



# **Risk- Based Security in Enterprises**

## **Focus on the Enterprise: Driving Efficiency & Innovation**

### **2008 Data Breach Investigations Report**

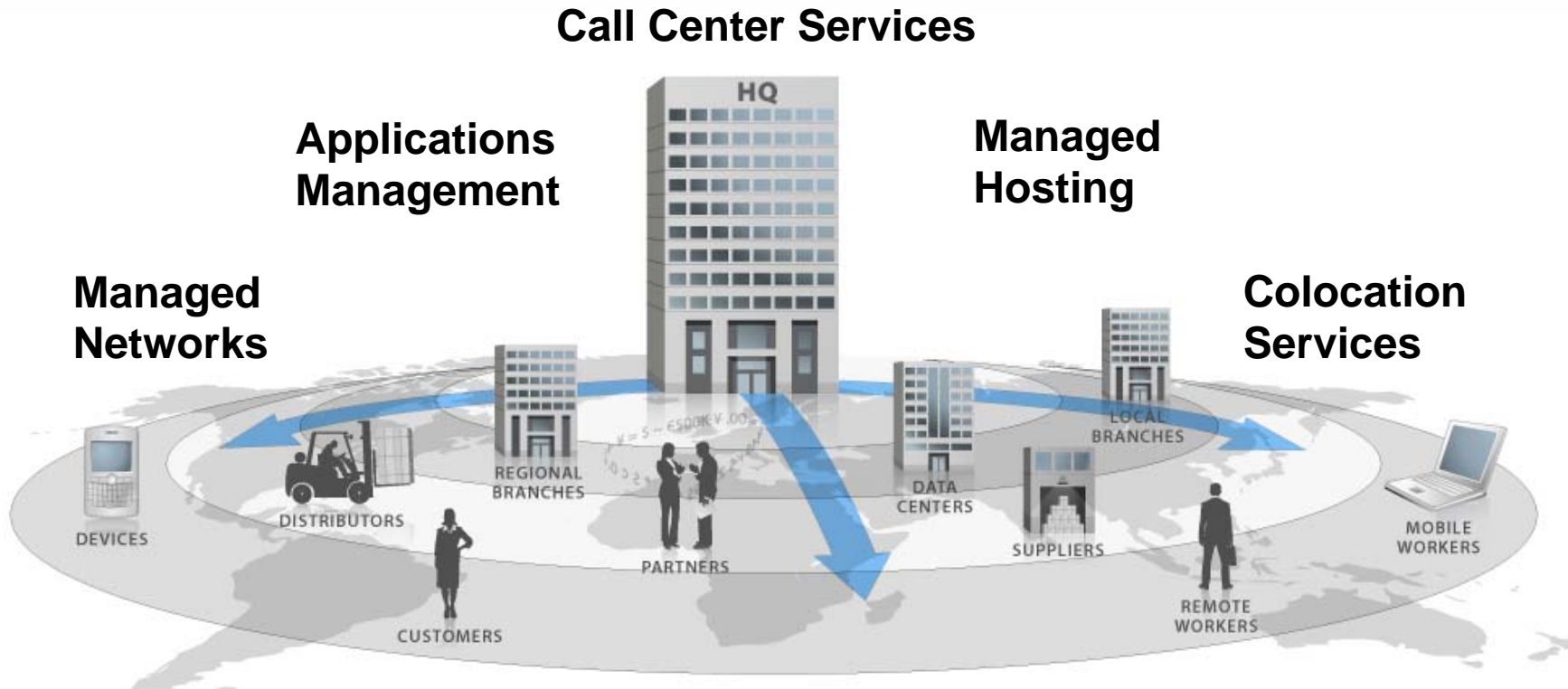
**Peter Tippett**

*Vice President*

*Security Solutions powered by Cybertrust*

[peter.tippett@verizonbusiness.com](mailto:peter.tippett@verizonbusiness.com)

# The Extended Enterprise



# The Extended Enterprise Comes with New Security Challenges

Measuring against risk

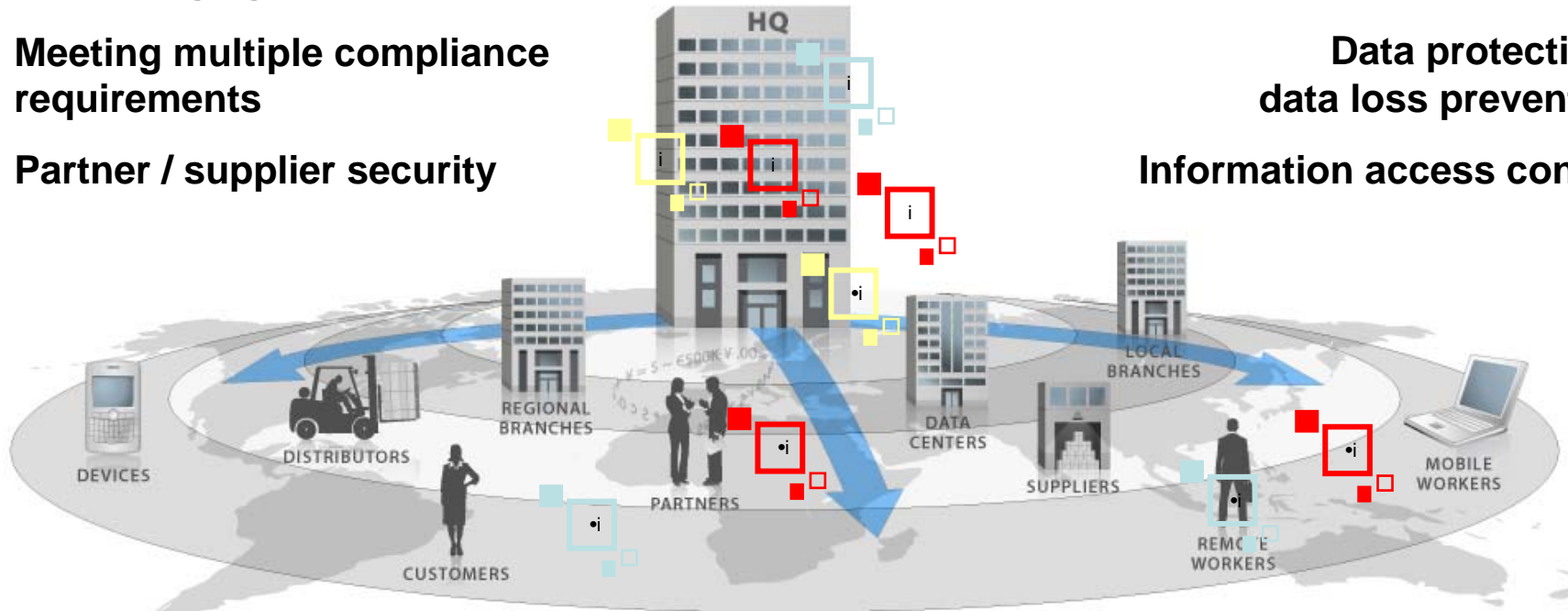
Meeting multiple compliance requirements

Partner / supplier security

Application security

Data protection / data loss prevention

Information access control



Ongoing monitoring and management

Security log data handling

Business continuity

Consumer / employee mobility



# Securing the Extended Enterprise

## Our Vision

### Wider

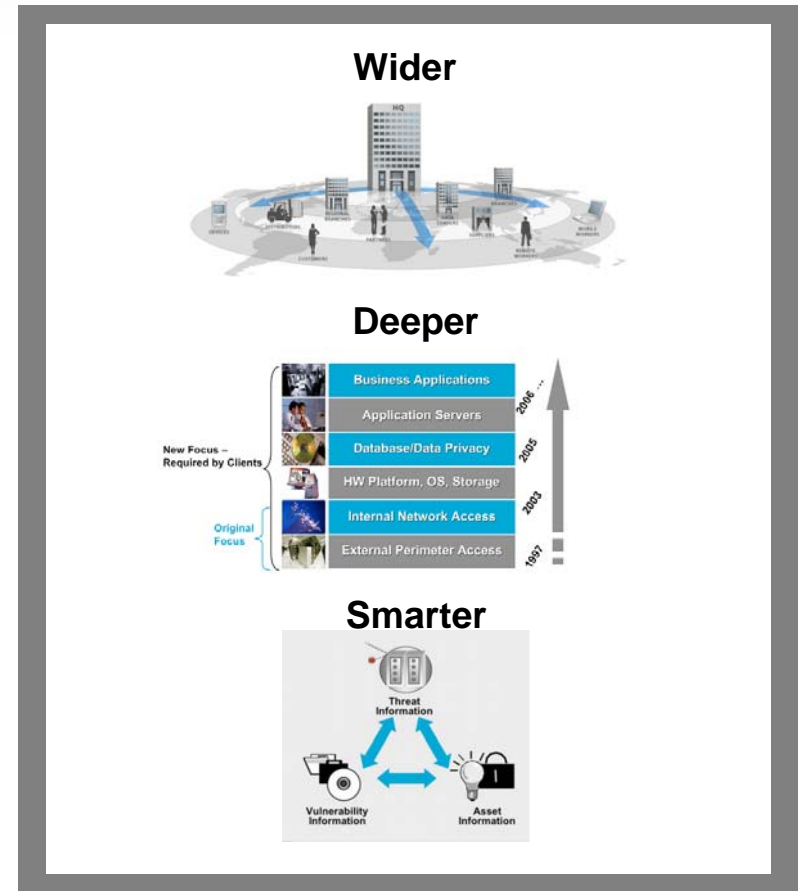
- Security controls should span the Extended Enterprise and should be executed where they are most effective and cost-efficient

### Deeper

- Security should span the entire IT stack, including the network, data, application user, and governance

### Smarter

- Security decisions should be based on risk, not just on threats and vulnerabilities



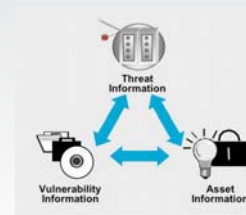
# Think Deeper


*More than network security*

	In the Cloud	At Premises
Governance	Regulation Partner Requirements	Compliance Standards
Users	Identity Management	User Provisioning
Applications	Application Threat Protection	Access Management
Data	Flow Source Destination Analysis	Data Loss / Leakage Prevention
Network	Mass Attack Protection	Targeted Attack & Insider Threat Protection

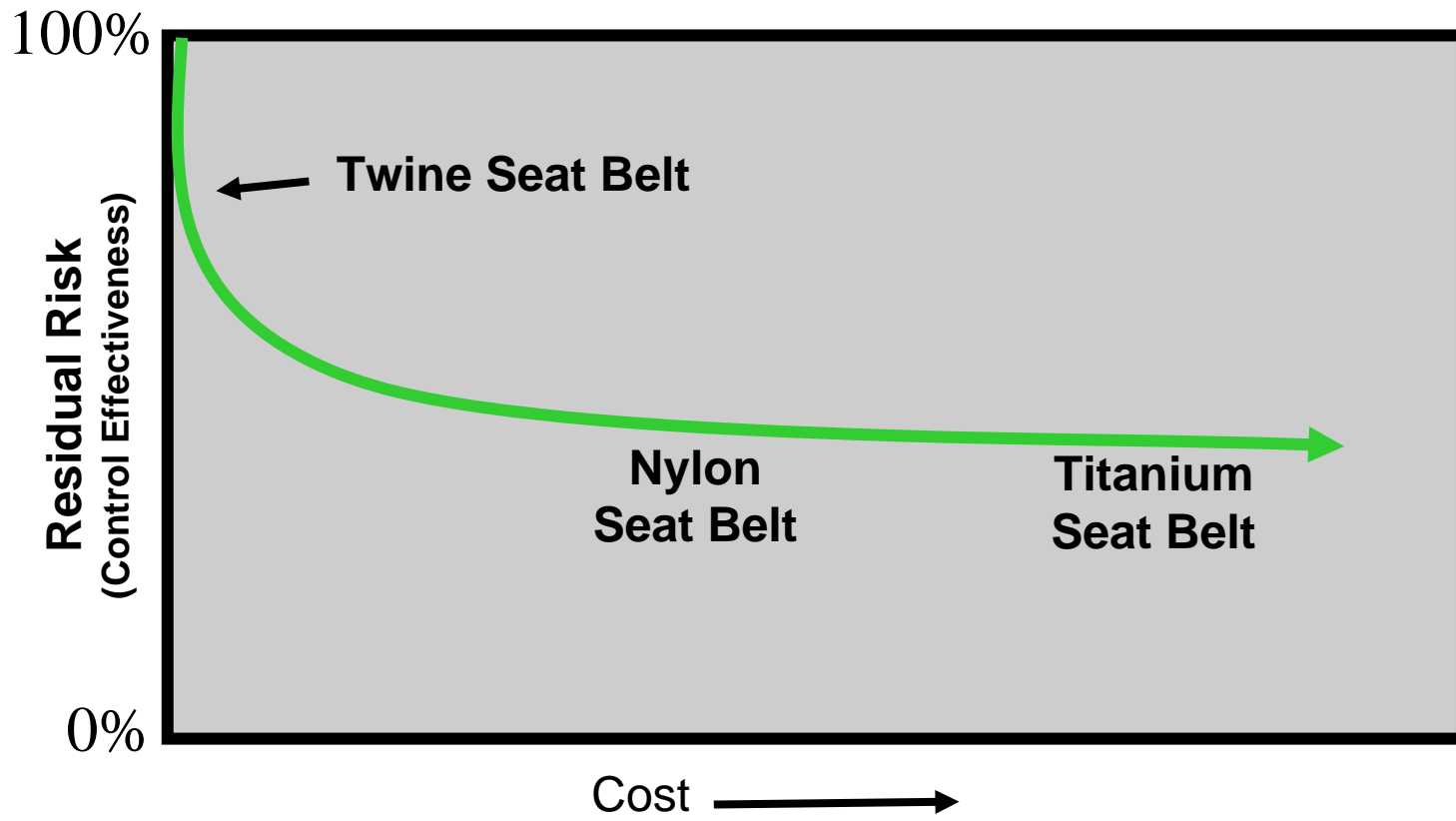


# Seven Types of Risk Intelligence



1	<b>Threat &amp; Vulnerability Intel</b> Track and analyze new software vulnerabilities and related attacks
2	<b>Underground Intel</b> Watch discussions, code sharing, planning,... Historically BBS, then Usenet, now more IRC and Cons...
3	<b>ICSA Labs Intel</b> Security product testing and security consortia operations. 400+ products 
4	<b>Forensics Intel</b> Data and Intel from forensics investigations (200+ cases per year).
5	<b>MSS Intel</b> Data from IDS, FW, IPS, Applications... Management & Monitoring SOC operations
6	<b>Net Intel</b> Data from backbone. Sensors on more than 1 Million VzB addresses. Netflow Honey nets, Honey Pots...
7	<b>Studies &amp; Surveys</b> VZB Studies, surveys (10+/yr), Others published data to drive Risk Models, equations & methodology

# Risk vs. Control Implementation



# More than 500 Data Breach Investigations Past 4 Years

From more than 700 Investigations performed by the Verizon Forensics IR Team during these 4 years.

Study Caseload includes only cases where:

1. Company was Attacked
2. Attack was Successful
3. Data was Breached
4. Breached Data was Exploited

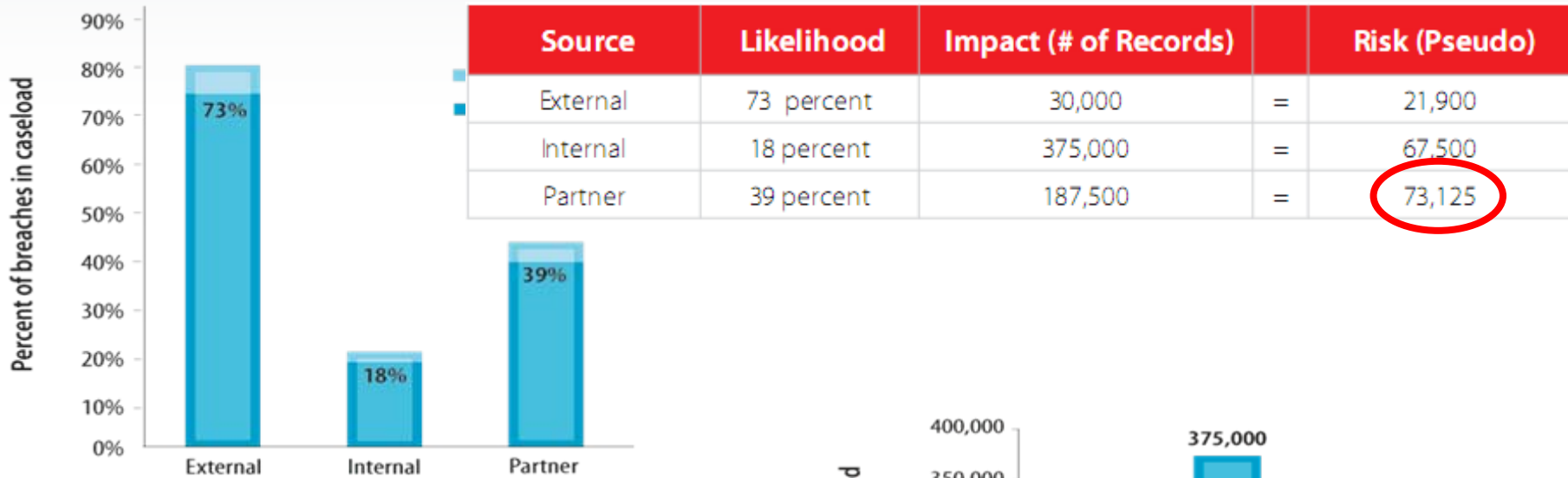
Caseload includes between  
1/4 and 1/3 of publicly  
disclosed breaches between  
2005-2007\*

Caseload includes 3 of the 5  
largest data breaches on record

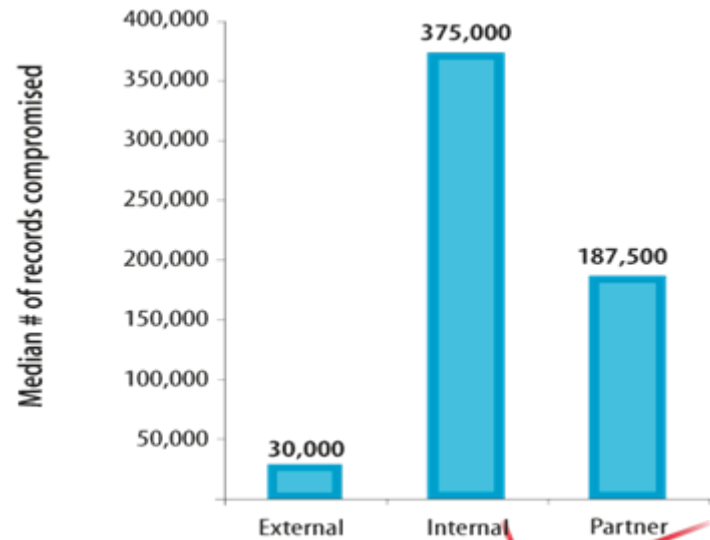
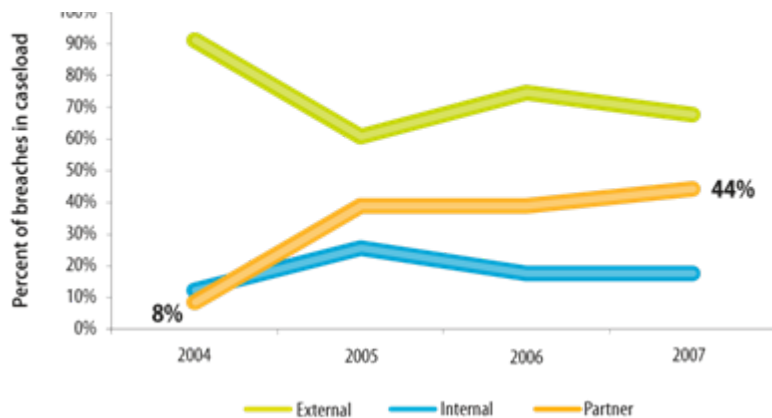
\*Source: <http://www.idtheftcenter.com/>

# Verizon 2008 DBIR

## Sources of Data Breaches

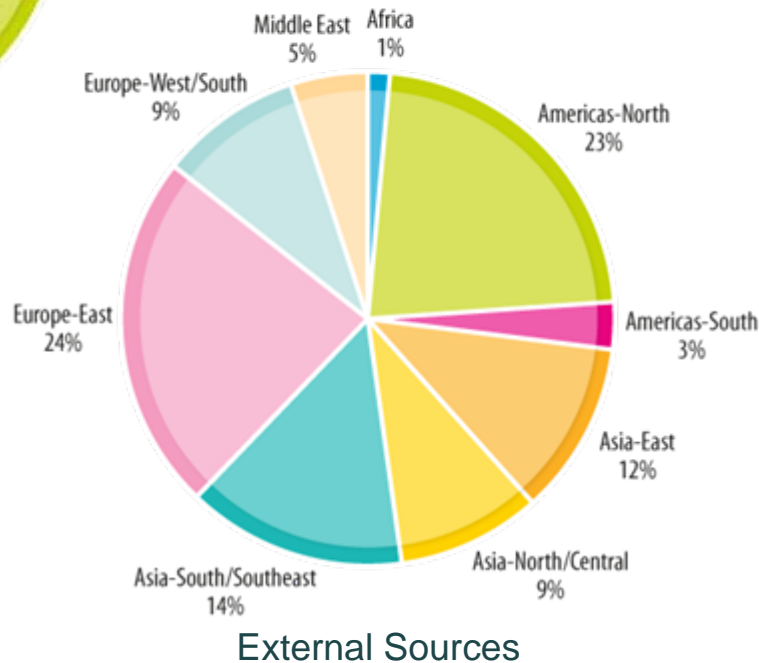
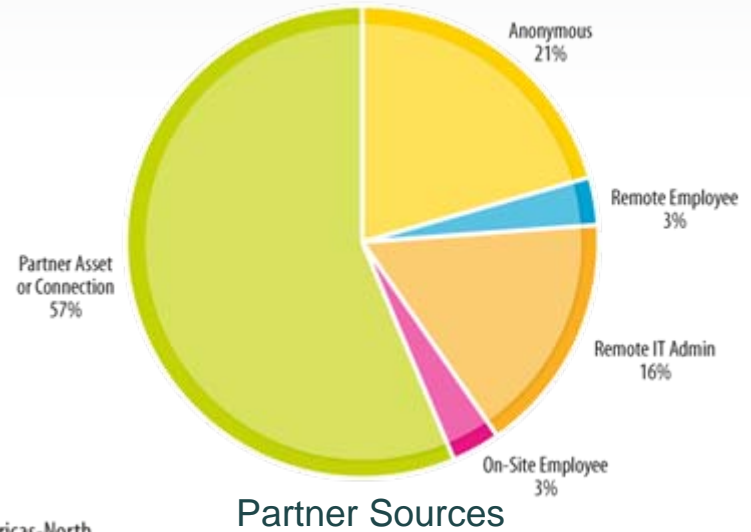
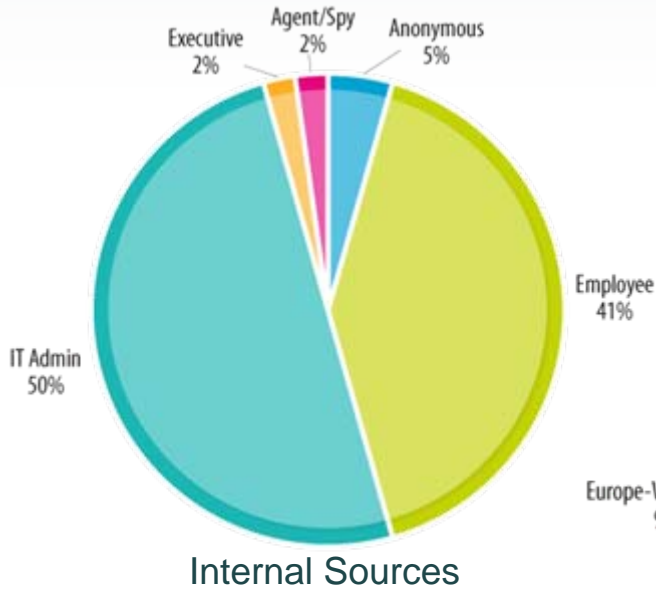


Trends in Data Breach Sources



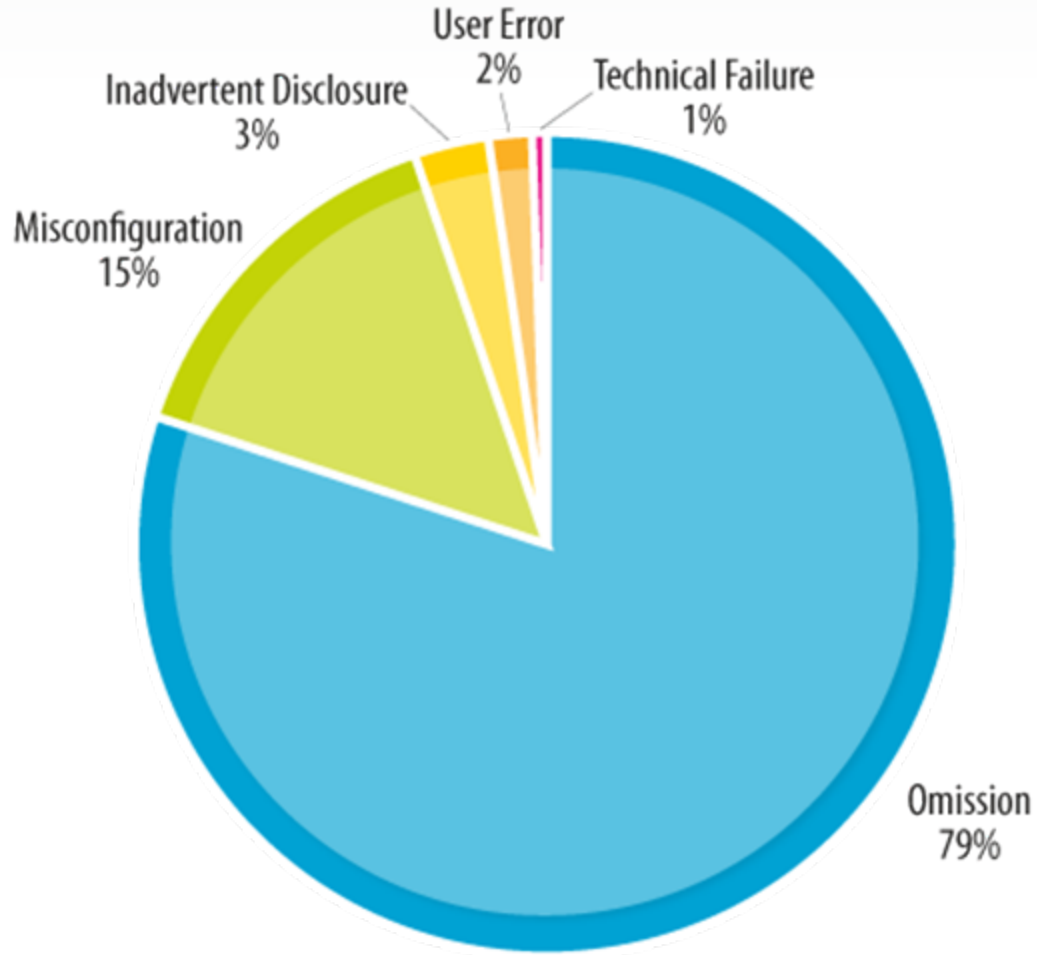
# Verizon 2008 DBIR

## Sources of Data Breaches: A Deeper Look



# Verizon 2008 DBIR

## Threat Categories: Error



Direct: 3%

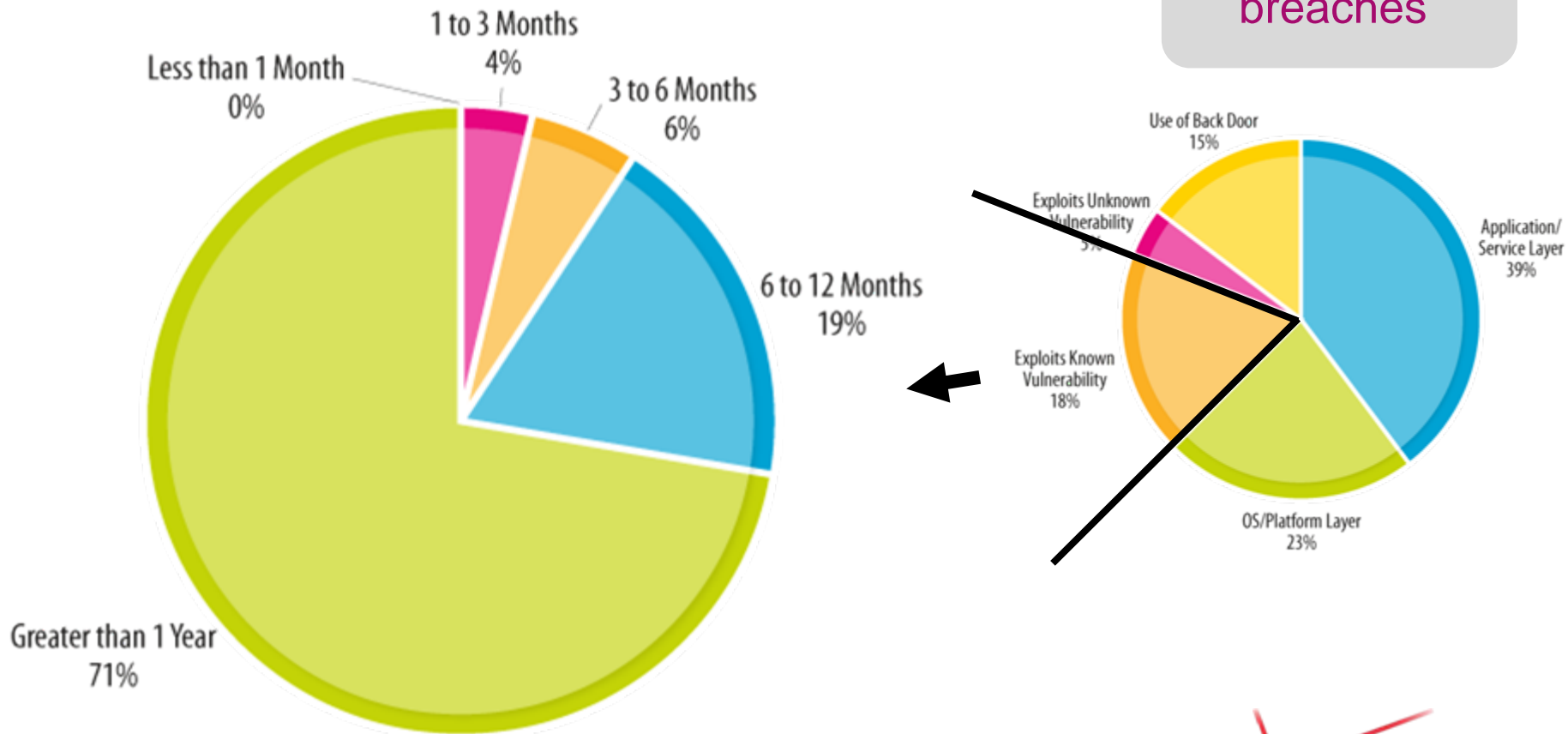
Factor in: 62%



# Verizon 2008 DBIR

## Threat Categories: Hacking - Vulnerabilities

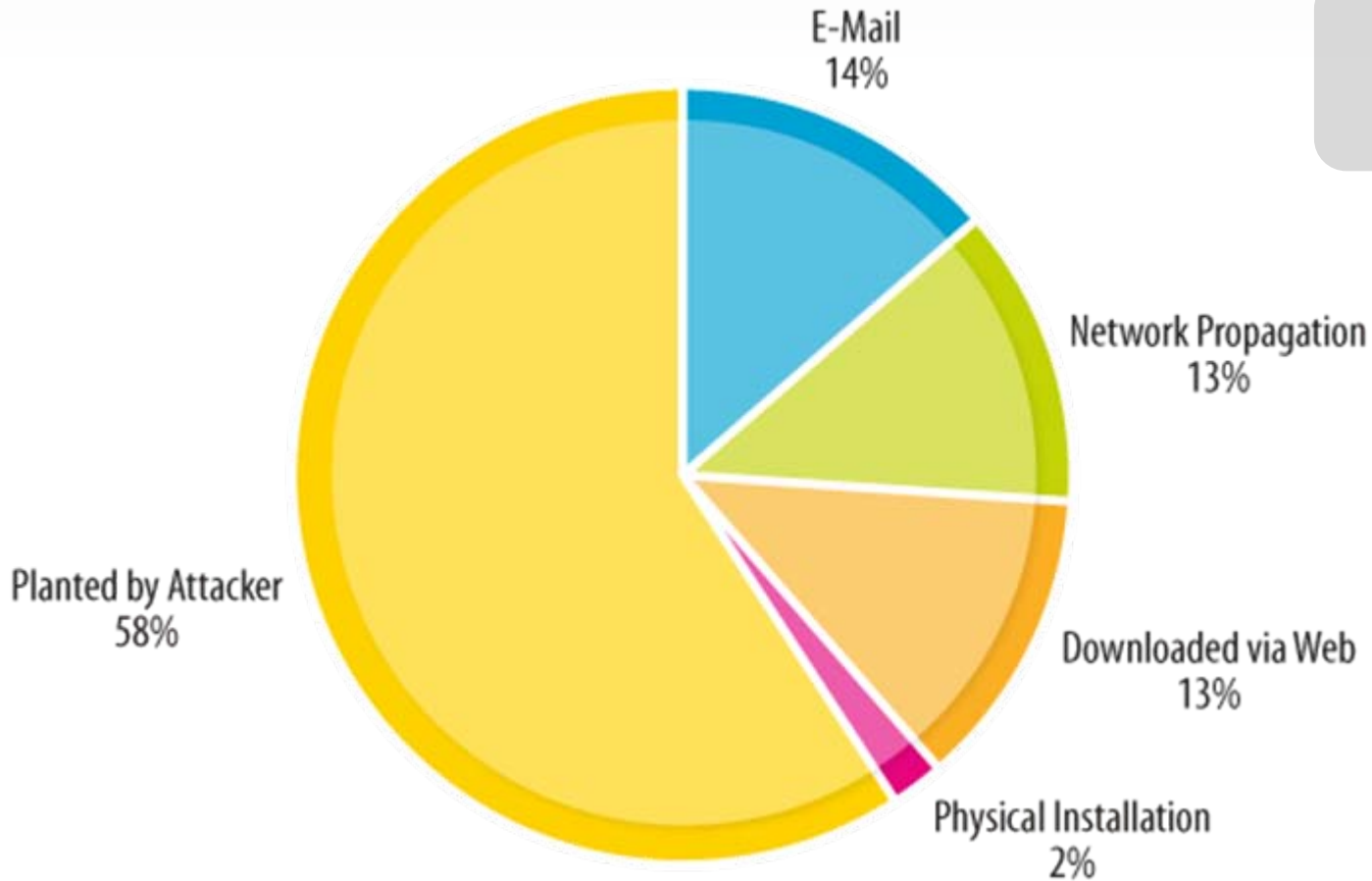
59% of breaches



# Verizon 2008 DBIR

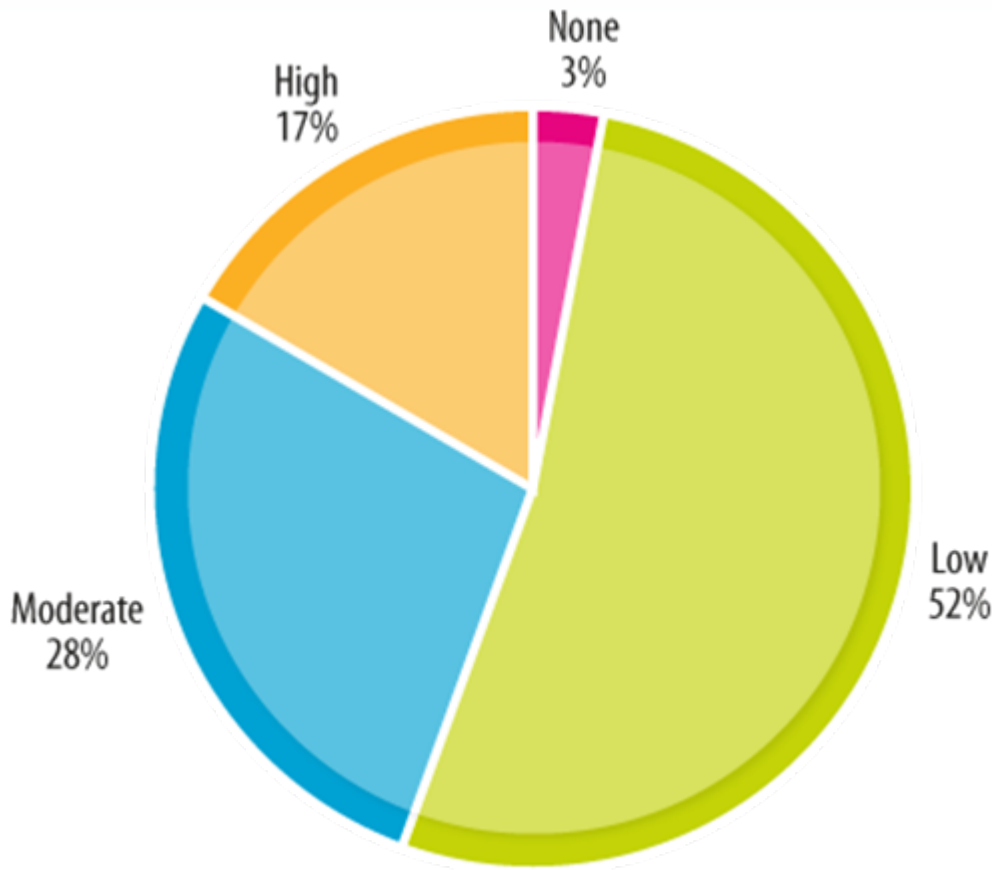
## Threat Categories: Malcode

31% of breaches



# Verizon 2008 DBIR

## Attack Difficulty



**None:** No special skills or resources were used. The average user could have done it.

**Low:** Low-level skills and/or resources were used. Automated tools and Script Kiddies.

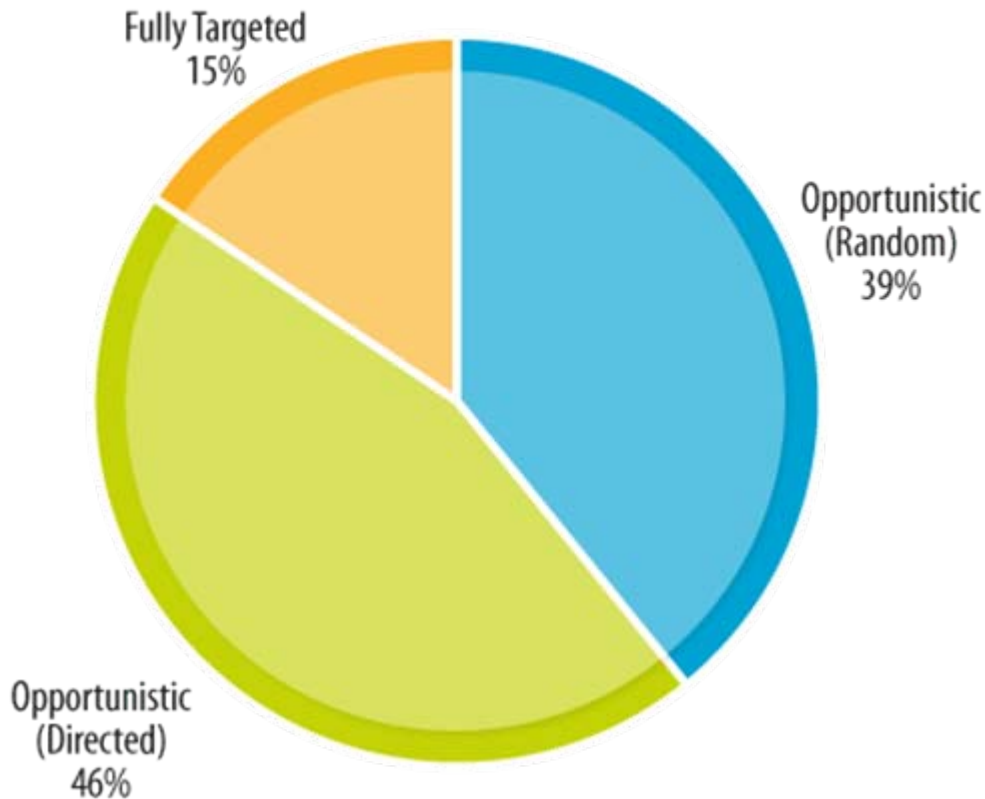
**Moderate:** The attack employed skilled techniques, minor customization, and/or significant resources.

**High:** Advanced skills, significant customization and/or extensive resources were used.



# Verizon 2008 DBIR

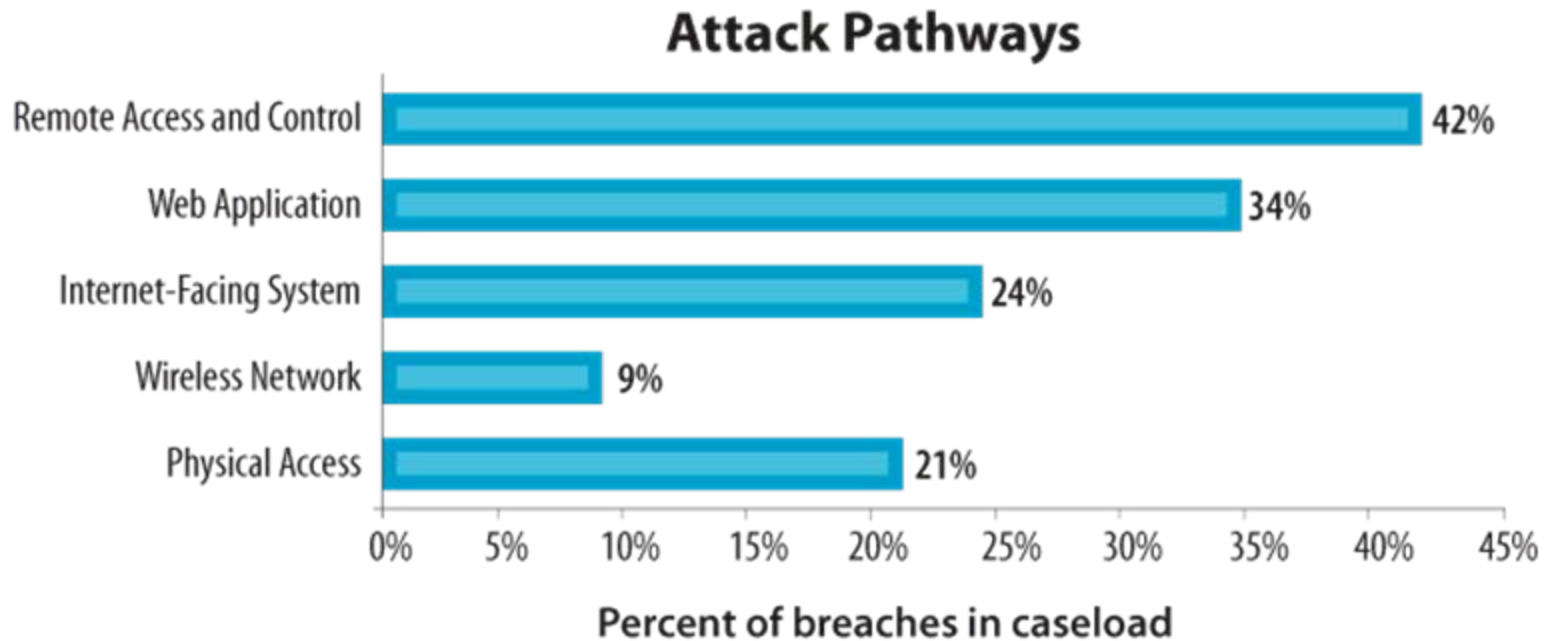
## Targeted vs. Opportunistic Attacks



- **Opportunistic (Random):** Attacker identified the victim while searching randomly or widely for weaknesses
- **Opportunistic (Directed):** Although the victim was selected, it was because they were known to have a particular weakness the attacker could exploit.
- **Fully Targeted:** Victim was first chosen as the target and then the attacker figured a way to exploit them.

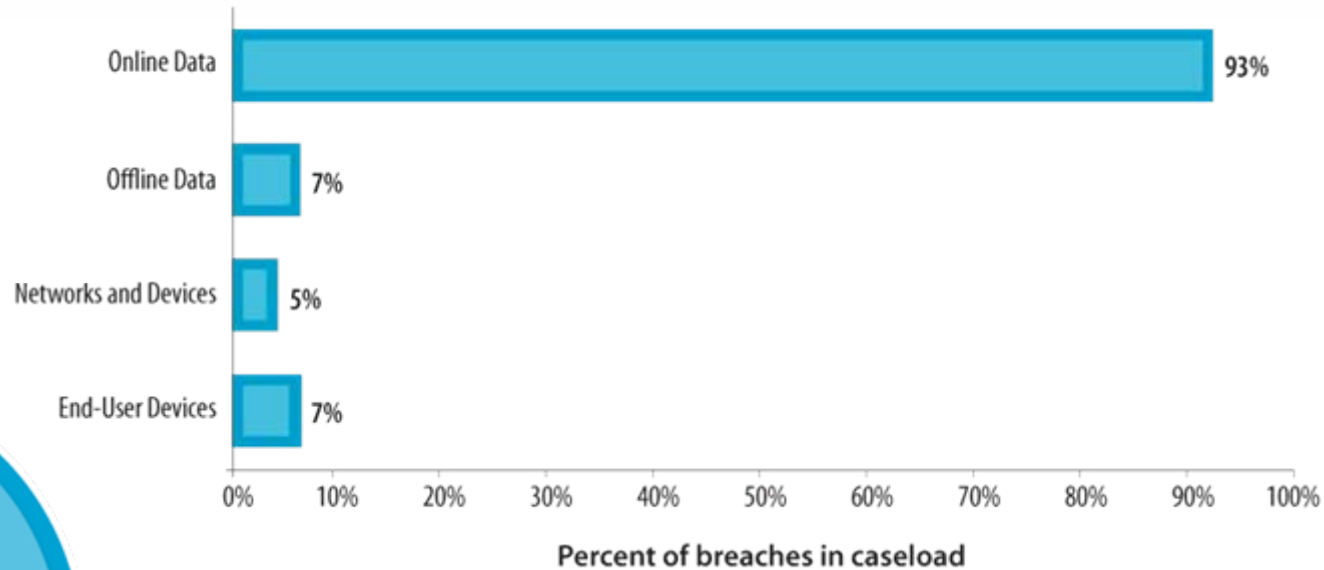
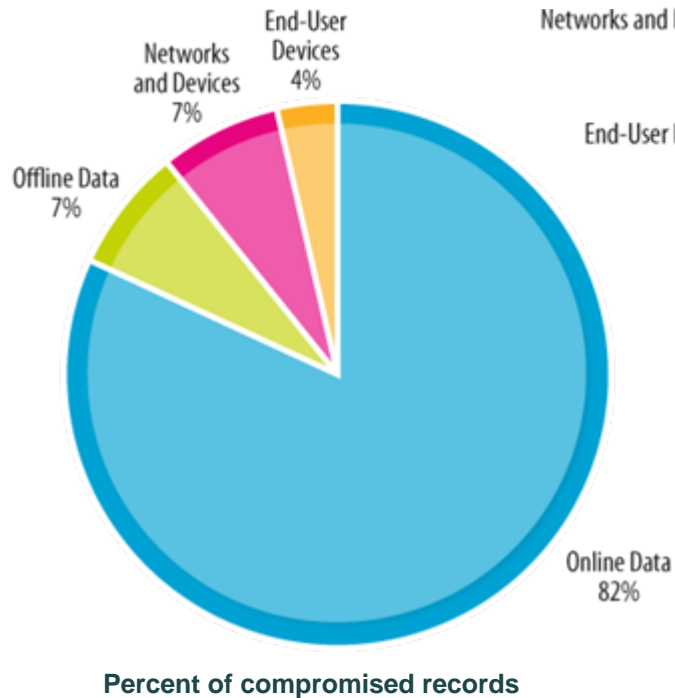
# Verizon 2008 DBIR

## Attack Pathways



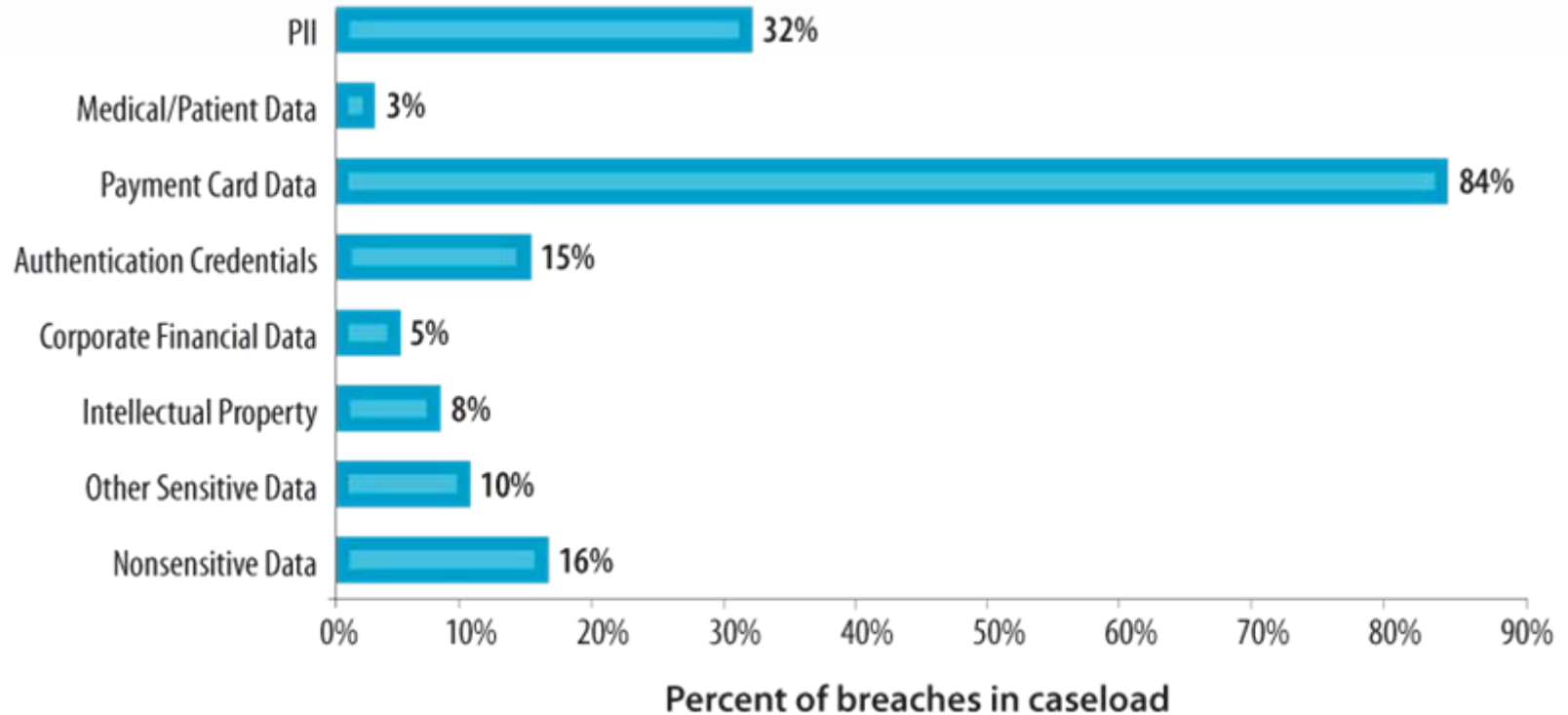
# Verizon 2008 DBIR

## Compromised Asset Types



# Verizon 2008 DBIR

## Compromised Data Types



Total: 230 Million records

Mean: 1.2 Million records

Median: 45,000 records



# Verizon 2008 DBIR

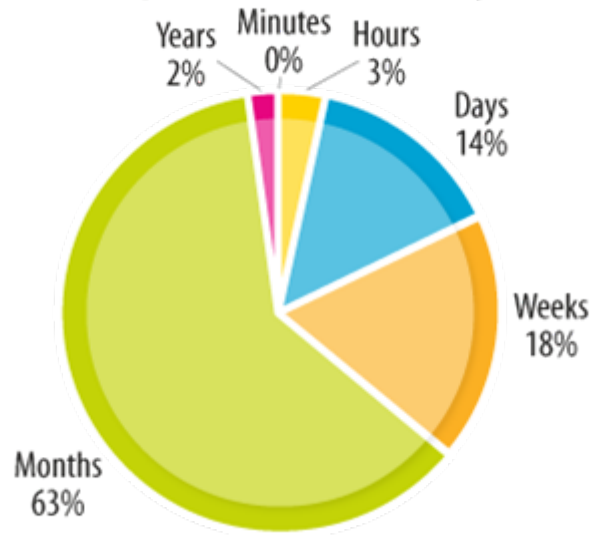
## Time Span of Events

### Point of Entry to Compromise



“Hours/Days”

### Compromise to Discovery



“Months”

### Discovery to Mitigation

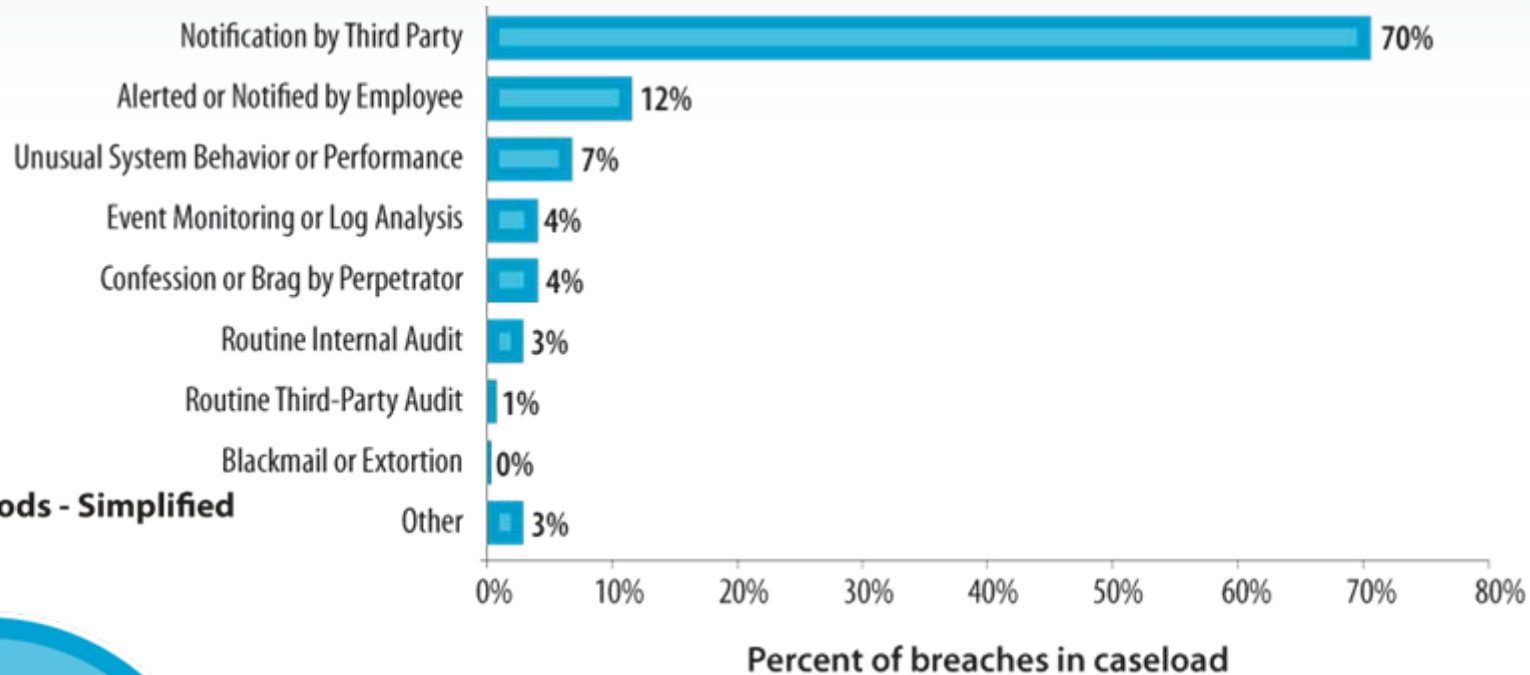


“Weeks”

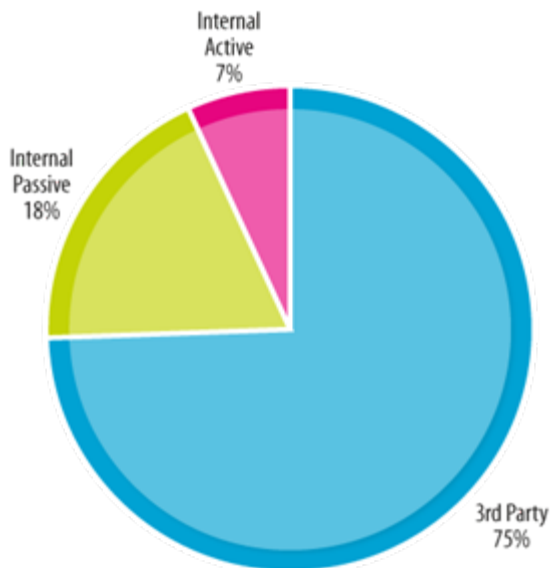


# Verizon 2008 DBIR

## Discovery Methods



**Discovery Methods - Simplified**

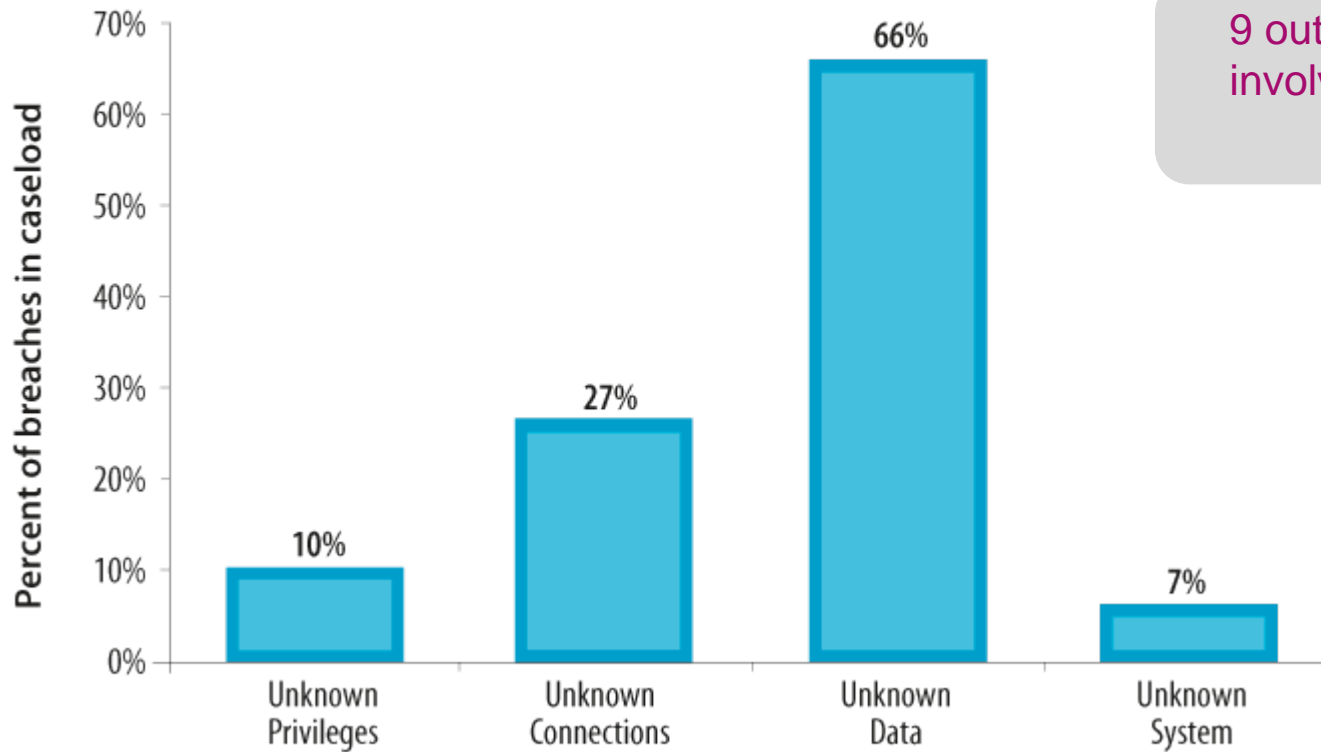


75% of breaches are discovered by a 3<sup>rd</sup> party



# Verizon 2008 DBIR

## Unknown Unknowns



9 out of 10 breaches involved at least one of these



# Verizon 2008 DBIR

## Conclusions & Recommendations

*Align process with policy* - In 59% of breaches, security policies were established but not enacted through actual process.

*Achieve “essential” then worry about “excellent”* - 83% of attacks were not difficult and 85% were opportunistic. Ensure basic controls are met ubiquitously then move to advanced measures if appropriate

*Secure partner connections* - 39% of breaches involved business partners. Standard controls must encompass the data, systems and connections used in partner relationships.

*Data Discovery* - 66% of breaches involved data not known to be on the system. Efforts to locate, catalogue, track and assess the risk of sensitive data are highly beneficial – especially on servers.



# Verizon 2008 DBIR

## Conclusions & Recommendations

- *Control data with transaction zones* - Zones provide a foundation for granular control measures around data, additional layers of accountability and more pointed event monitoring.
- *(Actually) Monitor event logs* - Evidence of 82% of breaches were available to the victim but this information was neither noticed or acted upon.
- *Create an incident response plan* - An incident response should detail effective handling of attacks, post-breach procedures, evidence collection, freeze points, relationships 3<sup>rd</sup> parties (i.e., law enforcement, legal counsel), and disclosure/notification policies.
- *Conduct mock incident testing* - A periodic step-by-step walkthrough of procedures during a simulated breach event is a valuable learning experience and critical to vetting the response plan.

# What is Wrong with our Security Thinking?



## World is Flat

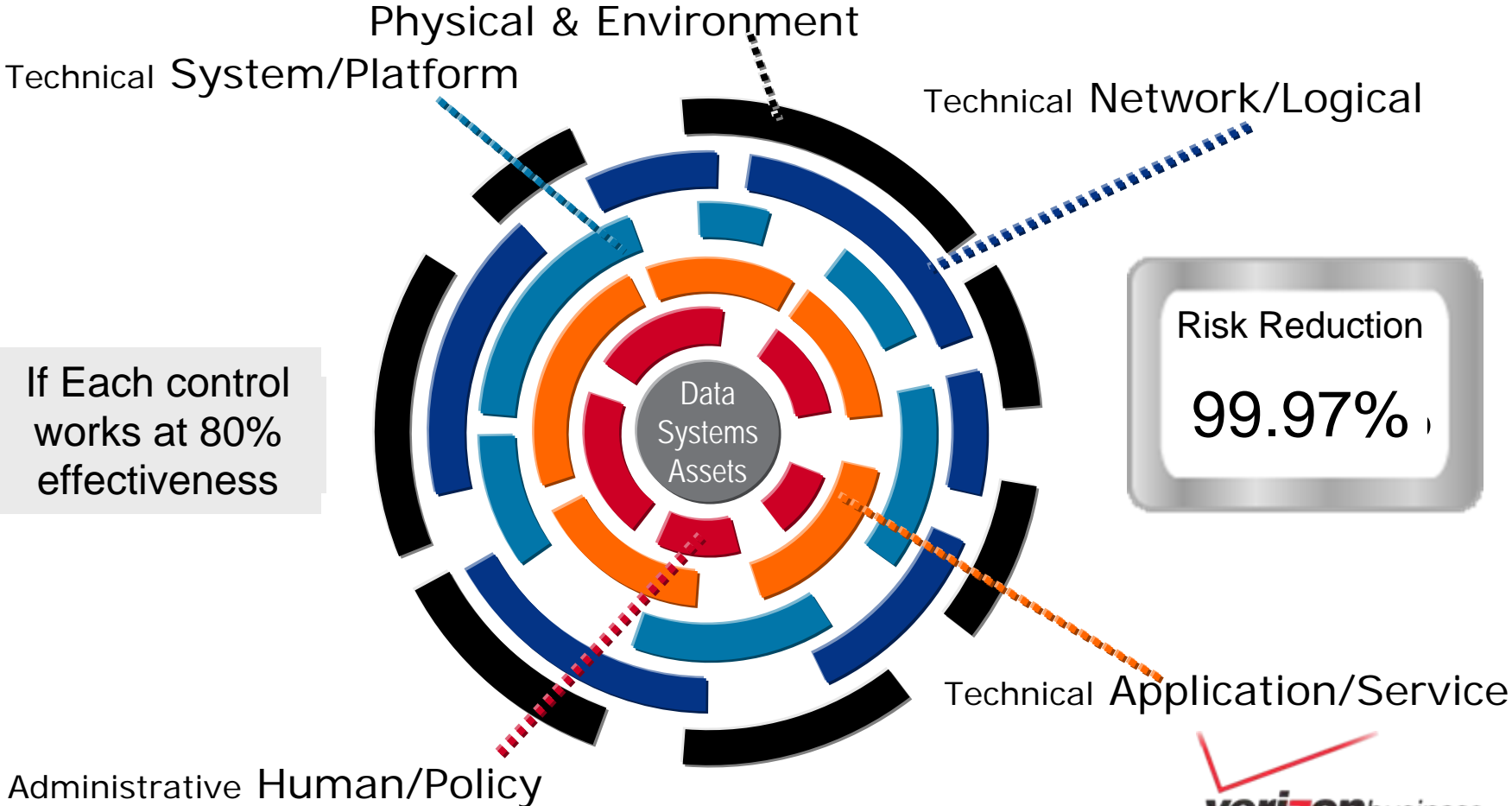
- Vulnerabilities
- Single Computer
- Binary
- Conflation
  
- Best Practices

## World is Round

- Risk
- Community of Computers
- Analog, Synergistic
- Discrete Concepts
  
- Essential Practices

# Synergistic Control Effectiveness

**Effectiveness:  $E_{total} = 1 - ((1 - E_1) * (1 - E_2) * (1 - E_3) \dots)$**



# The Better Approach

Use a risk based approach

Optimize all decisions with  
Risk-Intelligence Data

Leverage World-wide  
Experience from  
Thousands of Enterprises

Professional  
Security  
Services

Security  
Programs

Managed  
Security  
Services

