XXVII Bank Security Conference

CELAES 2012

"MITIGATING RISKS AND CONVERTING THEM INTO BUSINESS OPPORTUNITIES"

FIBA

Organized by:

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

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
2010 DATA BREACH INVESTIGATIONS RE
A study conducted by the Verizon RISK Team in cooperation with the United Stat
2012 DATA BREACH INVESTIGATIONS REPORT
verizon
ATTENTI
h4x0r5
WANTED
Acme Corp
For flagrant
and social
2011 Data Breach Investigations Report
A study conducted by the Verizon RISK Team with cooperation from the U.S. Secret Service and the Netherlands High Tech Crime Unit
POLITIE
verizon

An ongoing study into the world of cybercrime that analyzes forensic evidence to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and, of course, what might be done to prevent it.

DBIR Contributors

AFP
AUSTRALIAN FEDERAL POLICE

POLITIE
Korps landelijke politiediensten

UNITED STATES SECRET SERVICE

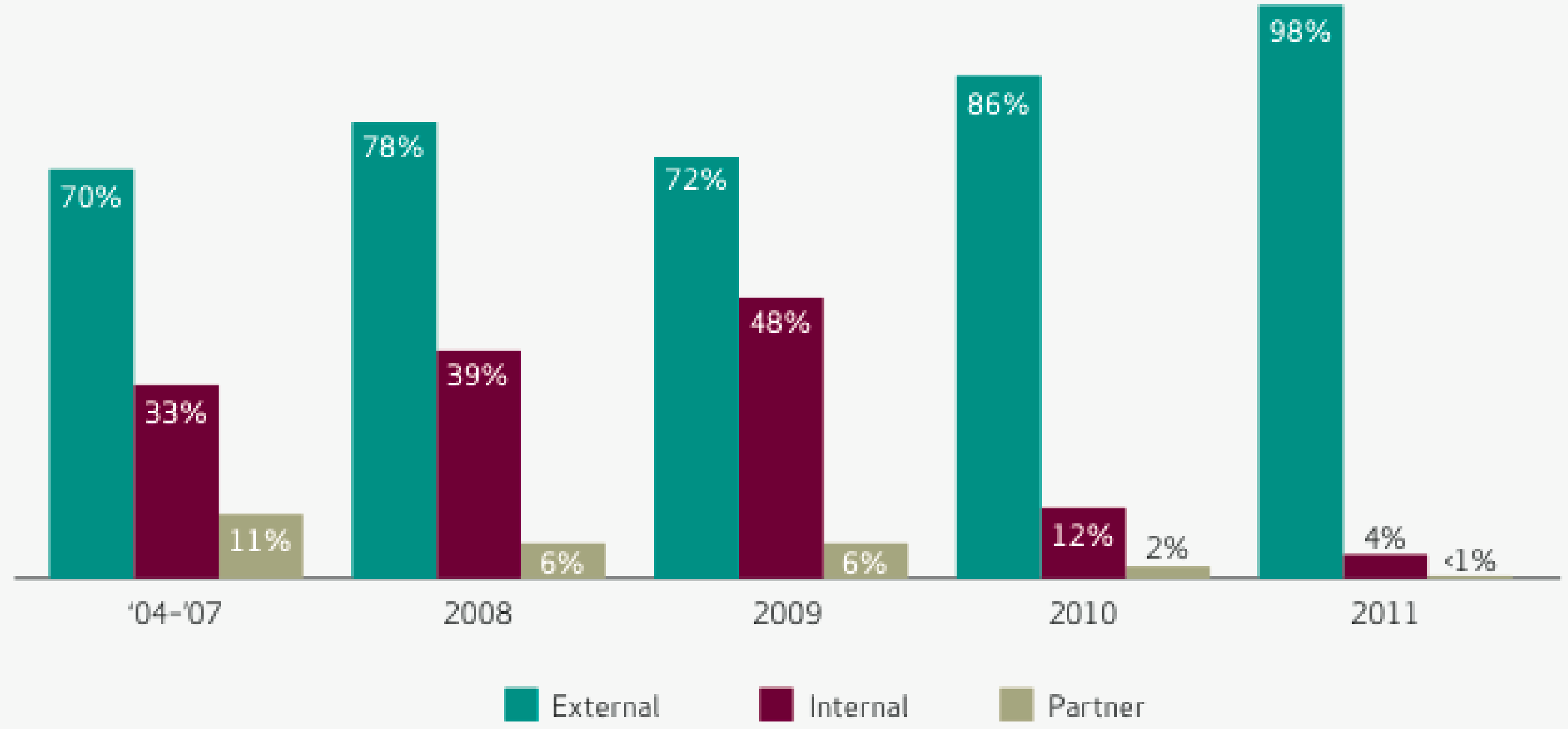
IRISS
Irish Reporting and
Information Security Service

PCeU
Police Central e-crime Unit

verizon

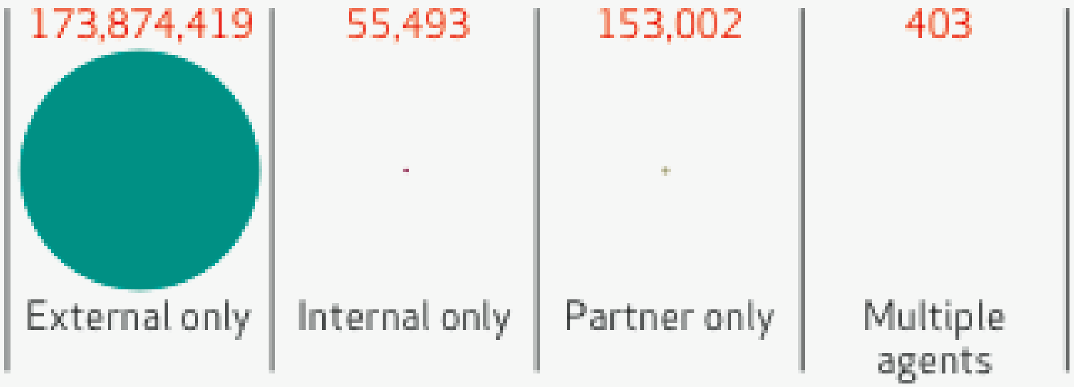
Threat Agents

Figure 10: Threat agents over time by percent of breaches



Threat Agents vs. Breached Records

Figure 13. Compromised records by threat agent, 2011



Threat Agents : External

Figure 15: Motive of external agents by percent of breaches within external

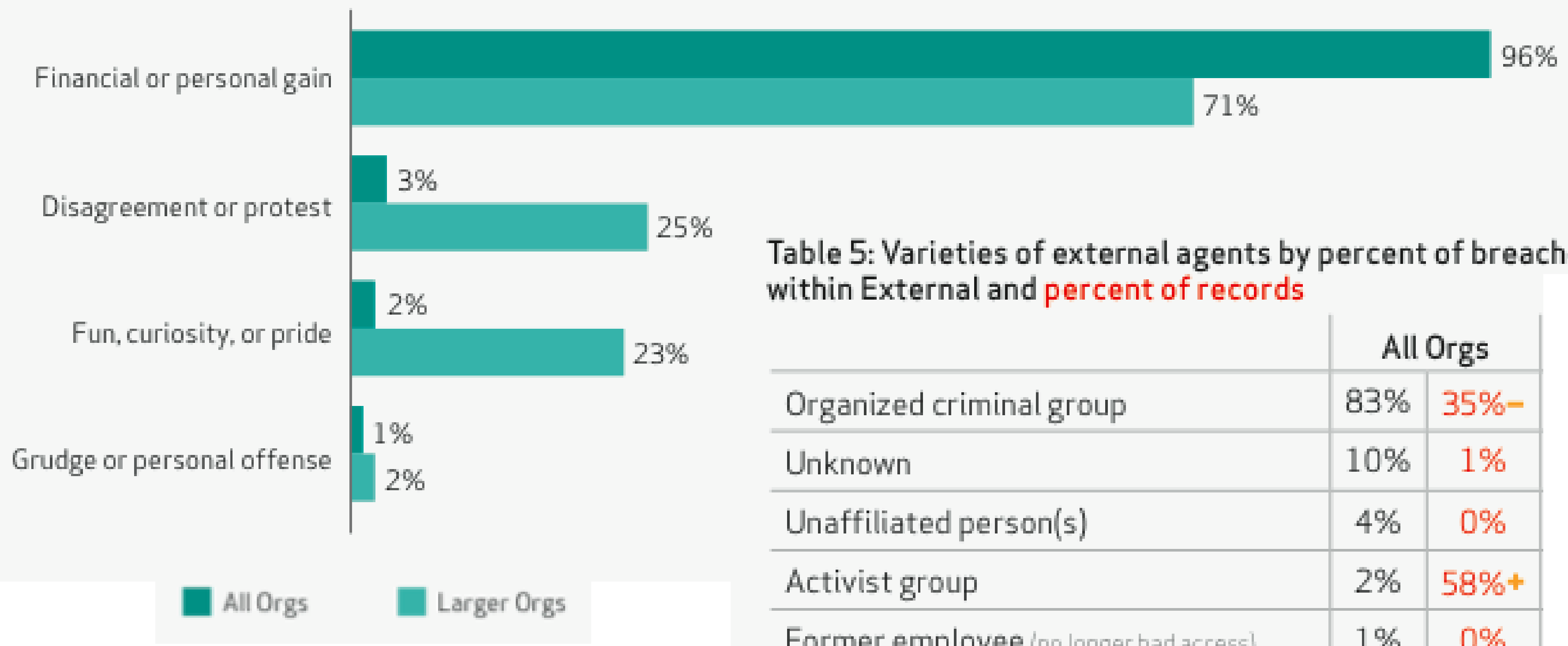
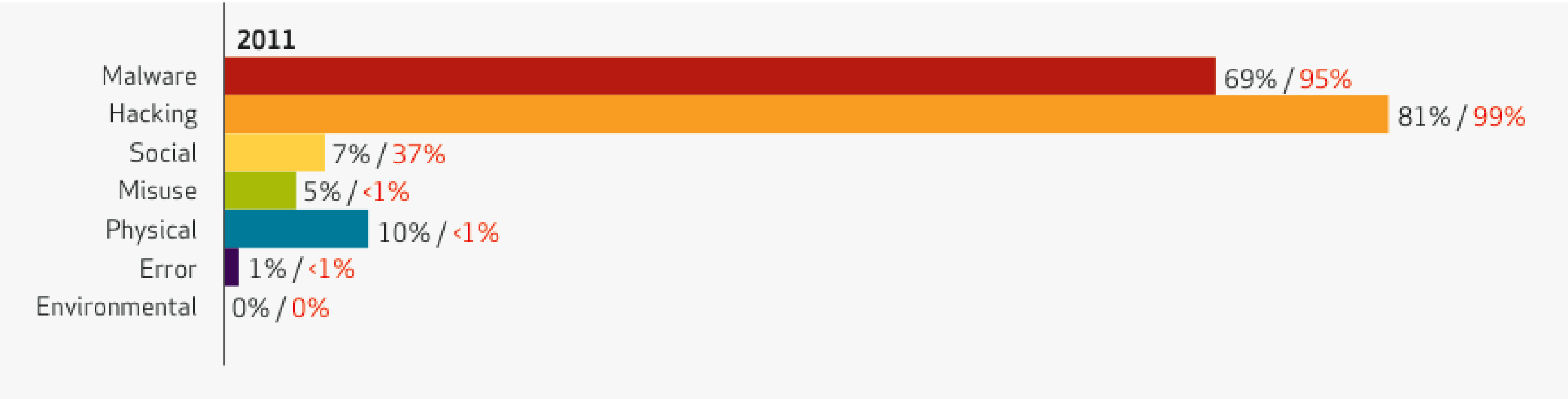


Table 5: Varieties of external agents by percent of breaches within External and percent of records

	All Orgs	
Organized criminal group	83%	35%−
Unknown	10%	1%
Unaffiliated person(s)	4%	0%
Activist group	2%	58%+
Former employee (no longer had access)	1%	0%
Relative or acquaintance of employee	0%	0%

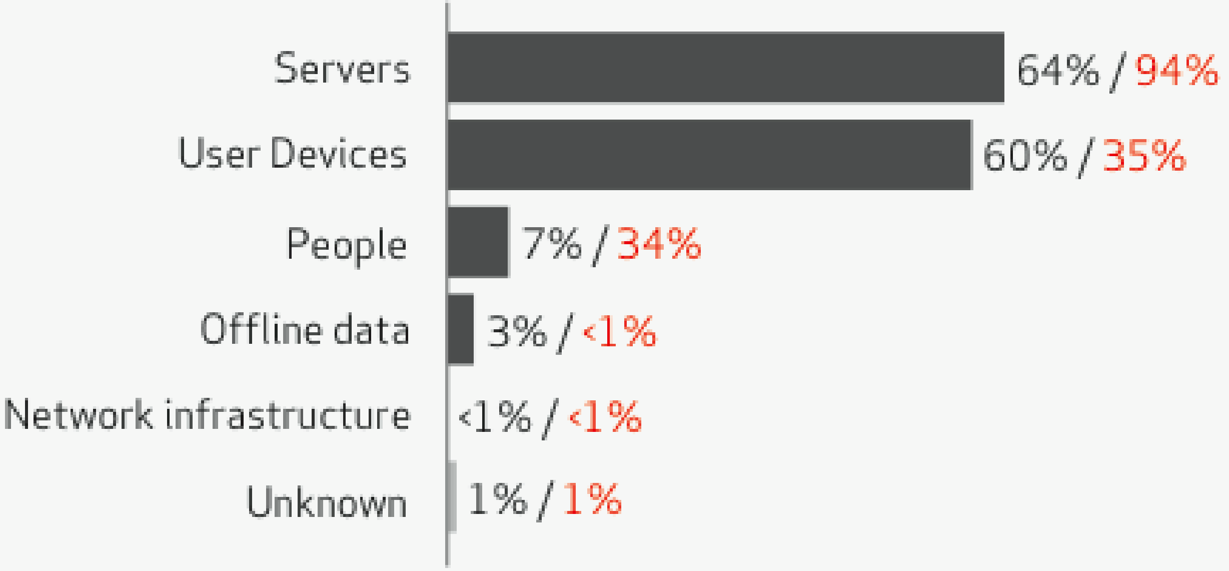
Threat Actions

Figure 17. Threat action categories over time by percent of breaches and percent of records



Compromised Assets

Figure 26. Categories of compromised assets by percent of breaches and percent of records



Asset Hosting, Management, Ownership

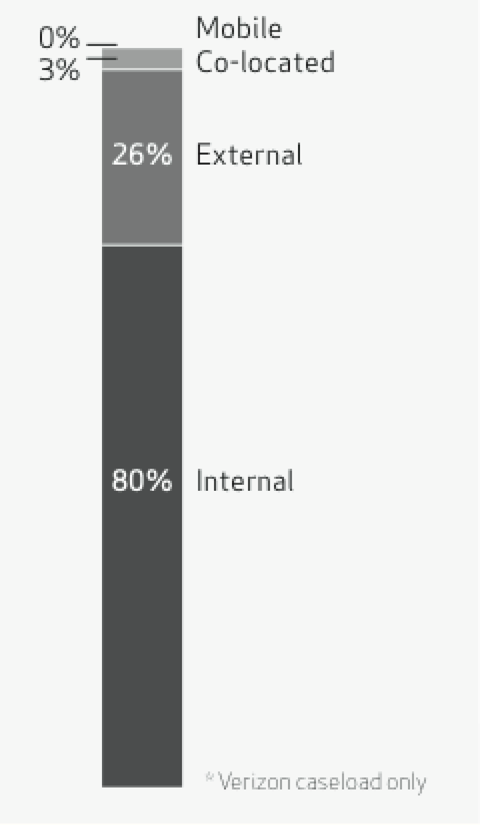


Figure 29. Hosting of assets by percent of breaches*

* Verizon caseload only

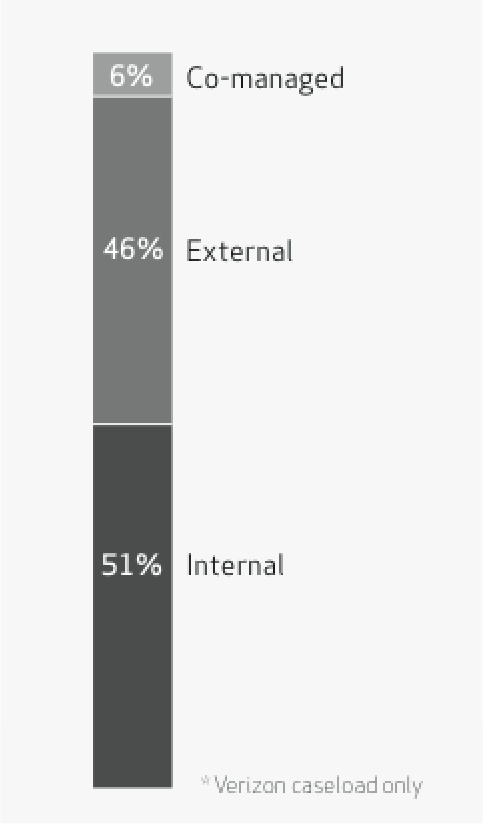


Figure 30. Management of assets by percent of breaches*

* Verizon caseload only

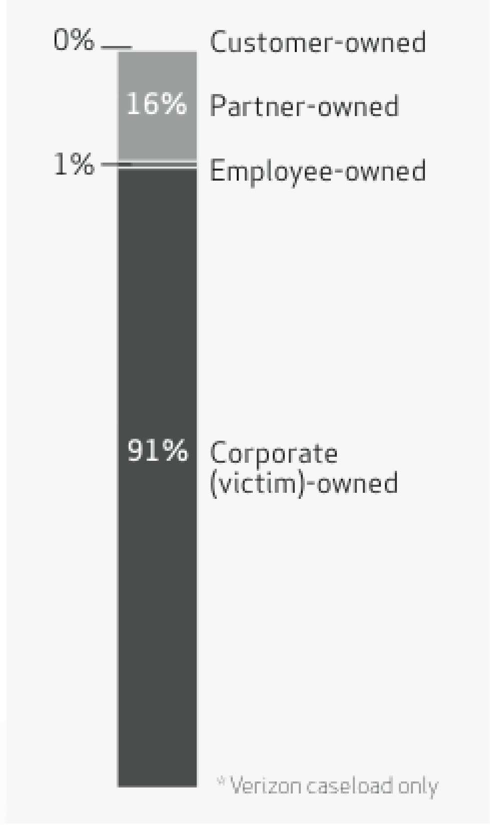
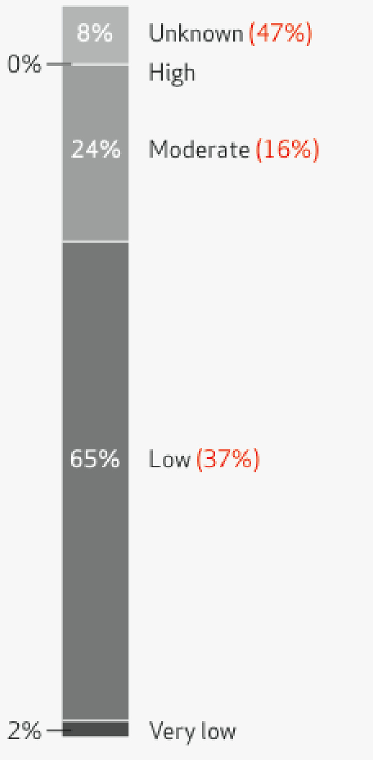


Figure 31. Ownership of assets by percent of breaches*

* Verizon caseload only

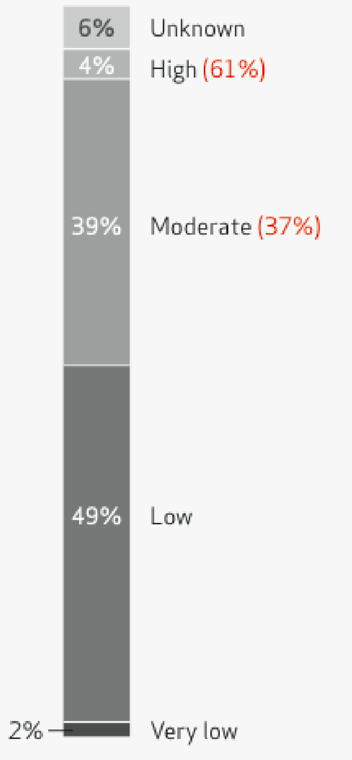
Attack Difficulty / Complexity

Figure 36. Difficulty of initial compromise by percent of breaches and percent of records*



* Verizon caseload only

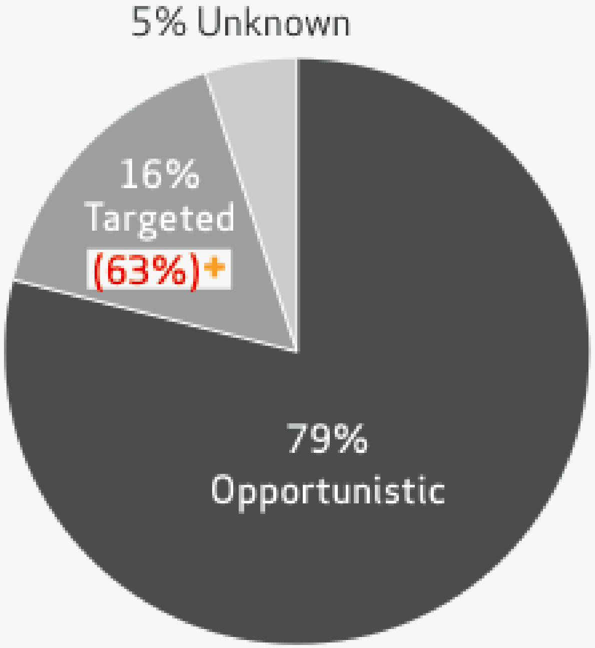
Figure 37. Difficulty of subsequent actions by percent of breaches and percent of records*



* Verizon caseload only

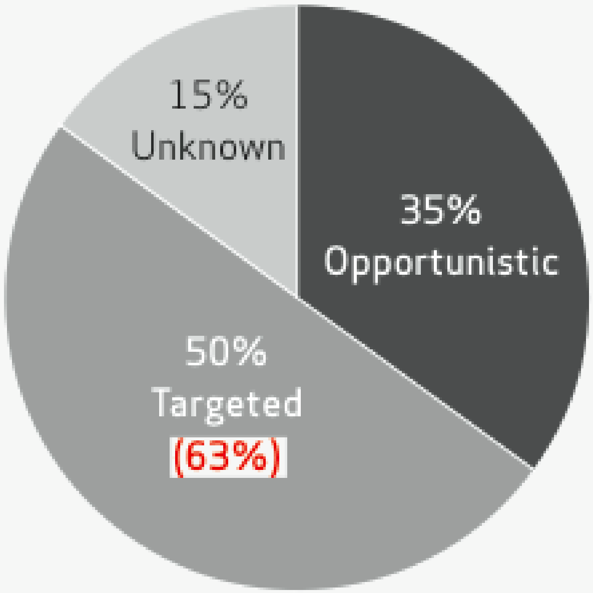
Attack Targeting

Figure 38. Attack targeting by percent of breaches and percent of records*



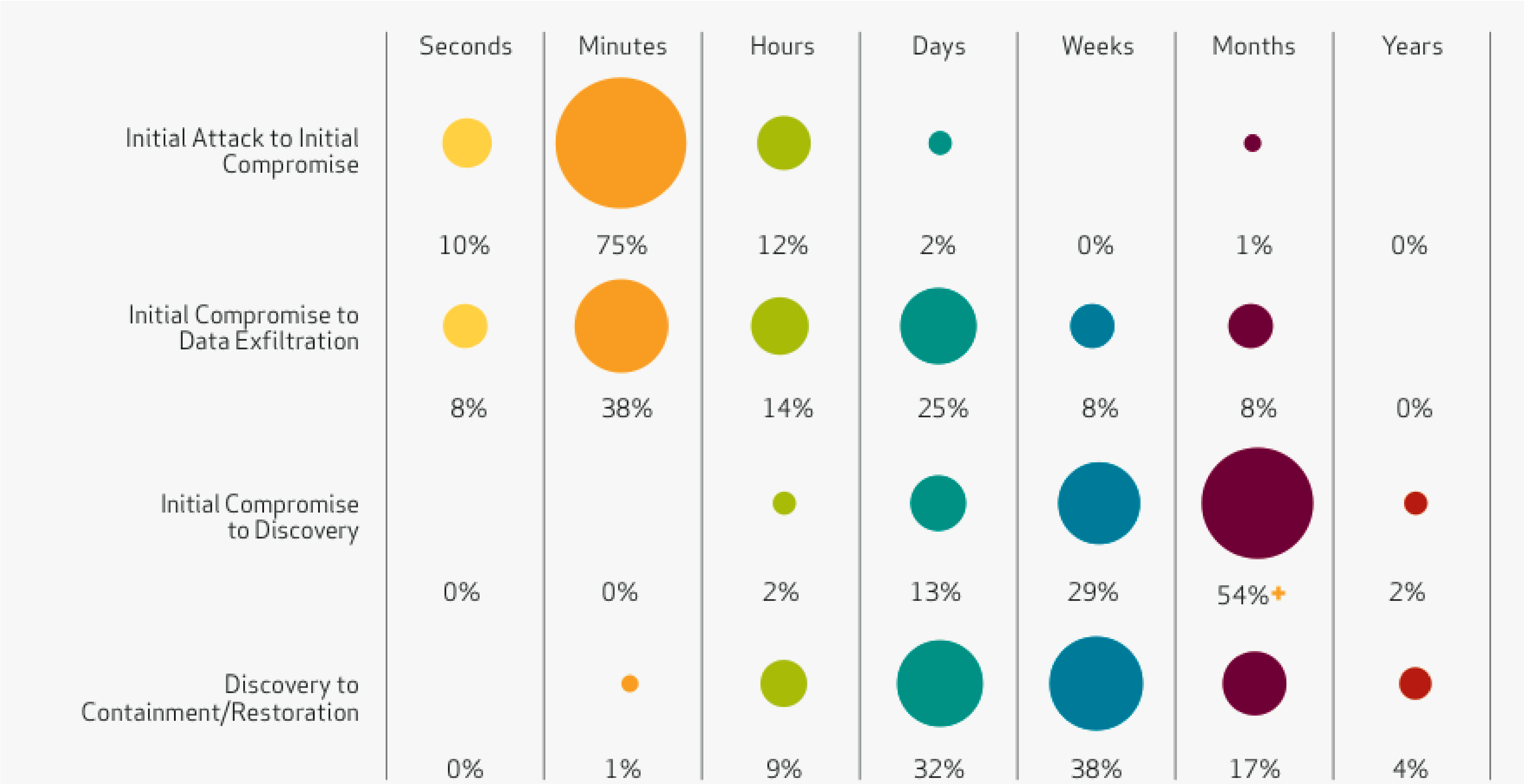
* Verizon caseload only

Figure 39. Attack targeting by percent of breaches and percent of records – LARGER ORGS*



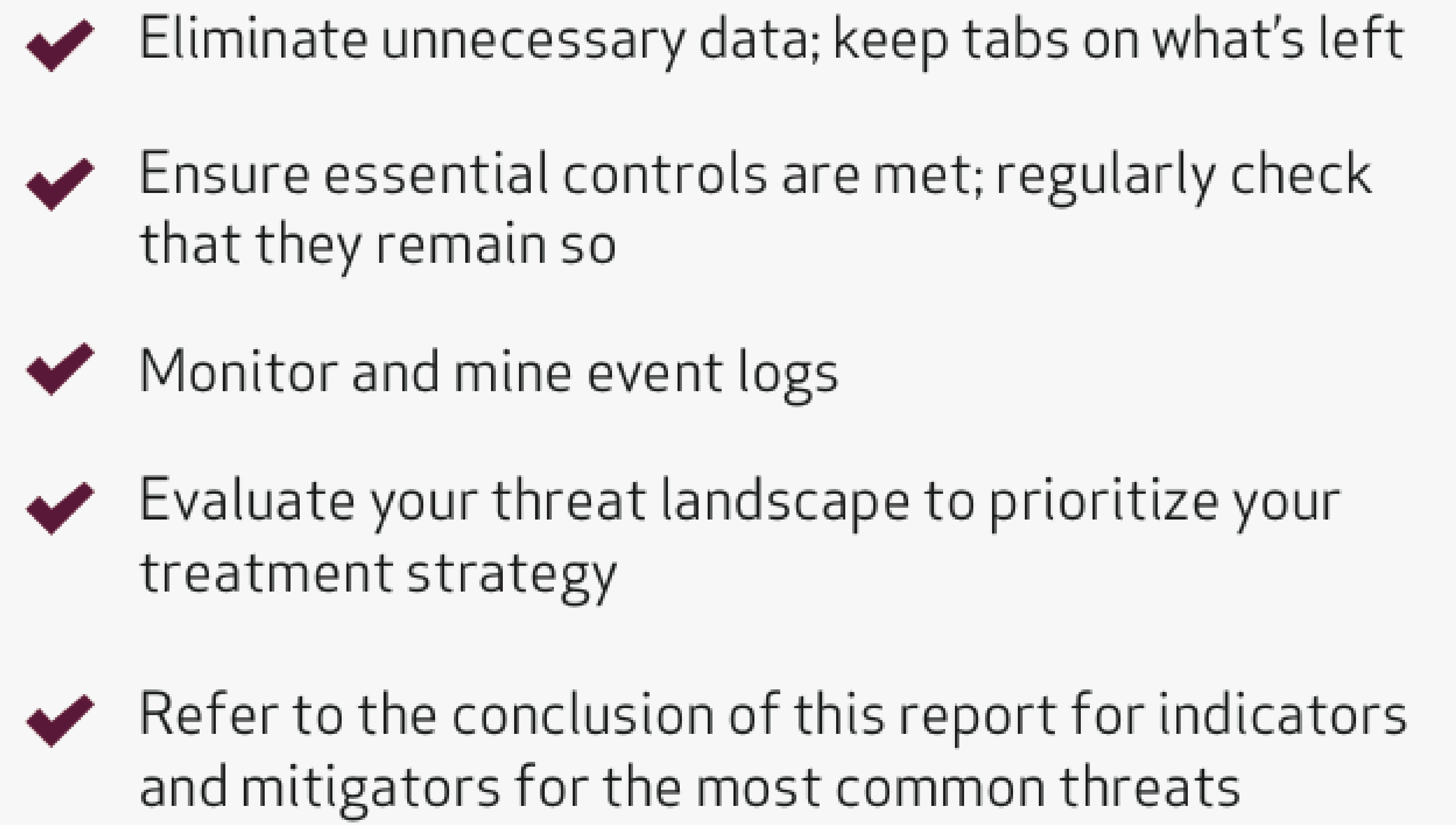
* Verizon caseload only

Timespan of Events



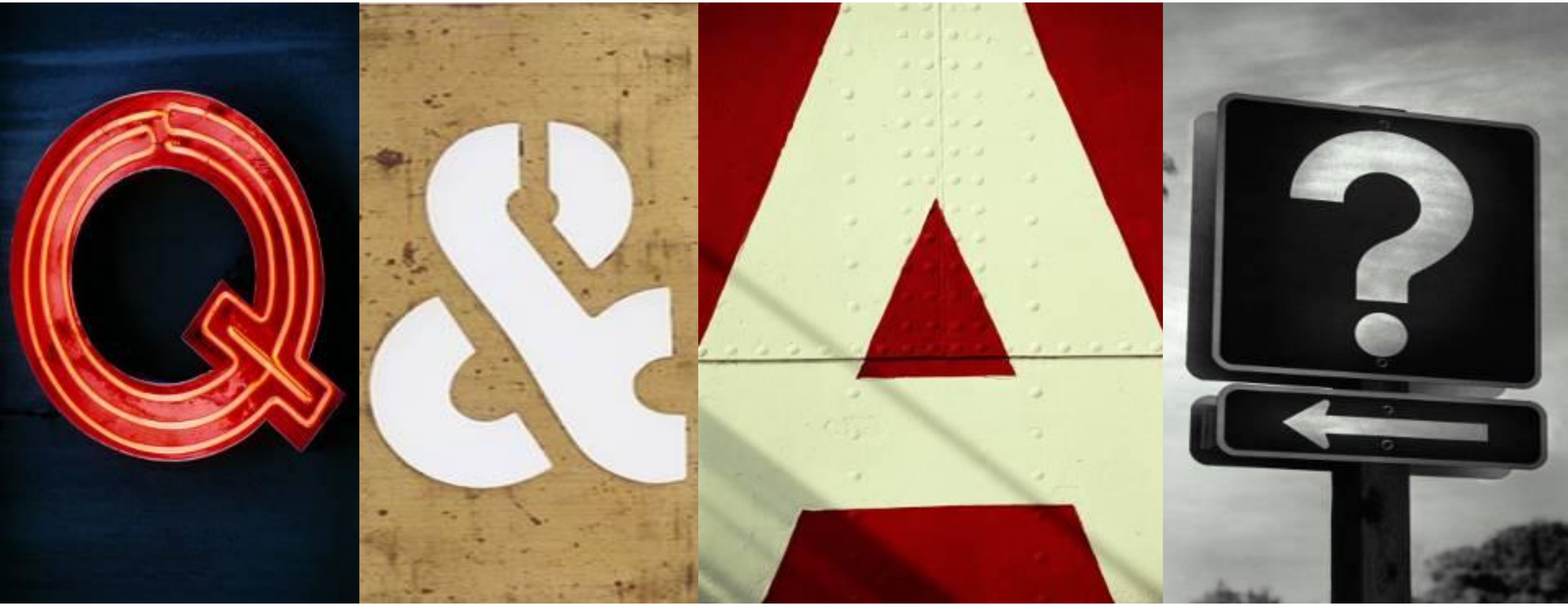
	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

Recommendations



- ✓ Eliminate unnecessary data; keep tabs on what's left
- ✓ Ensure essential controls are met; regularly check that they remain so
- ✓ Monitor and mine event logs
- ✓ Evaluate your threat landscape to prioritize your treatment strategy
- ✓ Refer to the conclusion of this report for indicators and mitigators for the most common threats

Questions & Answers



Christopher Novak
Verizon, Investigative Response
914-574-2805
chris.novak@verizon.com