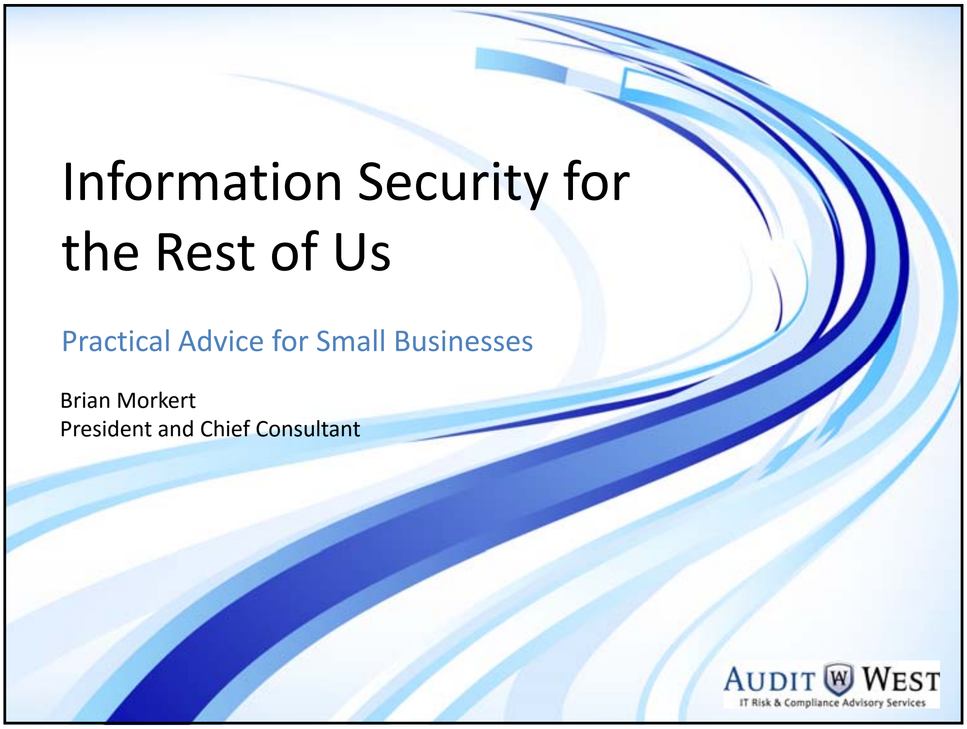
AUDIT WEST

IT Risk & Compliance Advisory Services

Secure… Your Way Forward.

AuditWest.com



Information Security for the Rest of Us

Practical Advice for Small Businesses

Brian Morkert
President and Chief Consultant

AUDIT WEST
IT Risk & Compliance Advisory Services

Introduction

President – Audit West
- IT Audit
- Security Assessment
- Incident Response & Forensics
- Consulting Services

Director of Security Services – GCSIT Solutions
- Managed Security Consulting Services

Senior Consultant – Parametrix, Inc.
- IT Project Management
- InfoSec Management

AUDIT WEST
IT Risk & Compliance Advisory Services

Agenda

- Attack Lifecycle
- Types of Attacks
- Traditional AV and Firewalls Don’t Work
- Testing – What is Appropriate
- Security Awareness Training
- Managed Services and Outsourcing
- Incident Response

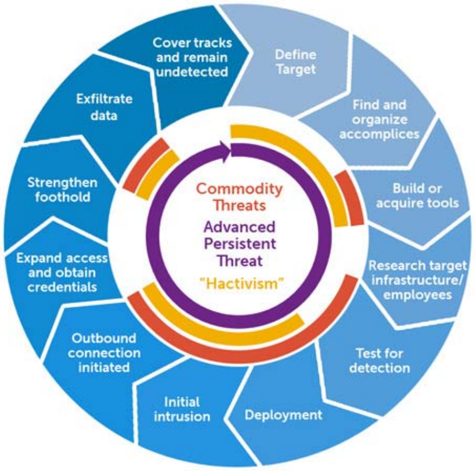
AUDIT WEST
IT Risk & Compliance Advisory Services

The Value of Information

- CC Information
- Banking Information
  - ACH Fraud
- Personal Information
  - Identity Theft
  - Account Hijacking
- Credentials
- Extortion
  - Ransomware
- Account Hijacking
- Industrial Espionage

AUDIT WEST
IT Risk & Compliance Advisory Services

Attack Lifecycle


Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Source: https://en.wikipedia.org/wiki/Advanced_persistent_threat

AUDIT WEST
IT Risk & Compliance Advisory Services

Attack Lifecycle

- Deployment to exfiltration can happen in minutes
- Most businesses never detect attacks
- Assume compromise
- 243 – Median number of days a breach is active before detection. Some as long as 5 years.

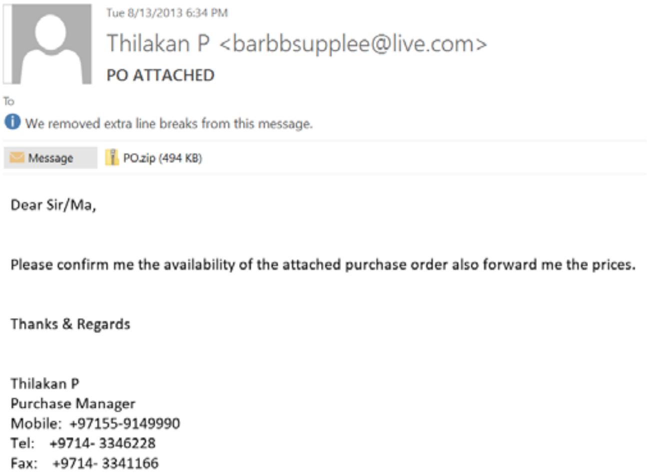
AUDIT WEST
IT Risk & Compliance Advisory Services

Threat Actor Tactics

- Watering Hole Attacks
- Social Engineering / Phishing
- 3rd party vendors (Target)
- Zero Day Malware
- Exploit Kits
- Stolen Equipment
- Stolen Credentials
- Insider
- Ransomware

AUDIT WEST
IT Risk & Compliance Advisory Services

Threat Actor Tactics



Tue 8/13/2013 6:34 PM

Thilakan P <barbbsupplee@live.com>

PO ATTACHED

To

We removed extra line breaks from this message.

Dear Sir/Ma,

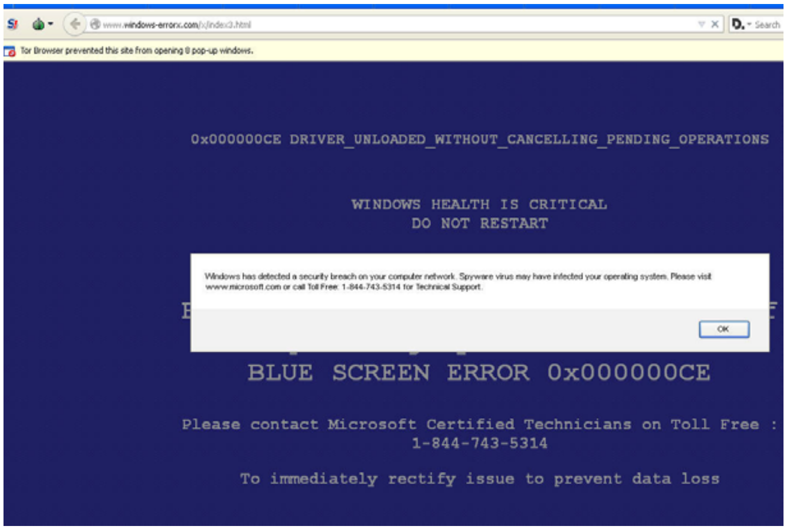
Please confirm me the availability of the attached purchase order also forward me the prices.

Thanks & Regards

Thilakan P
Purchase Manager
Mobile: +97155-9149990
Tel: +9714- 3346228
Fax: +9714- 3341166

AUDIT WEST
IT Risk & Compliance Advisory Services

Threat Actor Tactics



Tor Browser prevented this site from opening 0 pop-up windows.

0x000000CE DRIVER_UNLOADED_WITHOUT_CANCELLING_PENDING_OPERATIONS

WINDOWS HEALTH IS CRITICAL
DO NOT RESTART

Windows has detected a security breach on your computer network. Spyware virus may have infected your operating system. Please visit www.microsoft.com or call Toll Free: 1-844-743-5314 for Technical Support.

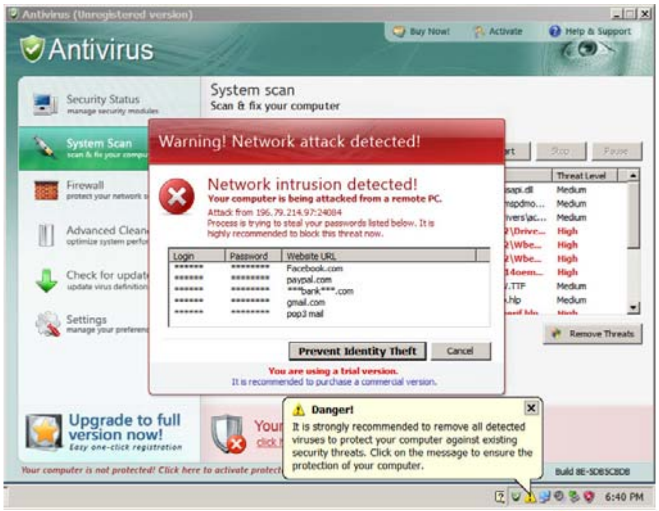
BLUE SCREEN ERROR 0x000000CE

Please contact Microsoft Certified Technicians on Toll Free :
1-844-743-5314

To immediately rectify issue to prevent data loss

AUDIT WEST
IT Risk & Compliance Advisory Services

Threat Actor Tactics



System scan
Scan & fix your computer

Warning! Network attack detected!

Network intrusion detected!
Your computer is being attacked from a remote PC.
Attack from 196.79.214.97:24084
Process is trying to steal your passwords listed below. It is highly recommended to block this threat now.

Login	Password	Website URL
******	*********	Facebook.com
******	*********	paypal.com
******	*********	***bank***.com
******	*********	gmail.com
******	*********	pop3 mail

	Threat Level
sapi.dll	Medium
nspdmo...	Medium
ivers\ac...	Medium
2\Drive...	High
2\Wbe...	High
2\Wbe...	High
14oem...	High
.TTF	Medium
.hlp	Medium

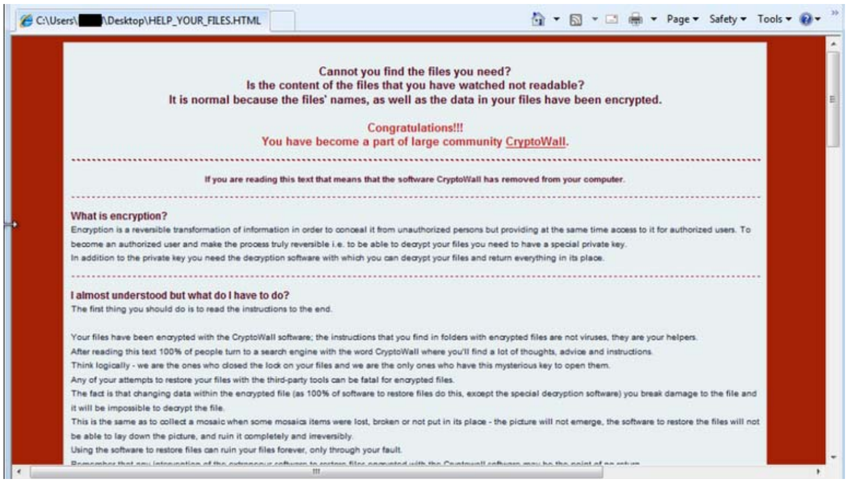
You are using a trial version.
It is recommended to purchase a commercial version.

Danger!
It is strongly recommended to remove all detected viruses to protect your computer against existing security threats. Click on the message to ensure the protection of your computer.

Your computer is not protected! Click here to activate protect

Build 8E-5D85C8D8

Threat Actor Tactics



Cannot you find the files you need?
Is the content of the files that you have watched not readable?
It is normal because the files' names, as well as the data in your files have been encrypted.

Congratulations!!!
You have become a part of large community CryptoWall.

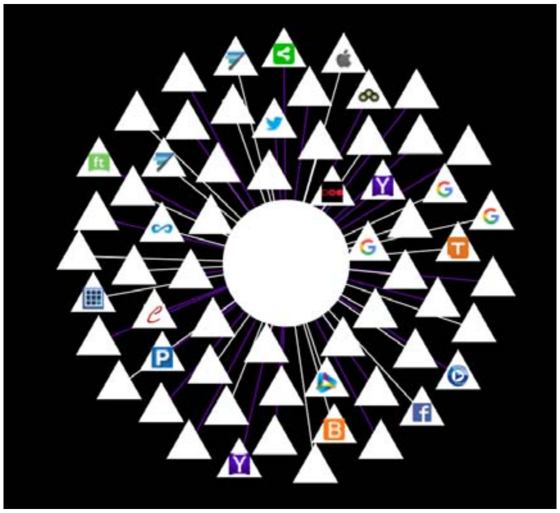
If you are reading this text that means that the software CryptoWall has removed from your computer.

What is encryption?
Encryption is a reversible transformation of information in order to conceal it from unauthorized persons but providing at the same time access to it for authorized users. To become an authorized user and make the process truly reversible i.e. to be able to decrypt your files you need to have a special private key.
In addition to the private key you need the decryption software with which you can decrypt your files and return everything in its place.

I almost understood but what do I have to do?
The first thing you should do is to read the instructions to the end.

Your files have been encrypted with the CryptoWall software; the instructions that you find in folders with encrypted files are not viruses, they are your helpers.
After reading this text 100% of people turn to a search engine with the word CryptoWall where you'll find a lot of thoughts, advice and instructions.
Think logically - we are the ones who closed the lock on your files and we are the only ones who have this mysterious key to open them.
Any of your attempts to restore your files with the third-party tools can be fatal for encrypted files.
The fact is that changing data within the encrypted file (as 100% of software to restore files do this, except the special decryption software) you break damage to the file and it will be impossible to decrypt the file.
This is the same as to collect a mosaic when some mosaics items were lost, broken or not put in its place - the picture will not emerge, the software to restore the files will not be able to lay down the picture, and ruin it completely and irreversibly.
Using the software to restore files can ruin your files forever, only through your fault.

Light Beam Demo…



AUDIT WEST
IT Risk & Compliance Advisory Services

Data Breach

An incident in which sensitive, protected or confidential ***data*** *has* *<u>potentially been viewed, stolen or used by an individual unauthorized to do so</u>*.

AUDIT WEST
IT Risk & Compliance Advisory Services

Security Incident

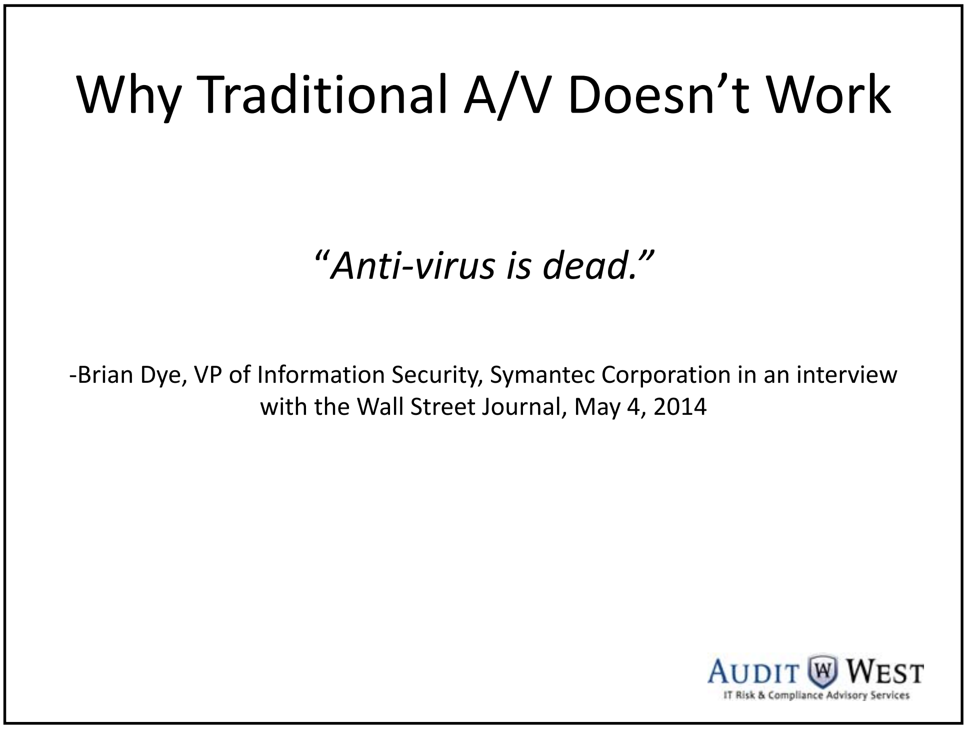
*An event that impacts the **Confidentiality, Integrity,** or **Availability** of an information resource or asset.*

AUDIT WEST
IT Risk & Compliance Advisory Services

Incident Identification

- Identified by CC Provider (CPP)
- 3rd Party Monitoring
- NextGen Firewall Appliances
- NetFlow Data
- Suspicious Activity
- Malware

AUDIT WEST
IT Risk & Compliance Advisory Services

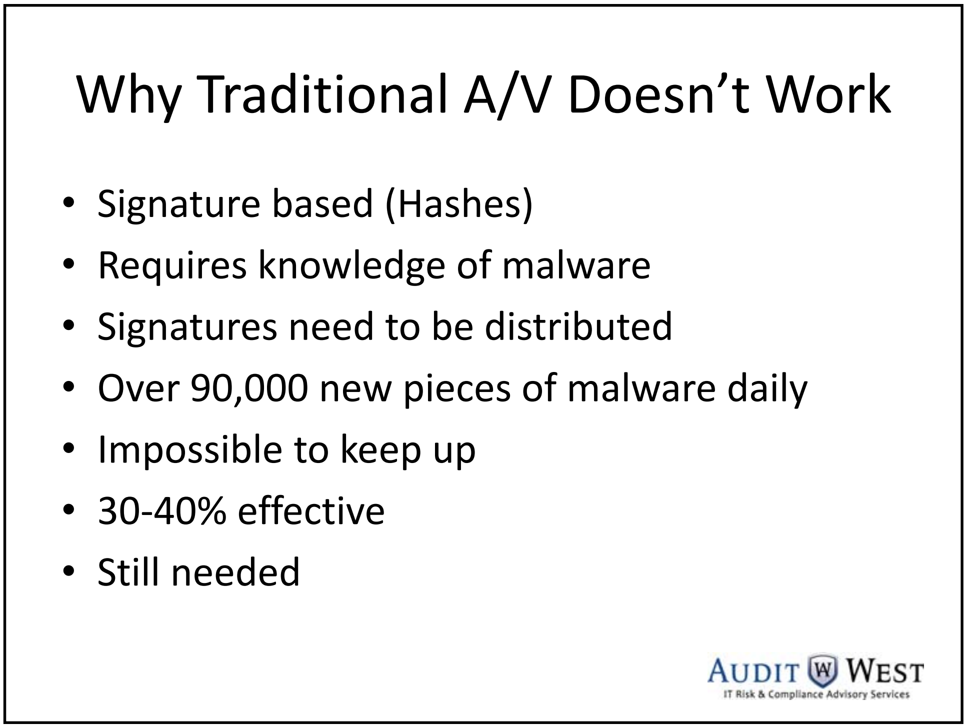


Why Traditional A/V Doesn’t Work

“Anti-virus is dead.”

-Brian Dye, VP of Information Security, Symantec Corporation in an interview with the Wall Street Journal, May 4, 2014

AUDIT WEST
IT Risk & Compliance Advisory Services



Why Traditional A/V Doesn’t Work

- Signature based (Hashes)
- Requires knowledge of malware
- Signatures need to be distributed
- Over 90,000 new pieces of malware daily
- Impossible to keep up
- 30-40% effective
- Still needed

AUDIT WEST
IT Risk & Compliance Advisory Services

Why Traditional Firewalls Don’t Work

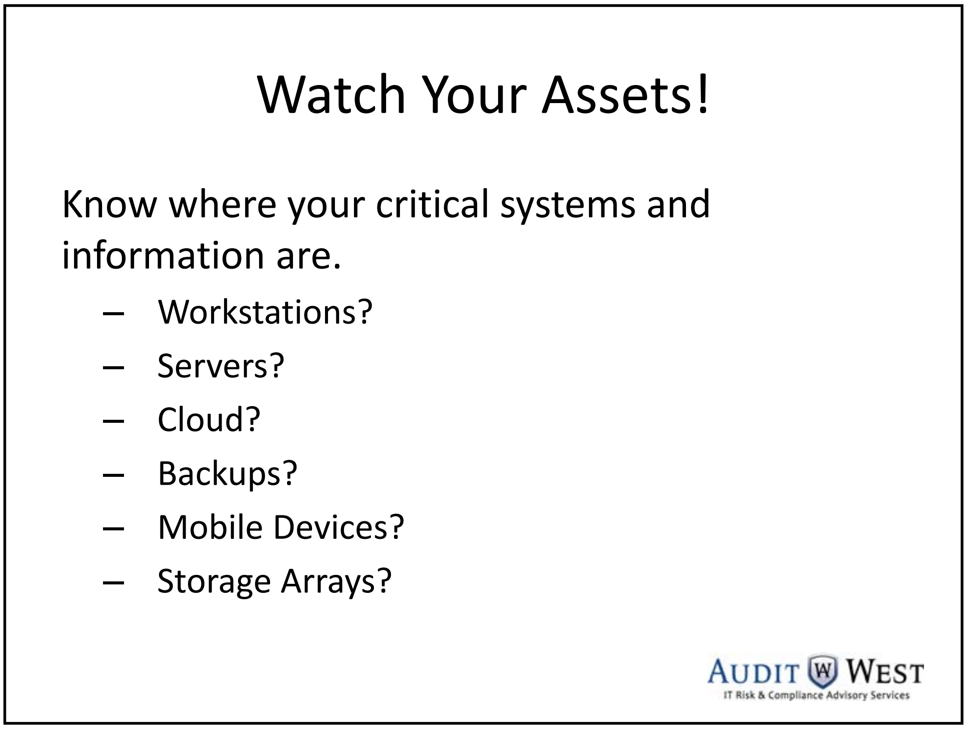
- Traditional filtering technology
- No application awareness / visibility
- Inability to extend architecture to mobile devices
- Signature based for IDS/AV
- No application level granularity

AUDIT WEST
IT Risk & Compliance Advisory Services

InfoSec for SMBs

- Know your assets
- Bad things happen
- Train your personnel
- Deploy the fundamentals
- Control access
- Trust but Verify
- Strategize on BYOD
- Have and enforce policies

AUDIT WEST
IT Risk & Compliance Advisory Services

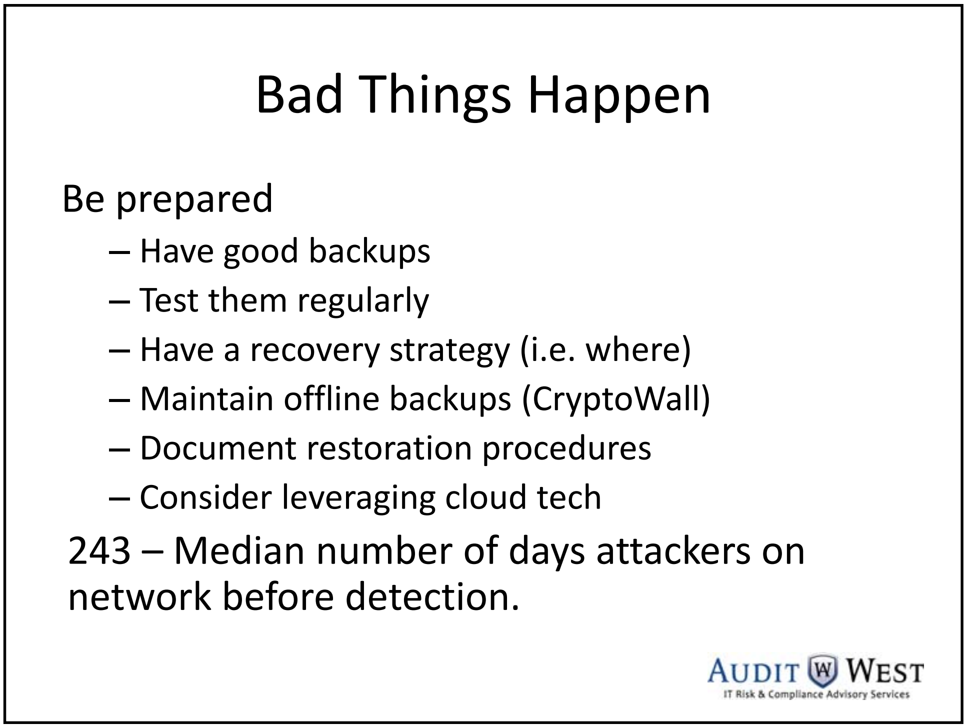


Watch Your Assets!

Know where your critical systems and information are.

- Workstations?
- Servers?
- Cloud?
- Backups?
- Mobile Devices?
- Storage Arrays?

AUDIT WEST
IT Risk & Compliance Advisory Services



Bad Things Happen

Be prepared

- Have good backups
- Test them regularly
- Have a recovery strategy (i.e. where)
- Maintain offline backups (CryptoWall)
- Document restoration procedures
- Consider leveraging cloud tech

243 – Median number of days attackers on network before detection.

AUDIT WEST
IT Risk & Compliance Advisory Services

Train Staff

- Security awareness training
- Conduct phishing tests regularly
- SMBs are a huge target
- Cloud based services provide this.

AUDIT WEST
IT Risk & Compliance Advisory Services

Deploy the Basics

- NextGen Firewalls (Palo Alto, Cisco, Juniper, Sonicwall, etc.)
- Wireless Security
- Anti-Malware on endpoints and servers
- Be rigorous about patching
  - OS and application (Flash, Java, etc.)
  - If short staffed, outsource
- Consider compliance requirements (PCI, HIPAA, FISMA, NIST, GLBA, etc.)

AUDIT WEST
IT Risk & Compliance Advisory Services

Control Access

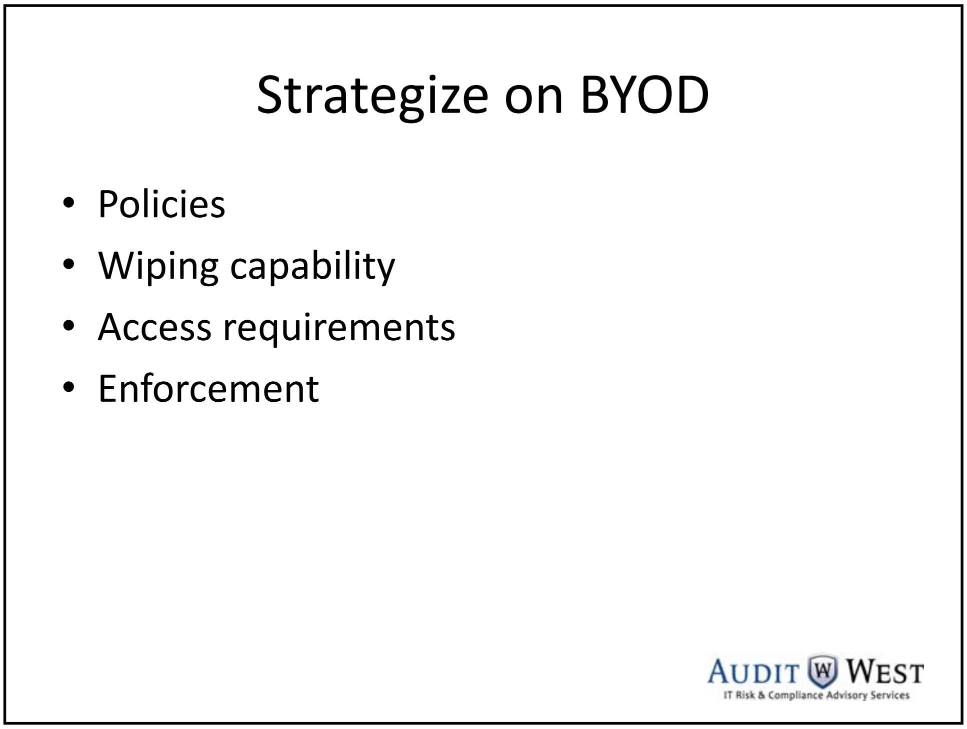
- Be granular about who has access to what, and when.
- Monitor for violation attempts
- Strict control on administrative accounts
- Require periodic password changes
- Remote users?
- Two-factor authentication?
- Consider outsourcing

AUDIT WEST
IT Risk & Compliance Advisory Services

Trust but Verify

- Conduct background checks
- Read vendor contracts
- If sharing customer data with another vendor, perform due diligence on controls

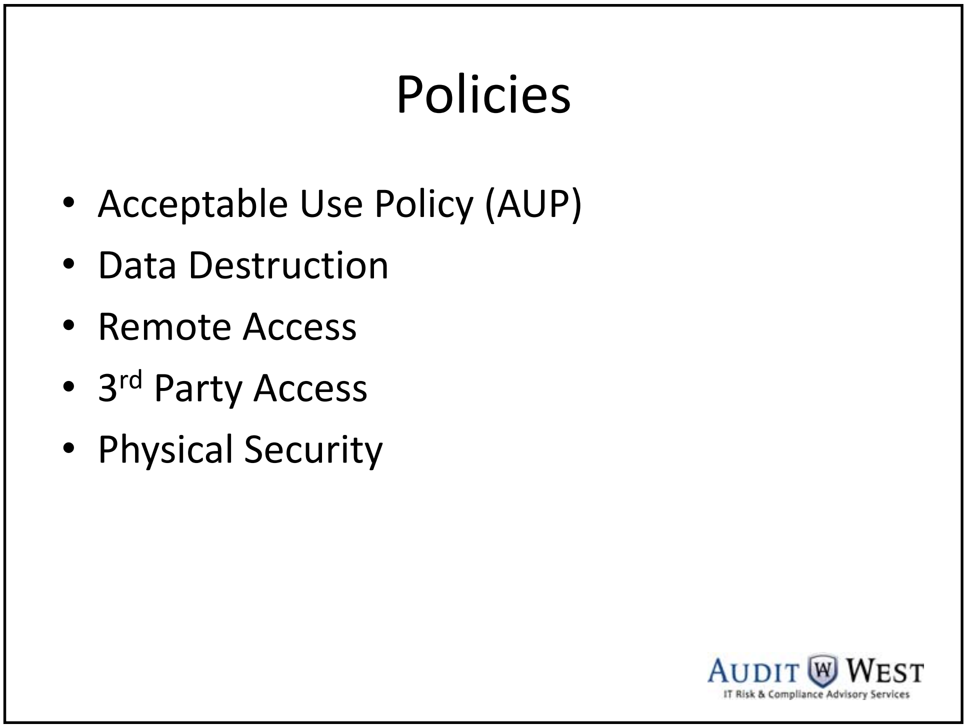
AUDIT WEST
IT Risk & Compliance Advisory Services



Strategize on BYOD

- Policies
- Wiping capability
- Access requirements
- Enforcement

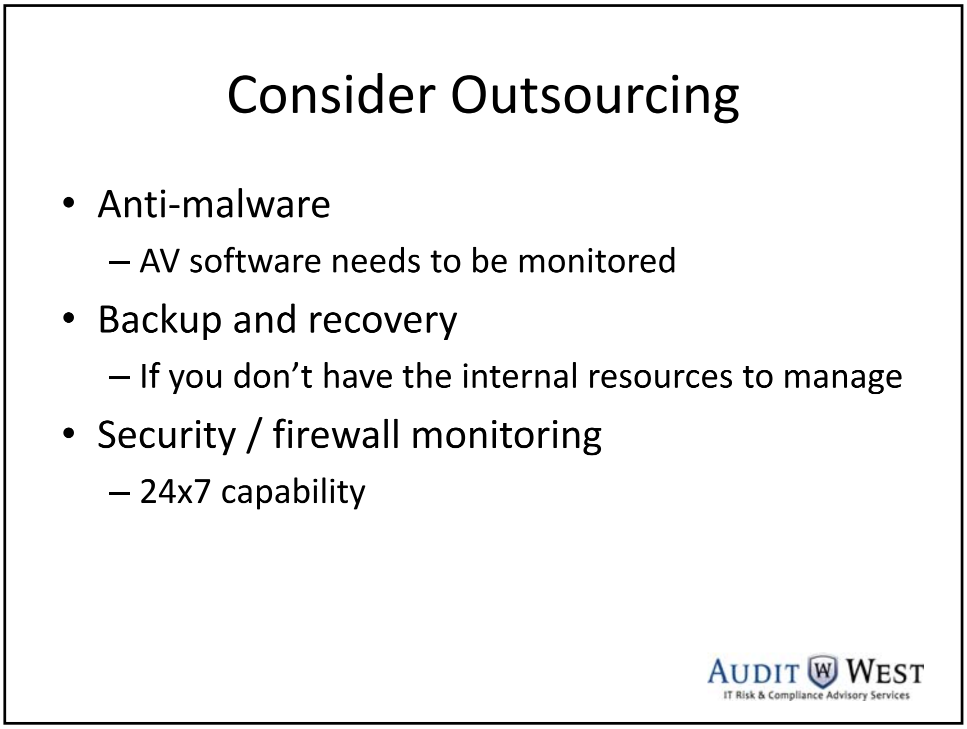
AUDIT WEST
IT Risk & Compliance Advisory Services



Policies

- Acceptable Use Policy (AUP)
- Data Destruction
- Remote Access
- 3rd Party Access
- Physical Security

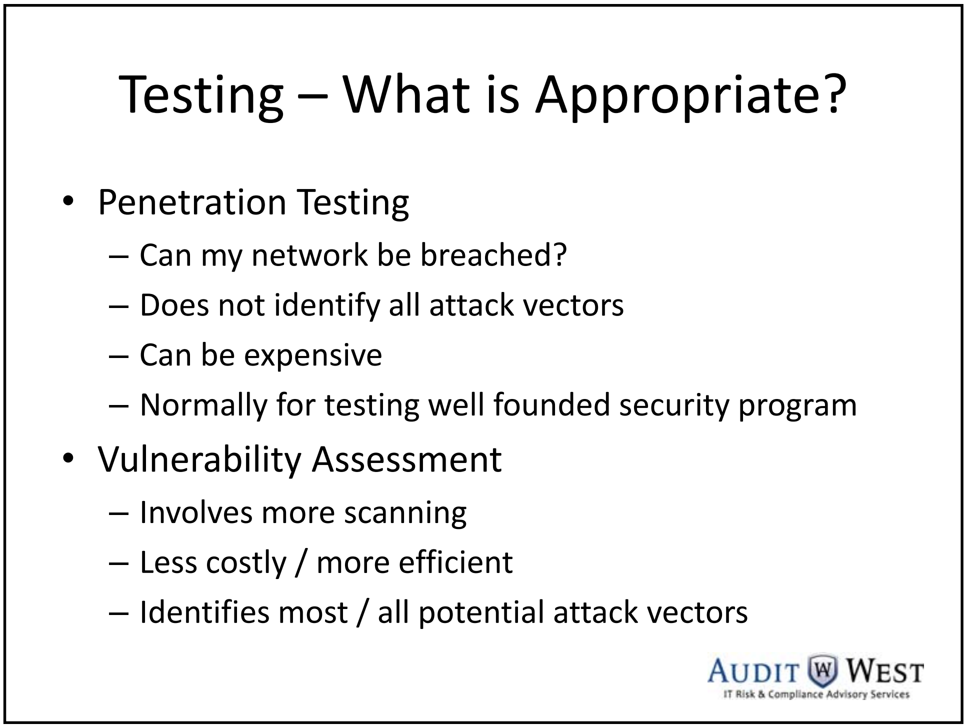
AUDIT WEST
IT Risk & Compliance Advisory Services



Consider Outsourcing

- Anti-malware
  - AV software needs to be monitored
- Backup and recovery
  - If you don’t have the internal resources to manage
- Security / firewall monitoring
  - 24x7 capability

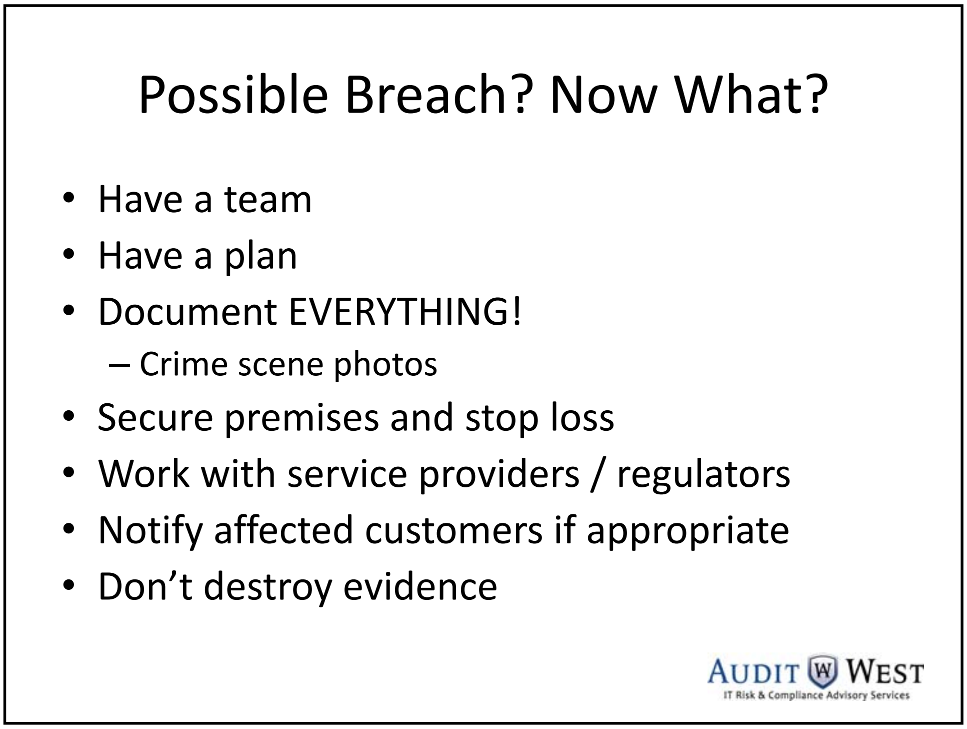
AUDIT WEST
IT Risk & Compliance Advisory Services



Testing – What is Appropriate?

- Penetration Testing
  - Can my network be breached?
  - Does not identify all attack vectors
  - Can be expensive
  - Normally for testing well founded security program
- Vulnerability Assessment
  - Involves more scanning
  - Less costly / more efficient
  - Identifies most / all potential attack vectors

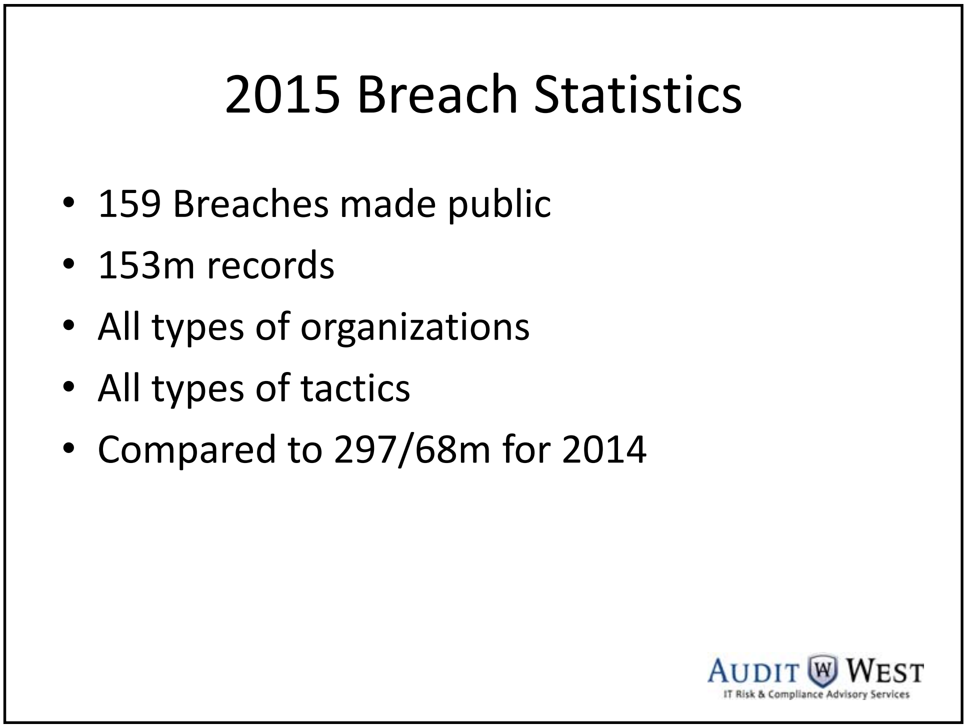
AUDIT WEST
IT Risk & Compliance Advisory Services



Possible Breach? Now What?

- Have a team
- Have a plan
- Document EVERYTHING!
  - Crime scene photos
- Secure premises and stop loss
- Work with service providers / regulators
- Notify affected customers if appropriate
- Don’t destroy evidence

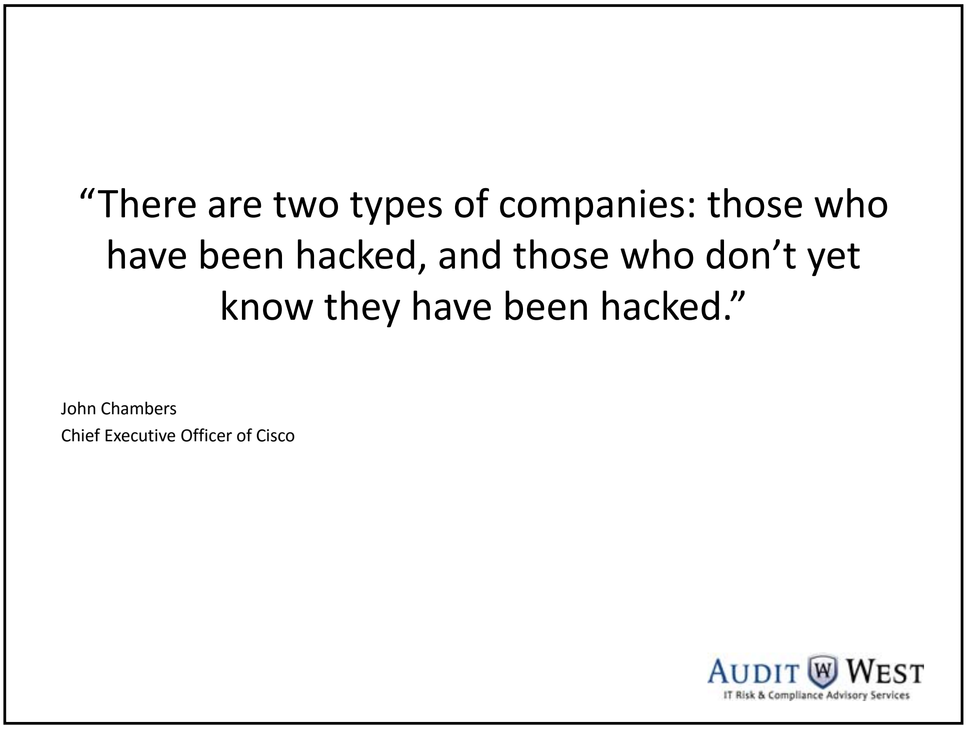
AUDIT WEST
IT Risk & Compliance Advisory Services



2015 Breach Statistics

- 159 Breaches made public
- 153m records
- All types of organizations
- All types of tactics
- Compared to 297/68m for 2014

AUDIT WEST
IT Risk & Compliance Advisory Services



"There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."

John Chambers
Chief Executive Officer of Cisco

AUDIT WEST
IT Risk & Compliance Advisory Services

Q&A

Brian Morkert
360-265-0421
bmorkert@auditwest.com
@bmorkert

AUDIT WEST
IT Risk & Compliance Advisory Services