Healthcare IT Transformation Evidence-Based Security & Privacy

Peter Tippett, M.D., PhD
Vice President, Technology & Innovation
Chief Medical Officer

peter.tippett@verizonbusiness.com

PROPRIETARY STATEMENT

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

verizon

Verizon

verizon wireless

- 86.6M subscribers
- Next-generation, high-speed broadband wireless network
- Broadband access in 245 U.S. Major Metropolitan Areas
- V CAST mobile content services
- Highest customer loyalty for U.S. wireless providers

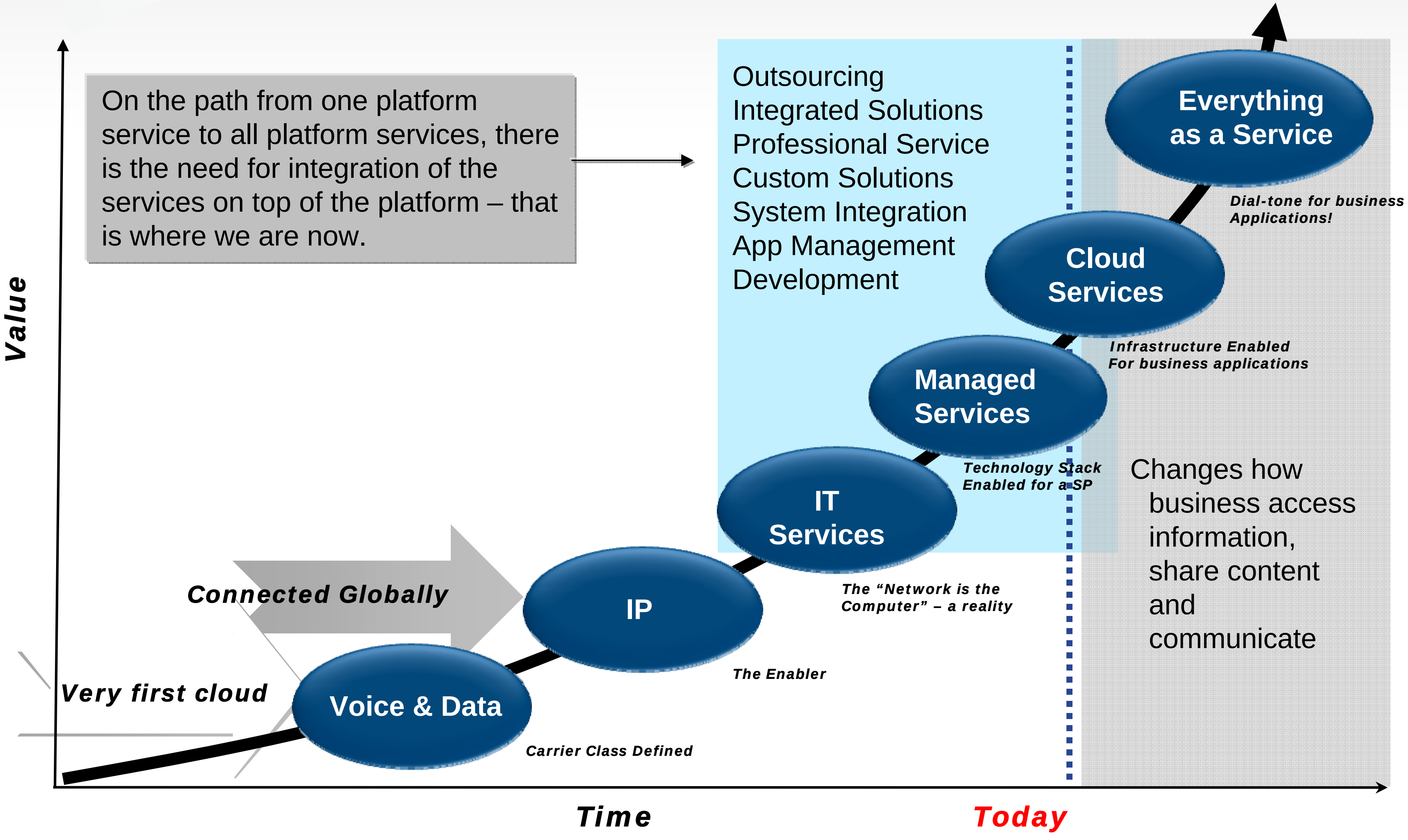
verizon Telecom

- U.S. domestic wireline, local and long distance services
- Consumer and small business
- Transforming the telecom franchise into a broadband and entertainment business
- 3.1M FiOS Internet subscribers and 2.5M FiOS TV subscribers

verizon business

- Enterprise and government customers worldwide include 98% of Fortune 500
- One of the world’s largest wholly owned, facilities-based global networks
- Manage 250K+ servers, routers, devices
- Leading provider of managed information security services in the world

Evolution of a Communication Provider



On the path from one platform service to all platform services, there is the need for integration of the services on top of the platform – that is where we are now.

Outsourcing
Integrated Solutions
Professional Service
Custom Solutions
System Integration
App Management
Development

Everything as a Service

Dial-tone for business Applications!

Cloud Services

Infrastructure Enabled For business applications

Managed Services

Technology Stack Enabled for a SP

IT Services

The "Network is the Computer" – a reality

IP

The Enabler

Connected Globally

Very first cloud

Voice & Data

Carrier Class Defined

Changes how business access information, share content and communicate

Value

Time

Today

What does a IT group actually DO?

Application

Computing

Voice

Network

Security

Collaboration

Mobility

Compliance

Support

- Strategy
- Architecture
- Design
- Purchasing
- Hosting
- Management

Oddly enough, this is pretty much exactly what we do at Verizon Business

Of course, you don't have just one application, or computer, or network, or security issue…

Application

Computing

Voice

Network

Security

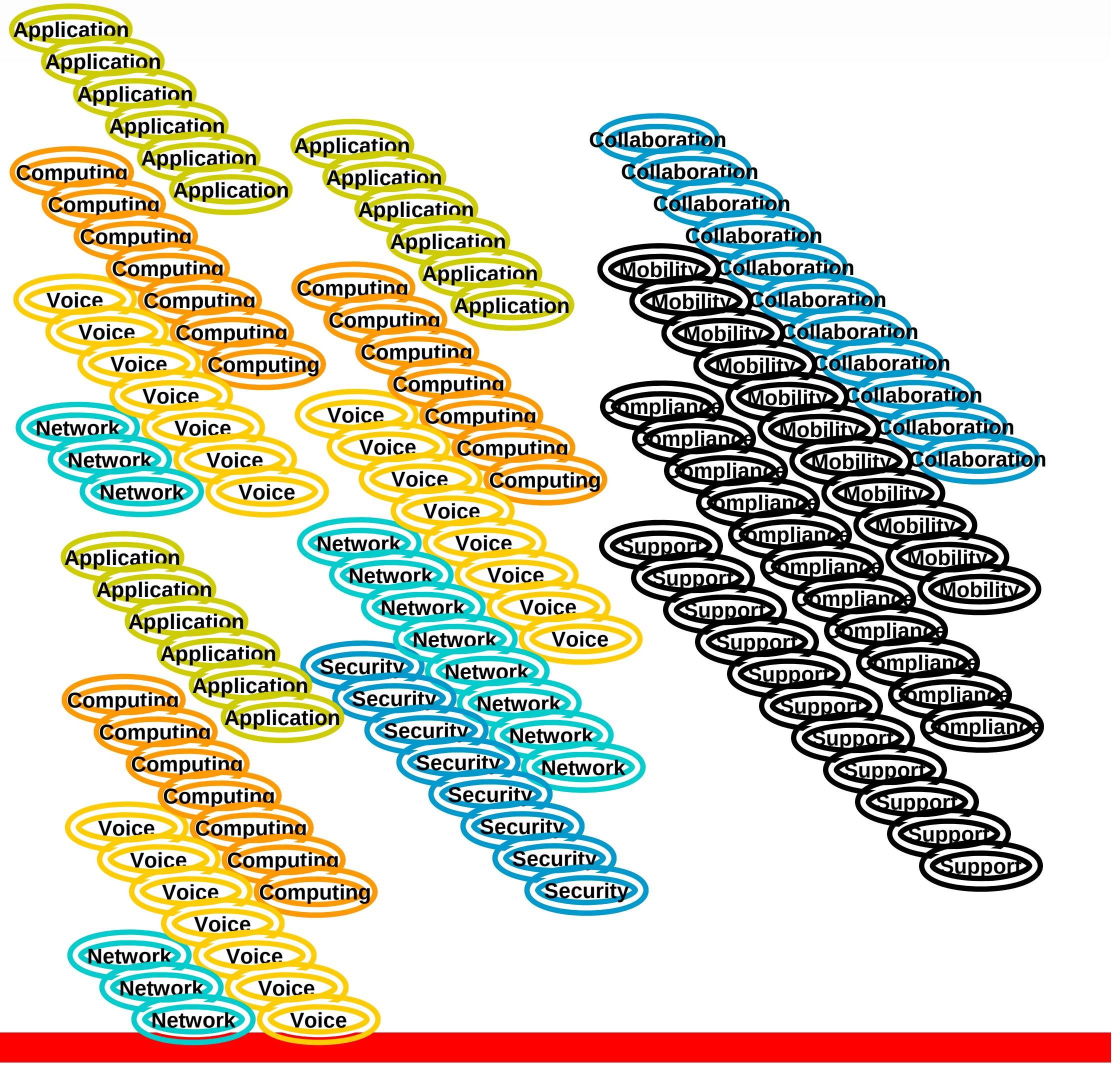
Collaboration

Mobility

Compliance

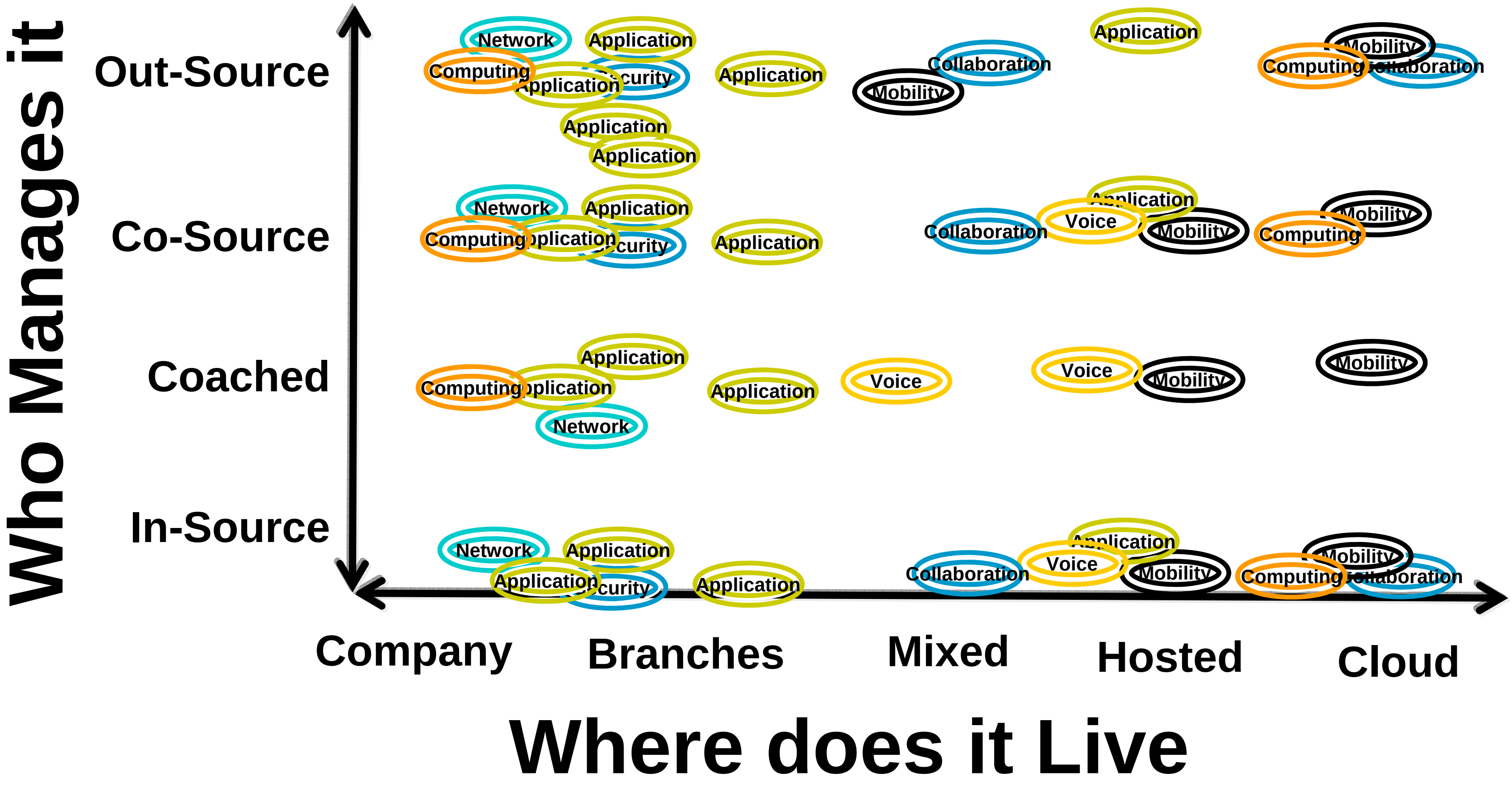
Support

You Have dozens or hundreds of each of these things.



But also…

Who makes the most sense to Manage each of these things



Who Manages it

Out-Source

Co-Source

Coached

In-Source

Company

Branches

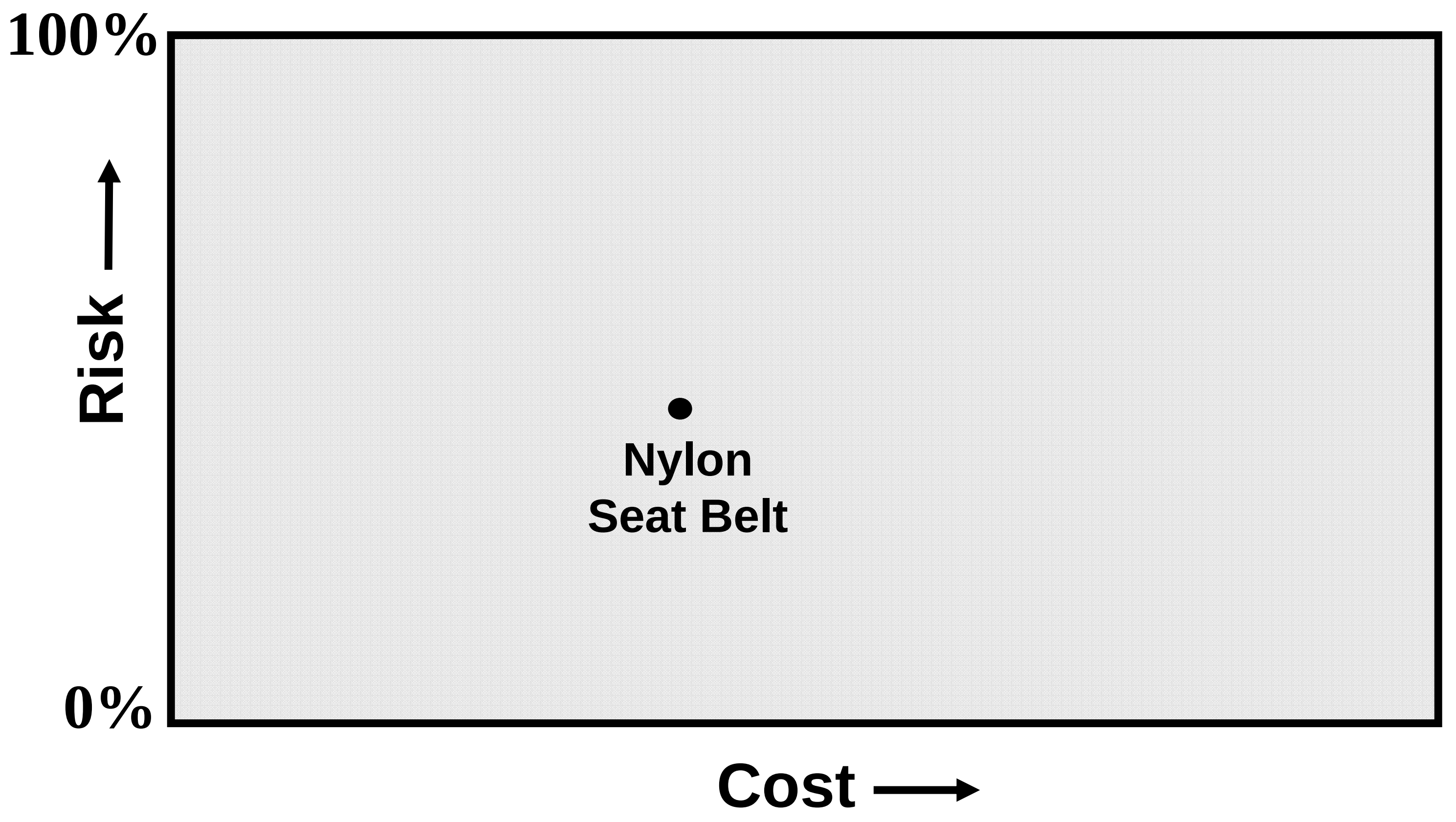
Mixed

Hosted

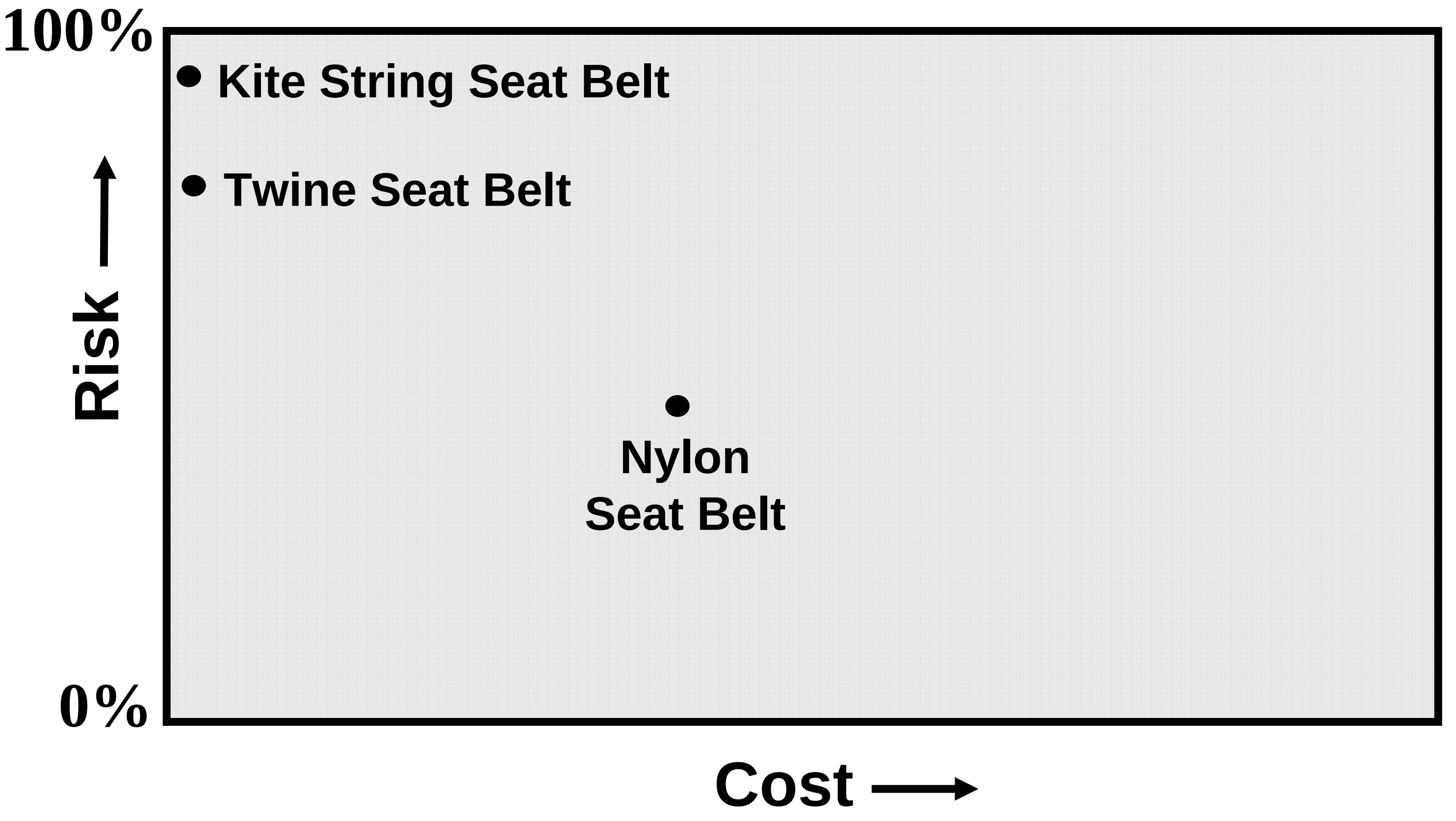
Cloud

Where does it Live

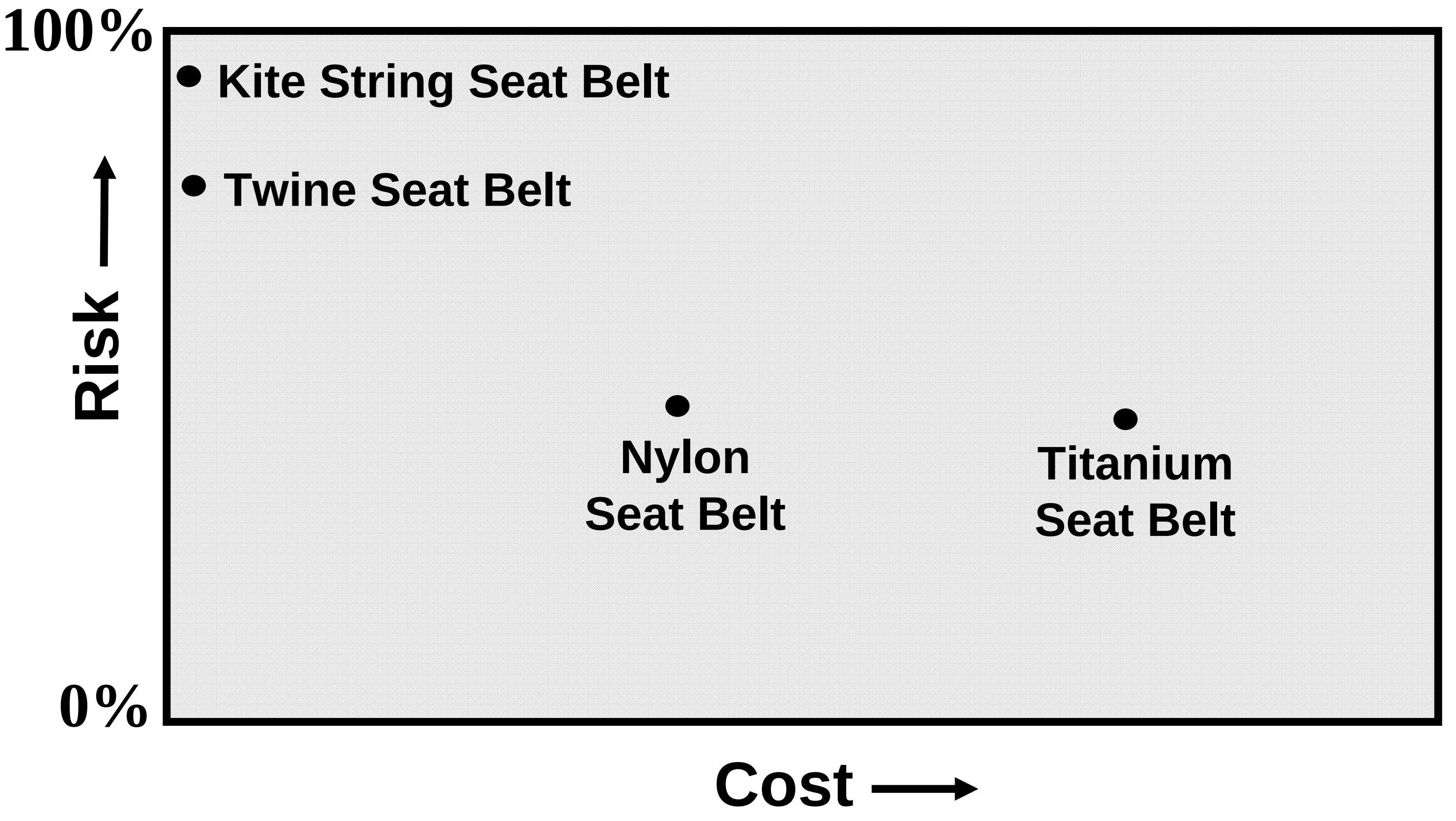
A Simple Thought Experiment



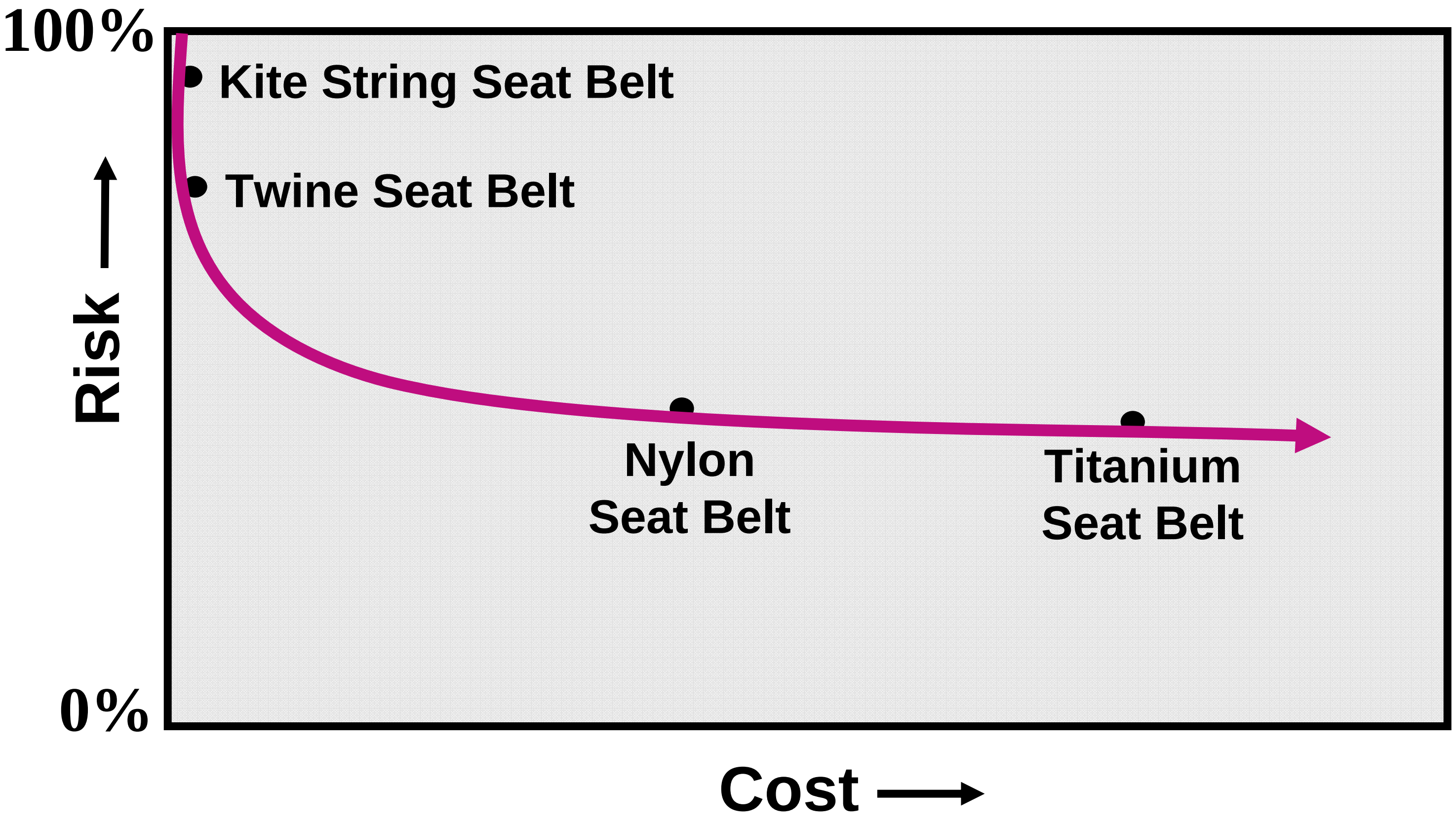
A Simple Thought Experiment



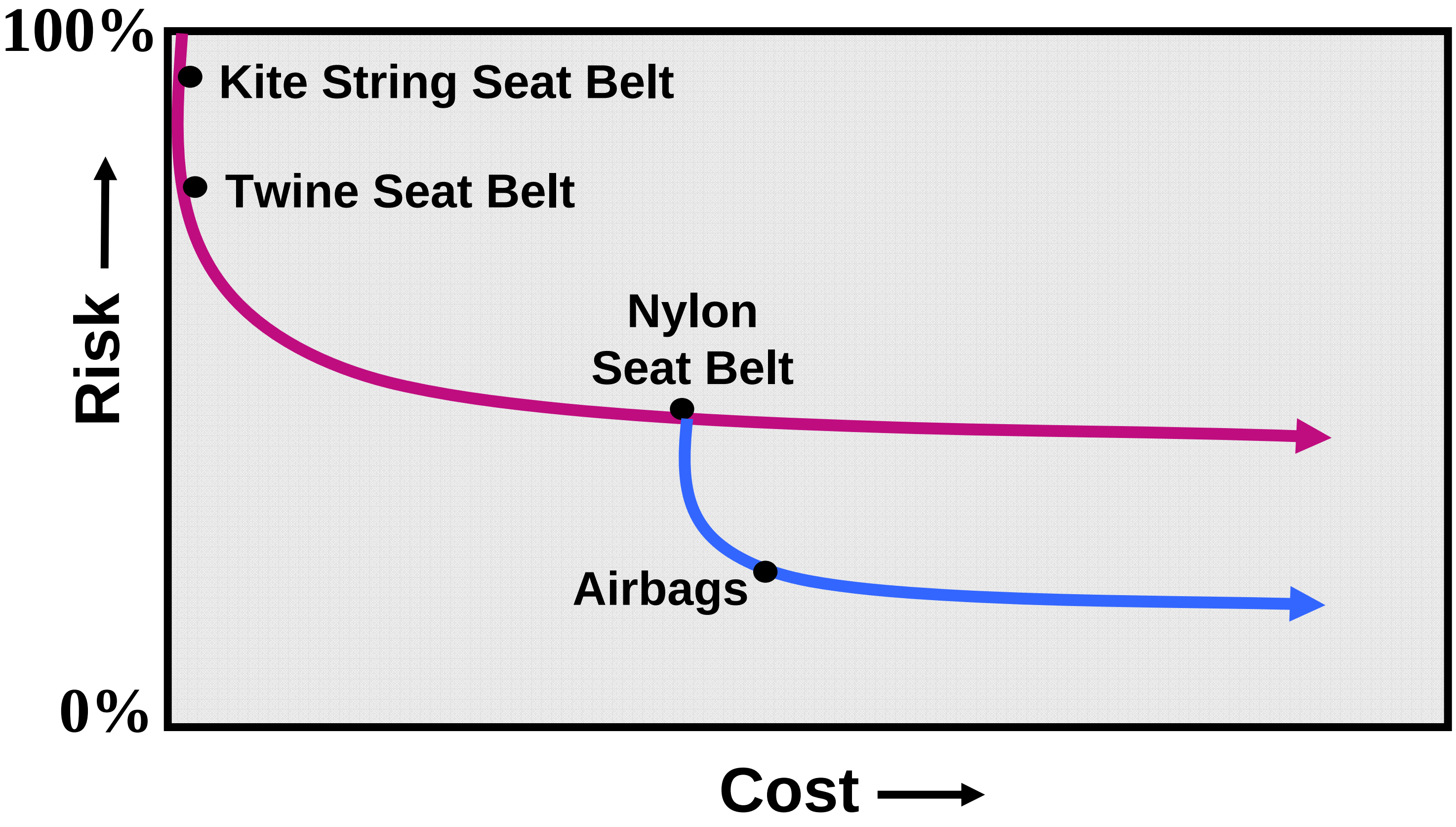
A Simple Thought Experiment



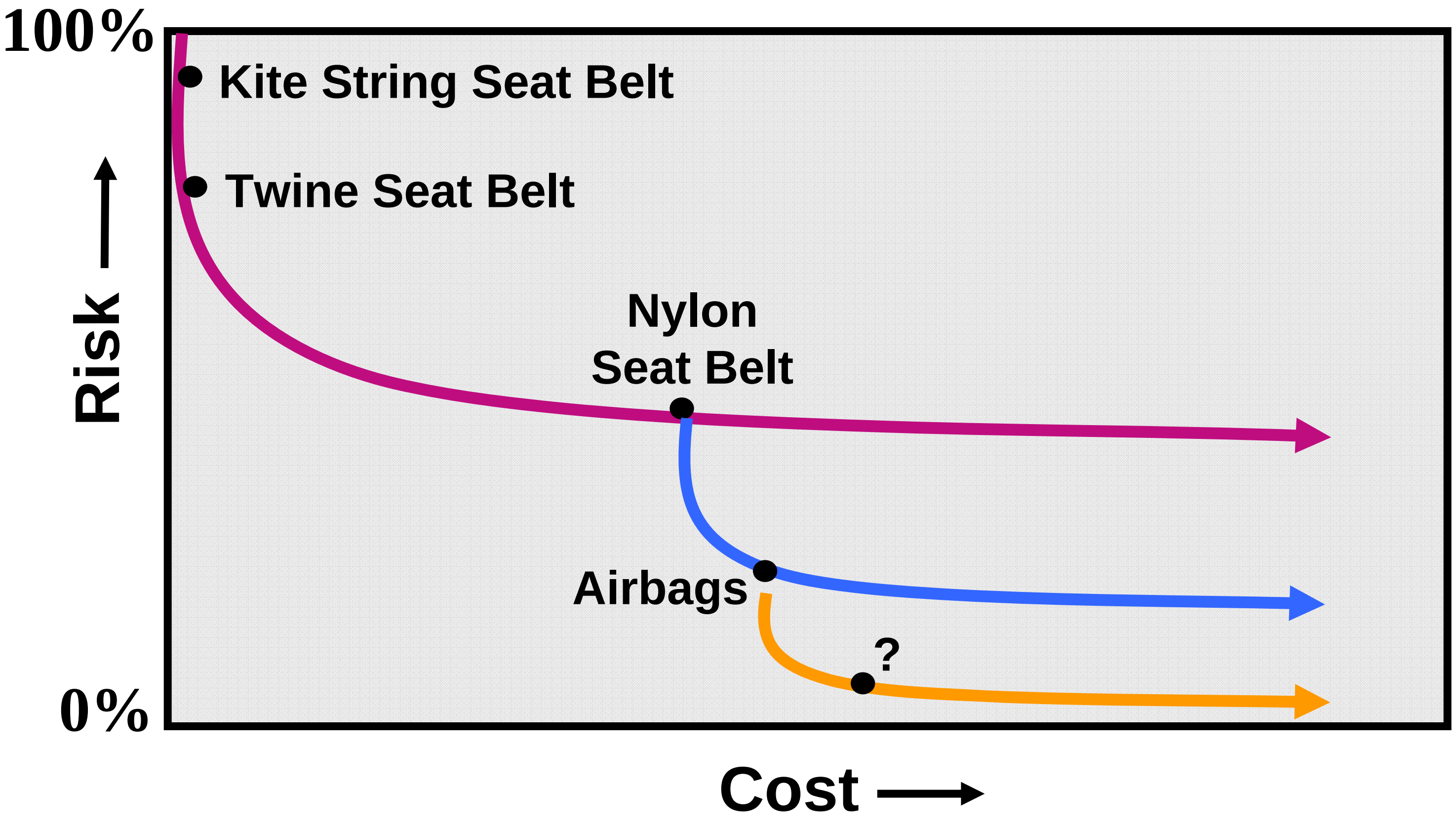
A Simple Thought Experiment



A Simple Thought Experiment



A Simple Thought Experiment



Seven Types of Risk Intelligence

1	Threat & Vulnerability Intel Track and analyze new software vulnerabilities and related attacks
2	Underground Intel Watch discussions, code sharing, planning,... Historically BBS, then Usenet, now more IRC and Cons...
3	ICSA Labs Intel Security product testing and security consortia operations. 400+ products
4	Forensics Intel Data and Intel from forensics investigations (200+ cases per year).
5	MSS Intel Data from IDS, FW, IPS, Applications… Management & Monitoring SOC operations
6	Net Intel Data from backbone. Sensors on more than 1 Billion VzB addresses. Netflow Honey nets, Honey Pots…
7	IT Services Intel Manage 4200 companies’ networks, thousands of applications, helpdesk data, etc…

Verizon Data Breach Investigations Reports

A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

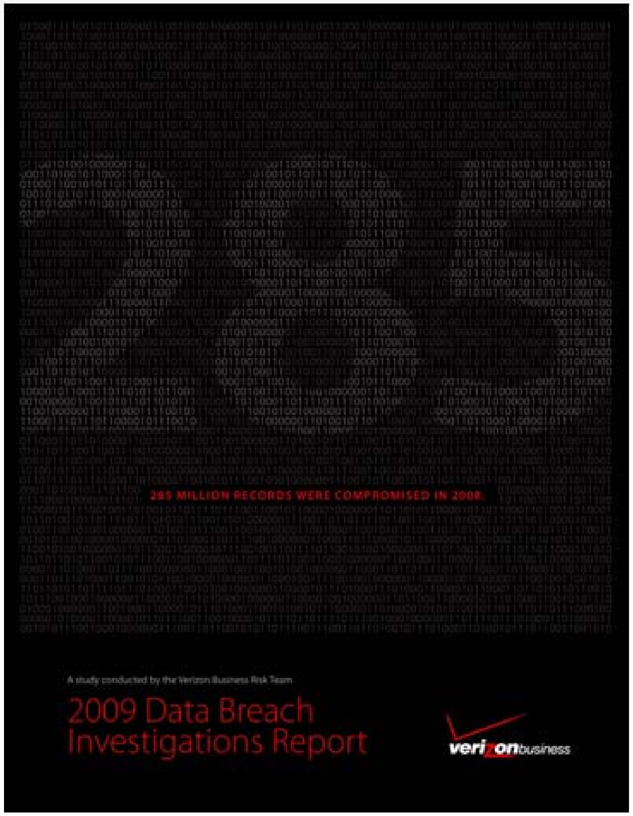
2008 DATA BREACH INVESTIGATIONS REPORT

Four Years of Forensic Research. More than 500 Cases.
One Comprehensive Report

A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

2008 DATA BREACH INVESTIGATIONS SUPPLEMENTAL REPORT

Industry Focus. More Analysis. Greater Insight.
A comparison of risk factors among the finance, food, retail, and tech industries.



285 MILLION RECORDS WERE COMPROMISED IN 2008.

A study conducted by the Verizon Business Risk Team

2009 Data Breach Investigations Report

638 Cases / 5 years

http://verizonbusiness.com/databreach
http://securityblog.verizonbusiness.com

Breach Sources

External sources

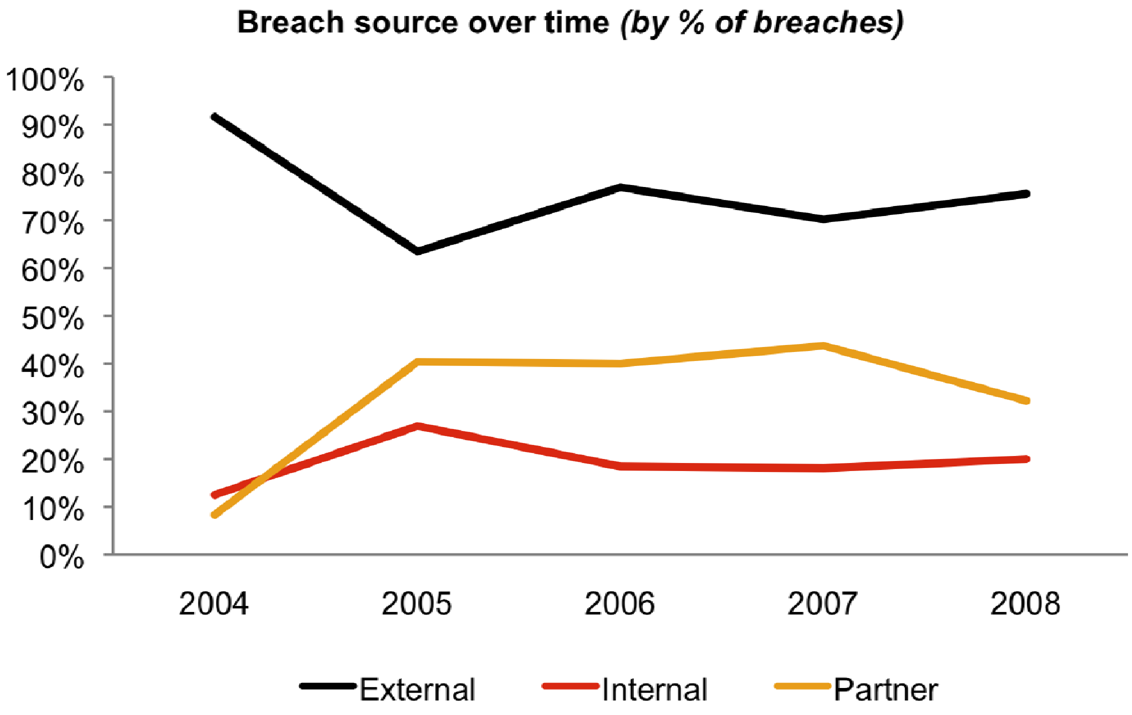
- 90+% of stolen records linked to organized crime

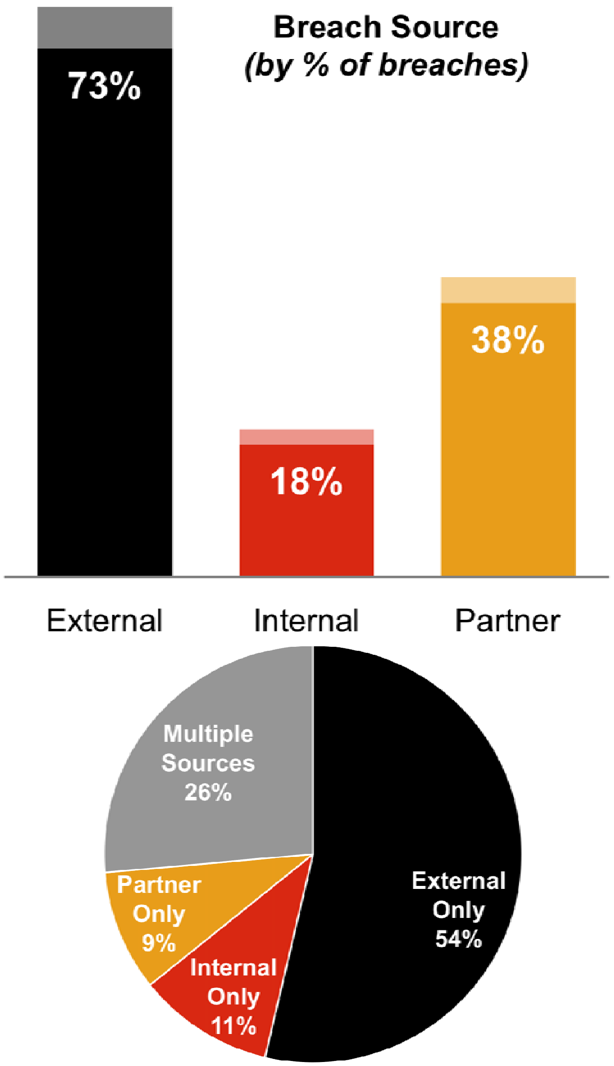
Internal sources

- Roughly equal between end-users and IT admins

Partner sources

- Mostly hijacked third-party accounts/connections

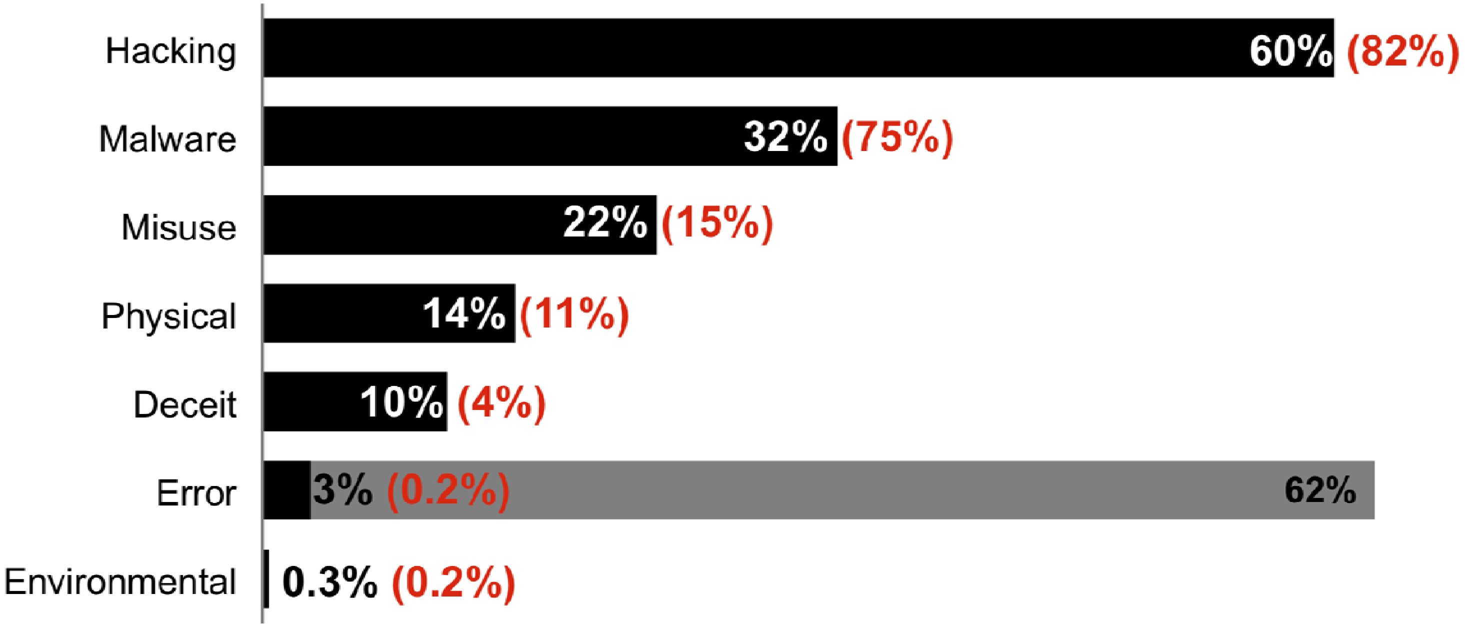




Breach Methods

- Most breaches and records linked to Hacking & Malware
- Misuse is fairly common
  - Mostly abuse of authorized access
- Physical attacks
  - Theft and tampering most common
- Deceit and social attacks
  - Varied methods, vectors, and targets
- Error is extremely common
  - Usually contributory (62%) rather than direct cause (3%)
  - Mostly omissions followed by misconfigurations

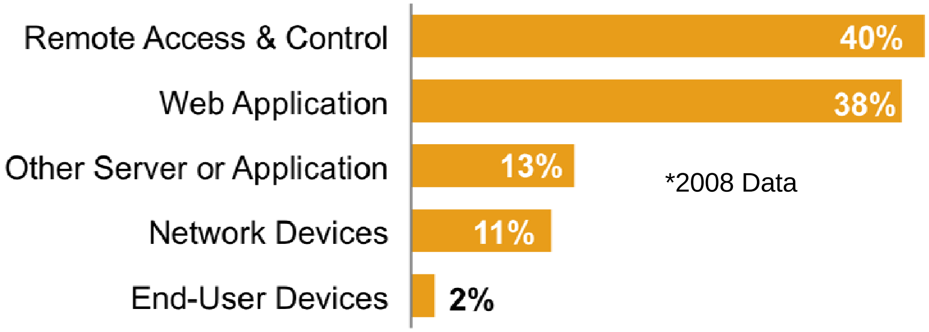
Threat Category ***(by % of breaches and records)***



Breakdown of Hacking
(60% of breaches)

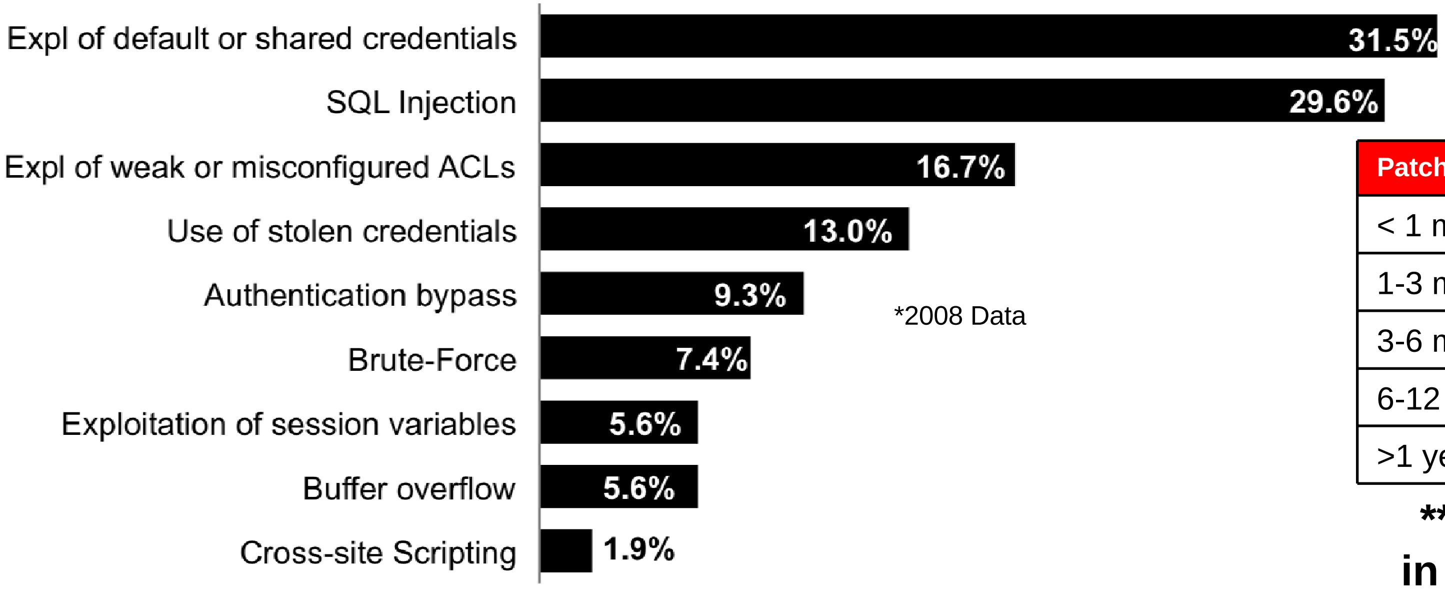
- Default credentials, SQL injection, weak ACLs most common methods
- Minority of attacks exploit patchable vulns; Most of them are old
- Web applications & remote access connections are main vectors

Hacking Vector *(by % of breaches)*



*2008 Data

Hacking Methods *(by % of breaches)*



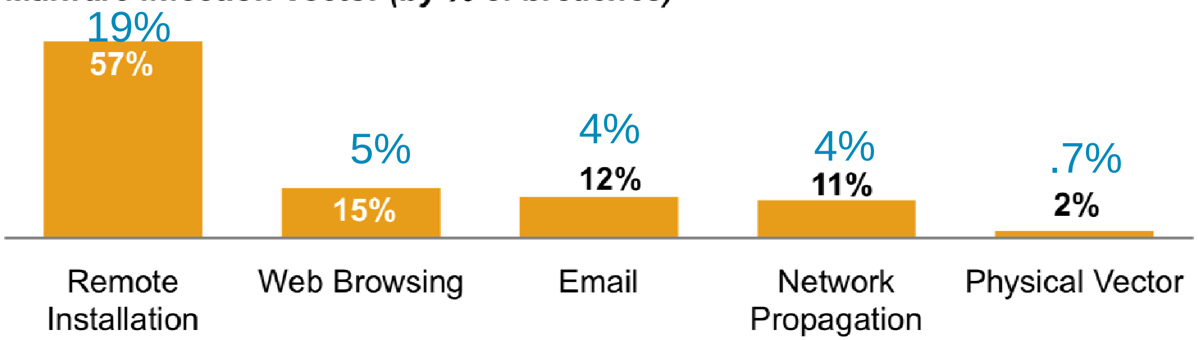
*2008 Data

Patch availability prior to breach		
< 1 month	0%	0%
1-3 months	4%	0.6%
3-6 months	6%	1%
6-12 months	16%	2.6%
>1 year	74%	12%

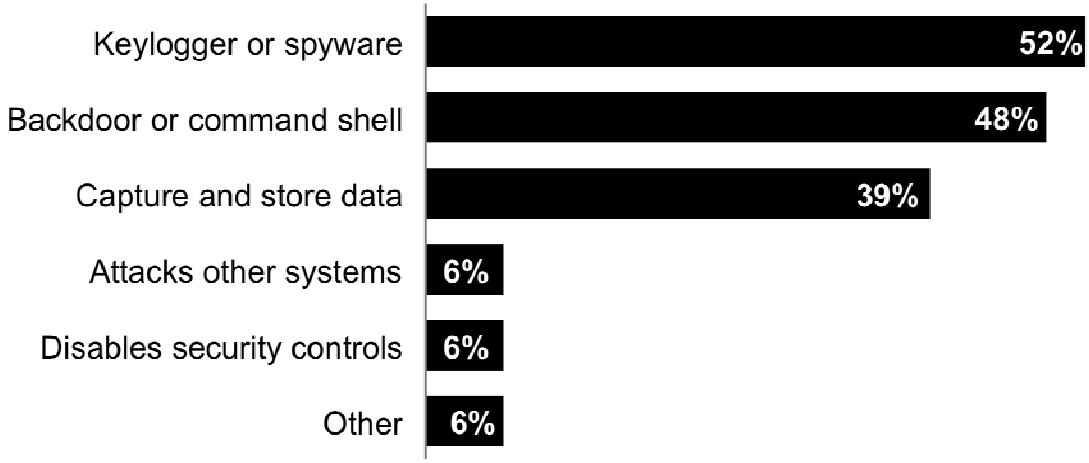
****Vulns exploited in 16% of breaches**

Breakdown of Malware (32% of breaches)

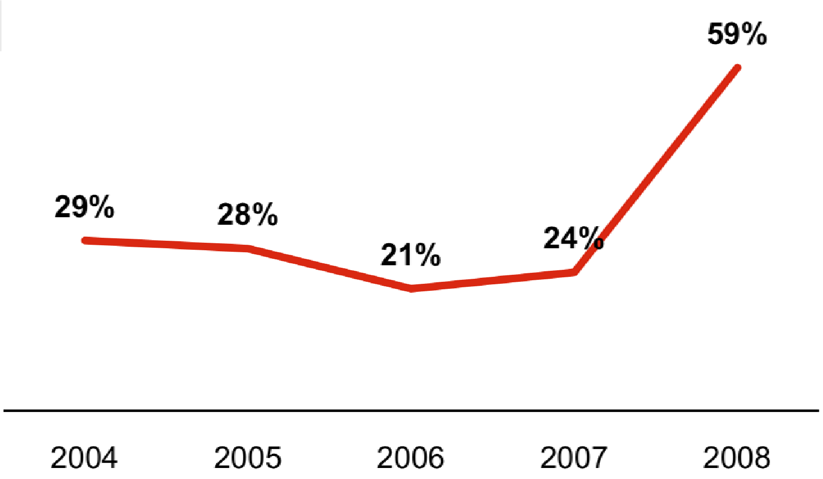
- Most malware installed by remote attacker
- Malware captures data or provides access/control
- Increasingly customized



Malware Infection Vector *(by % of breaches)*



Malware Function *(by % of breaches)*



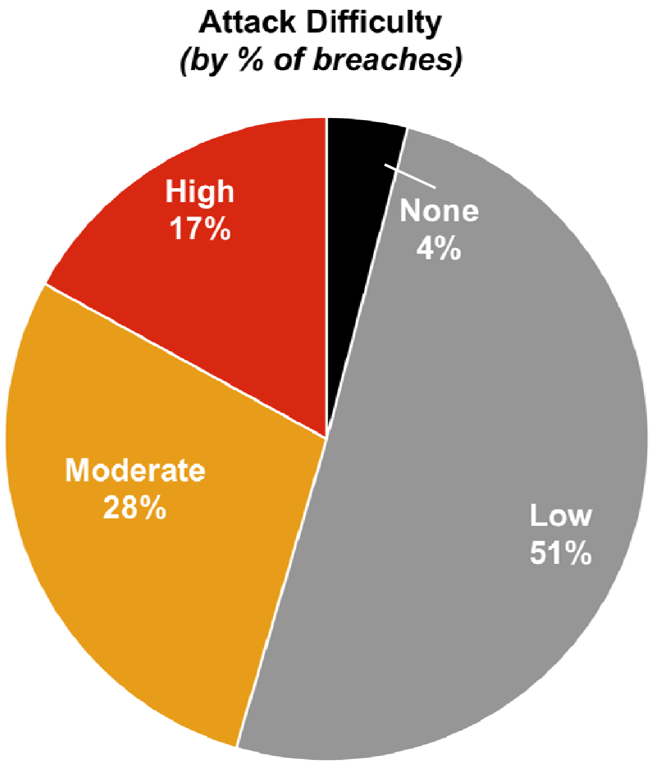
Malware customization *(by % of breaches)*

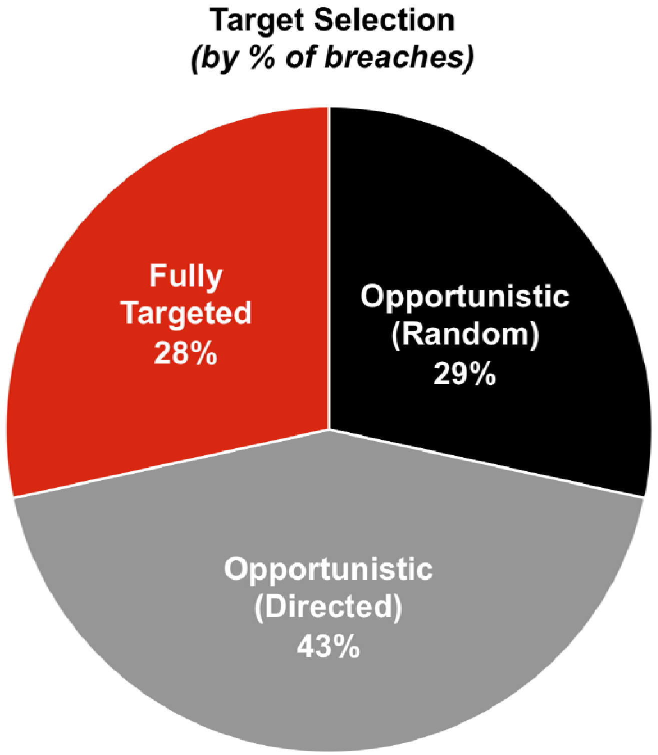
Attack Difficulty and Targeting

- Highly difficult & sophisticated attacks not the norm
  - Difficulty usually malware rather than intrusion
- Fully targeted attacks in minority but growing
  - % doubled in 2008
- Difficult and targeted attacks increasingly damaging
  - Shows ROI is good for skilled attackers

Percentage of Records Breached

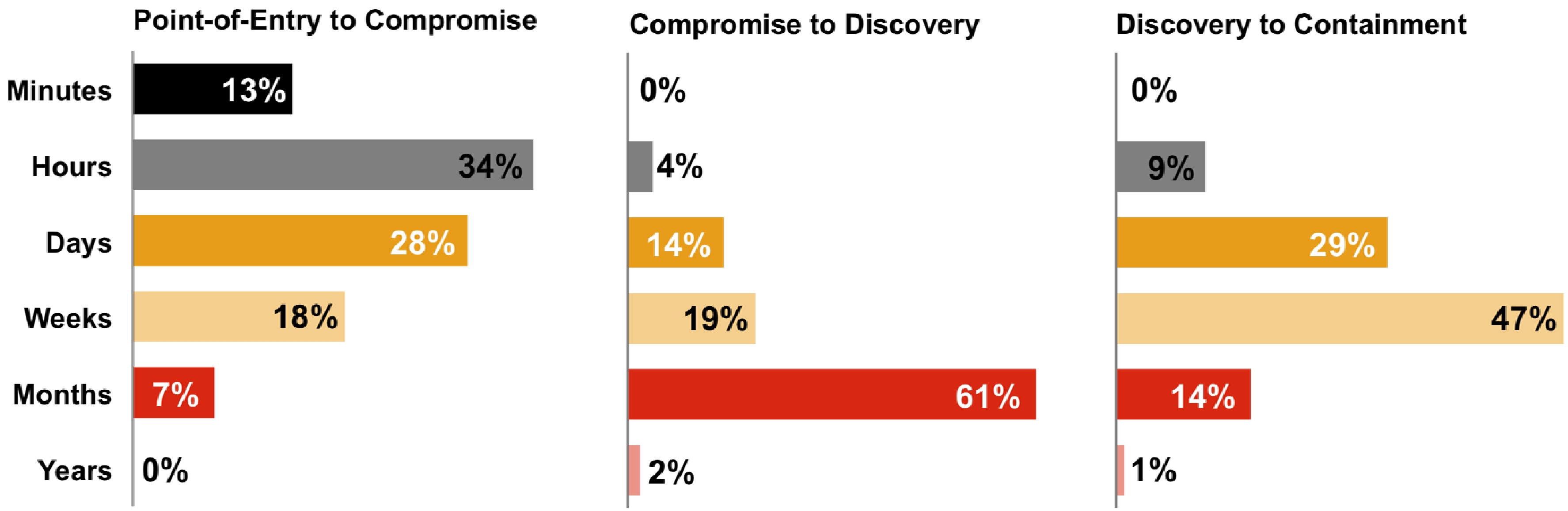
	'04-'07	2008
Highly Difficult	68%	95%
Fully Targeted	14%	90%



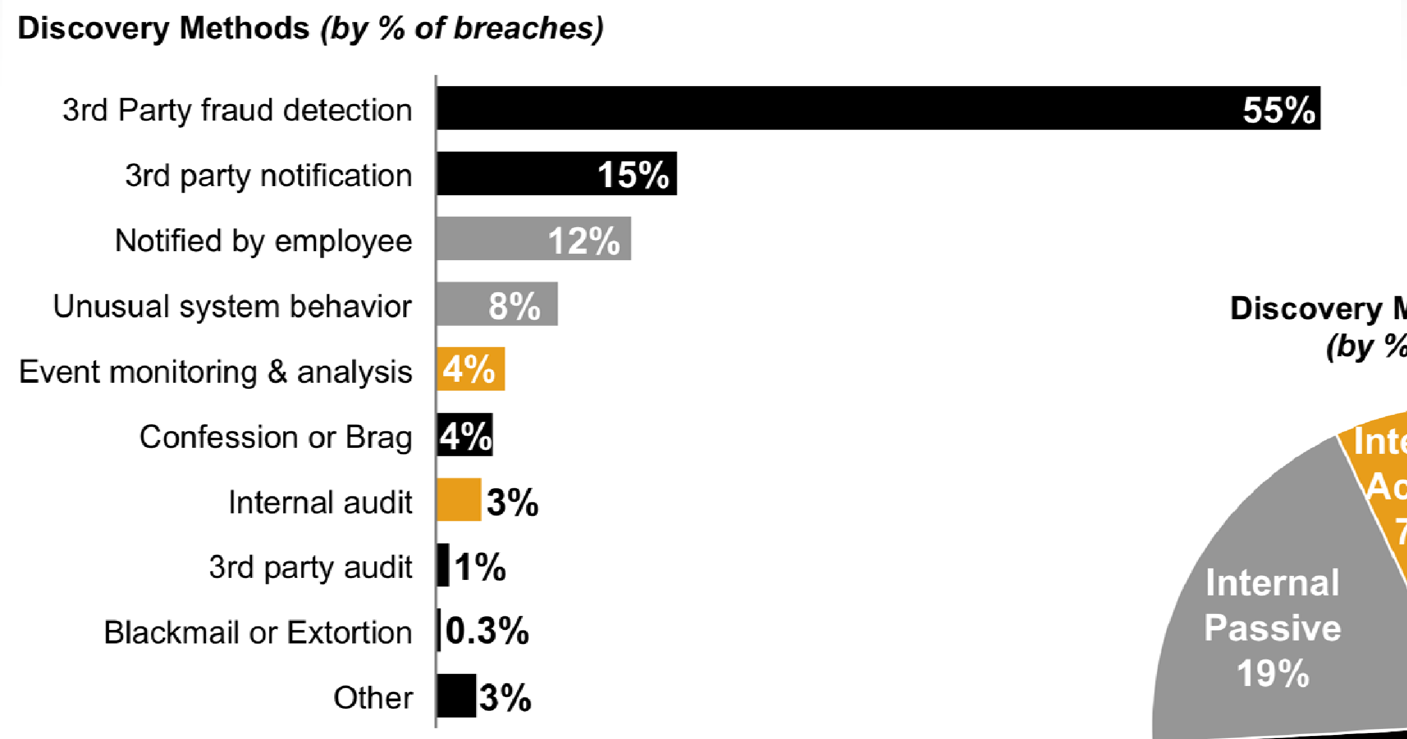


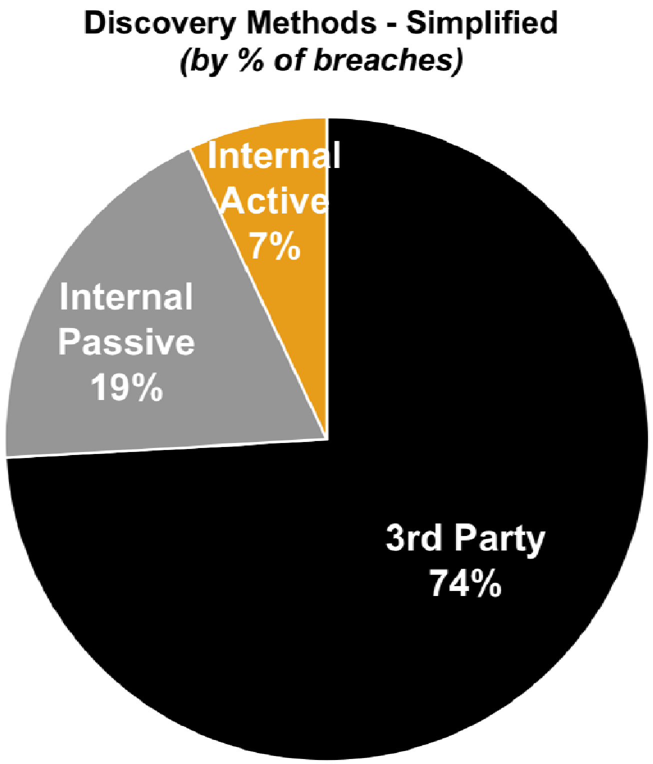
Breach Timeline

- Data compromised within hours/days after breaching perimeter
  - Actually good news for detection & prevention
- Breaches go undiscovered for months
  - Ability to detect breaches woefully inadequate (or at least inefficient)
- It typically takes days to weeks to contain a breach
  - Poor planning and response procedures



Breach Discovery Methods



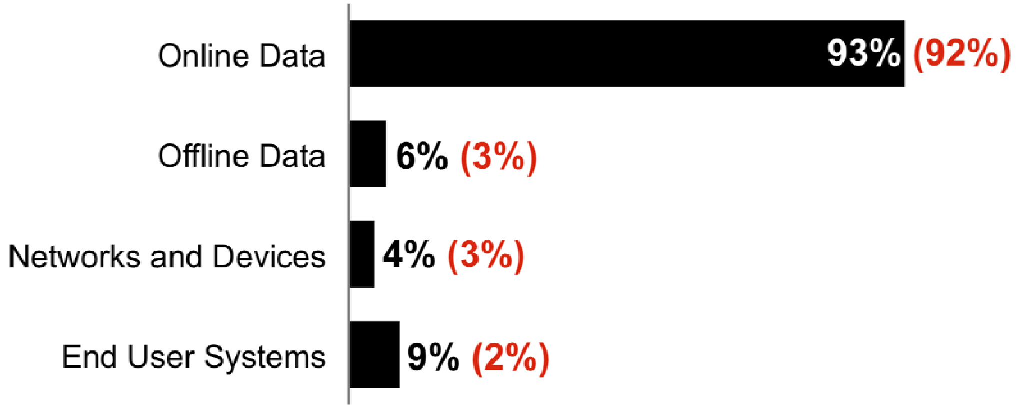


- Most breaches discovered by a third party
- Majority of internal discoveries are accidental
- Effectiveness of event monitoring far below potential
  - Evidence found in existing log files for 80% of breaches

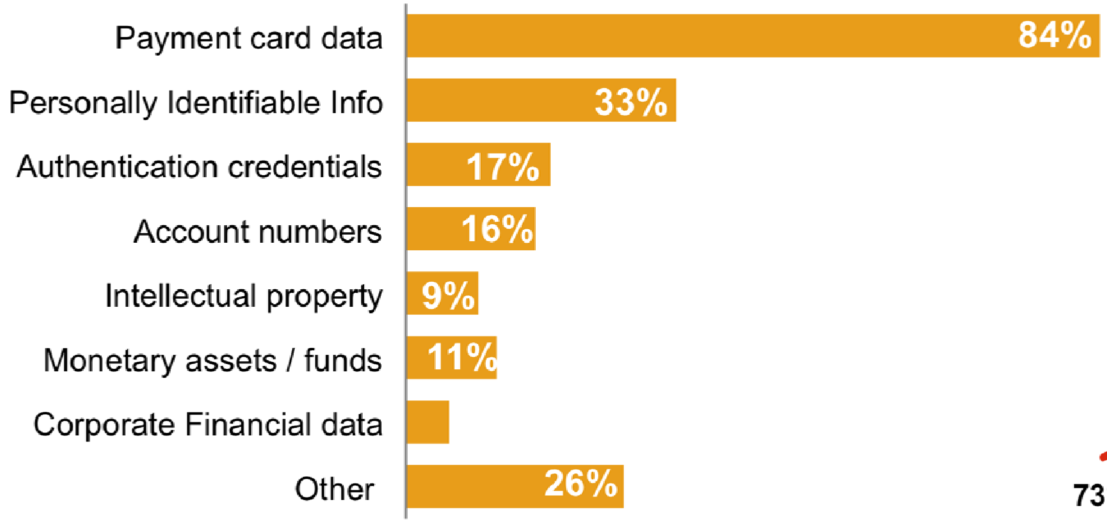
Compromised Assets and Data

- Most data breached from online systems
  - Conflicts with public disclosures
- Cybercrime is financially motivated
  - Cashable data is targeted
- Other types common as well
  - Auth credentials allow deeper access
  - Intellectual property at 5-year high

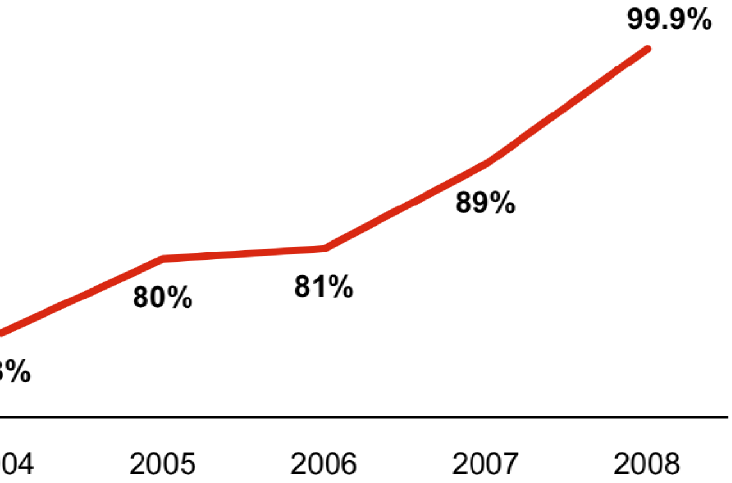
Compromised Assets *(by % of breaches and records)*



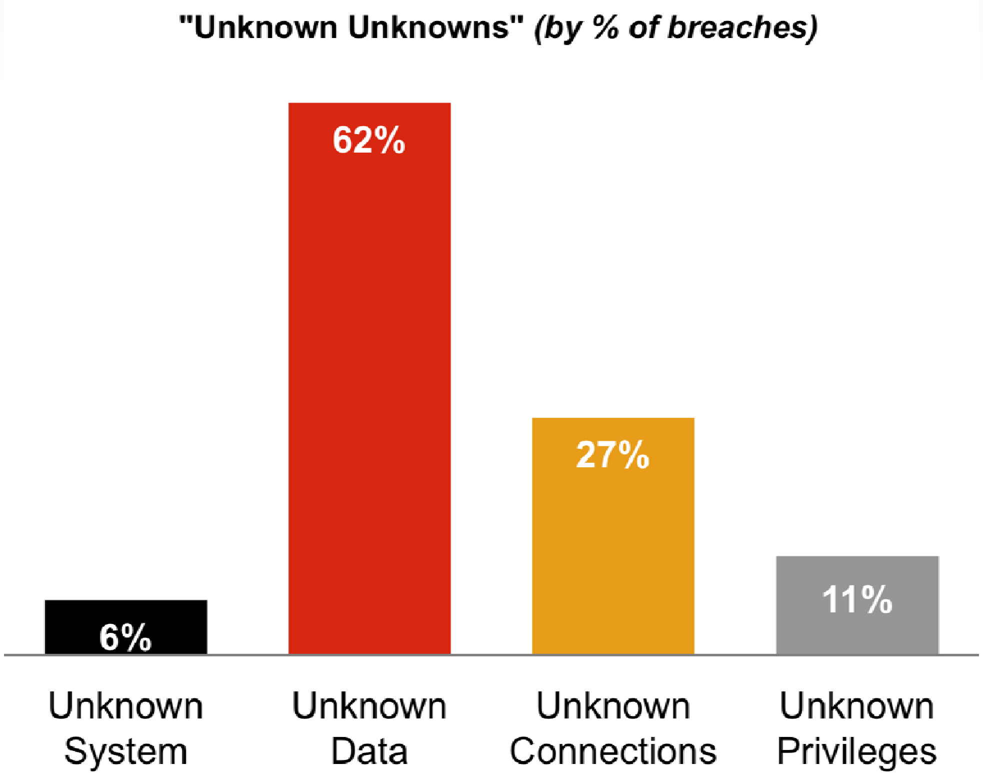
Data Types *(by % of breaches)*



% of records breached from Online Data Assets



Unknown Unknowns



An **SYSTEM** unknown to the organization

DATA unknowingly stored on an asset

Unknown or forgotten ICT **CONNECTIONS**

Accounts and **PRIVILEGES** not known to exist

"Yes, we're positive all sensitive data of that type is confined to these systems."

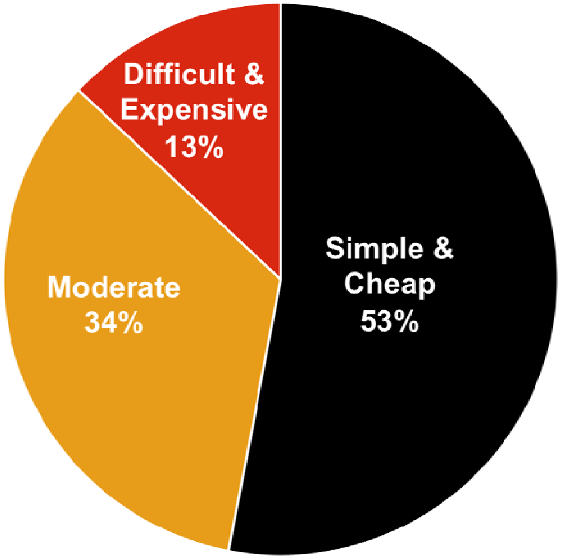
Victim Commonalities

- False assumptions regarding information assets
- Low awareness of network and system activity
- Do not necessarily have a terrible security program
- Fail to consistently and comprehensively follow “the basics”
- Lack of assurance and validation procedures
- Cost of prevention orders of magnitude less than impact
- An inefficient approach to security
  - Focus too much on things that don’t happen
  - Focus too little on the things that do happen

If you like mnemonics:

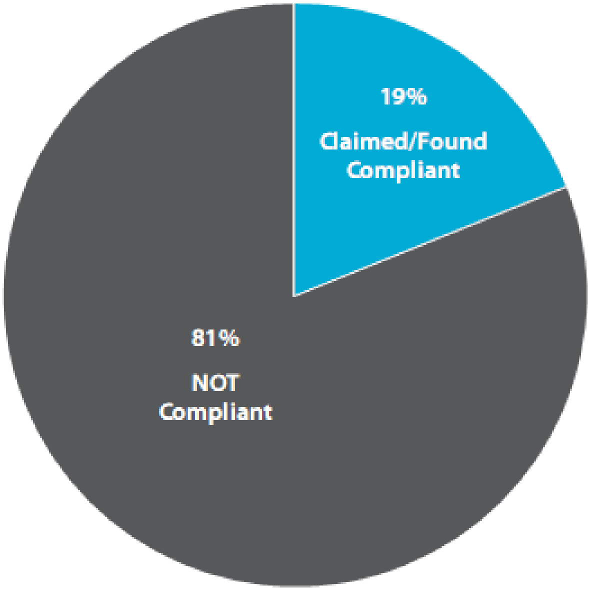
- **V**isibility
- **V**ariability
- **V**iability

Cost of Prevention (Hindsight)
(by % of breaches)



PCI DSS

Figure 37. PCI compliance status based on last assessment by percent of breach victims

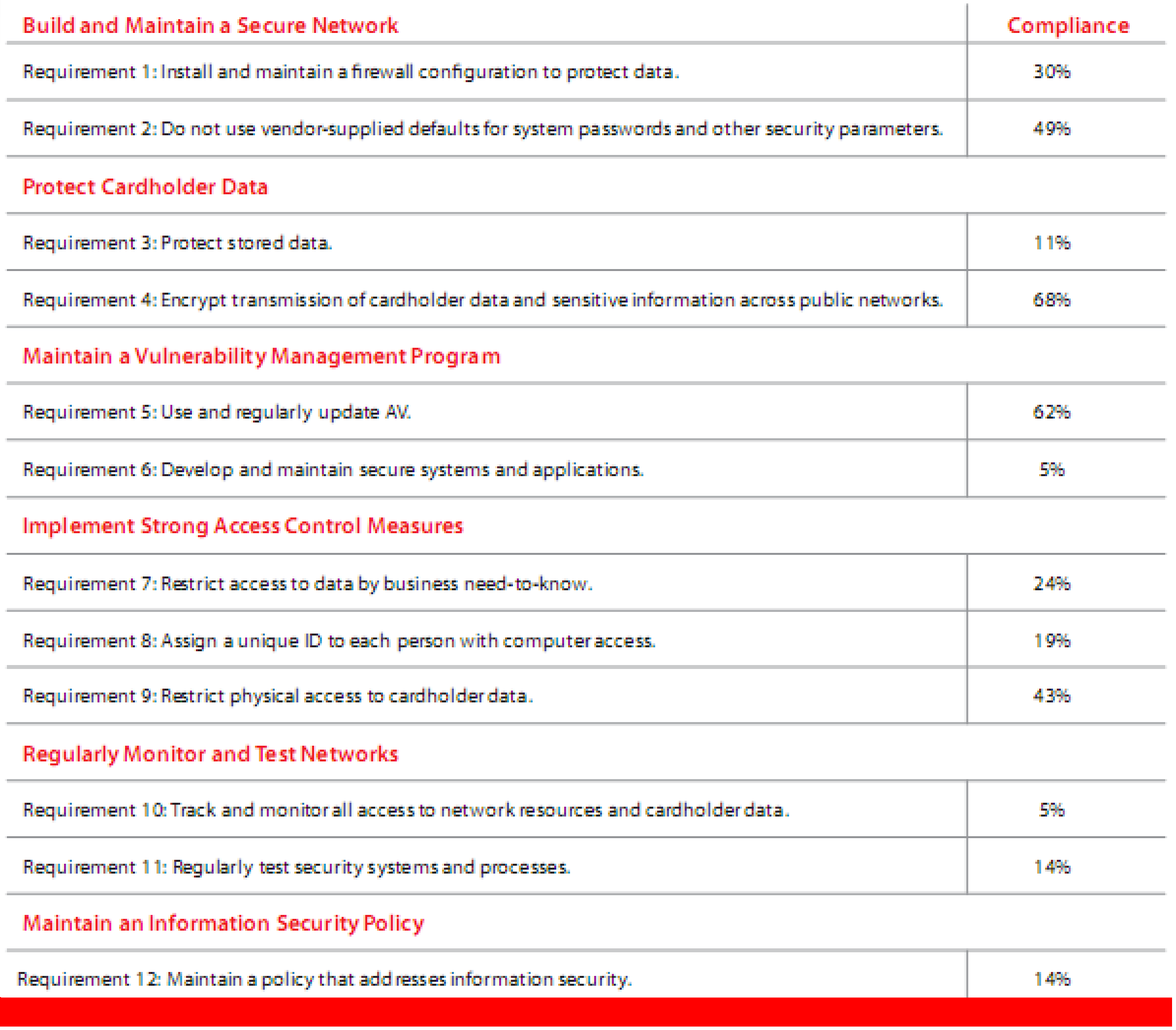


Is PCI a Failure? NO!

Then why were 19% breached?

- Self-attestation
- Study includes failures only
- Scope / Unknowns
- Assessment Sampling
- Partners (transitive trust)

Table 10. Results of post-breach PCI DSS reviews conducted by Verizon Business IR. Values represent the percentage of organizations for which each requirement was found to be in place.



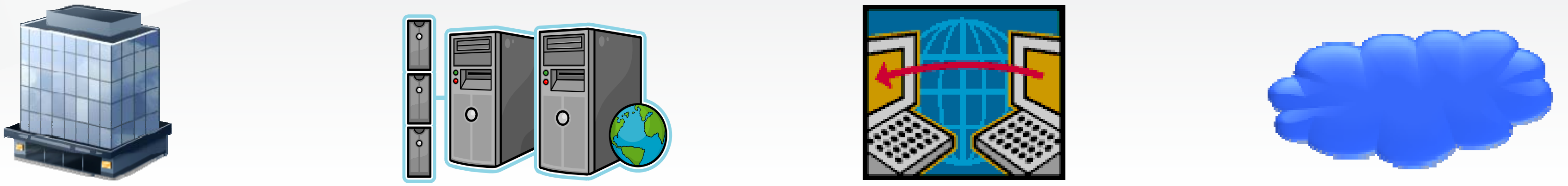
Build and Maintain a Secure Network	Compliance
Requirement 1: Install and maintain a firewall configuration to protect data.	30%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	49%
Protect Cardholder Data	
Requirement 3: Protect stored data.	11%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	68%
Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update AV.	62%
Requirement 6: Develop and maintain secure systems and applications.	5%
Implement Strong Access Control Measures	
Requirement 7: Restrict access to data by business need-to-know.	24%
Requirement 8: Assign a unique ID to each person with computer access.	19%
Requirement 9: Restrict physical access to cardholder data.	43%
Regularly Monitor and Test Networks	
Requirement 10: Track and monitor all access to network resources and cardholder data.	5%
Requirement 11: Regularly test security systems and processes.	14%
Maintain an Information Security Policy	
Requirement 12: Maintain a policy that addresses information security.	14%

Recommendations

- Align process with policy
- Achieve “Essential” then worry about “Excellent”
- Secure Business Partner Connections
- Create a Data Retention Plan
- Control data with transaction zones
- Monitor event logs
- Create an Incident Response Plan
- Increase awareness
- Engage in mock incident testing

- Changing default credentials is key
- Avoid shared credentials
- User Account Review
- Application Testing and Code Review
- Smarter Patch Management Strategies
- Human Resources Termination Procedures
- Enable Application Logs and Monitor
- Define “Suspicious” and “Anomalous” (then look for whatever “It” is)

Security Product Continuum



Prem-based

MSS

- FW
- IDS/IPS
- VM
- AV
- Content Filtering
- Log mon/mgmt
- App FW
- SSL VPN

Managed SEM

PKI/Unicert

Security Resale Services/CPE

Professional Services

- Forensics/IR
- Assessments/Remediation
- Design/implementation
- Strategy/IT Security road mapping

Hosted

MSS

Corp ID Auth

Managed PKI

Compliance Mgr for Med Biz

SaaS

Vuln Scanning

App Scanning

Web Scanning

Email Scanning

PCI Program

Partner Security

SSL OnDemand

SMP (has human delivery components)

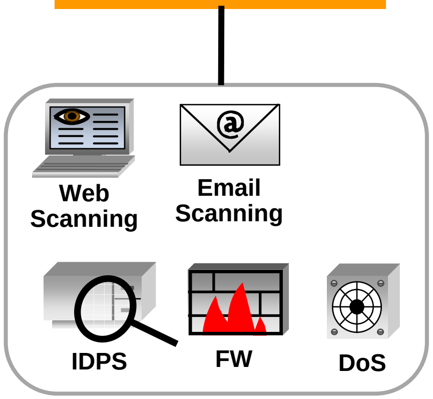
Web Access Mgmt

Network-based

DOS protection

NBFW (SG Overlay)

Reputational IDS



Evidence-Driven, External Facing (Thought Leadership)

A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

2008 DATA BREACH INVESTIGATIONS REPORT

Four Years of Forensic Research. More than 500 Cases. One Comprehensive Report

A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM

2008 DATA BREACH INVESTIGATIONS SUPPLEMENTAL REPORT

Industry Focus. More Analysis. Greater Insight.
A comparison of risk factors among the finance, food, retail, and tech industries.

A study conducted by the Verizon Bu

2009 Data B
Investigatio

ICSA Labs Product Assurance Report

A study conducted by the Verizon RISK Team

Table of Contents

Introduction 2

Methodology 2

285 MILLION RECORDS WERE COMPROMISED IN 2008.

A study conducted by the Verizon Business RISK Team

2009 Data Breach Investigations Supplemental Report

Anatomy of a Data Breach

Early 2010:

VERIS – Open Source

Verizon Incident Classification & Reporting

PCI Study

DBIR –USSS Study

Social Media Study

Accreditations

- ISO 9001:2008 – Quality (2005)
- ISO 17025:2005 – Competence (2009)
- Guide 65 – Commercial Certification Body (2010)
- Guide 7 – Standards Body (TBD)

IPv6 / USGv6

Standard for IPv6 testing and certification mandated by the US Federal Government (NIST)

- Conformance and Interoperability
  - **Host / Router**
  - **NPD – Network Protection Devices**

Common Criteria Scheme, FIPS 140, SCAP, FIPS 201 (PIV)

NAPS – Network Attached Peripheral Security

A Framework for testing “devices” that are IP connected. Wired or wireless.

Limitless Markets - Includes but not restricted to:

- HealthCare
    - **Medical Devices**
    - **BodyNet**
- SmartGrid
    - **Smart Meters**
    - **Monitoring devices**
    - **End point devices in the enterprise or the home**
- Consumer
    - **Set-top boxes**
    - **CPE**
- Enterprise
    - **Office productivity devices (postage machine, printers, copies, etc.)**
- Network Equipment / Infrastructure
    - **UPS, Power Strips, Management systems, Network KVM, HVAC**
- Physical Security
    - **Surveillance cameras, Access readers**

IT & Information Security Decision Making

Risk-Based Analytics

Peter Tippett, MD., PhD

VP Technology & Innovation