Payment Card Industry Compliance – Risk & Vulnerability Management

Step by step approach to evaluate threats, identify risks, and mitigation tools

October 12, 2016

Association of College & University Auditors

Webinar Moderator

ACUA Distance Learning Director

Jana Clark

Senior Internal Auditor

Kansas State University

Don't forget to connect with us on social media!

Today's Presenter

Shiva Hullavarad
Manager of Compliance, Information and Record Systems
University of Alaska
sshullavarad@alaska.edu

Agenda

- Payment Card Industry – Data Security Standard
- Threats & Vulnerability – why & how does it matter?
- Types, Sources and Tools
- Risks of non-compliance
- PCI DSS 3.2
- New technology(s) and unknown threats
- 5 basic steps for maintaining and achieving compliance
- Vulnerability Assessment and Pen Test (VAPT)
- Available tools for VAPT
- Q & A

Polling Question #1

Does your institution have a PCI Compliance Program?

- Yes. 0-5 years in existence
- Yes. 6-10 years in existence
- Yes. 11-15 years in existence
- Currently working on it
- No/unsure

PCI DSS

Payment Card Industry - Data Security Standard

- Standard that is applied to:
  - Merchants
  - Service Providers (Third Third-party vendor, gateways)
  - Systems (Hardware, software)
- That:
  - Stores cardholder data
  - *Transmits* cardholder data
  - Processes cardholder data
- Applies to:
  - Electronic Transactions
  - Paper Transactions

PCI Council – Consortium

- All merchants are subject to the standard and to card association rules
  - **No exemption provided to anyone**
- Immunity does not apply because
  - Requirement is contractual - not regulatory or statutory
  - Card associations can be selective who they provide services to
  - Merchants accept services on a voluntary basis
  - Merchants agree to abide by association rules when they execute e-merchant bank agreement
- Merchant banks are prohibited by association rules from indemnifying a merchant from not being compliant with the standard
- Association Rules require merchant banks to monitor merchants to ensure their compliance
  - Failure of a merchant bank to require compliance jeopardizes the merchant bank bank's right to continue to be a merchant banks
  - Any fines levied are against the merchant bank, which in turns passes the fines onto the merchant

Levels of Merchants

Level	Transactions per Year	Types of Targets
1	➢More than 6 million ➢Anyone with breach	Merchants, Merchant Agents, Processors, Direct Connects
2	➢1 – 6 million	Merchants, Merchant Agents, Processors
3	➢20K – 1million	eCommerce Merchants
4	➢All other Merchants	Merchants

- **All merchants must perform external network scanning** to achieve compliance.

The PCI compliance - 12 security requirements

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored data.
4. Encrypt *transmission* of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications

The PCI compliance - 12 security requirements

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data.
11. Routinely test security systems and processes.

Maintain an Information Security Policy.

12. Establish high-level security principles and procedures.

Polling Question #2

What are the top security requirement priorities for your institution?

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks

Compliance Vs Validation

- Compliance – Means **adherence** to the standard
  - Applies to every merchant regardless of volume
  - Technical and business practices
- Validation – **Verification** that merchant (including its services providers) is compliant with the standard
  - Applies based on Level assigned to merchant & transaction volume
  - Two types of Validation
    - Self-Assessment
    - Certified by a Qualified Security Assessor (QSA)
- Attestation – Letter to card issuer (bank) signed by both merchant and acquirer bank attesting that validation has been performed

12

Two Components to Validation

- **Annual Assessment Questionnaire**
  - **Required of all merchants** – regardless of level
  - Applies to both technical and business
- **Security Vulnerability Scan - Quarterly**
  - Required for External facing IP addresses
    - Web applications
    - POS Software and databases on networks
    - Applies even if there is a re-direction link to third third-party
  - Must be performed by Approved Scanning Vendor (ASV)
  - Validation based on Level assigned to merchant, based on transaction volume

Validation requirements

- **Level 1-Visa/MasterCard--** Annual onsite review by merchant's internal auditor or a **Qualified Security Assessor** (QSA) or Internal Audit if signed by Officer of the company, and a quarterly network security scan with an **Approved Scanning Vendor** (ASV).
- **Level 2--** Completion of PCI DSS Self Assessment Questionnaire annually, **and** quarterly network security scan with an approved ASV.
- **Level 3--** Completion of PCI DSS Self Assessment Questionnaire annually, **and** quarterly network security scan with an approved ASV.
- **Level 4--** Completion of PCI DSS Self Assessment Questionnaire annually, **and** quarterly network security scan with an approved ASV.

Vulnerability Vs Threat

Vulnerability

Any **flaw** in the design, implementation or administration of a system that provides a mechanism for a threat to **exploit** the weakness of a system or process

They are weaknesses in networked environments, web applications and physical premises

Threat

Any person, circumstance or event that has the **potential** to cause **damage** to an organizational asset or business function

Advanced Persistent Threat

"An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)."

" These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future." ---- NIST

Hacker

https://www.youtube.com/watch?v=bjYhmX_OUQQ

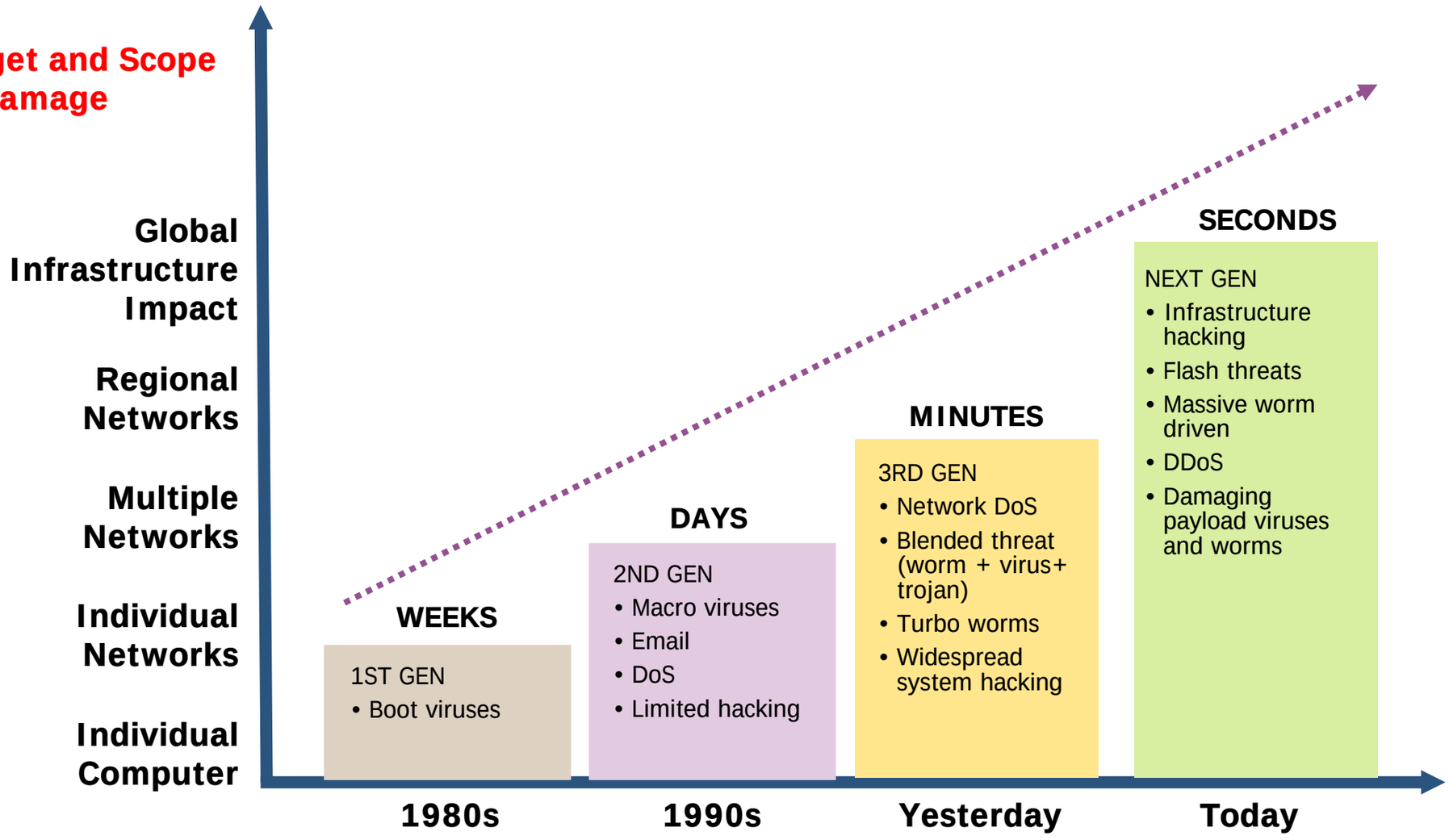
Advanced Persistent Threat

- pursues its objectives repeatedly over an extended period of time
- adapts to defenders' efforts to resist it
- targetetted approach
- is determined to maintain the level of interaction needed to execute its objectives

Threat landscape – Moving target!!

All entry points need to be secured from hackers:

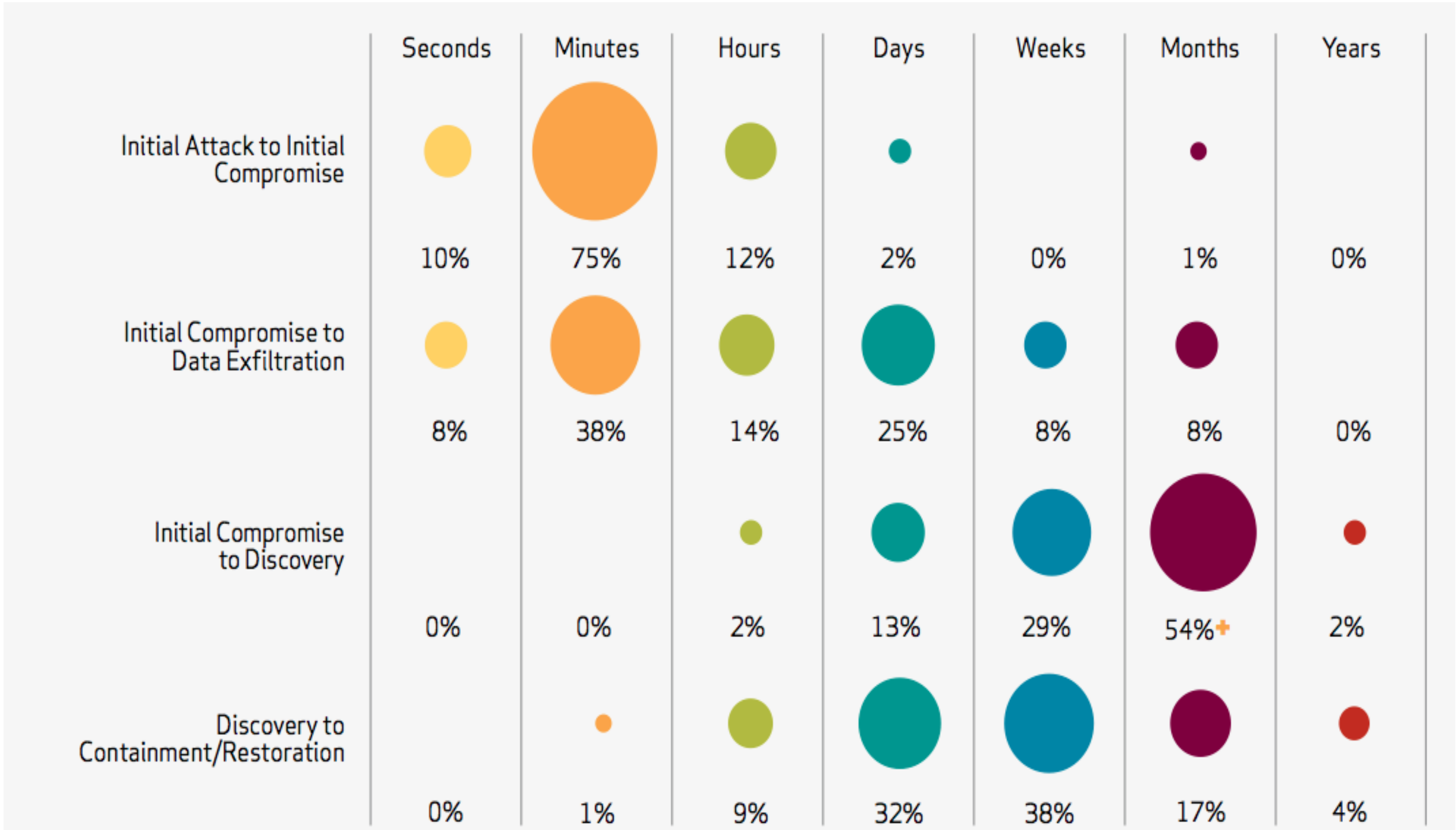
Wi-Fi, security cameras, wireless credit card processors, digital menu boards and more interface to networks via IP addresses



Threats follow technology trends

- Bring Your Own Device: Personnel Vs Professional usage
- Web Exploits: Cross-site scripting /SQL injection
- Botnets: Updating and modification
- Data loss: Student, finance, health, IP – data theft
- Big Data: Ability to gather & store data equals greater liability
- Targeted and Persistent attacks
- Sponsored cyber operations: Attacks, espionage

Threat – Detect, Response and Recovery



Source: Cisco Threat Report


IN ADDITION TO ISO 9000, WE WILL STRIVE TO BE QS-9000 COMPLIANT.
THAT MEANS FALSIFYING THE FOLLOWING DOC-UMENTS: QSR, APQP, FMEA, MSA, SPC, PPAP AND QSA.
REMEMBER, YOU CAN'T SPELL COMPLIANCE WITHOUT "LIANCE."
scottadams@aol.com
www.dilbert.com
© 1999 United Feature Syndicate, Inc.
11/29/99


DOGBERT IS CHAIRING THE INTERNATIONAL DATA SECURITY STANDARDS GROUP.
THE GOAL OF OUR ORGANIZATION IS TO MAKE YOUR SECURITY PROCEDURES SO INCONVENIENT THAT YOU GIVE UP HOPE AND DIE FROM BED SORES.
WE TAKE PRIDE IN BEING INDEPENDENT FROM THE COMPANIES THAT FUND US.
Dilbert.com DilbertCartoonist@gmail.com
8-1-11 ©2011 Scott Adams, Inc./Dist. by Universal Uclick

Polling Question #3

What merchant level is your institution?

- Level 1 (greater than 6 million cc transactions per year)
- Level 2 (1-6 million transactions per year)
- Level 3 (20k-1 million transactions per year)
- Level 4 (less than 20k transactions per year)
- Unsure

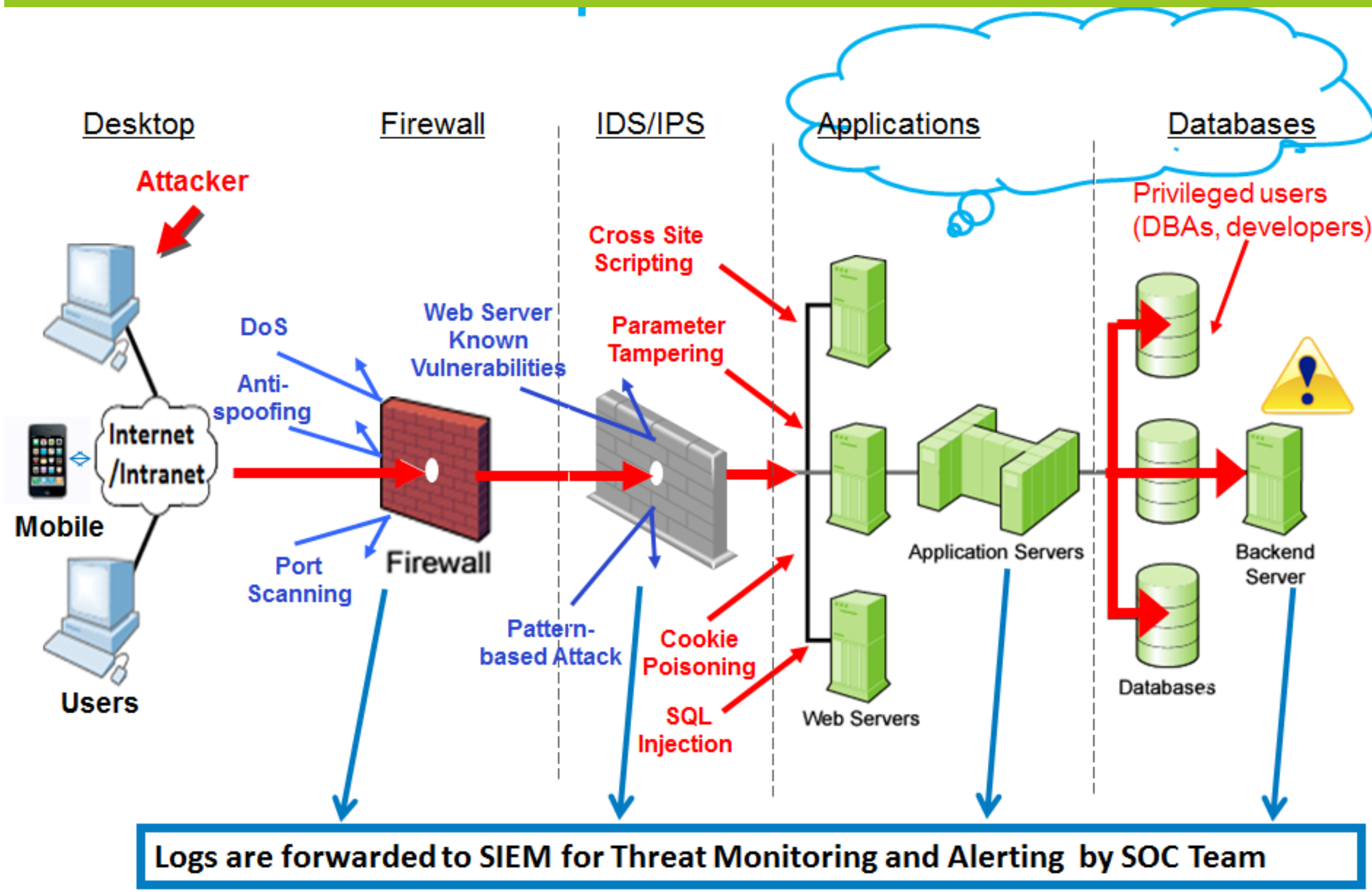
PCI DSS 3.2 - Threat is the main driver

- Changing payment and threat environment
- Breach reports and compromise trends
- Feedback from industry

Key changes

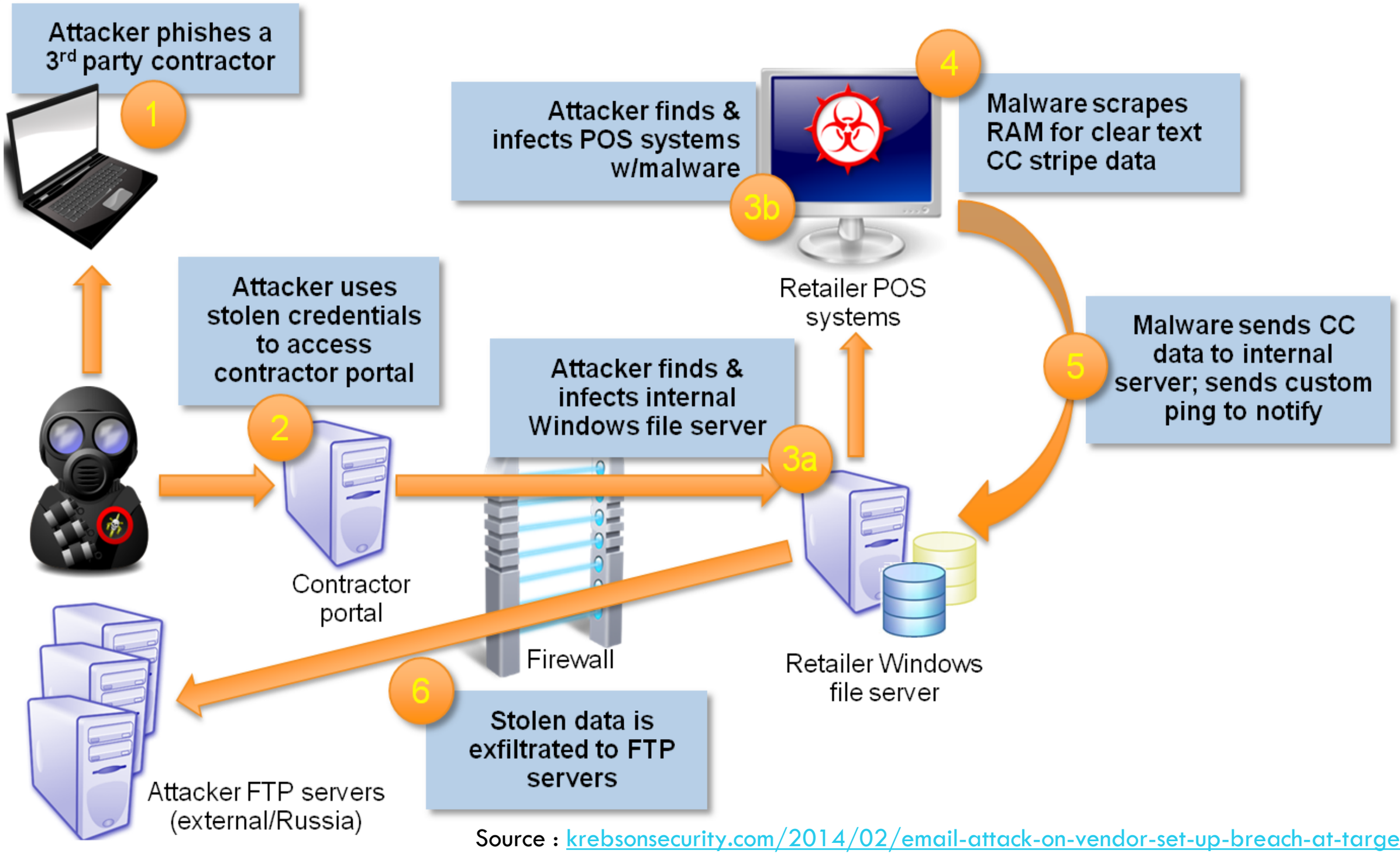
- Multi factor authentication for admins (8.3.1)
- 5 new sub requirements for service providers (3,10,11,12)
- 2 new appendices
  - SSL/TLS migration deadline
  - Designated entities supplemental validation

Threat flow landscape



Retail Chain CC Data Security Breach

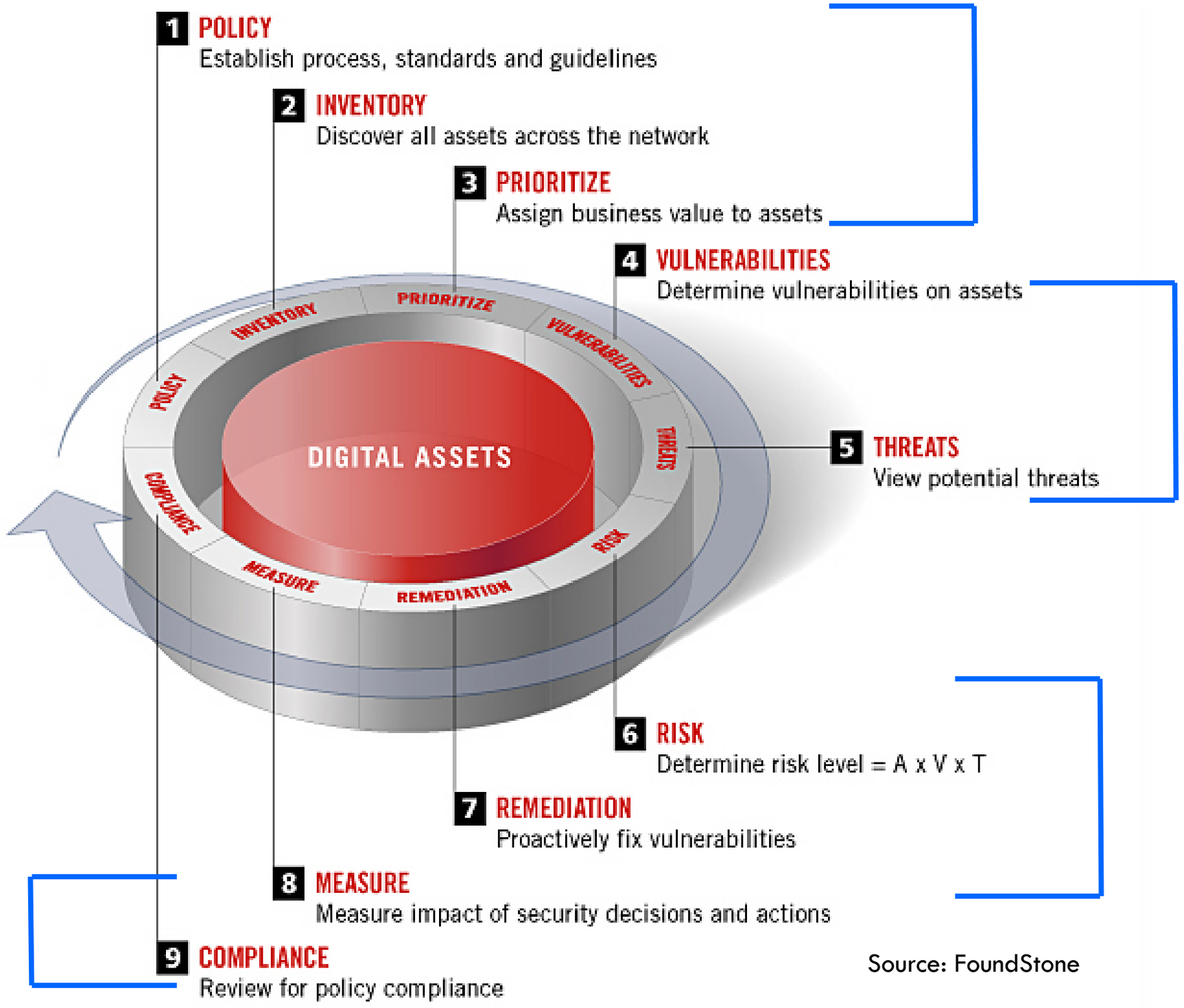
Researchers view



Source : krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/.

Vulnerability Management Lifecycle

- Business unit
- IT Security
- Compliance
- Legal
- Risk Services



Source: FoundStone

Vulnerability management approaches

- Focus on 5 key areas:
  - Prioritize Assets
  - Assess threats
  - Quantify Risk Level (assets, threats, vulnerabilities)
  - Remediate Vulnerabilities
  - Measure

Step 1:Prioritize Assets (Policy, Inventory & Prioritize)

- Identify assets by:
  - **Networks**
    - Logical groupings of devices
    - Connectivity - None, LAN, broadband, wireless
  - **Network Devices**
    - Wireless access points, routers, switches
  - **Operating System**
    - Windows, Unix
  - **Applications**
    - IIS, Apache, SQL Server
  - **Versions**
    - IIS 5.0, Apache 1.3.12, SQL Server V.7

Step 1: Continued…

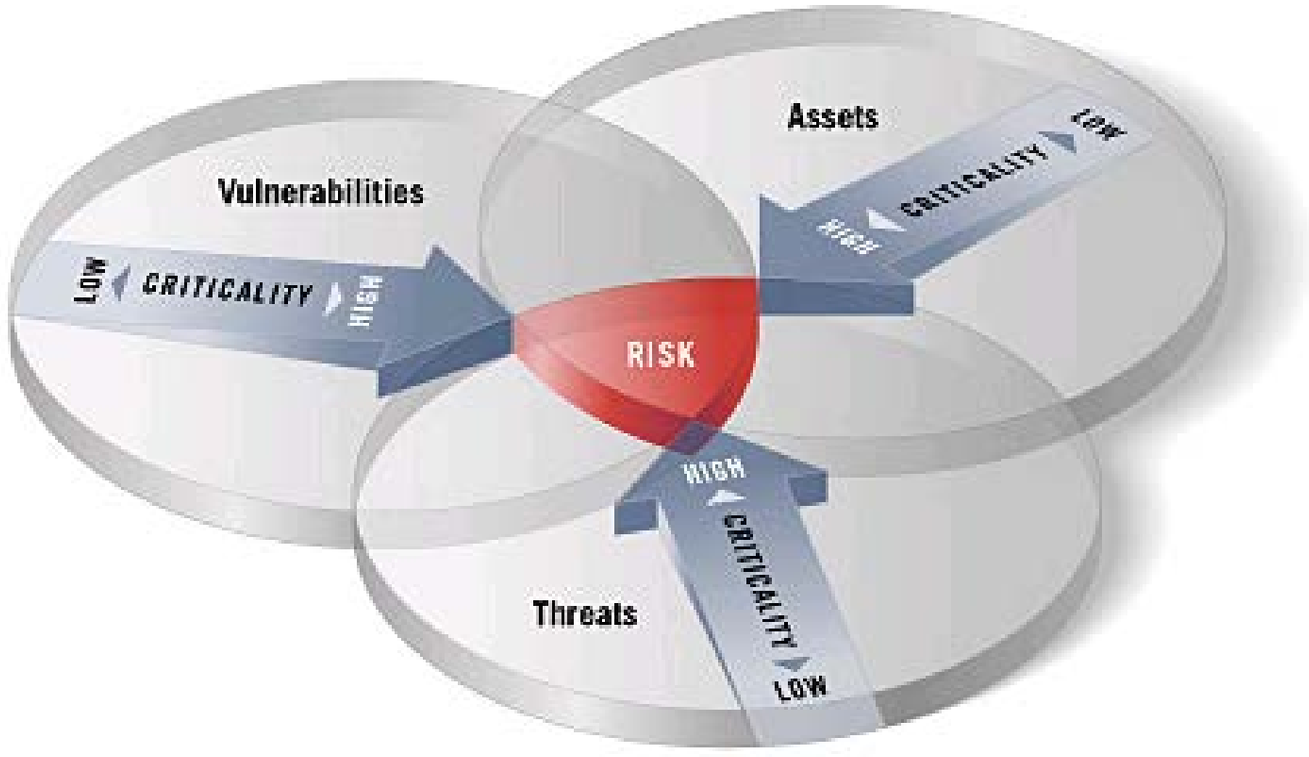
- Network-based discovery
  - Known and “unknown” devices
  - Determine network-based applications
  - Excellent scalability
- Agent-based discovery
  - In-depth review of the applications and patch levels
  - Deployment disadvantages
- Network- and agent-based discovery techniques are optimal
  - *Agents* - Cover what you already know in great detail
  - *Network* - Identify rogue or new devices
- Frequency
  - Continuous, daily, weekly
  - Depends on the asset

Step 2:Assess threats – Goal: Protect most critical assets

- Threat and vulnerability data have varied priority
- Identify threats
  - Worms
  - Exploits
  - Wide-scale attacks
  - New vulnerabilities
- Correlate with your most critical assets
- Result = Prioritization of vulnerabilities within your environment

Step 3: Quantify Risk Level - (AVT)

- The product of:
  - **A**ssets
  - **V**ulnerabilities
  - **T**hreats
- Based upon the criticality of AVT
- Focus your resources on the *true* risk



Step 4: Remediate Vulnerabilities

- Patch or Mitigate
  - Impact on availability from a bad patch vs. the risk of not patching
  - Patch or mitigate
  - Recommendations:
    - QA security patches 24 hours
    - Determine if there are wide spread problems
    - Implement defense-in-depth

Step 5: Measure

- Current state of security metrics
- Future Look:
  - Common nomenclature
  - Dashboard view of risk and vulnerabilities across disparate organizations
  - Technologies that will help answer the questions:
    - How am I trending over time?
    - How do I compare to my peers?
    - How do I compare outside my industry?

Assess Compliance

- PCI DSS – Current standard
  - Assess the environment for the qualifying SAQ
  - Develop reports
  - Training
  - Upgrade

Polling Question #4

Has your institution had a review of its PCI Compliance Program?

- Yes, by an external qualified security assessor (QSA)
- Yes, by Internal Audit staff
- On the audit plan in the next two years
- No/unsure

10 Steps to Effective Threat Management

1. Identify all the assets in your purview
2. Create an Asset Criticality Profile (ACP)
3. Determine exposures and vulnerabilities
4. Track relevant threats – realized and unrealized
5. Determine Risk - product of Assets x Vulnerabilities x Threats
6. Take corrective action if risk > cost to eliminate or mitigate
7. Create meaningful metrics and hold people accountable
8. Identify and address compliance gaps
9. Implement an automated vulnerability management system
10. ***Convince someone with a budget that vulnerability management is important***

Vulnerability Assessment and Penetration Testing (VAPT)

- Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that.
- Vulnerability types
  - Access control,
  - Boundary condition,
  - Input validation,
  - Authentication,
  - Configuration Weakness,
  - Exception Handling etc.

VAPT continued…

- Penetration testing is the next step after vulnerability assessment.
- Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system.
- In penetration testing, the tester (QSA) intently exploits the system and find out possible exploits.

VAPT – 8 Step process

1. Scope
2. Reconnaissance
3. Vulnerability detection
4. Information analysis and planning
5. Penetration testing
6. Privilege escalation
7. Result analysis
8. Reporting

VAPT – Top15 Tools (OpenSource & Proprietary)

#	Name	License	Type	Operating System
1	Metasploit	Proprietary	Vulnerability scanner and exploit	Cross-platform
2	Nessus	Proprietary	Vulnerability scanner	Cross-platform
3	Kali Linux	GPL	Collection of various tools	Linux
4	Burp Suite	Proprietary	Web vulnerability scanner	Cross-platform
5	w3af	GPL	Web vulnerability scanner	Cross-platform
6	OpenVAS	GPL	Vulnerability scanner	Cross-platform
7	Paros proxy	GPL	Web vulnerability scanner	Cross-platform
8	Core Impact	Proprietary	Vulnerability scanner and exploit	Windows
9	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
10	GFI LanGuard	Proprietary	Vulnerability scanner	Windows
11	Acunetix WVS	Proprietary	Web vulnerability scanner	Windows
12	QualysGuard	Proprietary	Vulnerability scanner	Cross-platform
13	MBSA	Freeware	Vulnerability scanner	Windows
14	AppScan	Proprietary	Web vulnerability scanner	Windows
15	Canvas	Proprietary	Vulnerability scanner and exploit	Cross-platform

Microsoft Baseline Security Analyzer 2.3

Microsoft
Baseline Security Analyzer

Microsoft

Administrative Vulnerabilities

Score	Issue	Result
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
	Password Expiration	All user accounts (3) have non-expiring passwords. What was scanned Result details How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned
	Windows Firewall	Windows Firewall is managed through Group Policy on this computer and the policy has exceptions configured. Windows Firewall is enabled and has exceptions configured. Windows Firewall is enabled on all network connections. What was scanned Result details How to correct this
	Local Account Password Test	Some user accounts (1 of 3) have blank or simple passwords, or could not be analyzed. What was scanned Result details
	File System	All hard drives (1) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned

Greenbone Security Assistant - Firefox

File Edit View History Bookmarks Tools Help

Greenbone Security Assi...

https://192.168.201.250/omp

Wikipedia (en)

Greenbone Security Assistant

Logged in as User **demouser** | Logout

Tue Jul 15 10:52:34 2014 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Help

Tasks 1 - 11 of 11 (total: 11) Refresh every 10 Sec.

Filter: apply_overrides=1 rows=20 permission=any owner=any first=1 sort Tasks Filter

Name	Status	Reports Total	Reports Last	Severity	Trend	Actions
Alterable Task (All assigned elements in this task can be modified)	Stopped at 20 %	4 (5)	Jul 4 2014	0.0 (Log)		
Container Task (This does contain several imported reports)	Container	2 (2)	Jun 20 2014			
Deep Scan Linux (This does a deep scan of our linux test-system)	Done	2 (2)	Jun 25 2014	N/A		
Deep Scan Windows (This does a deep scan of our Windows lab test-machines)	Done	1 (1)	Jun 20 2014	10.0 (High)		
Discovery Scan (This Scan Configuration applies any NVTs that discover as many details about the target system)	Requested	7 (9)	Jul 15 2014	0.0 (Log)		
IT-Grundschutz Scan (Tests for Compliance with IT-Grundschutz, 12. EL)	Paused at 1 %	2 (4)	Jun 24 2014	2.6 (Low)		
Nightly Scan with Schedule (This scan does a nightly scan of the entire network and sends a mail if the threat level increases)	Done	1 (1)	Jun 21 2014	2.6 (Low)		
Quick Scan Linux (This does a quick scan of our GNU/Linux lab machine)	Done	2 (4)	Jun 20 2014	4.3 (Medium)		

Burp Suite Professional

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Options

Results | Scan queue | Live scanning | Options

- http://0b7bd624bab7.mdseclabs.net
  - /
  - addressbook
  - admin
  - cclookup
  - employees
  - filestore
  - labs
  - search
  - settings
  - updates
- https://0b7bd624bab7.mdseclabs.net

- SQL injection [7]
- Cross-site scripting (stored)
- HTTP header injection
- Cross-site scripting (reflected)
- Cleartext submission of password [2]
- OS command injection
- LDAP injection
- Open redirection
- Password field with autocomplete enabled [2]
- Cross-domain Referer leakage [2]

Advisory | Request | Response

Cross-site scripting (reflected)

Issue: **Cross-site scripting (reflected)**
Severity: **High**
Confidence: **Certain**
Host: **http://0b7bd624bab7.mdseclabs.net**
Path: **/search/11/Default.aspx**

Issue detail

The value of the **SearchTerm** request parameter is copied into t
between tags. The payload **1d329<script>alert(1)</script>27a3**
SearchTerm parameter. This input was echoed unmodified in the

Map Results: mapped IP range

Turn help tips: On | Off

Domain: none:[10.10.10.2-10.10.10.100]
Network: Global Default Network

Results are listed with the total number of findings sorted by IP address.

Attributes Scannable Search results by Clear

Actions (1) Tools

Search results by IP, hostname, other attributes

Take actions on hosts

Summary | Results

Total Hosts in Domain **17**

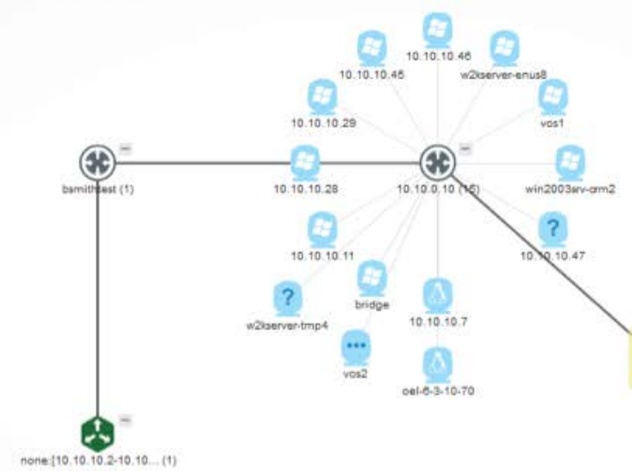
Newly Discovered Hosts **2**

New	2	Approved	0
Scannable	15	Live	17
In Netblock	15	Rogue	17

Operating System Families **5**

Windows	9	Linux	3
Mac	0	Router	2
Other	1	Unknown	2

Map



Click any host to view host details in the Preview

Preview

10.10.10.65 / krb5.qa.qualys.com

Scannable | Live | In Netblock | Rogue

Router: 10.10.0.10 | OS: Linux 2.2-2.6 | Last scan: 06/11/2014 Scan now

Discovery Method

DNS ICMP TCP PORT 111 TCP PORT 22 TCP RST UDP PORT 111

Summary and Conclusions

- Threats of data compromise are dynamic and global in scope
- Assess the risk, vulnerability and threat – develop the risk tolerance model
- Have risk mitigation plan in place
- Vulnerability is more of a reputational risk to the institution than the financial threat
- PCI DSS is an effective tool to ensure minimal risk

Contact Information

Shiva Hullavarad
Manager of Compliance, Information and Record Systems
University of Alaska
sshullavarad@alaska.edu

Upcoming ACUA Events

- **Construction Auditing: Where to Start and How to Make It Work for Your Organization**
  - November, 1, 2016
- **Auditing for Title IX Compliance**
  - December 7, 2016

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS
Advancing Auditing in Higher Education