Trustwave®

SpiderLabs℠

Global Security Report 2010
Analysis of Investigations and Penetration Tests

Nicholas J. Percoco

Senior Vice President, Trustwave SpiderLabs

Agenda

- **About the Report**
- **Analysis of 2009 Incident Response Investigations**
  - About the Sample Set
  - Investigative Conclusions
  - Anatomy of a Data Breach
- **Analysis of 2009 Penetration Tests**
  - About the Sample Set
  - Top 10 Lists
- **The Global Remediation Plan**
- **Conclusions**
- **Bonus Material in the Report**
- **Where to get it?**
- **Contacts**

About The Report

- Planning started in early 2009
- 10x the number of PenTest vs. Investigations
- A tool for organizations in prioritizing 2010 initiatives
- This is NOT a survey; only real-life data
- Also, we did NOT try to pass the weight test

Analysis of Incident Response Investigations

Why? Organizations are Reacting!

- Perform Actions to Stop an Attack
  - Understand the attack
  - Understand the losses
- Provide Reporting to Interested Parties
- Assist Law Enforcement
  - Apprehend criminals

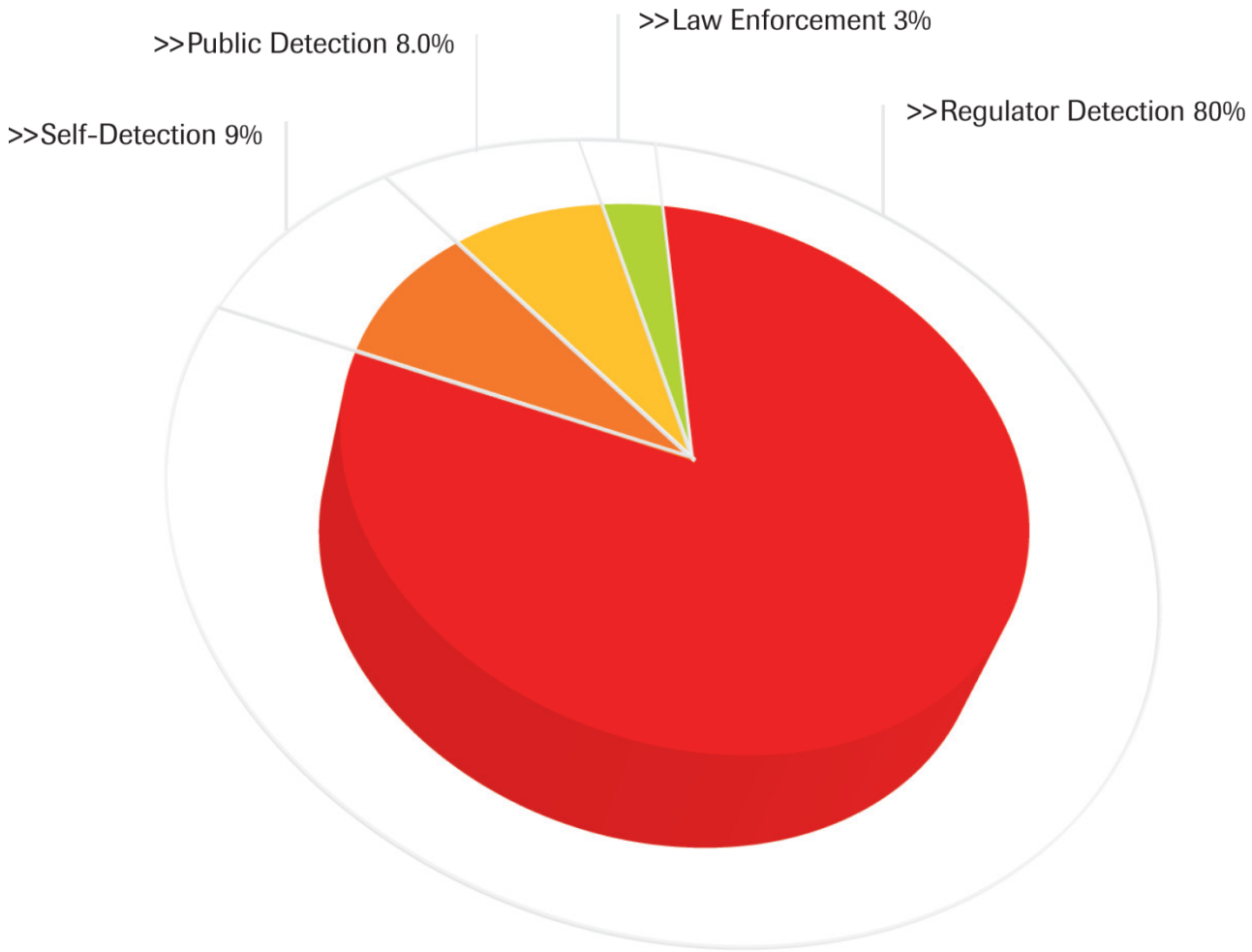
Incident Response – About the Sample Set

218 Investigations

- 24 countries
- 18% Found Inconclusive
  - No evidence of critical data leaving
  - Many factors impact an inconclusive case
- Average of 156 Days Lapse Between Initial Breach and Detection (!?!?!)

Incident Response – About the Sample Set

Types of Detection



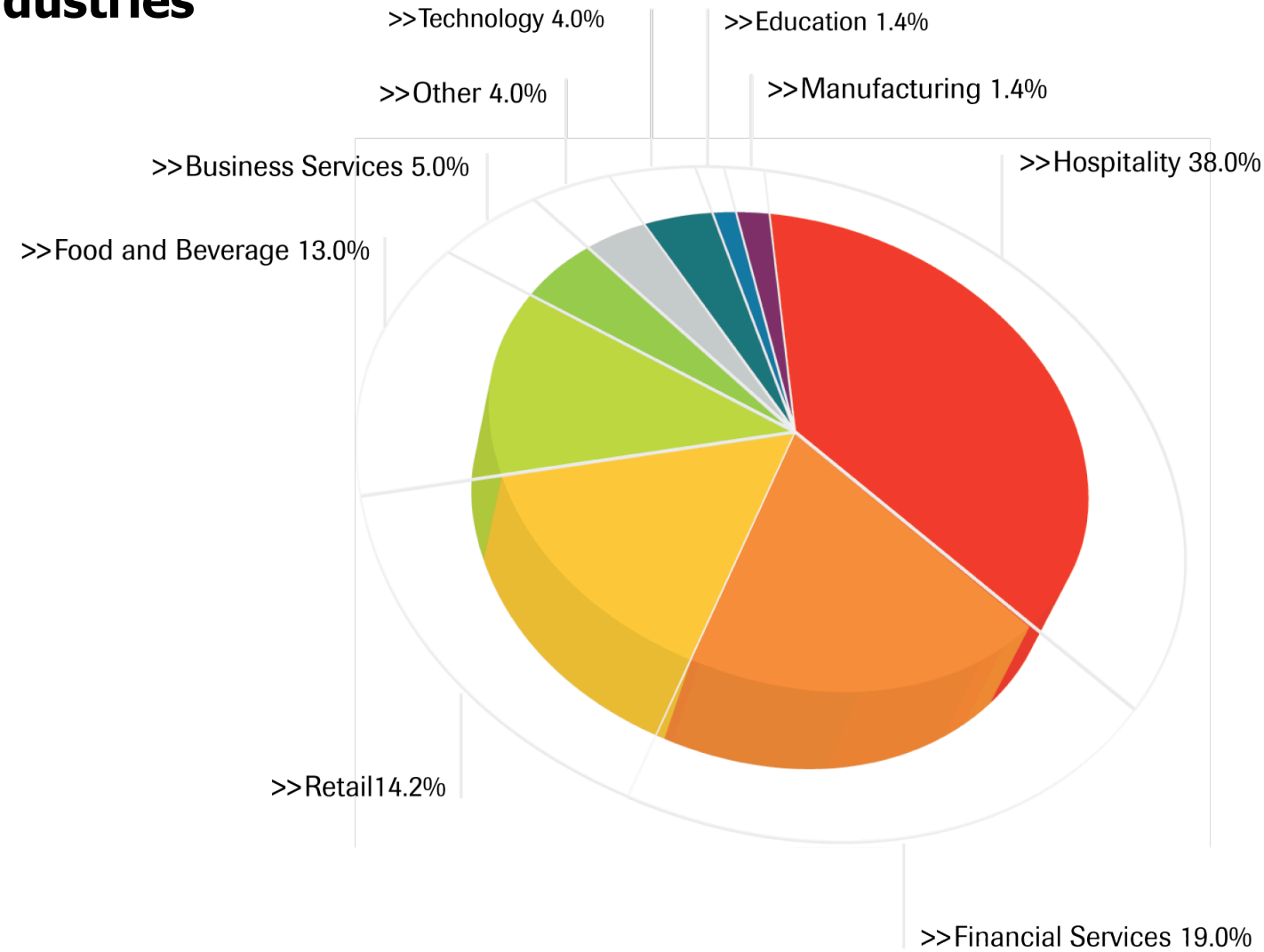
Incident Response – About the Sample Set

Countries Represented in 2009

Australia
Belgium
Canada
Chile
Cyprus
Denmark
Dominican Republic
Ecuador
Germany
Greece
Hong Kong
Ireland
Luxembourg
Malaysia
Puerto Rico
Saudi Arabia
South Africa
Sri Lanka
Switzerland
Ukraine
United Arab Emirates
United Kingdom
United States
Virgin Islands

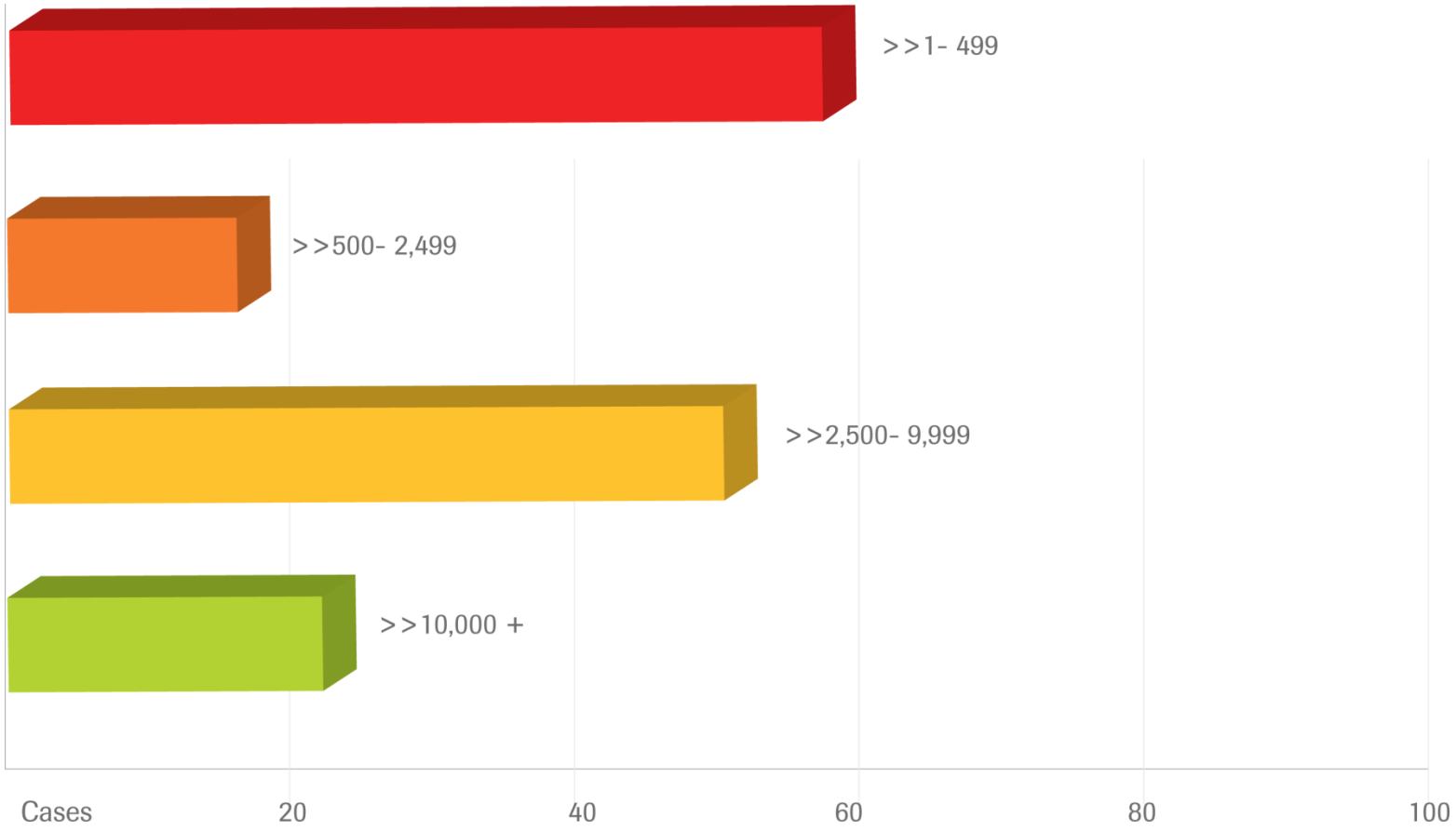
Incident Response – About the Sample Set

Industries



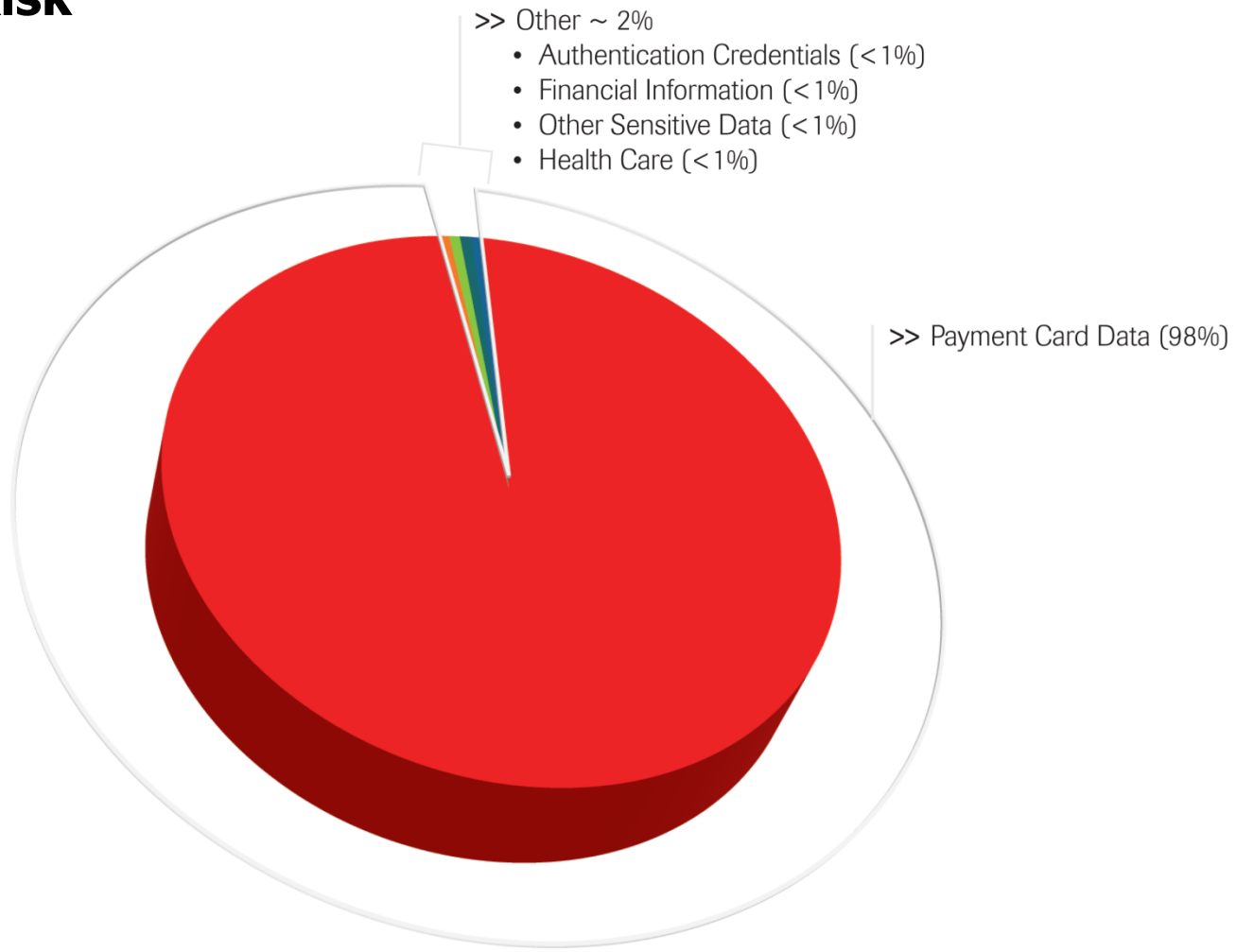
Incident Response – About the Sample Set

Company Size



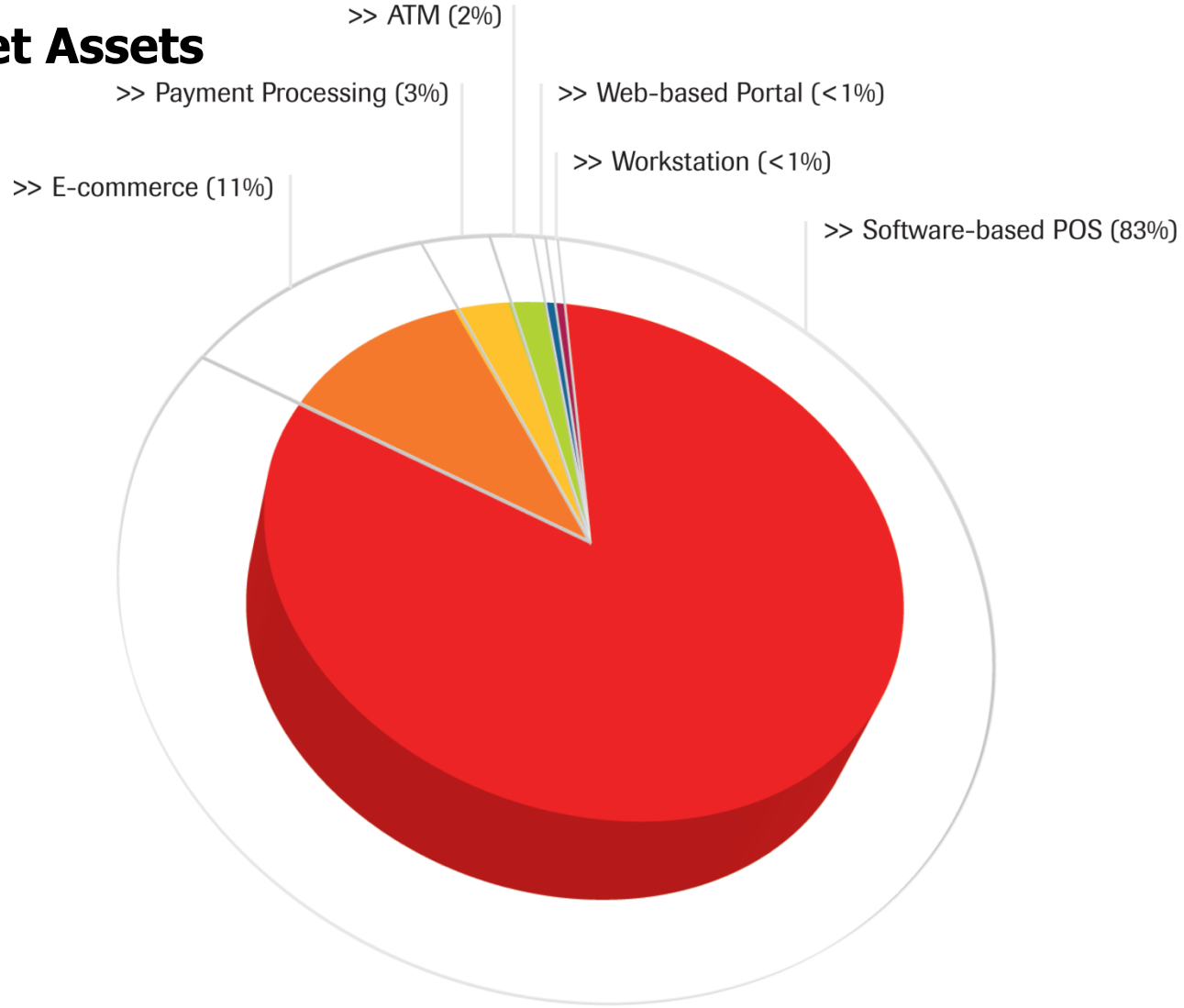
Incident Response – Investigative Conclusions

Types of Data at Risk



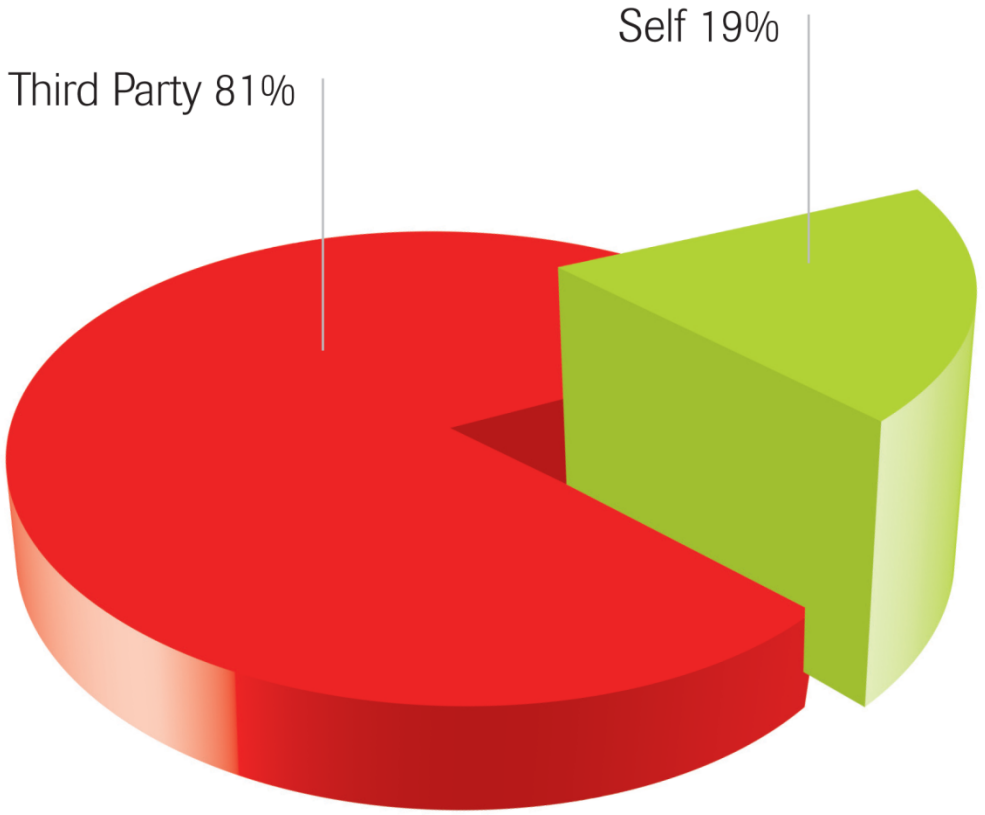
Incident Response – Investigative Conclusions

Types of Target Assets



Incident Response – Investigative Conclusions

System Administration Responsibility

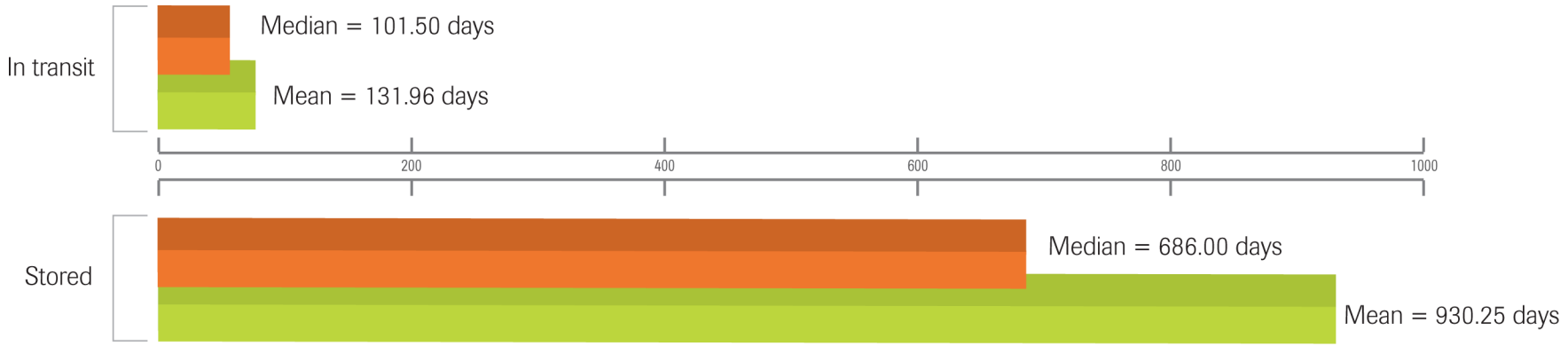


Incident Response – Investigative Conclusions

Attacker Source Address Geography

Incident Response – Investigative Conclusions

Window of Data Exposure



Anatomy of a Data Breach

Three Components:

1. Initial Entry
2. Data Harvesting
3. Exfiltration

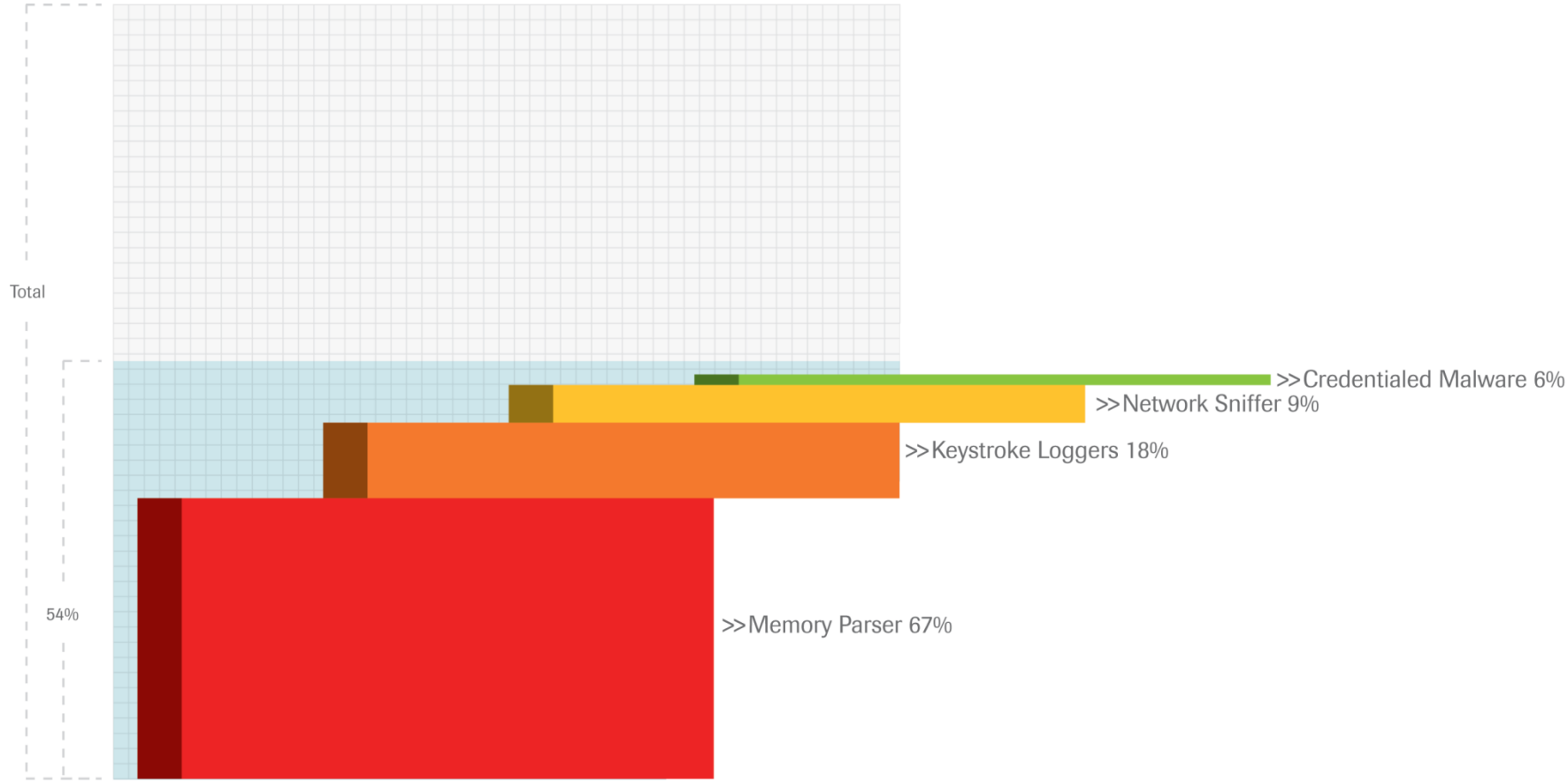
Anatomy of a Data Breach – Initial Entry

Top Methods of Entry Included:

- **Remote Access Applications [45%]**
  - Default vendor supplied or weak passwords [90%]
- **3rd Party Connections [42%]**
  - MPLS, ATM, frame relay
- **SQL Injection [6%]**
  - Web application compromises [90%]
- **Exposed Services [4%]**
- **Remote File Inclusion [2%]**
- **Email Trojan [<1%]**
  - 2 recent Adobe vulnerability cases
- **Physical Access [<1%]**

Anatomy of a Data Breach – Data Harvesting

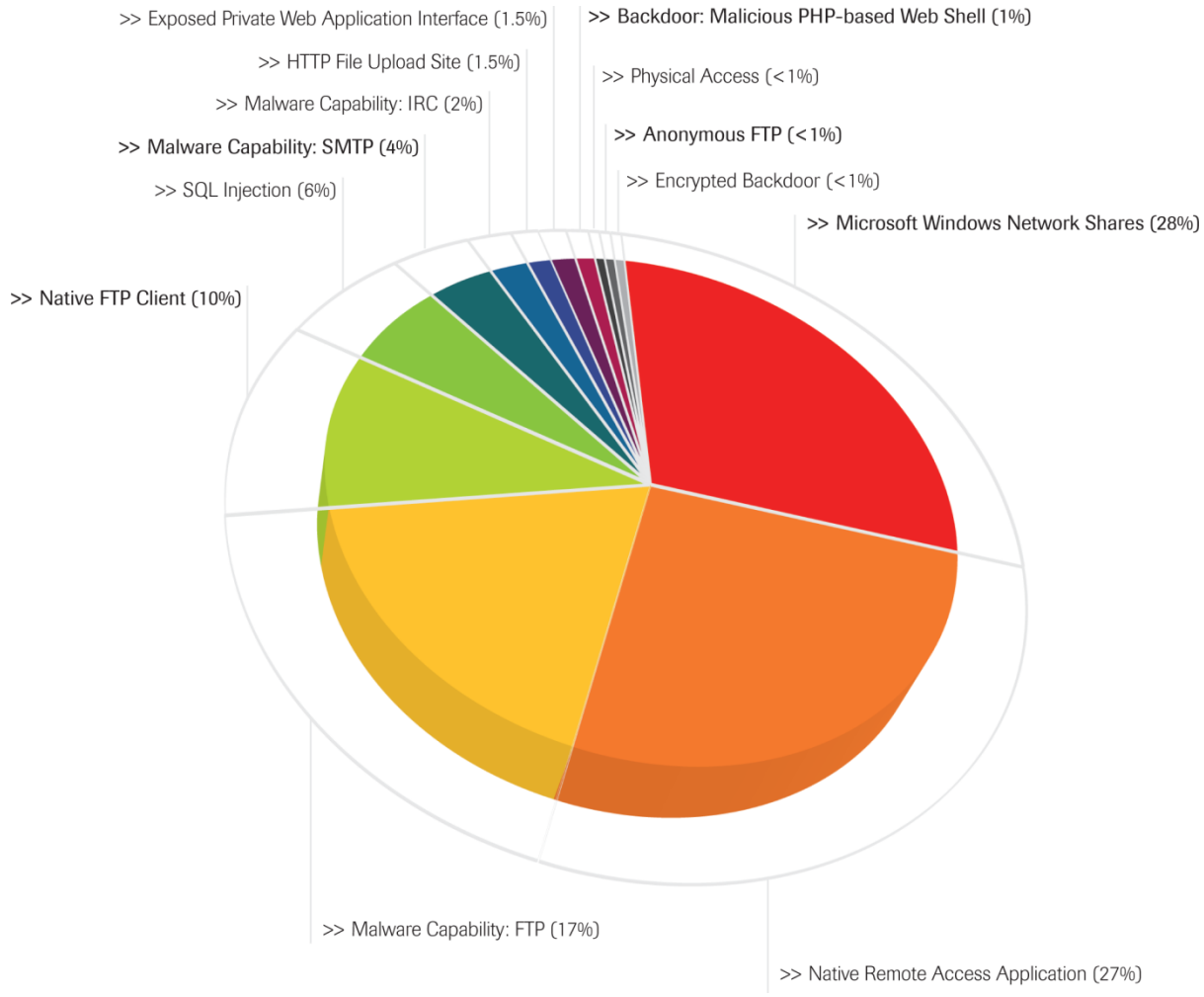
Top Methods of Harvesting (using Malware):



In 54% of our case, attackers used Malware to harvest data.

Anatomy of a Data Breach – Exfiltration

Top Methods of Data Exfiltration:



Analysis of Penetration Tests

Why? Organizations are Proactive!

- Understand Security Posture
  - Multiple vectors
    - External network
    - Internal network
    - Wireless
    - Physical/social
    - Application
  - "What is our risk to compromise?"
- Provide Reporting to Executives and Technical Staff
- Assist in Prioritization of Risks

Penetration Tests – About the Sample Set

- 1,894 Penetration Tests
  - 48 countries
- Many Included a Mixture of Vectors
  - Network, application, wireless, physical
- Tests Averaged 80 hours in Length

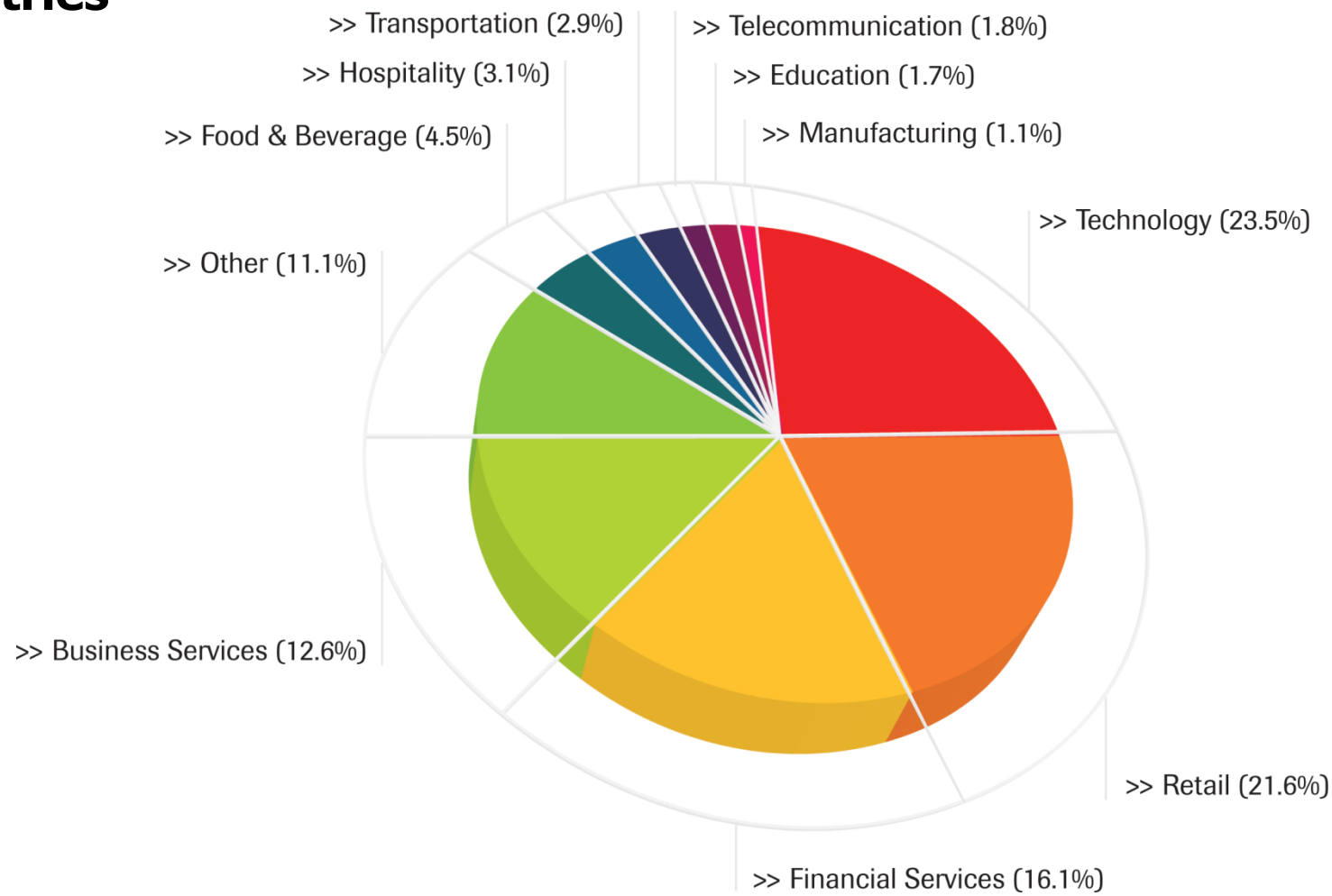
Penetration Tests – About the Sample Set

Countries Represented in 2009

Australia
Argentina
Belgium
Brazil
Bulgaria
Canada
Chile
China
Colombia
Croatia
Denmark
Dominican Republic
Ecuador
Egypt
France
Georgia
Germany
Greece
Hungary
Hong Kong
India
Japan
Iceland
Ireland
Lithuania
Luxembourg
Macedonia
Malaysia
Malta
Mexico
Moldova
Netherlands
Nigeria
Rep. of Cape Verde
Romania
Russian Federation
Saudi Arabia
Singapore
South Africa
Sri Lanka
Sweden
Switzerland
Taiwan
Turkey
Ukraine
United Arab Emirates
United Kingdom
United States

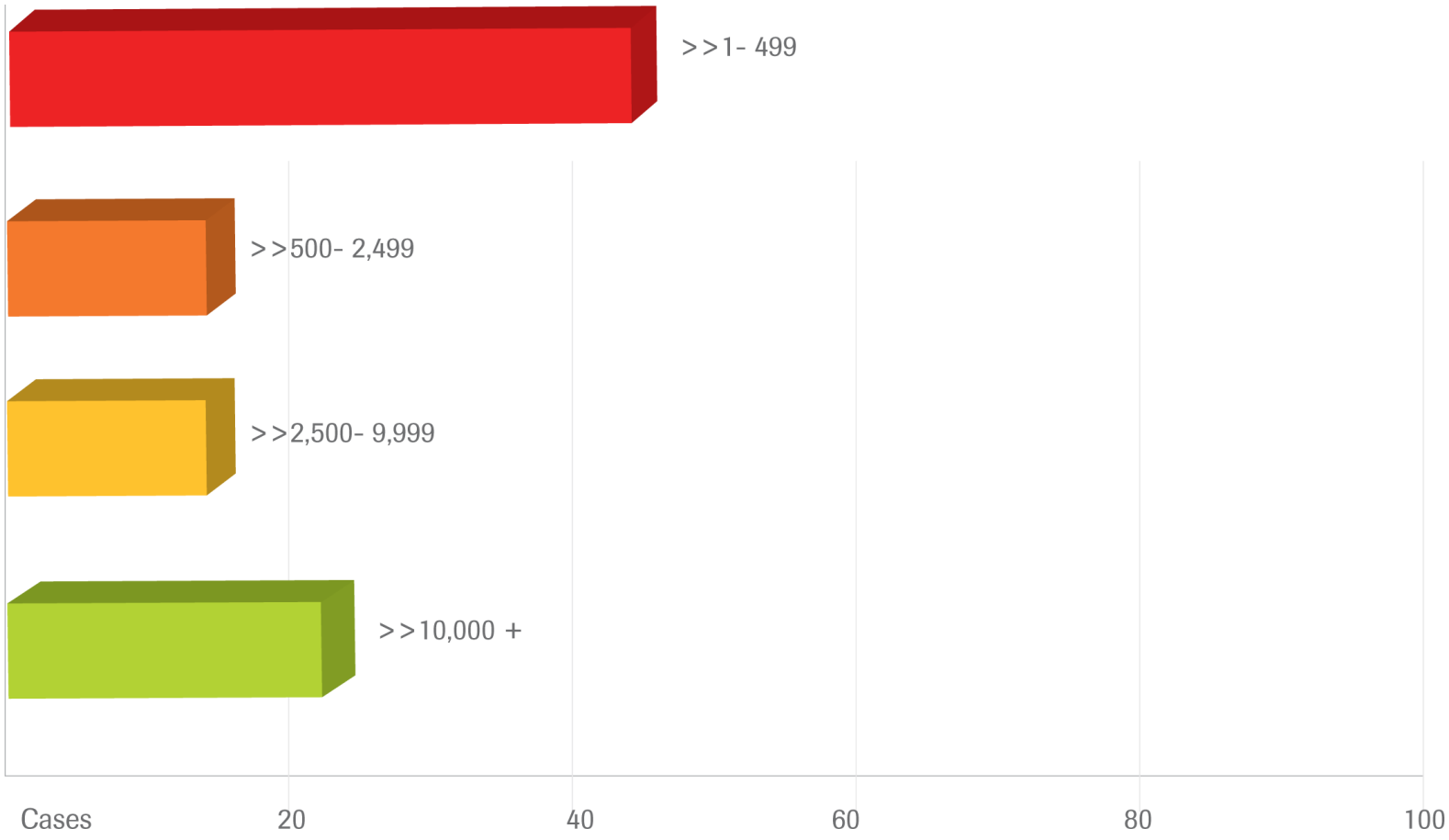
Penetration Tests – About the Sample Set

Industries



Penetration Tests – About the Sample Set

Company Size



Penetration Tests – About the Top 10s

- Intersection of Frequency & Criticality
- Not Meant to Replace other Industry Lists
  - Validate them?
- Organized in the Following Way:
  - Vulnerability
  - Definition
  - Impact
  - Circa
  - Attack Difficulty

Penetration Tests – Top 10 – External Network

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Unprotected Application Management Interface	1994	Easy
2	Unprotected Infrastructure Management Interface	1993	Easy
3	Access to Internal Application via the Internet	1997	Medium
4	Misconfigured Firewall Permits Access to Internal	1993	Hard
5	Default or Easy to Determine Credentials	1979	Trivial
6	Sensitive Information, Source Code, etc. in Web Dir	1990	Easy
7	Static Credentials Contained in Client	1980	Easy
8	Domain Name Service (DNS) Cache Poisoning	2008	Medium
9	Aggressive Mode IKE Handshake Support	2001	Easy
10	Exposed Service Version Issues (Buffer Overflows)	1996	Hard

Penetration Tests – Top 10 – External Network

#1 and #2 – Unprotected Management Interfaces

Definition: Leaving a default application (#1) or infrastructure (#2) management interface available from the Internet.

Impact: Complete control of an organization externally facing environment; loss of data is eminent.

Circa: Both 1994 (applications) and 1993 (infrastructure). Referencing early commercial Web server software and web-based managed devices.

Attack Difficulty: Easy-Medium

Penetration Tests – Top 10 – Internal Network

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Address Resolution Protocol (ARP) Cache Poisoning	1999	Medium
2	Microsoft SQL Server with Weak Creds for Admin	1979	Trivial
3	Weak Password for Admin Level System Account	1979	Trivial
4	Client Sends LM Response for NTLM Authentication	1997	Medium
5	Crypto Keys Stored Alongside Encrypted Data	1974	Easy
6	Cached Domain Credentials Enabled on Hosts	1999	Easy
7	NFS Export Share Unprotected	1989	Medium
8	Sensitive Information Transmitted Unencrypted	1991	Trivial
9	Sensitive Info Stored Outside Secured Zone	1993	Trivial
10	VNC Authentication Bypass	2006	Trivial

Penetration Tests – Top 10 – Internal Network

#1 – Address Resolution Protocol (ARP) Cache Poisoning

Definition: This is an OSI Layer 2 attack where messages are sent to local machine announcing the MAC address change for their default gateway.

Impact: Man in the middle attacks of many protocols are possible rendering credentials and even data exposed to the attacker.

Circa: Many articles and discussions around this method appeared in 1999 leading to the development of Dsniff MITM toolkit in 2000.

Attack Difficulty: Medium

Penetration Tests – Top 10 – Wireless

Rank	Vulnerability Name	Circa	Attack Difficulty
1	Wireless Client Associates While on Wired Network	2004	Medium
2	Wireless Client Probes from Stored Profiles (KARMA)	2005	Medium
3	Continued Use of WEP Encryption	2004	Easy
4	Easily Determined WPA/WPA2 Pre-Shared Key	2006	Easy
5	Legacy 802.11 FHSS with No Security Controls	1999	Hard
6	Lack of Publicly Secure Packet Forwarding Enabled	2004	Medium
7	Wireless Clients Using "Guest" Instead of "Secured"	2003	Easy
8	Lack of Segmentation Between Wireless and Wired	1993	Easy
9	Wireless Device Connected and Left Unattended	2000	Easy
10	WPA used with TPIK and 802.11e QOS	2008	Hard

Penetration Tests – Top 10 – Wireless

#1 – Wireless Clients Associates While on Wired Network

Definition: In many cases, wireless clients will probe and associate with known networks broadcasting in the local vicinity.

Impact: Attackers can use this technique to compromise the wireless host and in turn gain access to the wired network.

Circa: In 2004, hostapd was introduced and popularized this attack vector.

Attack Difficulty: Medium

Penetration Tests – Top 10 – Physical/Social

Rank	Vulnerability Name	Attack Difficulty
1	Lack of Plate Covering Gap from Door Lock to Strike Plate	Medium
2	Motion Sensors Allow Egress from Sensitive Areas	Medium
3	Sensitive Data Left in Plain View	Trivial
4	Credentials/Pretext Not Verified Effectively	Easy
5	Dumpsters are Accessible and Unlocked	Easy
6	Bypass Route to Secured Areas Available	Easy
7	Motion Sensors Mounted Incorrectly – No Coverage	Medium
8	Unlocked and Otherwise Accessible Computers	Trivial
9	Network Not Protected Against Rogue Devices	Easy
10	Sensitive Data Cabling is Accessible from Public Areas	Easy

Penetration Tests – Top 10 – Physical/Social

#1 – Lack of Plate Covering Gap from Door Latch to Strike Plate

Definition: Using a stiff card or needle nose pliers, one can release the magnetic retainer and open the door.

Impact: Complete access control fail with little to no evidence of attack.

Attack Difficulty: Medium

Circa: Old as dirt or at least as long as lock-based access controls have been around.

Penetration Tests – Top 10 – Application

Rank	Vulnerability Name	Circa	Attack Difficulty	OWASP (2010)
1	SQL Injection	1998	Medium	A1
2	Logic Flaw	1985	Easy	None
3	Authorization Bypass	1997	Easy	A3
4	Authentication Bypass	1960	Easy	A4/A7
5	Session Handling	1997	Medium	A3
6	Cross-Site Scripting (XXS)	2000	Hard	A2
7	Vulnerable Third-Party Software	1960	Medium	A6
8	Cross-Site Request Forgery (CSRF)	1988	Hard	A5
9	Browser Cache-Related Flaws	1998	Medium	None
10	Verbose Errors	1980	Medium	None

Penetration Tests – Top 10 – Application

#2 – Logic Flaw

Definition: A flaw that allows an attacker to bypass intended applications controls/functions.

Impact: Typically fraud related. Depending on the application this could have devastating effects on the data used by the system.

Circa: Logic flaws have been part of computing since the beginning, but started to gain recognition as a security issue in the mid-1980s.

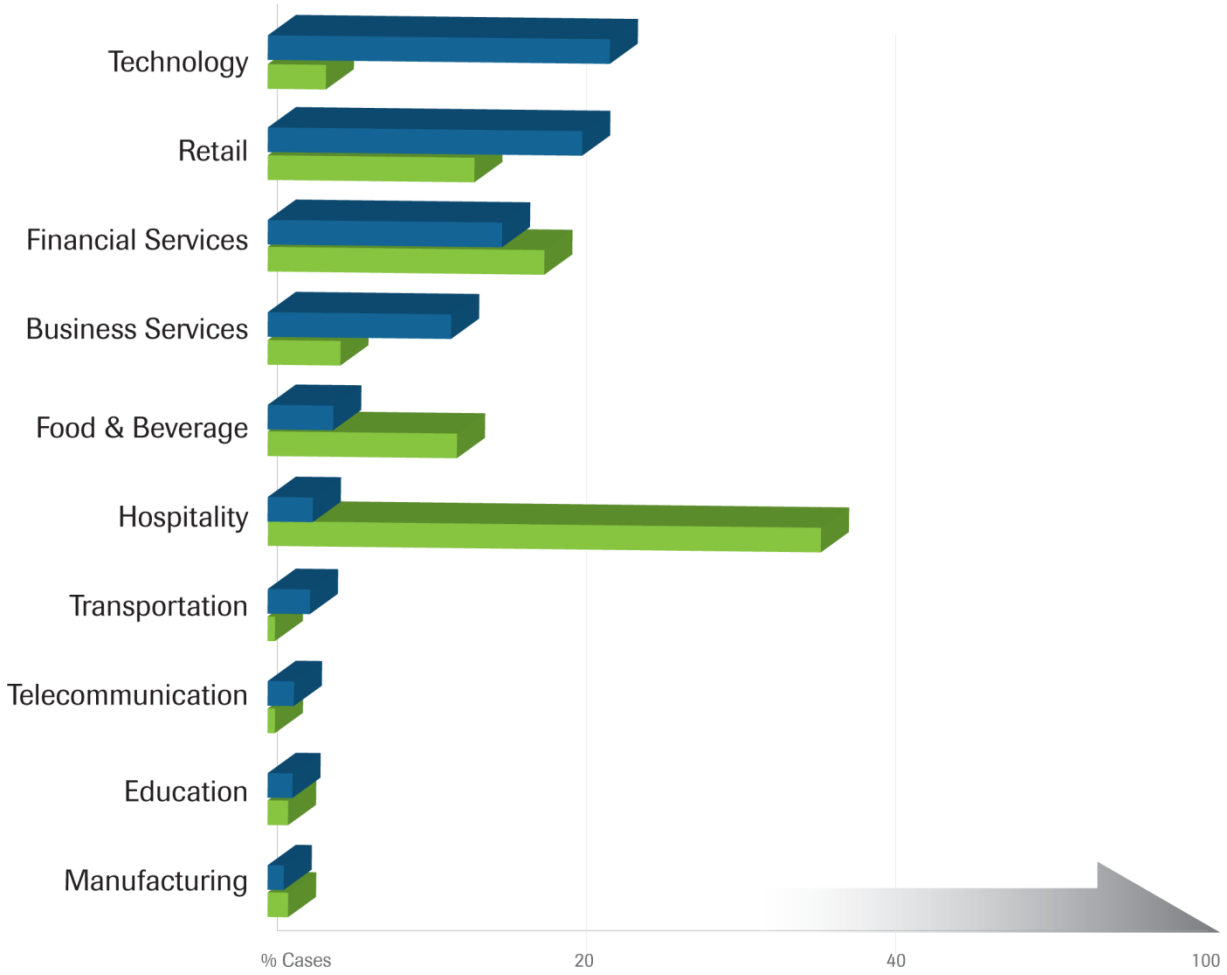
Attack Difficulty: Easy

The Global Remediation Plan - Clarity

- Compromise = Major Loss of Business
- Overlooked systems and vulnerabilities
  - Lead to compromises
- Targeted Attacks
  - On the rise
  - In 2009, Hospitality was hit HARD; who is next?

The Global Remediation Plan – Industry Comparison

Penetration Tests vs. Investigations



The Global Remediation Plan – The Plan

Rank	Strategic Initiative
1	Perform and Maintain a Complete Asset Inventory; Decommission Old Systems
2	Monitor Third Party Relationships
3	Perform Internal Segmentation
4	Rethink Wireless
5	Encrypt Your Data
6	Investigate Anomalies
7	Educate Your Staff
8	Implement and Follow a Software Development Life Cycle (SDLC)
9	Lock Down User Access
10	Use Multifactor Authentication Every Where Possible

Conclusions

- Attackers are using old vulnerabilities
- Attackers know they won't be detected
- Organizations do not know what they own or how their data flows
- Blind trust in 3rd parties is a huge liability
- Fixing new/buzz issues, but not fixing basic/old issues
- In 2010, take a step back before moving forward

Bonus Material in The Report

The Global Security Report 2010 contains details of the content in this presentation plus many informative pieces:

- **"Off-the-Shelf versus Custom Malware"**
- **"Penetration Testing versus Vulnerability Scanning"**
- **"How Layer 2 Attacks Work"**
- **"The FHSS Myth"**
- **"Top 5 Techniques to Unlawfully Enter a Data Center"**
- **"Automated versus Manual"**

Where to get it?

- **On the Black Hat Web site**
  - http://www.blackhat.com
  - Immediately following this talk!

- **On the Trustwave Web site**
  - https://www.trustwave.com/whitePapers.php
  - February 9th, 2010

Contacts

Phone: +1 312 873-7500
E-mail: GSR2010@trustwave.com
Web: https://www.trustwave.com/spiderlabs
Twitter: @SpiderLabs / @Trustwave

Nicholas J. Percoco
Senior Vice President, SpiderLabs
Trustwave
Phone: +1 312 873-7471
Email: npercoco@trustwave.com
Twitter: @c7five

Trustwave®

SpiderLabs℠

Thank You!