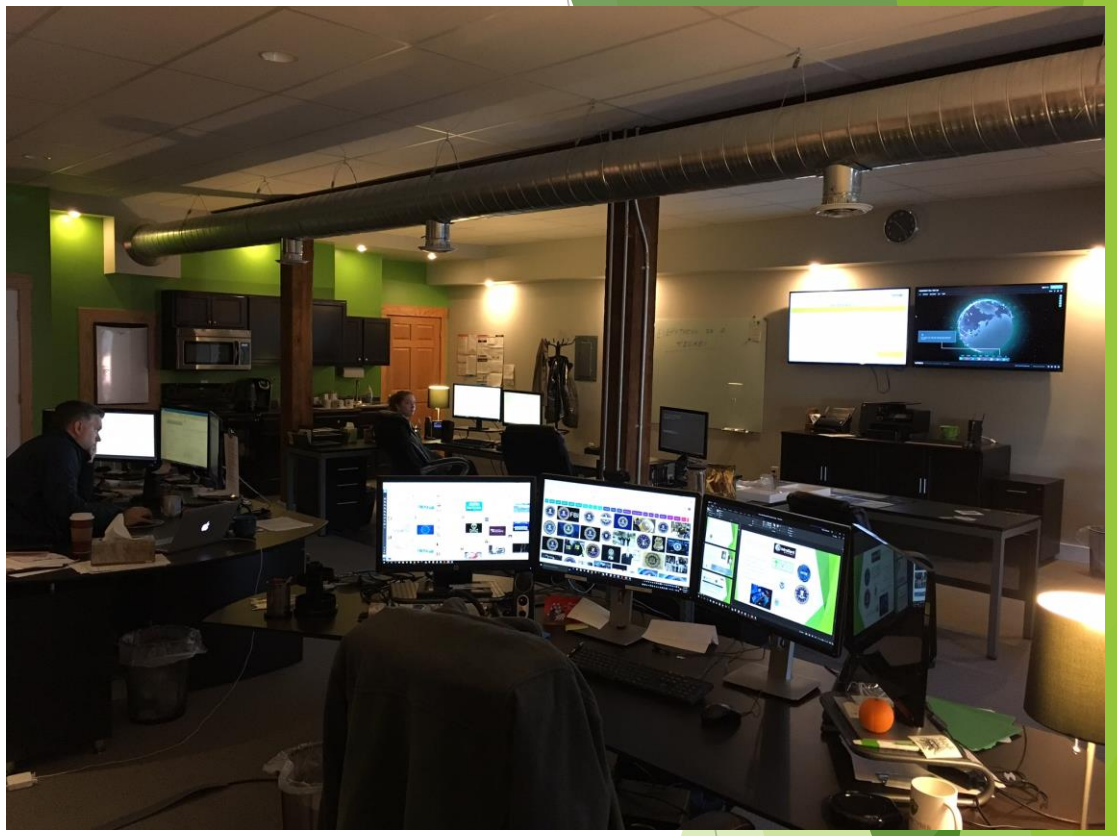
CyberSecurity Workshop: Incident Response

SECURECYBER
DEFENSE

Shawn Waldman – CEO
Shawn.Waldman@securecyberdefense.com
937-388-4405

Who are we?

- We are NOT an MSP
- Founded Jan 1 2015
- Founders former Law Enforcement and Military
- Dedicated to the small to mid-market
- Affordable entry to advanced Cybersecurity solutions
- Regions only small business Cyber firm



SECURECYBER
DEFENSE

CYBER SECURITY FOR YOUR BUSINESS

Your organization will be hacked, what you do right now will determine if you and your organization end up in the headlines and on the wrong side of a press release.

A Word About Security

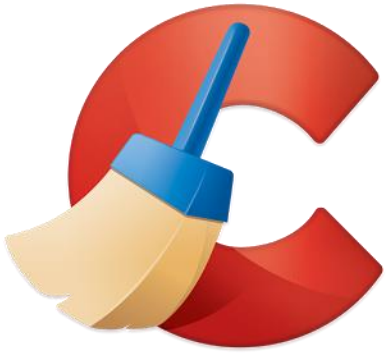
- It's a Layered Approach
- It's Continuous
- It's Not Popular
- It's Not Convenient
- It Doesn't Have to be Expensive
- Do What is Reasonably Required

Data Breach History

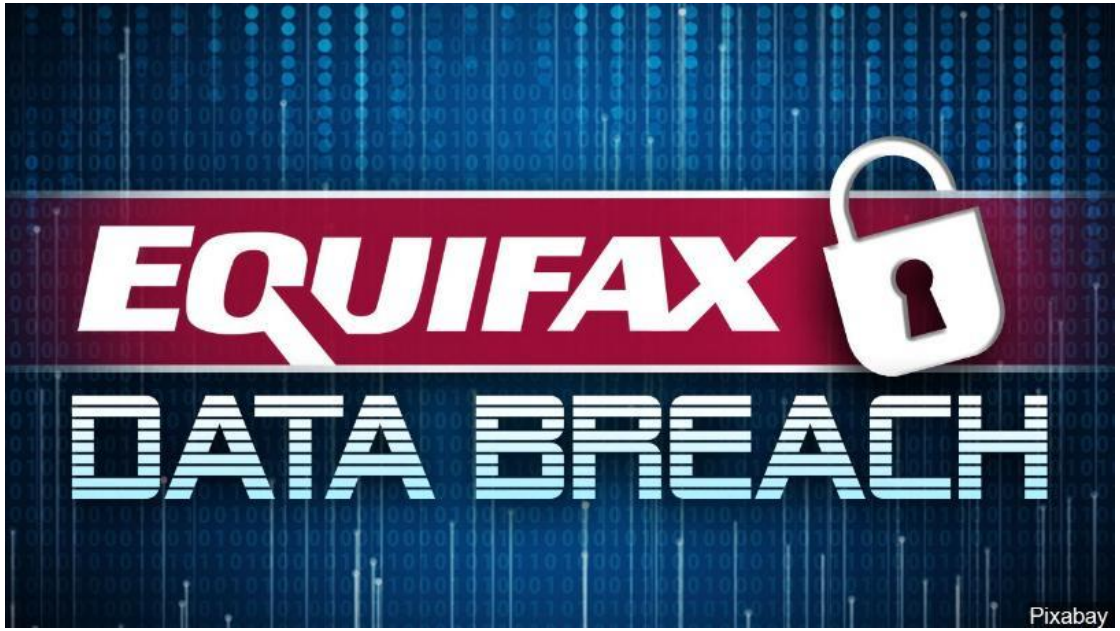
- EquiFax
- HBO
- Anthem (80 million records)
- OPM
- Uber
- Dow Jones
- E-Trade
- Scottrade

Today's Threats

- Ransomware/Cryptolocker
- W2 Scam
- CEO Fraud
- Apache Struts
- CCleaner

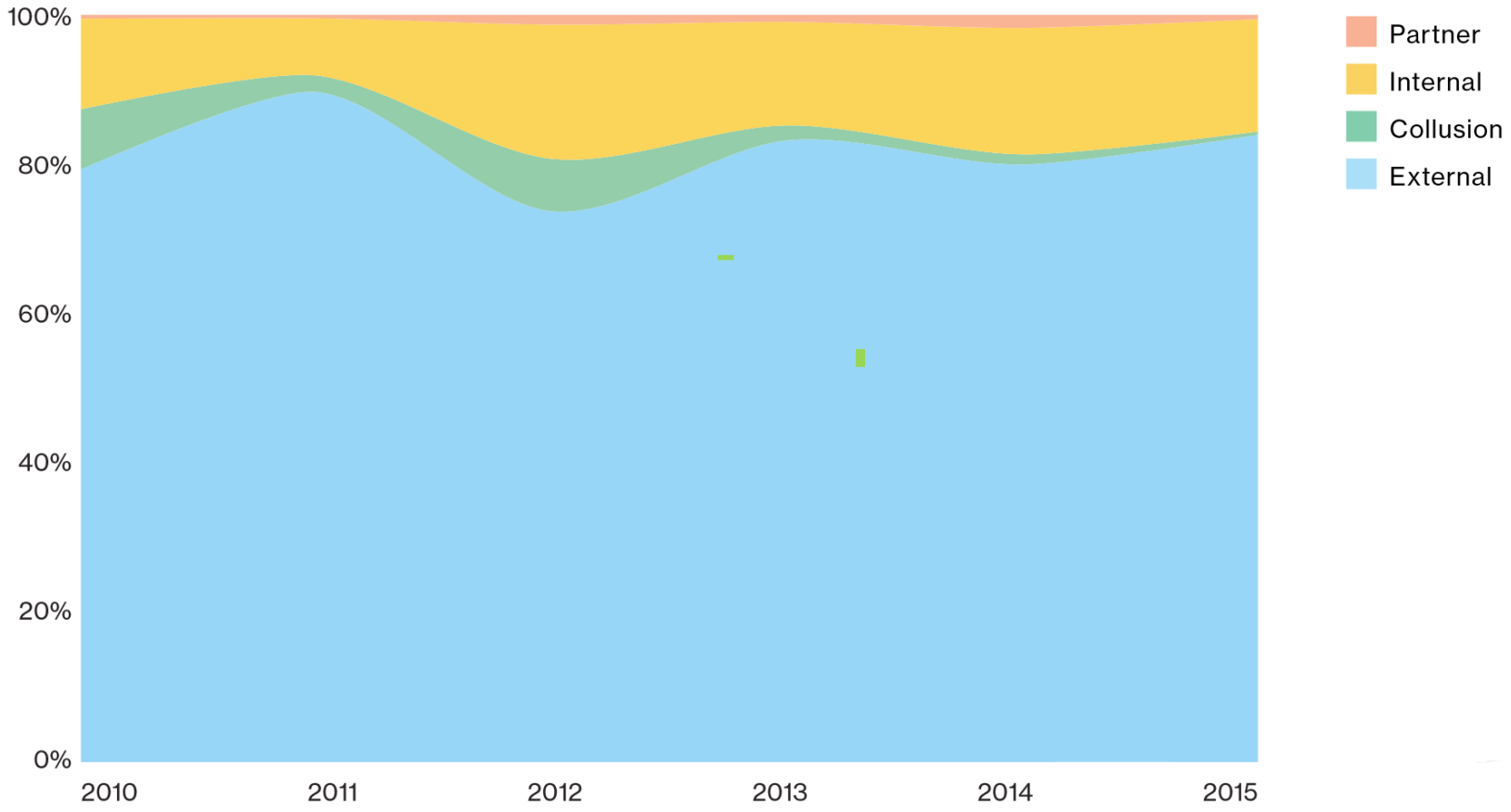


EquiHacked

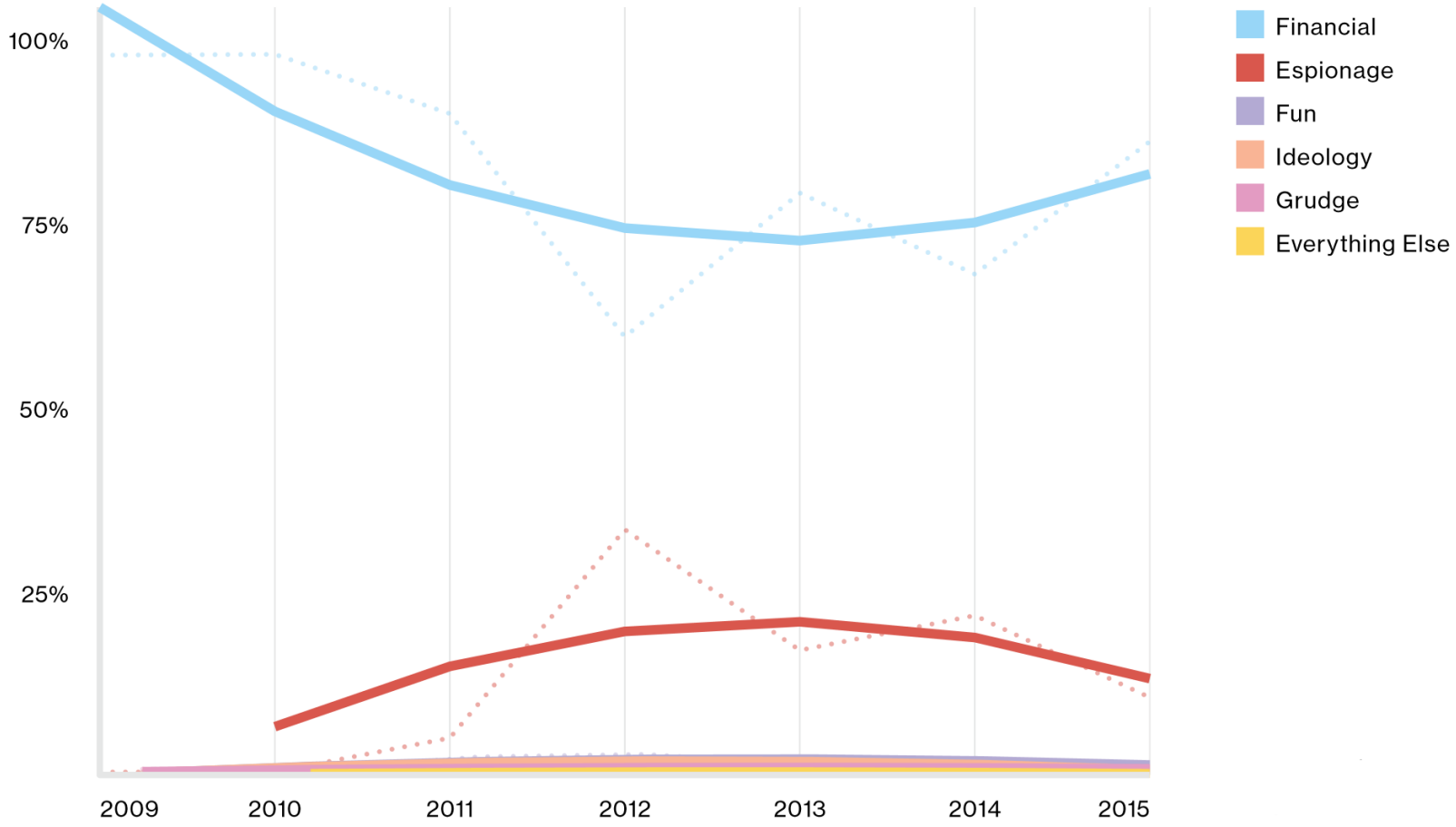


- Over 143 Million Americans, UK and Canadian Citizens Effected
- Breach was the result of an unpatched Apache Struts Vulnerability
- It was known for over 45 days that someone had compromised Equifax
- Equifax failed at Incident Response
- Equifax failed at public relations
- Equifax failed at Cyber Security

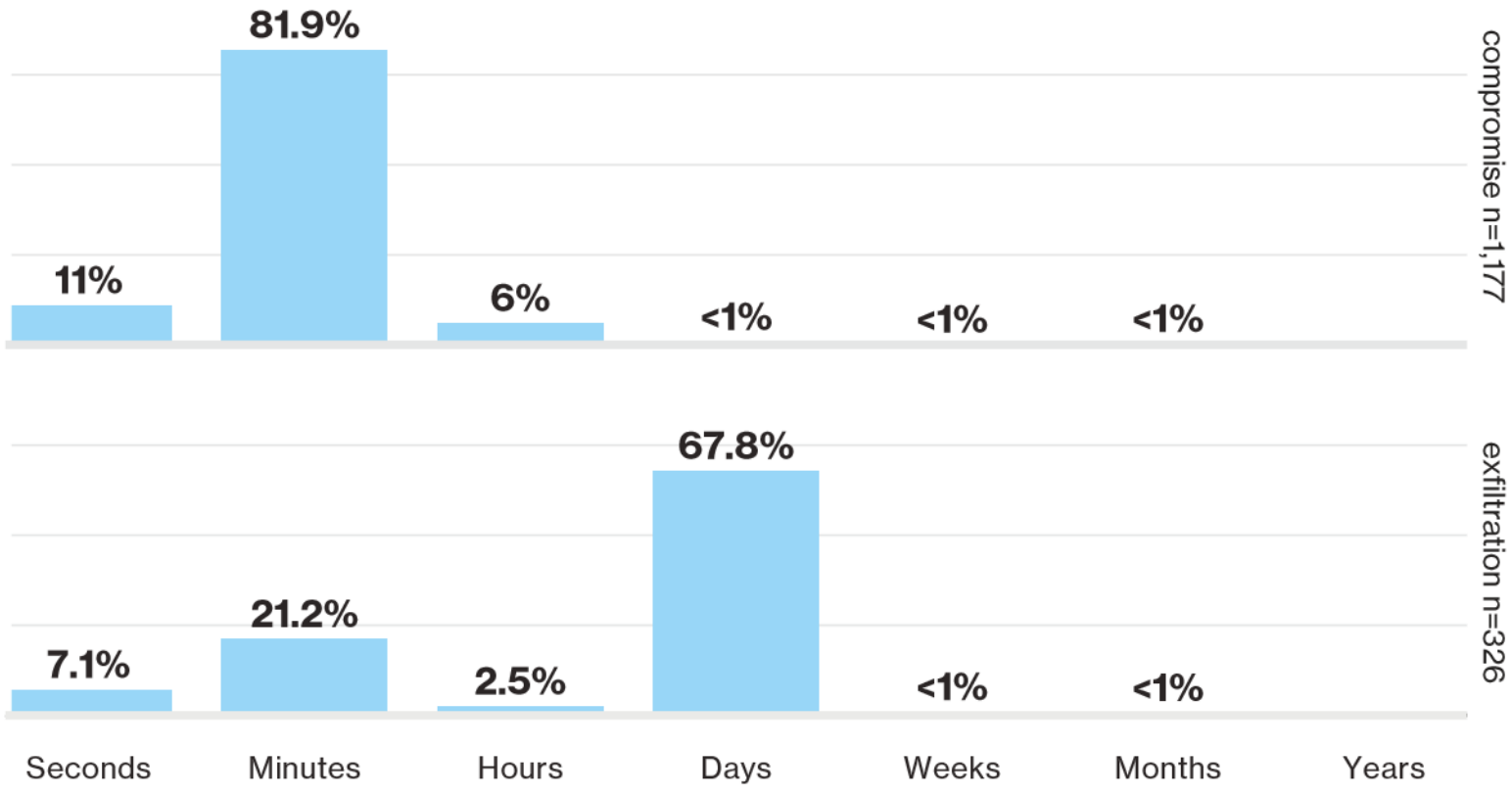
Breach Vector



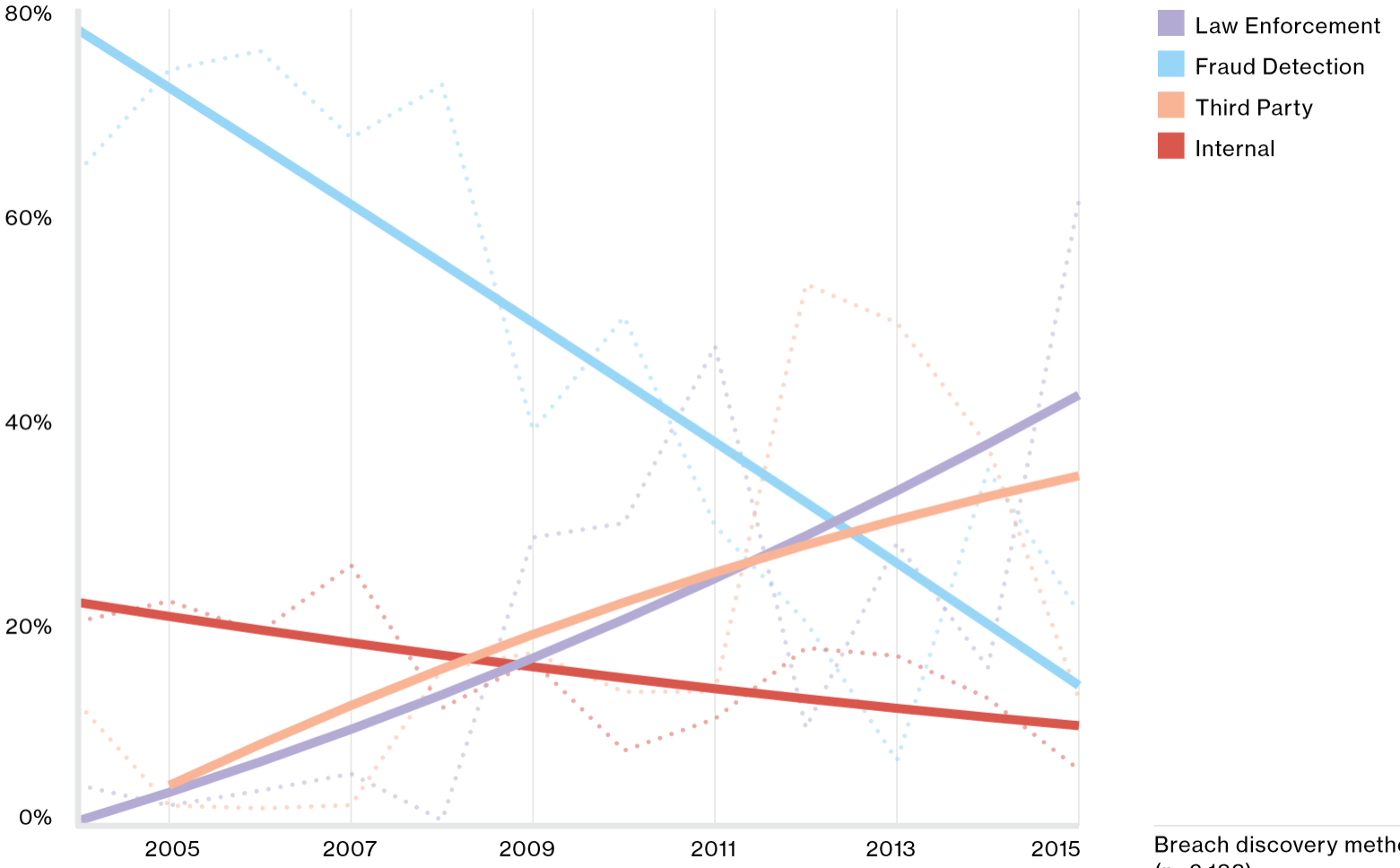
Why are they attacking me?



Compromise vs. Exfiltration



Breach Notification Methods



Breach discovery methods over time, (n=6,133).

Incident Response

The need for Incident Response (IR)

- Recover Quickly from an Incident
- Implement a Pre-Planned Strategy
- Protect the Company's Interests
- Maintain Compliance

Focus Areas for IR

- Scope and Purpose
- IR Roles and Responsibilities
- Internal Stakeholders
- External Entities
- IR Process Flow/Phases
- Revision History
- Stakeholder Contact List
- First Responder Checklist
- Incident Report Template
- Evidence/Chain of Custody

Incident Response Demo

Ransomware Attack

1

A user calls the help desk and tells you that something is happening to her PC. Boxes are flashing and icons are appearing on her desktop. While on the call they report that there is a red screen with an FBI logo on it telling them that all their files are encrypted and saying something about Bitcoin.

2

What is your response?

3

Let's Discuss This!

Incident Response Process

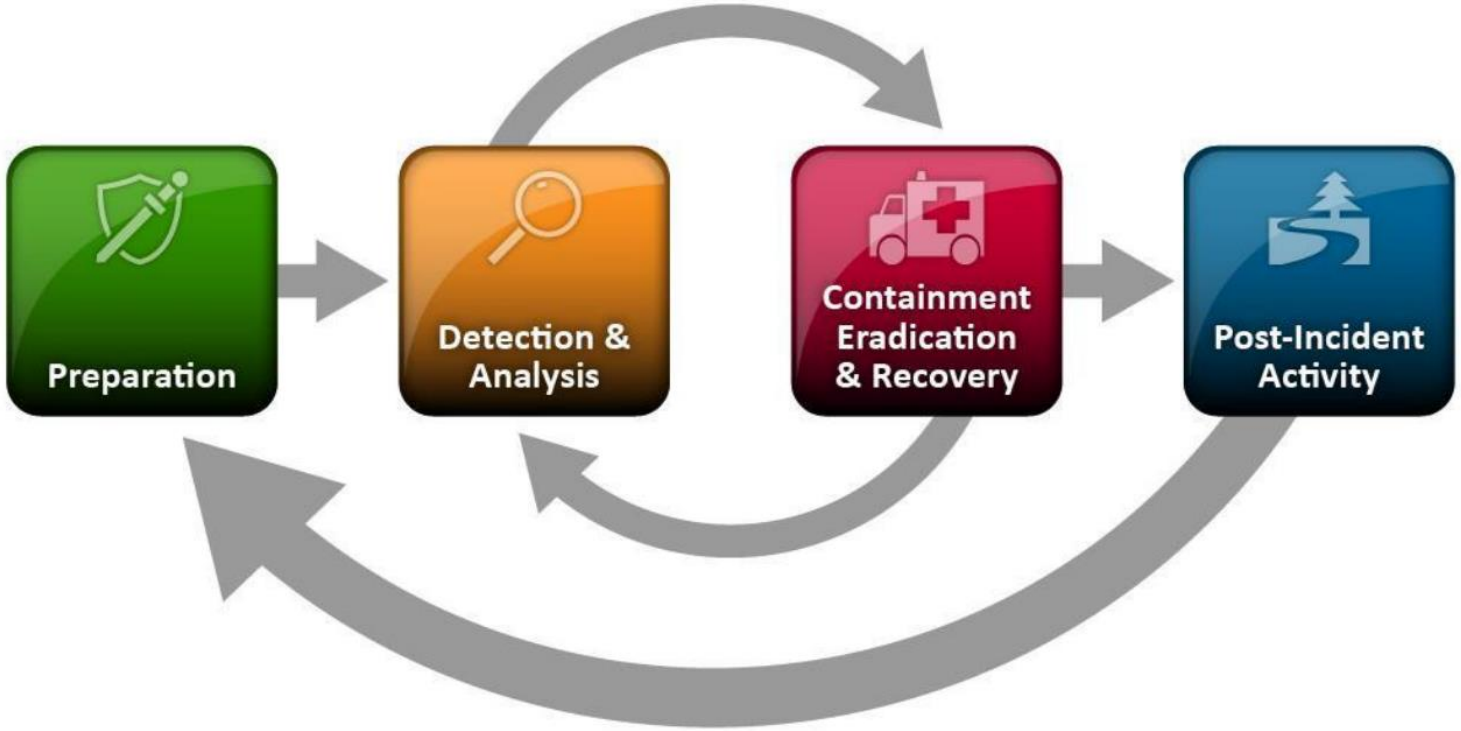
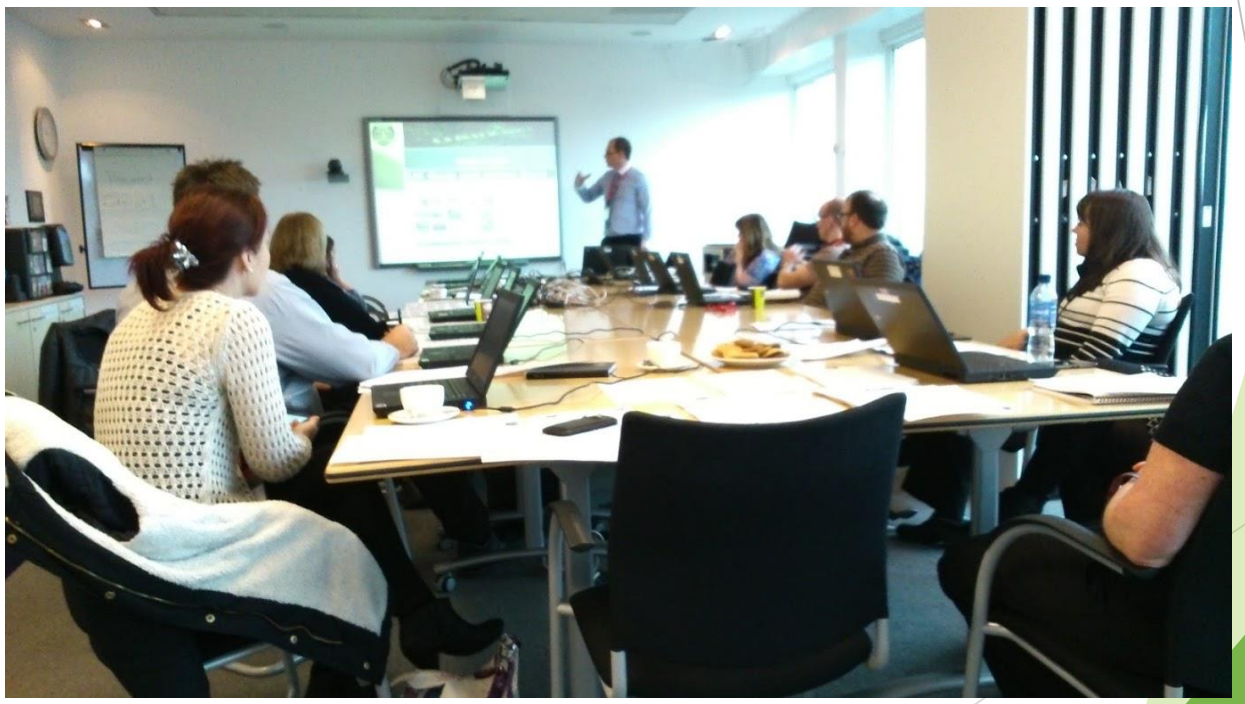


Table Top Exercises

- Practice against real-world scenarios
- Non-IT exposure
- See holes in the process
- Go-Bag testing
- Tweak documentation



Training

- Keep staff up-to-date
- Include Newsletters with Tips
- Show examples of real threats
- Practice phishing employees
- Measure training and controls effectiveness

Where do you start?

- Know Your Environment
  - Hardware and Software
  - Documentation
- Patches
  - Both Microsoft AND
  - 3rd Party Patches
- Vulnerability Assessment
  - Know Your Weaknesses

Where do you start?

- Secure Wireless Access
  - Disable Broadcasting
  - Enable Encryption
  - Reduce Power
  - Enable a Guest Network
- Backups! Backups! Backups!
  - Test Them
  - Have both on and offsite copies
- Limit Administrator Access

Where do you start?

- Firewalls
  - Not Set it and Forget it
  - Continuous Updates Needed
  - Auditing and Change Control
- Log Monitoring
- Incident Response and Policy
- Training
- New! - Sandboxing

Cyber Security Then vs. Now

- Then
  - Firewall
  - AntiVirus
  - Email Scanning
- NOW!
  - Monitored UTM Firewall
  - Active AntiVirus
  - Multiple Email Scanners or a Sandbox
  - Proactive/Auto-Quarentining solutions when business rules are not met
    - Too many missing patches

Staying Updated

- FBI Cyber Liaison Program
- FBI Infraguard
- Open Threat Exchange
- US-Cert/Homeland Security
- Twitter
- National Vulnerability Database

InfraGard
Secure Network ®

OPEN THREAT EXCHANGE

US-CERT
United States
Computer Emergency Readiness Team

FINANCIAL SERVICES ISAC

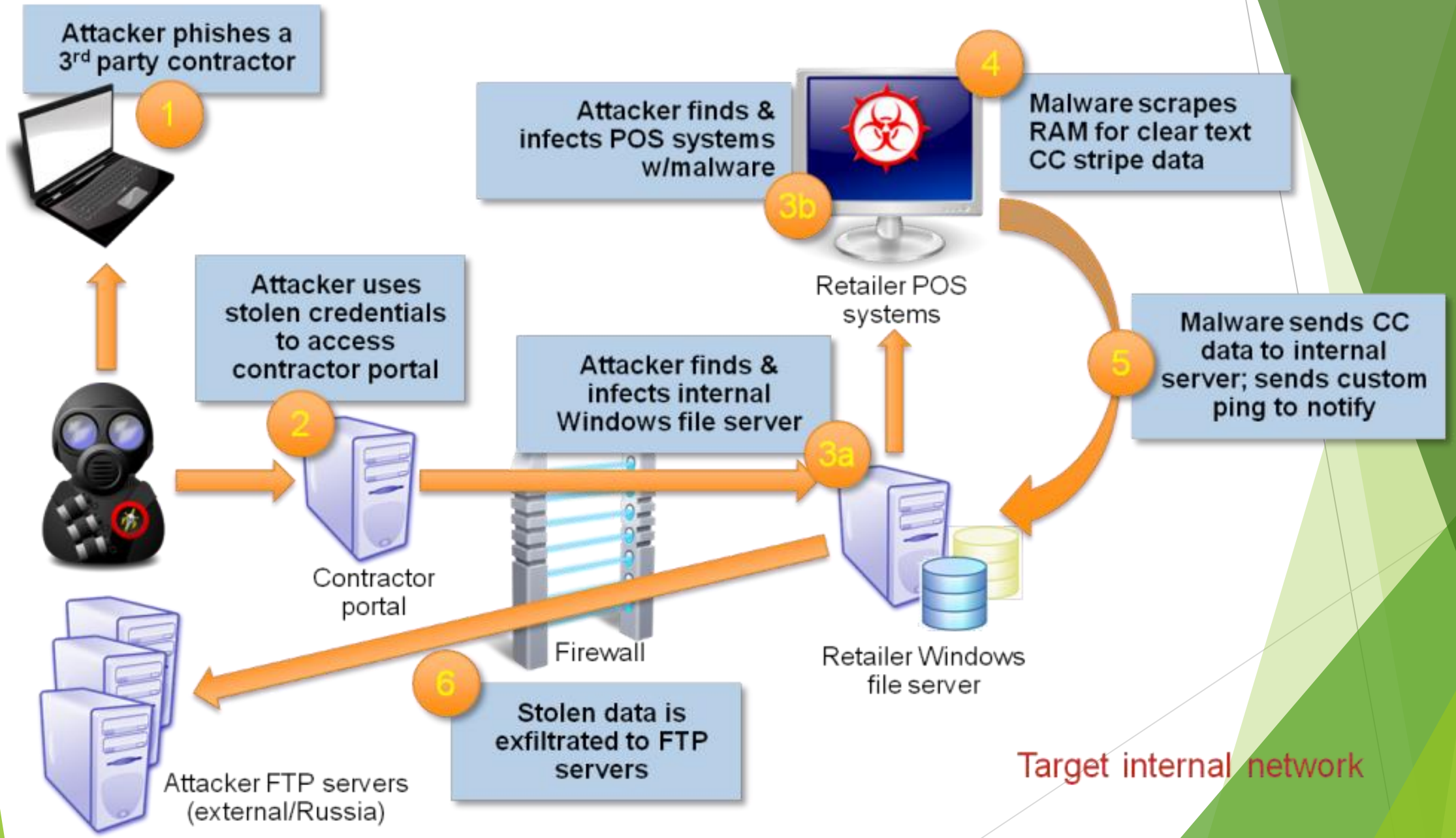
Cyber Insurance

- Know your policy
- Fill out the assessment accurately
- Have a lawyer review the policy
- Get it!

Target Hack Stats

- 40 million credit/debit cards
- 70 million personal records
- 100 million to upgrade system
- Chip and Pin wouldn’t help

Anatomy of the Target Retailer Breach



Helpful Links

- *There are numerous publications available to assist in the hardening of Windows devices. Things like uninstalling services and software titles that aren't in use go great lengths to reducing your cyber exposure. Below are some guides that are publicly accessible.*
- *Guide to General Server Security - http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf*
- *National Checklist Program Repository - https://web.nvd.nist.gov/view/ncp/repository*
- *The Checklist Program Repository will allow you to access detailed secure configuration guides for almost any software title available. These configurations are approved by the National Institute of Standards and Technology SP 800-70 Rev. 3.*