Investigative Response Case Metrics Initiative

Preliminary findings from 700+ data compromise investigations

GLOBAL CAPABILITY.
PERSONAL ACCOUNTABILITY.

Wade Baker

MiniMetricon 2.5

April 07, 2008

Agenda

Investigative Response @ Verizon Business

IR Case Metrics Initiative

IR Statistics & Trends

Who am I?

About Me – Hats I Wear

About Me – Hat I’d Never be Caught Wearing

About Me – Hat I'd Never be Caught Wearing

r = +.998

About Me – Hat I'm trying to Wear

About Me – Hats I Wear

About Me – Hats I Wear

About Me – Hats I Wear

Research

About Me – Hats I Wear

Intel

About Me – Hats I Wear

Innovate

About Me – Hats I Wear

Risk

About Me – Hats I Wear

Metrics

About Me – Hats I Wear

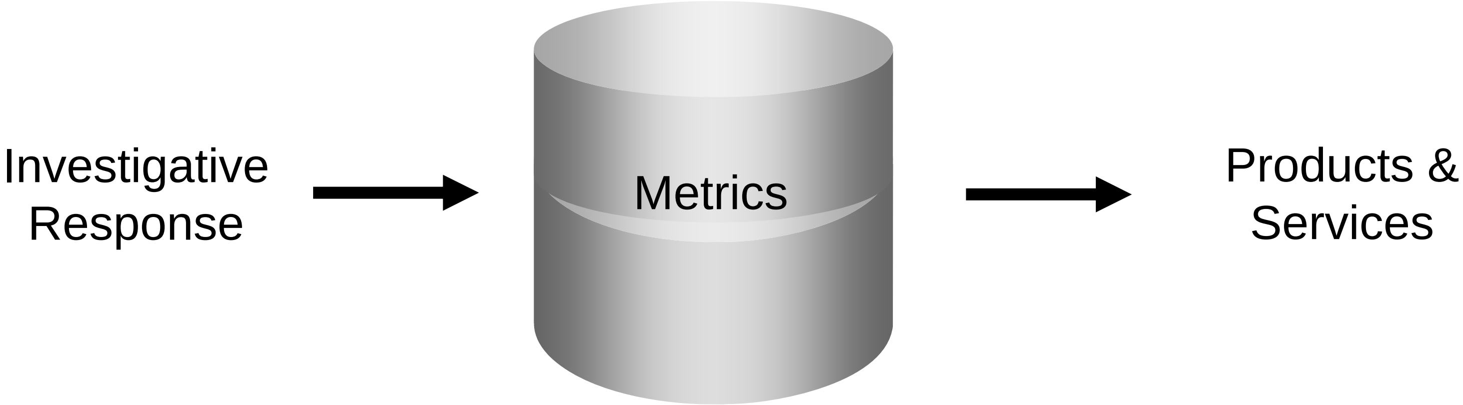
DSS

About Me – Hats I Wear

About Me – Hats I Wear

“Then why are you here talking to us about investigative response trends?”

About Me – Hats I Wear



Investigative Response

Metrics

Products & Services

About Me – Hats I Wear

Metrics

About Me – Hats I Wear

Investigative Response @ Verizon Business

Investigative Response @ Verizon Business

IT Investigative Support (On-demand)
Guaranteed Response (Retainer-based)
Incident Response Training (CIRT)
Computer Forensic Training
Electronic Data Recovery / Destruction

Services

Expert Witness Testimony
Mock-Incident Testing
Corporate IR Program Development
Litigation Support & eDiscovery
Tactical Management Briefings

Investigative Response @ Verizon Business

230 cases in 2007 (1/4 of disclosures*)

185 cases in 2006 (1/4 of disclosures*)

166 cases in 2005 (1/3 of disclosures*)

130 cases in 2004

*Source: http://www.idtheftcenter.com/

Investigative Response @ Verizon Business

3 of the 5 largest data breaches

Overview: IR Metrics Initiative

Overview: IR Metrics Initiative

2004 – Q3 2007: Some high-level statistics & trends; some diffusion of insight and data

Q4 2007 – Present: Hundreds of case metrics defined & operationalized; systematic collection for all previous cases

Near Future: Diffusion of data internally and externally; Reoccurring public report of findings

Overview: IR Metrics Initiative

What’s the current status of this effort?

What’s the dataset for this talk?

Overview: IR Metrics Initiative

Sampling of cases from 2004-Present

High-level caseload statistics and trends from each investigator

Data collection on case backlog: Mostly complete for 2007, Majority for 2006, Partial for 2005 & 2004

Overview: IR Metrics Initiative

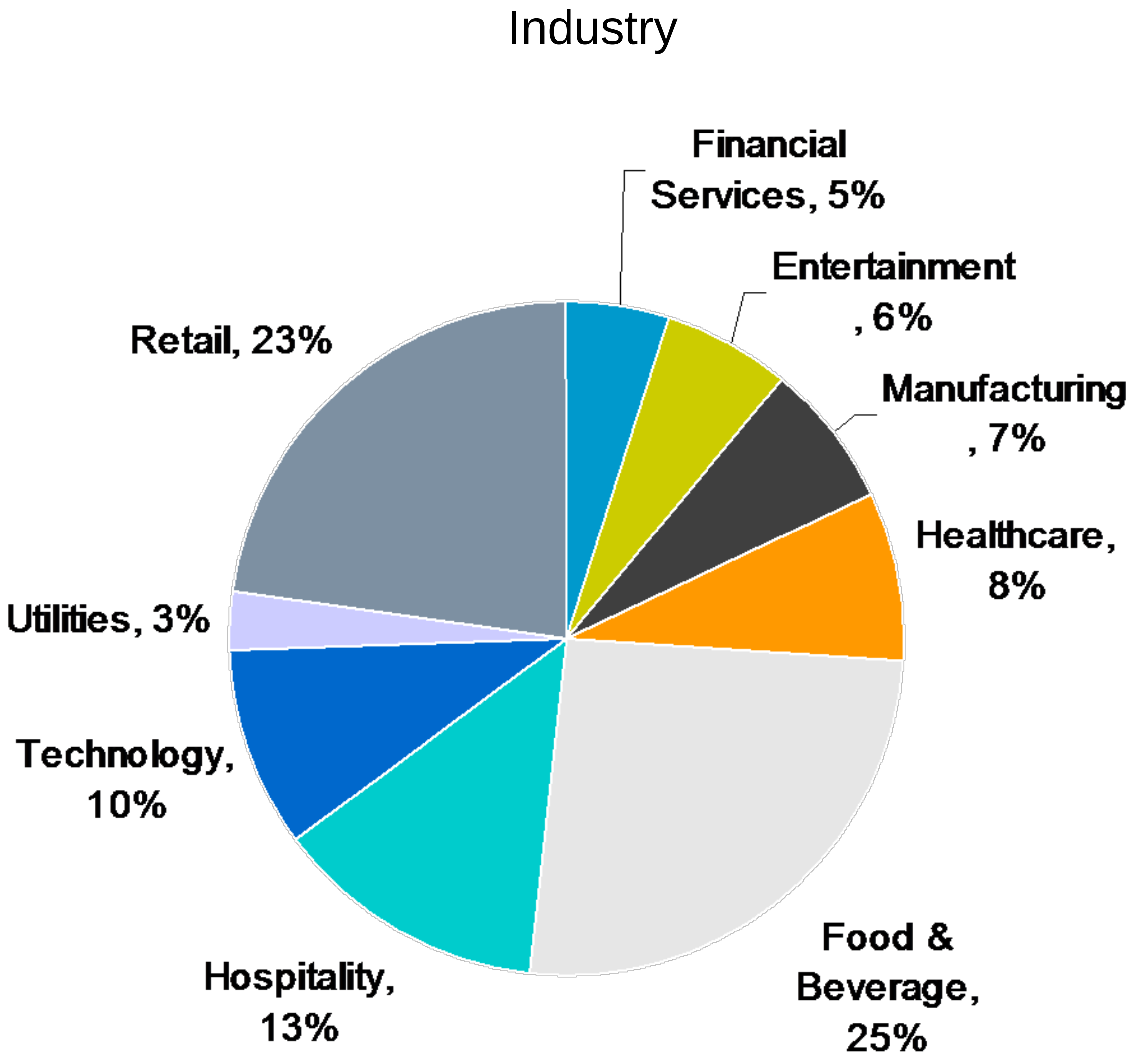
Bottom Line: This is a work in progress but there is more than enough data to support these findings…

Overview: IR Metrics Initiative

…just add “-ish” to the end of all numbers

IR Case Metrics: Statistics and Trends

IR Case Metrics: Statistics and Trends

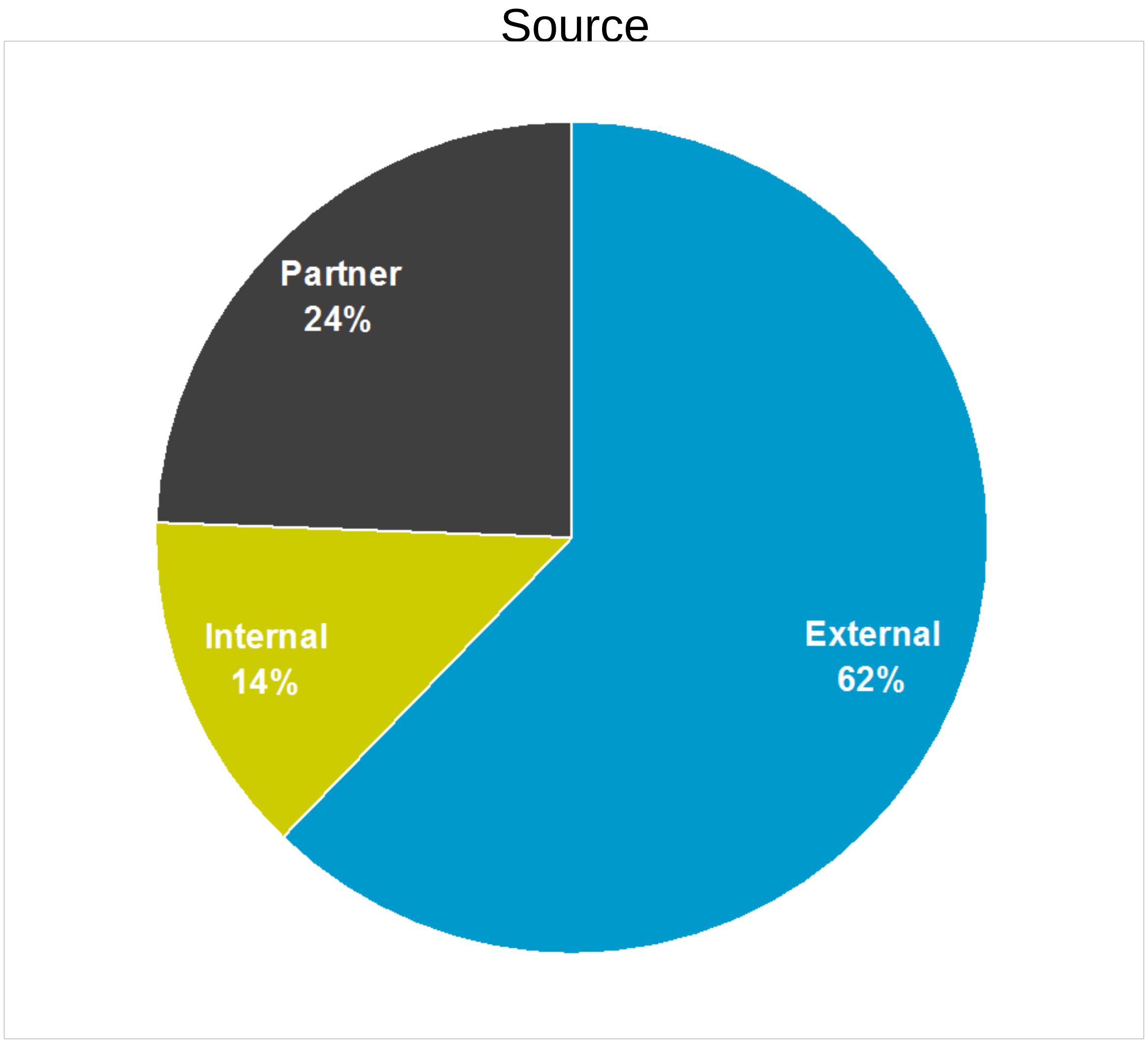


Note: 2007 cases only

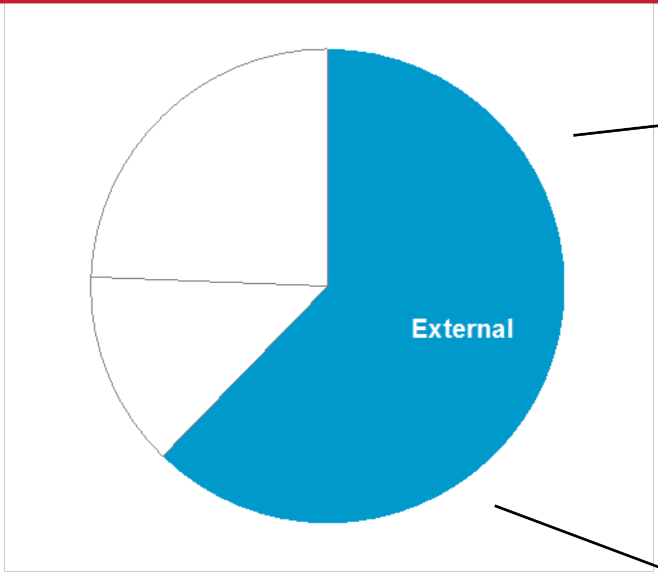
IR Case Metrics: Statistics and Trends

What is the source of breaches?

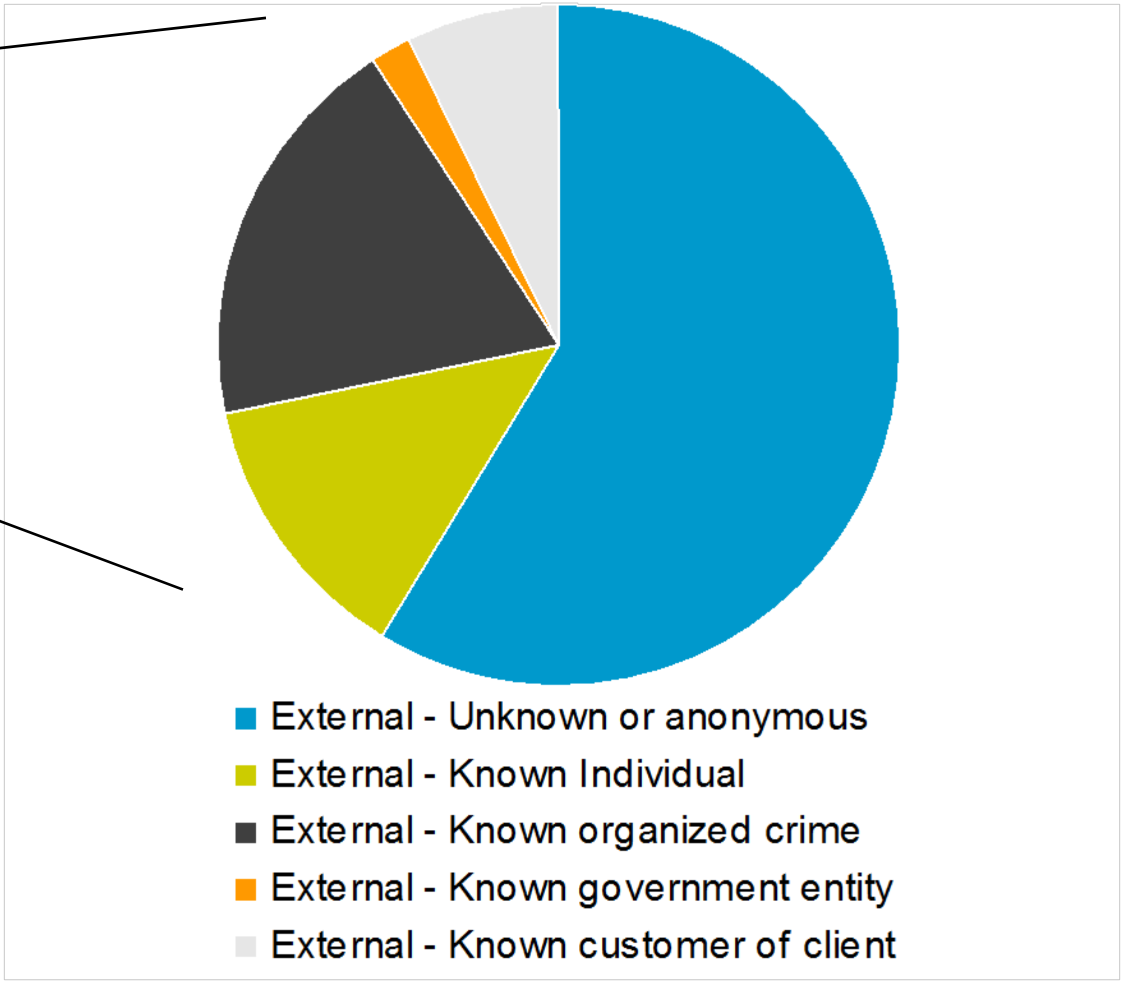
IR Case Metrics: Statistics and Trends



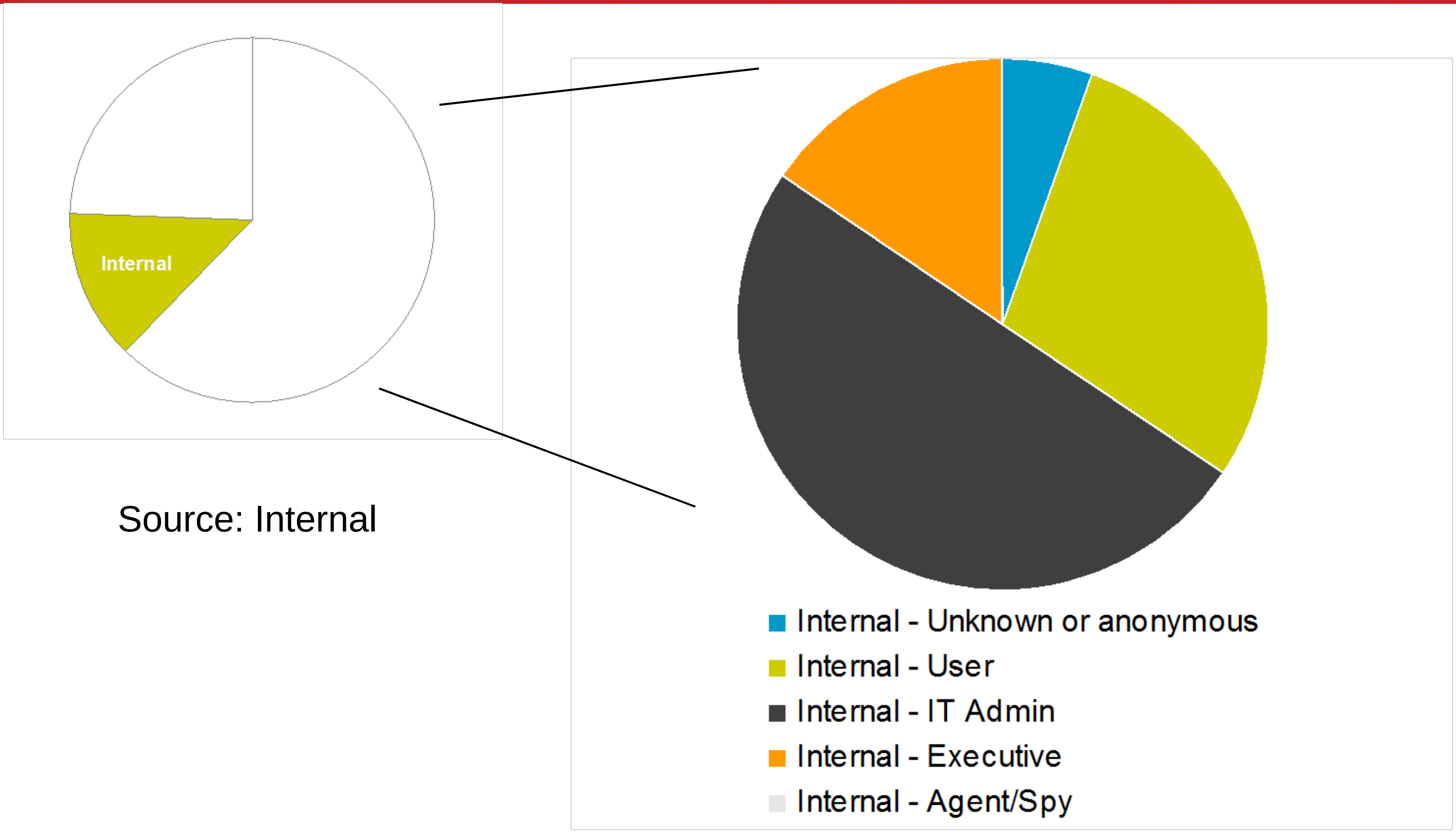
IR Case Metrics: Statistics and Trends



Source: External

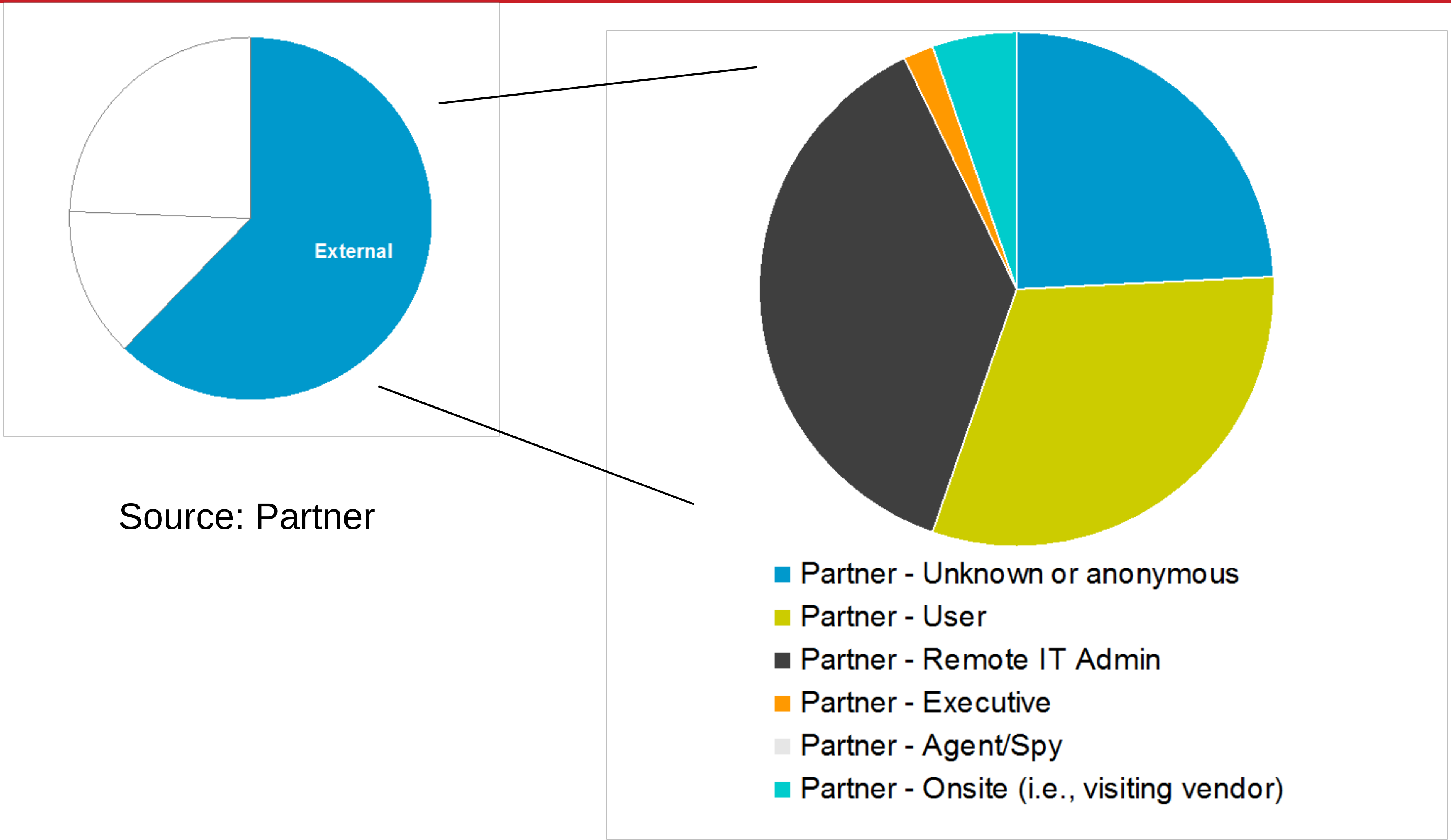


IR Case Metrics: Statistics and Trends



Source: Internal

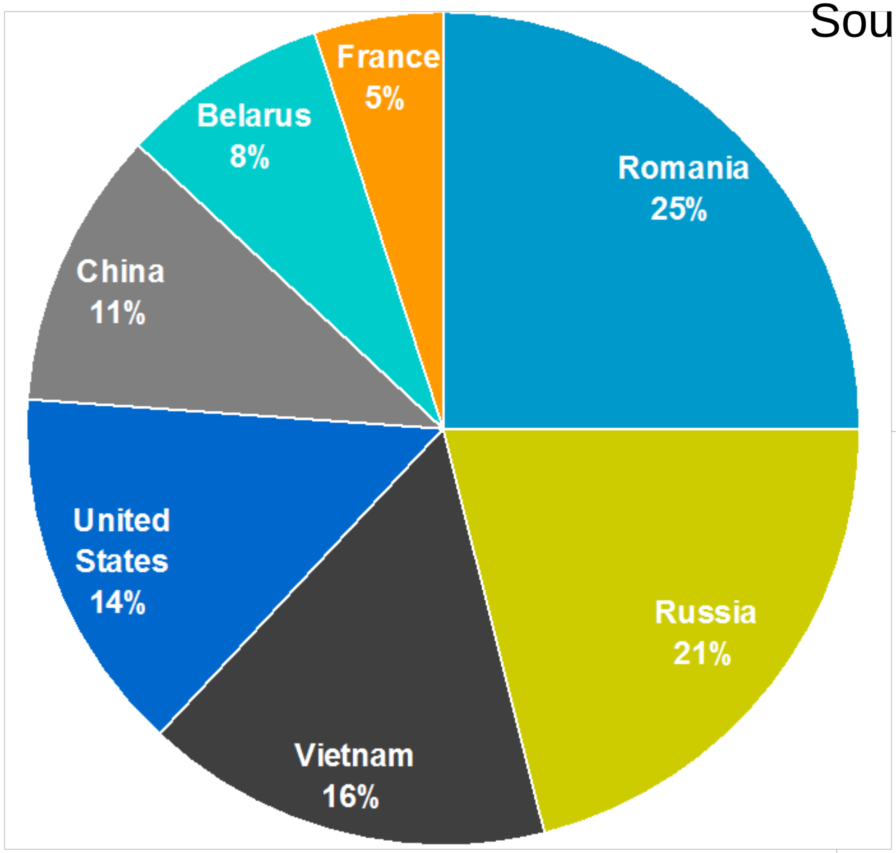
IR Case Metrics: Statistics and Trends

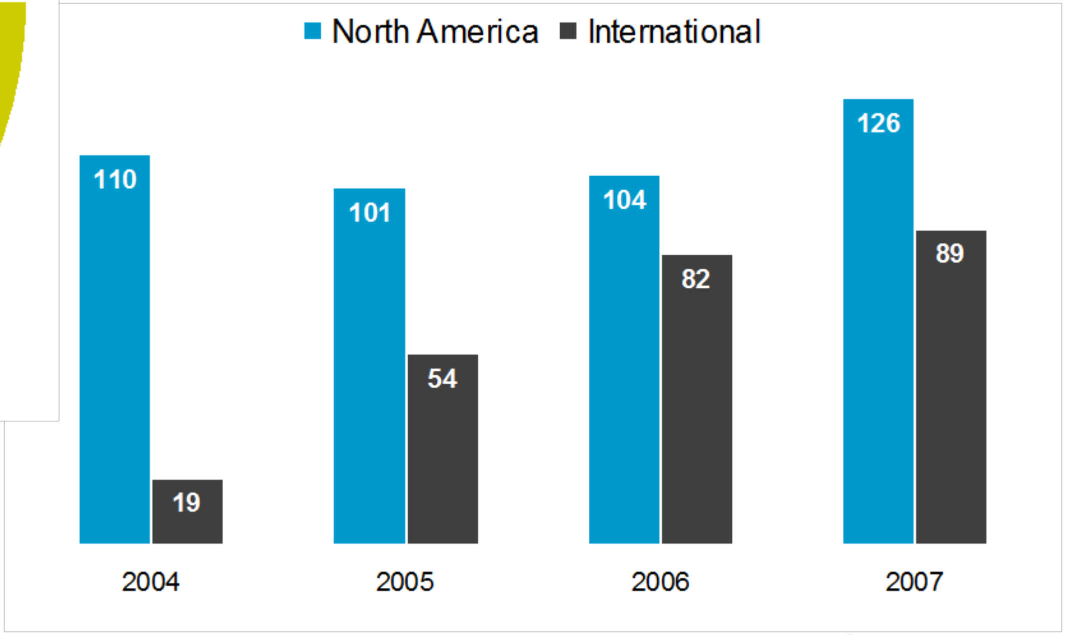


Source: Partner

IR Case Metrics: Statistics and Trends

Source Geo





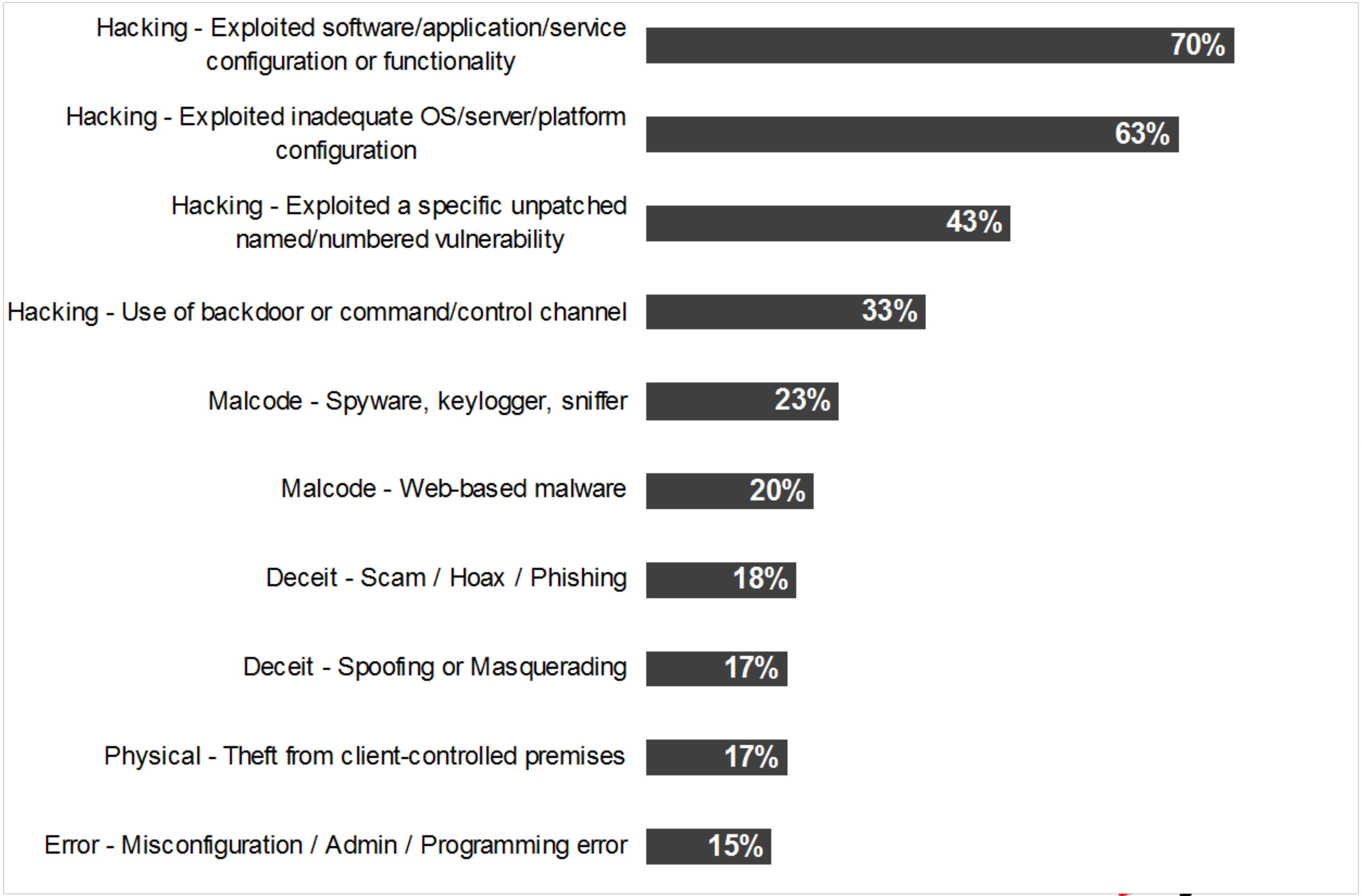
Note: 2007 cases only

IR Case Metrics: Statistics and Trends

How do breaches occur?

IR Case Metrics: Statistics and Trends

Methods, Top 10

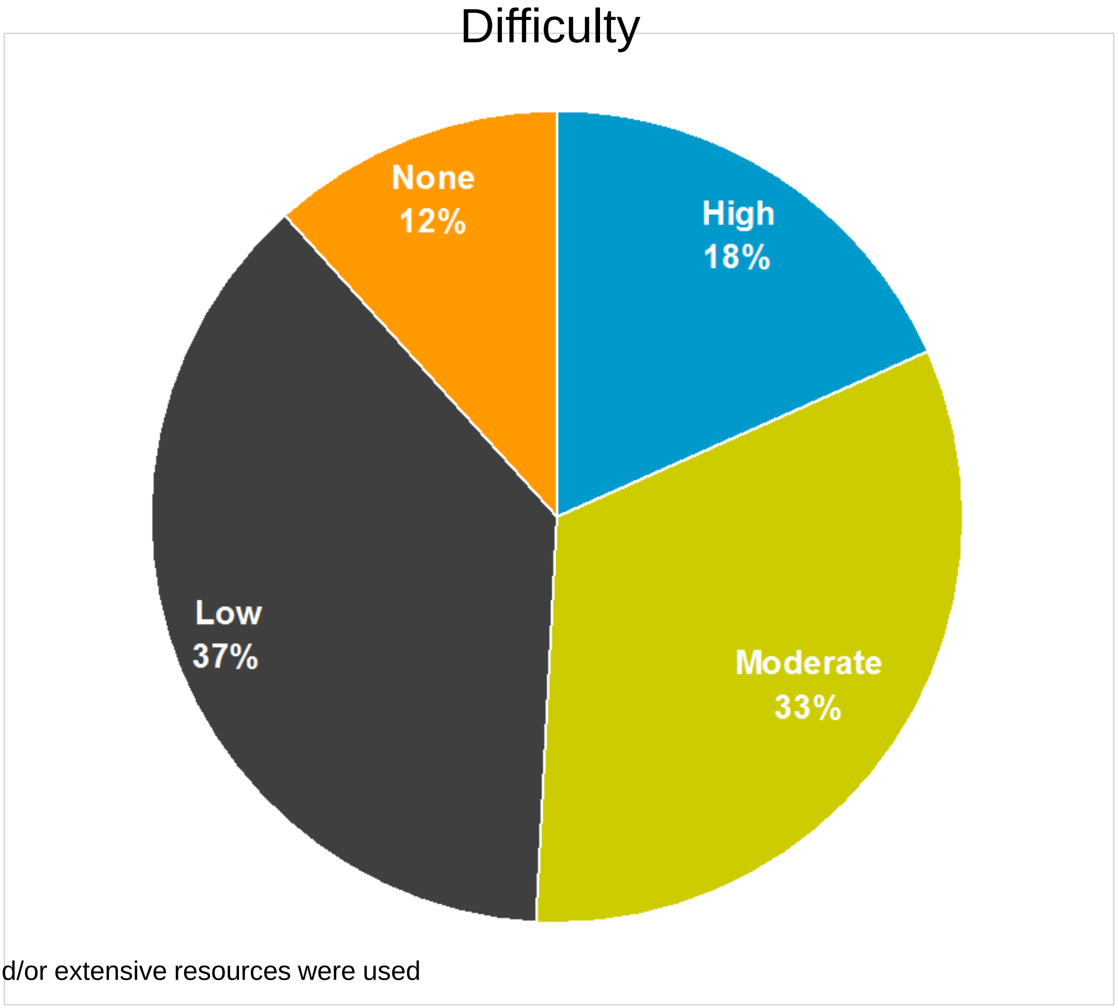


IR Case Metrics: Statistics and Trends

Methods, Continued

Deceit - Social Engineering	**13%**
Misuse - Non-malicious misuse of corporate resources	**13%**
Malcode - Worm or Virus	**13%**
Error - User error	**13%**
Physical - Wiretapping / Sniffing	**12%**
Misuse - Malicious misuse / abuse of access or privilege	**12%**
Error - Inadvertent disclosure of sensitive data via web	**10%**
Physical - Theft from external location	**8%**
Error - Technical / system failure	**8%**
Physical - Loss or misplacement of asset	**7%**
Physical - System access or tampering	**7%**

IR Case Metrics: Statistics and Trends



High - Advanced skills and/or extensive resources were used

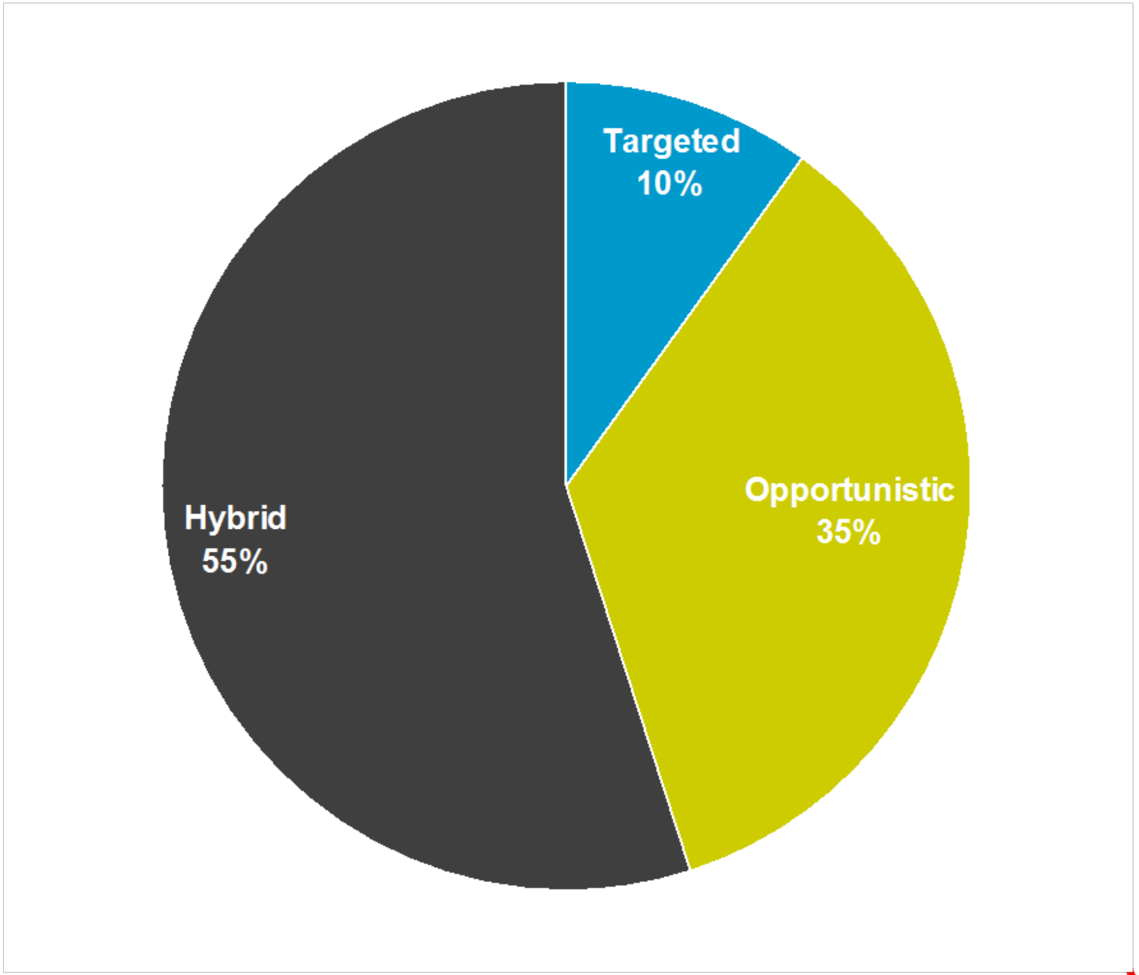
Moderate - The attack involved skilled attacks and/or significant resources

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

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

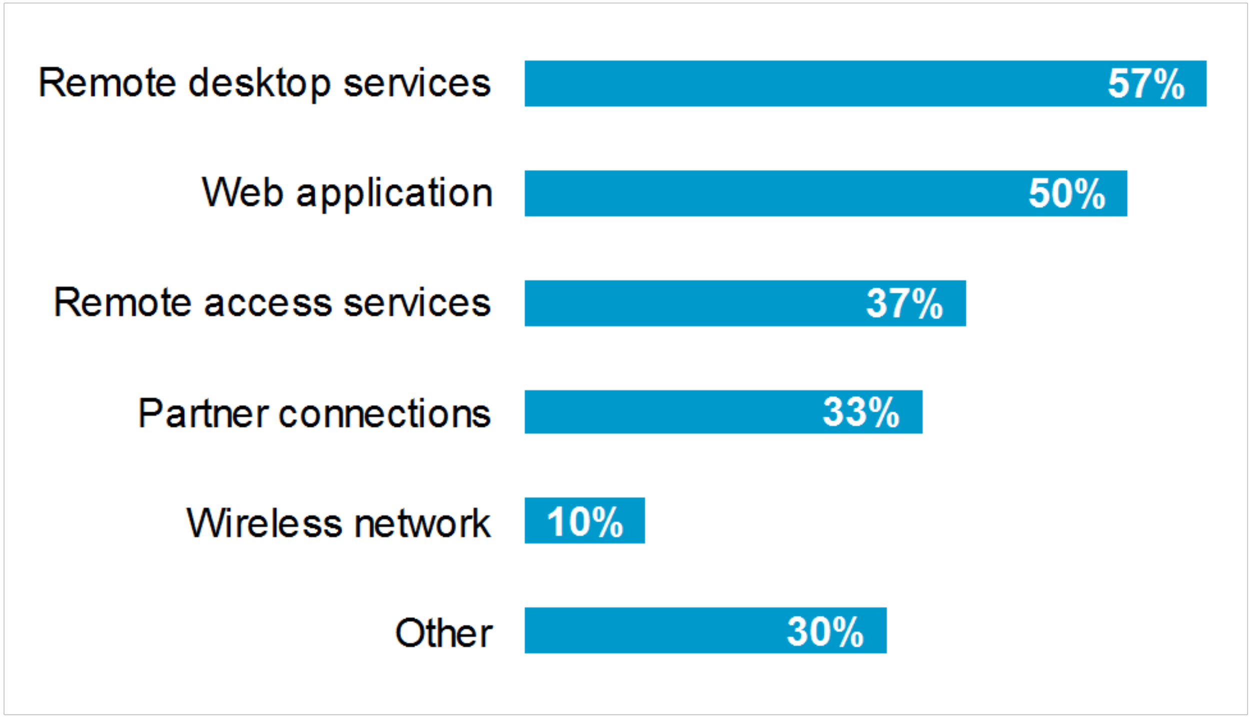
IR Case Metrics: Statistics and Trends

Targeted vs Opportunistic



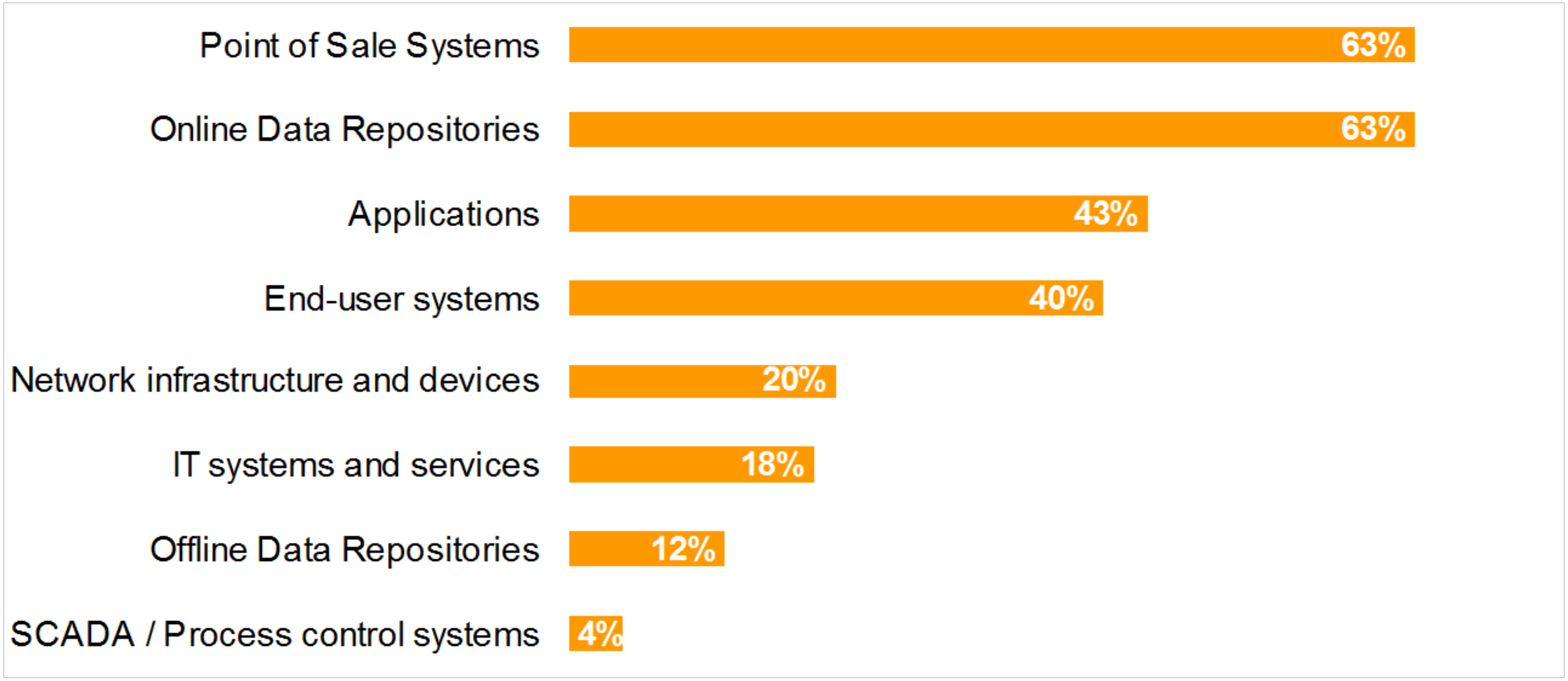
IR Case Metrics: Statistics and Trends

Vector



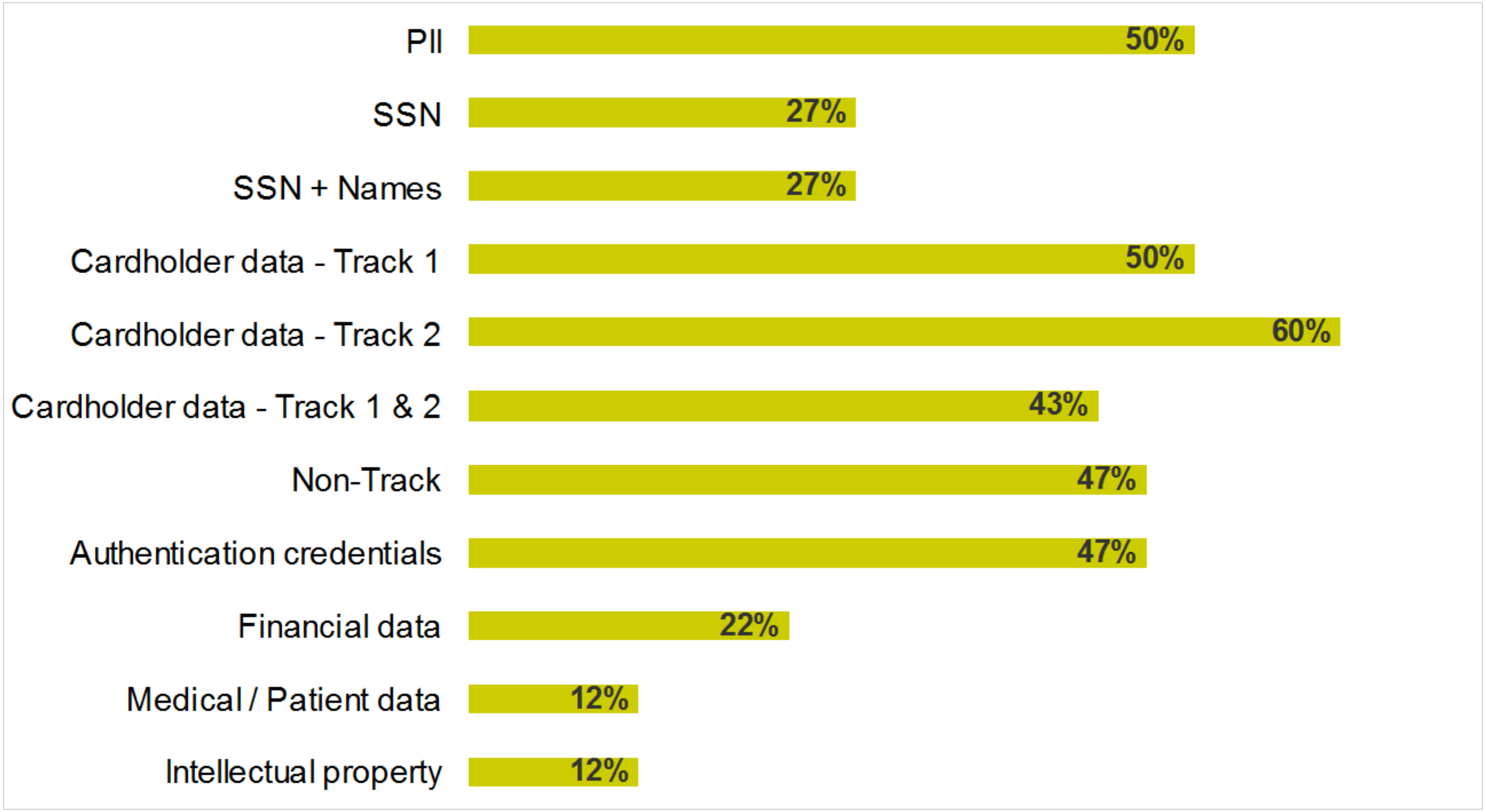
IR Case Metrics: Statistics and Trends

Compromised Asset



IR Case Metrics: Statistics and Trends

Compromised Data



IR Case Metrics: Statistics and Trends

Time Span

Point of entry to compromise = ~**Hours**

Compromise to discovery = ~**Months**

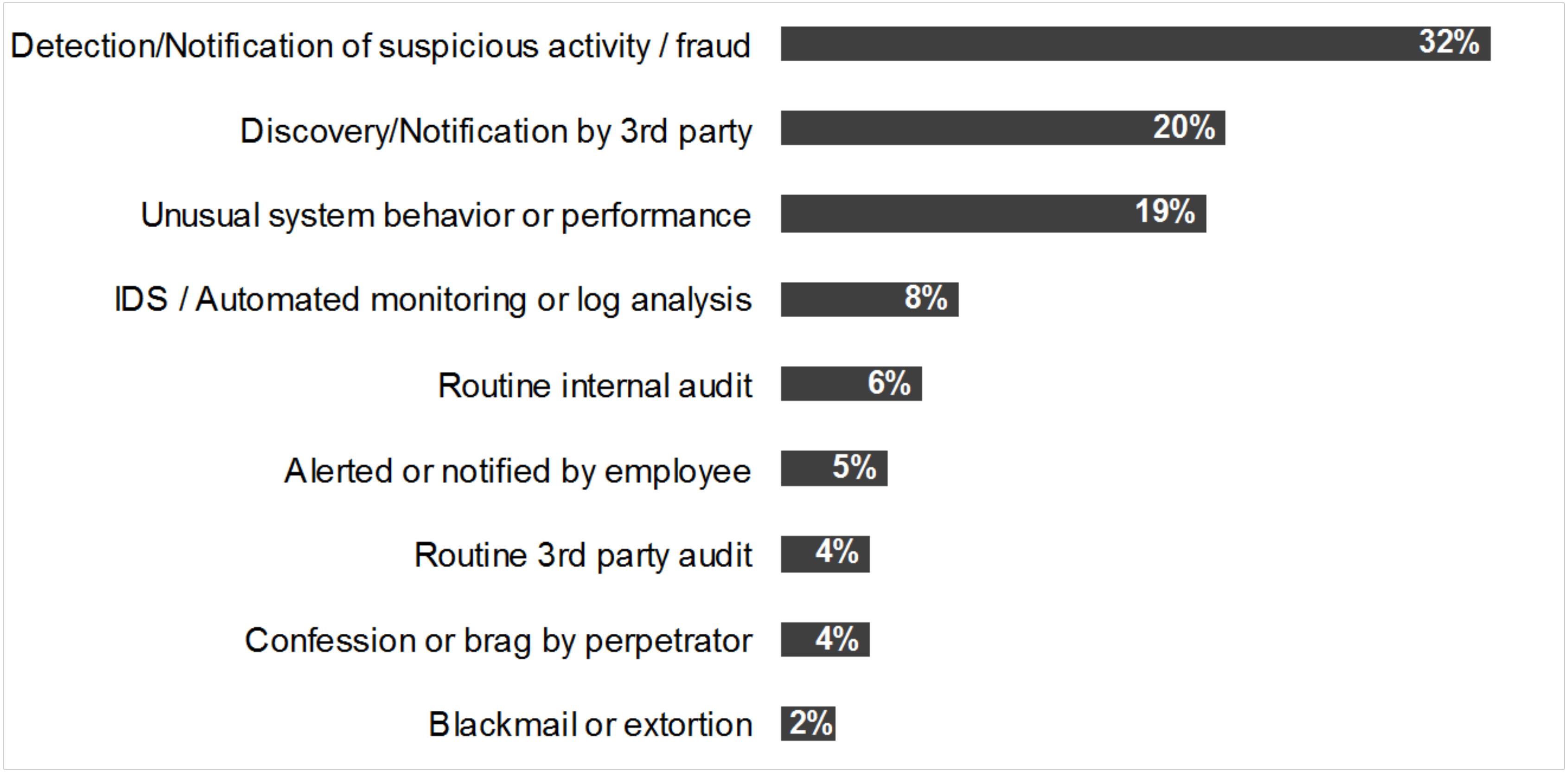
Discovery to mitigation = ~**Weeks**

IR Case Metrics: Statistics and Trends

How are breaches discovered?

IR Case Metrics: Statistics and Trends

Incident Discovery



IR Case Metrics: Statistics and Trends

Anti-forensics

Q4 2006 = **14%** of cases

Q4 2007 = **67%** of cases

IR Case Metrics: Statistics and Trends

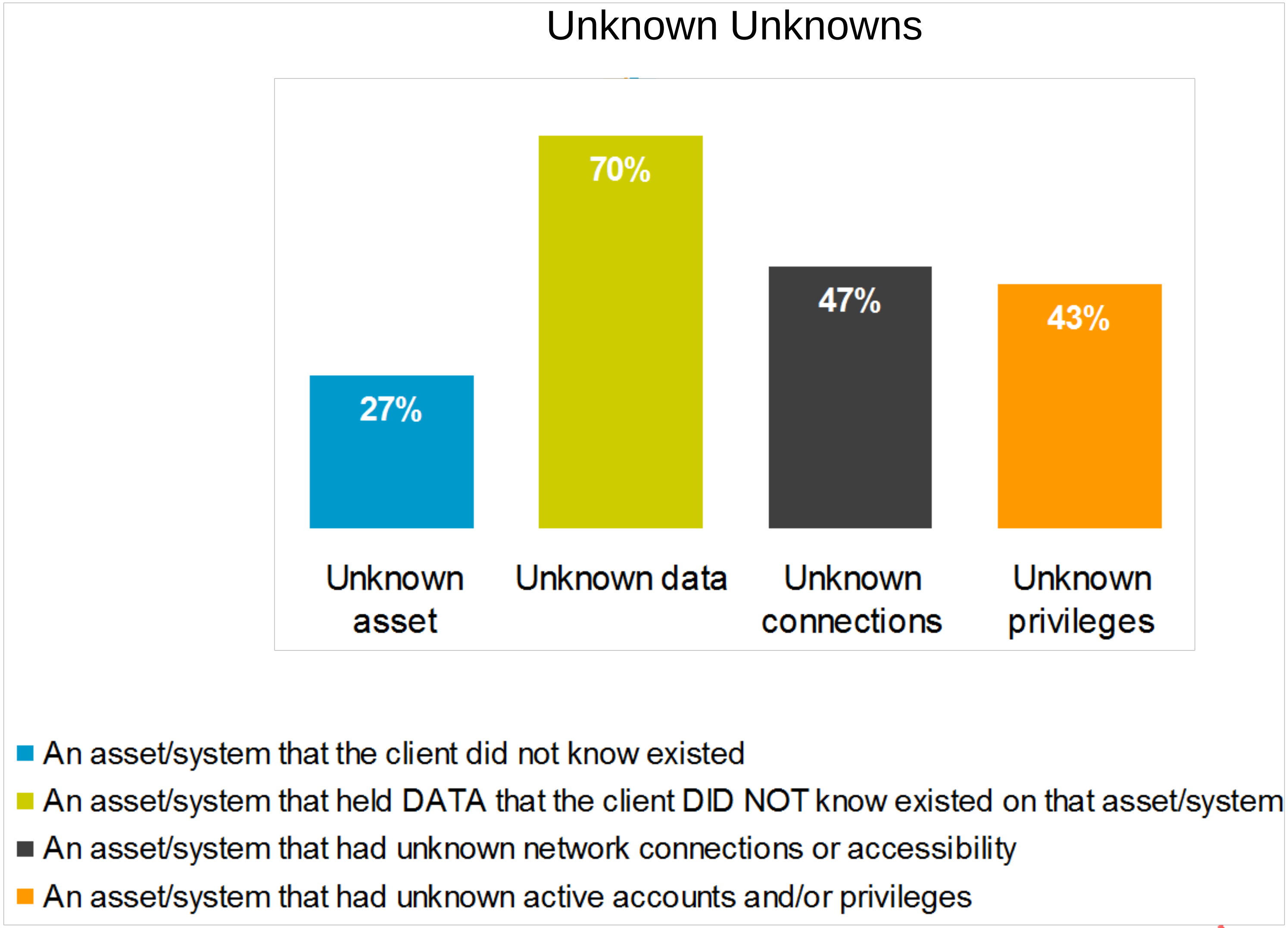
Can breaches be prevented?

IR Case Metrics: Statistics and Trends

Yes.

87% of incidents could have been avoided through the use of "due diligence" or "reasonable" security controls.

IR Case Metrics: Statistics and Trends



IR Case Metrics: Statistics and Trends

Asset / Data discovery & classification	70%
Software / App development standards	57%
Minimization or removal of replicated data	52%
Identity Management	50%
More restrictive access privileges	50%
Firewalls / Routers configured for default-deny	47%
Network segmentation or zoning	47%
More consistent vulnerability patching	47%
System hardening / minimal config	47%
Disk Encryption	47%
IDS / Network monitoring	43%

% of cases that would likely have been prevented (or at least substantially mitigated) if the control had been in place (or of better quality) at the time of the attack

IR Case Metrics: Statistics and Trends

Intrusion Prevention System	40%
User awareness & training	40%
Checks to identify technical non-compliance	40%
Data Loss Prevention / Content filtering	30%
Client / personal firewall	30%
Antivirus software	23%
Physical security controls	13%
Anti-Spyware	13%
USB Blocking	8%
More frequent vulnerability patching	2%

% of cases that would likely have been prevented (or at least substantially mitigated) if the control had been in place (or of better quality) at the time of the attack

verizonbusiness