

Evidence Based Risk Management



When analysis is used to uncover how sensitive data is stolen from organizations, who's doing it, why they're doing it, and what might be done to prevent it

Seán Paul McGurk

January 24, 2013



The RISK Team

More than an acronym

Research

Uncover the who, what, when, how and why behind computer security incidents.

Investigations

Study and understand the ever-changing risk and threat environment. It all starts here.

Solutions

Leverage lessons learned from “R” and “I” to create new products and enhance our existing portfolio.

Knowledge

Cultivate and disseminate our information resources to make our people, products, and brand smarter than the competition.

The RISK Team = Risk Intel + Investigative Response + eDiscovery



RISK Team Overview

(Research, Investigations, Solutions, Knowledge)

Approach: IT Investigative focus

Diverse Investigator Backgrounds

Licensed Private Investigators

Truly Global Coverage – 24x7x365

- Investigators based in 16 countries
- Forensic labs and evidence storage facilities in Americas, Europe, and Asia-Pacific

No Subcontractors

Global PFI Firm

Annual Data Breach Investigations Report

Service offerings:

- IT Investigative Support (On-demand)
- Guaranteed Response (Retainer-based)
- eDiscovery and Litigation Support
- PCI Forensic Investigations
- Electronic Data Recovery / Destruction
- Incident Response Training
- Mock-Incident Exercises
- Corporate IR Program Development

Verizon RISK team has handled 8 of the world's 10 largest data compromise investigations! *

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



RISK Team *Global Reach*





Seven Sources of Threat 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 Million VzB addresses. Netflow Honey nets, Honey Pots...
7	Studies & Surveys VZB Studies, surveys (10+/yr), Others published data to drive Risk Models, equations & methodology





Knowledge improves operations

For over 10 years, the **Security Management Program** has looked after the *deployment, configuration, and upkeep of thousands of client systems* on an ongoing basis.

Our **Vulnerability Management Services** identify and track common vulnerabilities and weaknesses present across clients systems and applications.

The **RISK team** monitors criminal activity and collaborates with law enforcement to understand the motives and methods that drive cybercrime.

The **Penetration Testing** team provides visibility into the numerous ways malicious agents can subvert defenses to exploit information assets.

Our **Investigative Response** unit investigates hundreds of cases per year, providing quality metrics on the agents and actions that frequently contribute to security incidents.

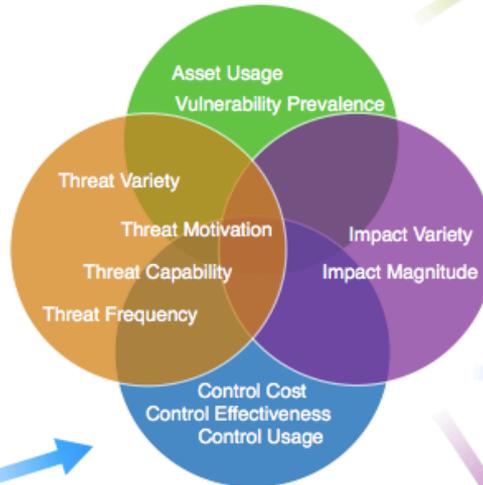
Sensors and systems spread across Verizon's vast network infrastructure collect data 24/7 to stay abreast of current and emerging threats.

Verizon's **PCI-DSS consultants** work with hundreds of clients each year and provide assessment results for the body of controls required in that standard.

ICSA Labs continually tests the reliability and effectiveness of security products against an ever-changing threat environment.

As our **Governance, Risk, and Compliance** services work with clients to align security posture with risk tolerance, they gain perspective into how incidents affect organizations.

We track the growing number of **external reports on organizational losses** (i.e., corporate 10Ks) and studies that quantify the consequences of security incidents.



Applied Asset Data

The **RISK Intelligence** team tracks asset usage to help assess the criticality of published vulnerabilities and guide recommendations to our client base.

Knowledge of prevalent vulnerabilities and related exploits guides our **Application Risk Assessment and SDLC training teams** in delivering more effective services.

Applied Threat Data

Our top-rated **Managed Security Services** incorporate intelligence on emerging threat sources and patterns to better protect client assets.

The **Virtual Discovery and Classification** service draws from intelligence around threat capabilities to better identify and classify suspicious network activity.

Verizon's **PCI-DSS consultants** use lessons learned from our forensic investigators about financially-motivated crime to deliver more informed and relevant assessments.

The **Security Management Program** incorporates threat frequency data into the models that drive risk scoring and reporting to clients.

Applied Control Data

Professional Services teams utilize control usage data to drive baseline comparisons for clients and enhance the value of deliverables.

Quantitative Risk Management (QRM) service leverages control effectiveness data to prioritize security initiatives and provide managerial decision support.

Applied Impact Data

A new **Incident Analytics Service** leverages the VERIS impact model as well as loss data collected by RISK Intel to create unique and powerful metrics.

The **Governance, Risk, and Compliance** group uses historical impact data to improve the accuracy of risk assessments and better counsel clients.



- **Malicious cyber activity is routinely directed at the U.S. Government, private sector, and academia**
 - Growing more sophisticated, targeted, and prevalent
 - Nature and source of the threat is diverse
 - Designed to
 - Exploit data gathered from information systems or networks (computer network exploitation)
 - Disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves (computer network attack)
- **We have insight on intrusions into private sector networks, but are becoming more aware of U.S. information infrastructure vulnerabilities to cyber attacks**
 - Key factors: dynamic business environment, reliance on open systems and COTS, management/enterprise networks' Internet connections
 - Key challenges: Your sensitive data isn't just on your network, it is on your vendors networks, consultants networks, suppliers networks, etc.



Cyber Security Consequences

- The Intelligence Community has information from multiple sources of cyber intrusions followed by extortion demands
 - Encrypting corporate data/demanding money to decrypt the data
- Theft of sensitive corporate data
 - Industrial espionage costs US businesses up to \$250 billion per year
 - 98% of breaches were attributed to external agents
- Theft of personal data
 - Attacker/there is typically motivated by profits (value is approximately \$8 per record)
 - 855 investigated incidents with over 174 million records compromised
- Cyber attacks have been used to disrupt critical services in several regions outside the U.S.

Threat Level 1

“Garden Variety”

- Inexperienced
- Limited funding
- Opportunistic behavior
- Target known vulnerabilities
- Use viruses, worms, rudimentary trojans, bots
- Acting for thrills, bragging rights
- Easily detected

Threat Level 2

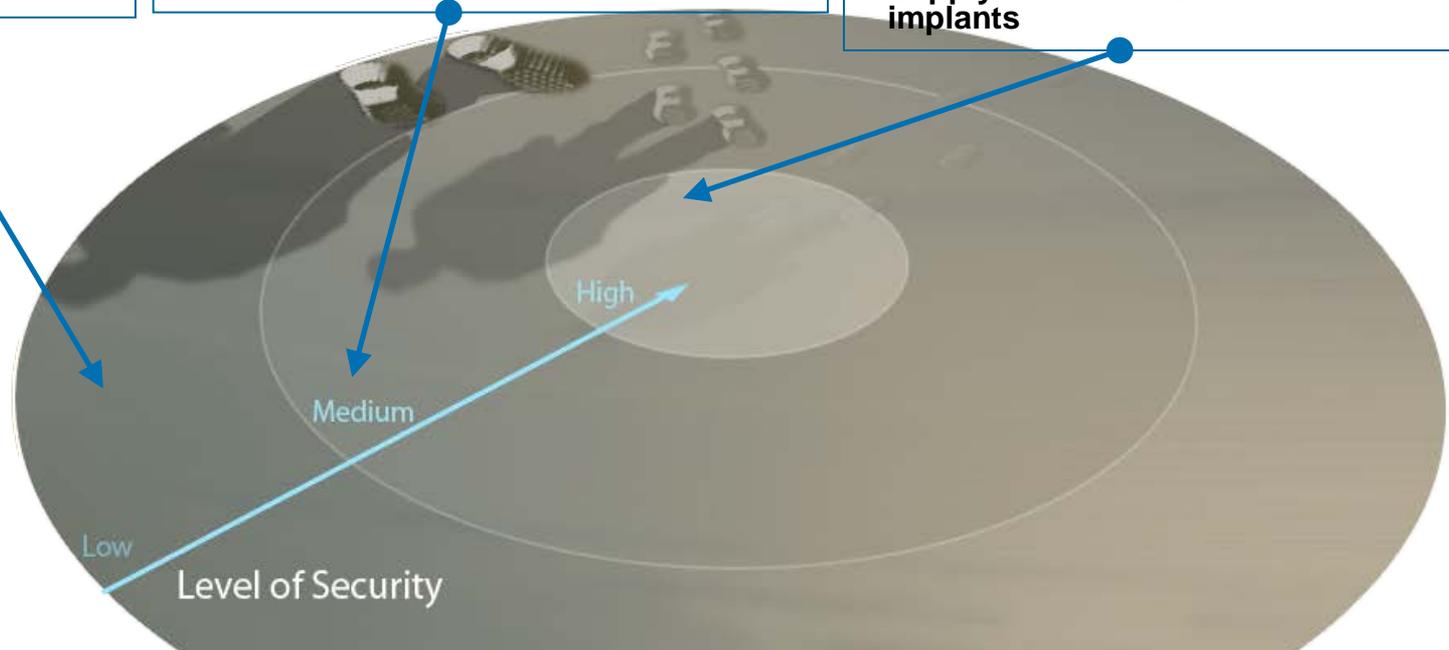
“Mercenary”

- Higher-order skills
- Well-financed
- Targeted activity
- Target known vulnerabilities
- Use viruses, worms, trojans, bots as means to introduce more sophisticated tools
- Target and exploit valuable data
- Detectable, but hard to attribute

Threat Level 3

“Nation State”

- Very sophisticated tradecraft
- Foreign intel agencies
- Very well financed
- Target technology as well as info
- Use wide range of tradecraft
- Establish covert presence on sensitive networks
- Difficult to detect
- Supply Interdiction/hardware implants





2012 DBIR Contributors



Working together for a safer London



AFP
AUSTRALIAN FEDERAL POLICE



8 years of investigations and research
2000+ confirmed data breach cases
More than **1 billion** stolen records

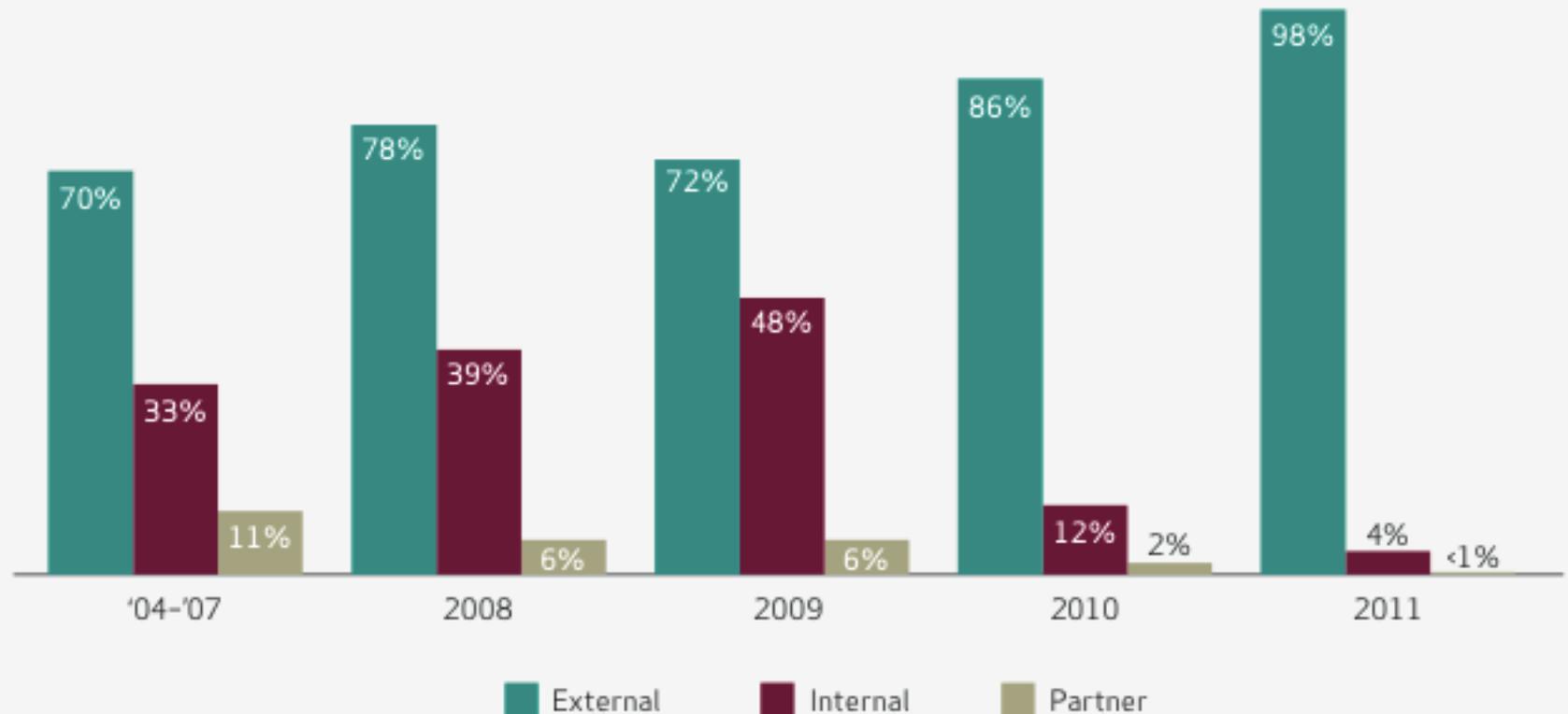
Figure x. Countries represented in combined caseload



Countries in which a breach was confirmed

Australia	France	Jordan	Poland	Turkey
Austria	Germany	Kuwait	Romania	United Arab Emirates
Bahamas	Ghana	Lebanon	Russian Federation	Ukraine
Belgium	Greece	Luxembourg	South Africa	United Kingdom
Brazil	India	Mexico	Spain	United States
Bulgaria	Ireland	Netherlands	Taiwan	
Canada	Israel	New Zealand	Taiwan, Province of China	
Denmark	Japan	Philippines	Thailand	

Figure 10: Threat agents over time by percent of breaches





Threat Agents: External

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

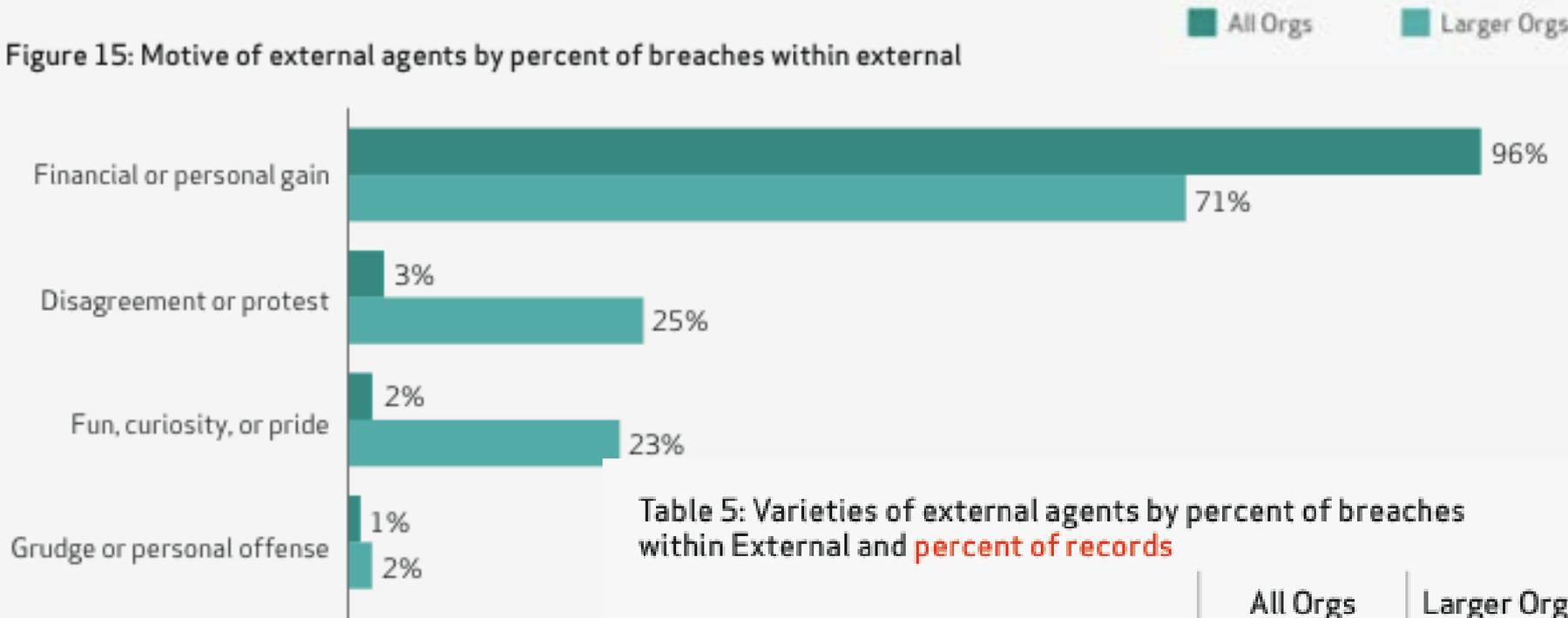


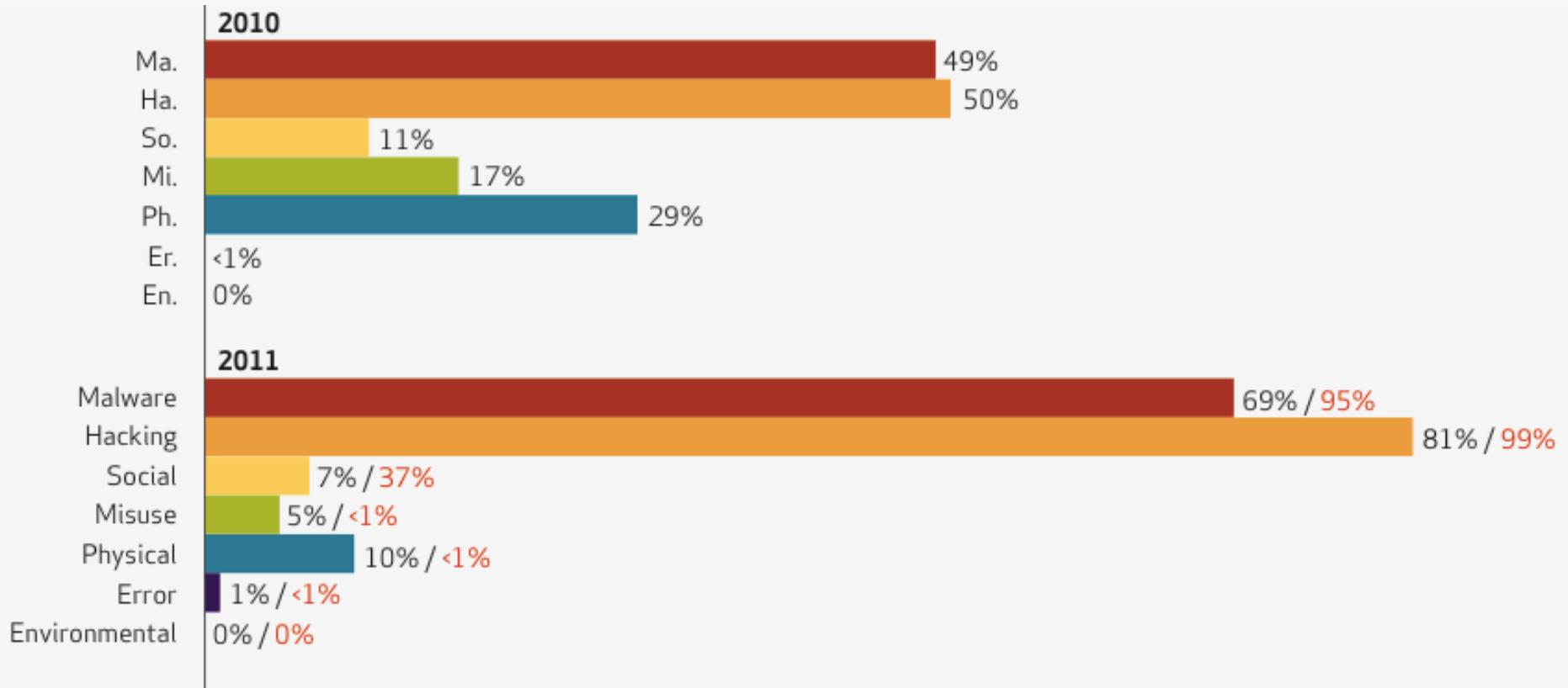
Table 5: Varieties of external agents by percent of breaches within External and percent of records

Agent Type	All Orgs		Larger Orgs	
	Percent of Breaches	Percent of Records	Percent of Breaches	Percent of Records
Organized criminal group	83%	35% ⁻	33%	36%
Unknown	10%	1%	31%	0%
Unaffiliated person(s)	4%	0%	10%	0%
Activist group	2%	58% ⁺	21%	61%
Former employee (no longer had access)	1%	0%	6%	0%
Relative or acquaintance of employee	0%	0%	2%	0%



Threat Actions

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





Top Threat Actions

Table 7. Top 10 Threat Action Types by number of breaches and records

Rank	Variety	Category	Breaches	Records
1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	48%	35%
2	Exploitation of default or guessable credentials	Hacking	44%	1%
3	Use of stolen login credentials	Hacking	32%	82%
4	Send data to external site/entity	Malware	30%	<1%
5	Brute force and dictionary attacks	Hacking	23%	<1%
6	Backdoor (allows remote access/control)	Malware	20%	49%
7	Exploitation of backdoor or command and control channel	Hacking	20%	49%
8	Disable or interfere with security controls	Malware	18%	<1%
9	Tampering	Physical	10%	<1%
10	Exploitation of insufficient authentication (e.g., no login required)	Hacking	5%	<1%



Top Threat Actions: Larger Orgs

Table 8. Top 10 Threat Action Types by number of breaches and records - LARGER ORGS

Rank	Overall Rank	Variety	Category	Breaches	Records
1	3	Use of stolen login credentials	Hacking	30%	84%
2	6	Backdoor (allows remote access/control)	Malware	18%	51%
3	7	Exploitation of backdoor or command and control channel	Hacking	17%	51%
4	9	Tampering	Physical	17%	<1%
5	1	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	13%	36%
6	11	Pretexting (classic Social Engineering)	Social	12%	<1%
7	5	Brute force and dictionary attacks	Hacking	8%	<1%
8	15	SQL Injection	Hacking	8%	1%
9	20	Phishing (or any type of *ishing)	Social	8%	38%
10	22	Command and Control (listens for and executes commands)	Malware	8%	36%



Compromised Assets

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

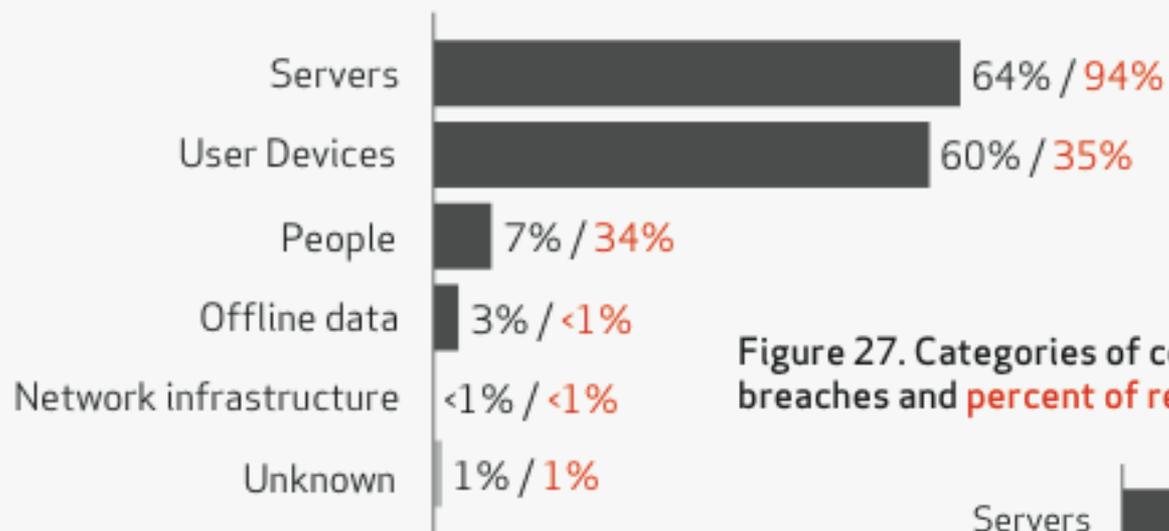


Figure 27. Categories of compromised assets by percent of breaches and **percent of records** - LARGER ORGS

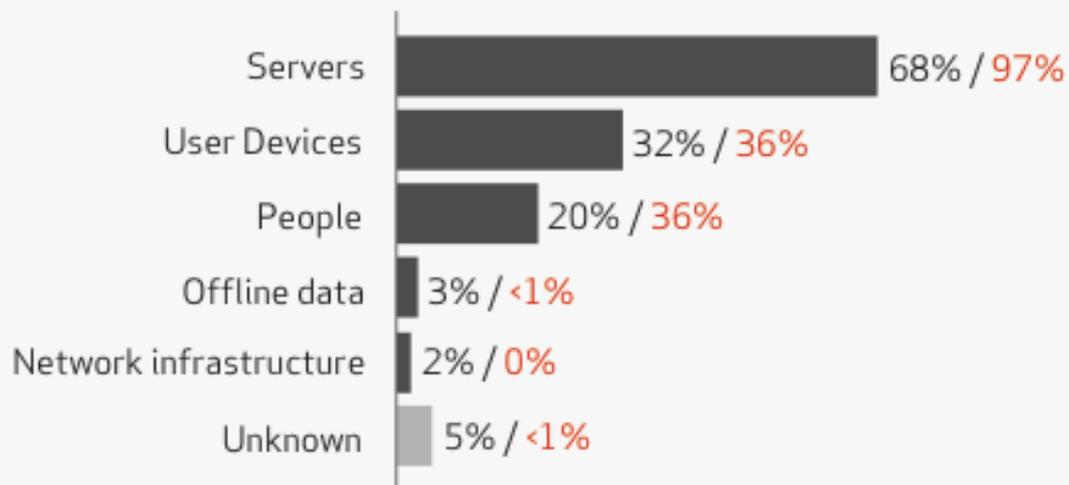


Figure 33. Role of organization size in type of record compromise

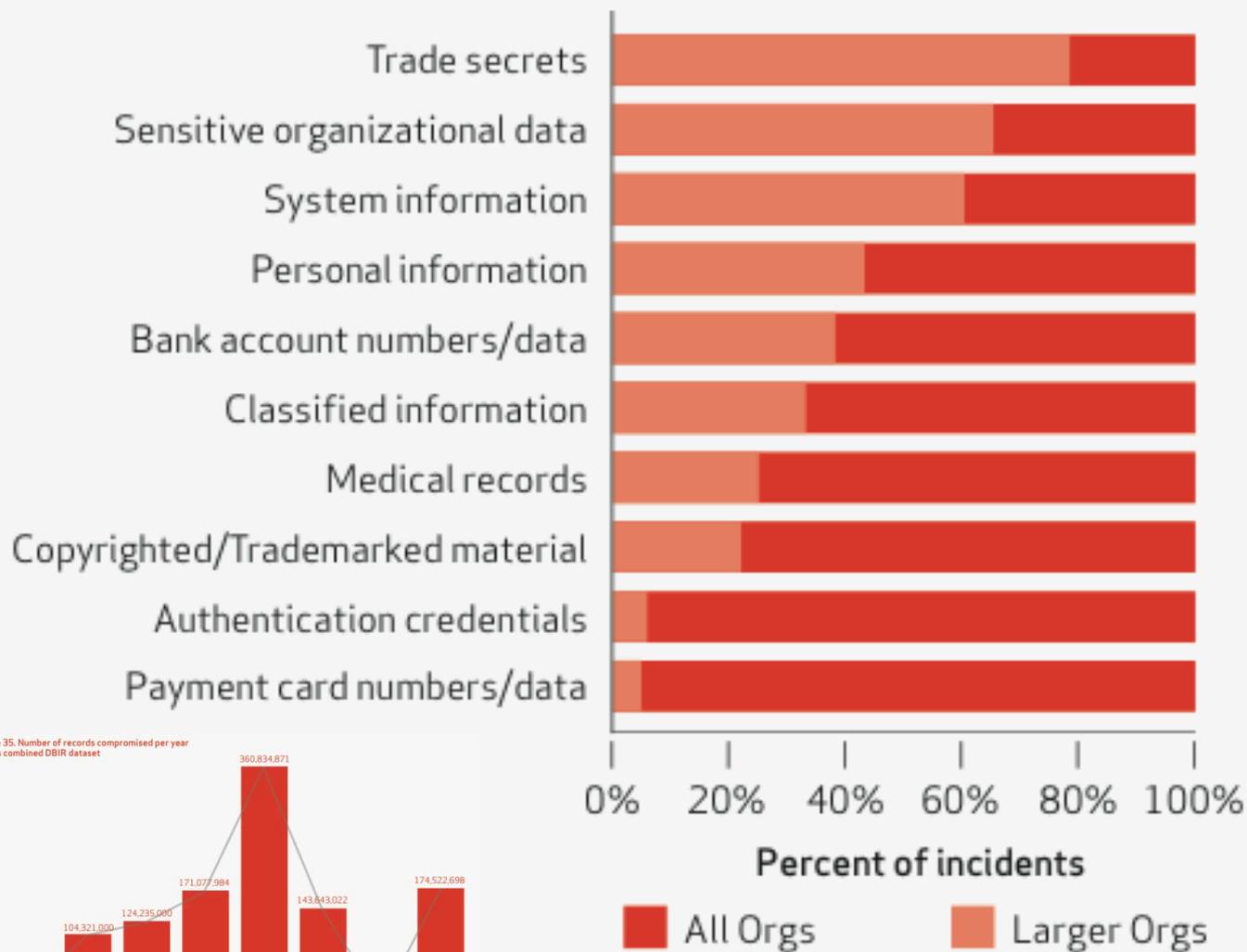
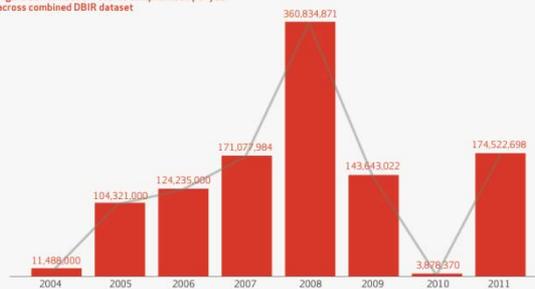


Figure 35. Number of records compromised per year across combined DBIR dataset





Timespan of events

Figure 40. Timespan of events by percent of breaches

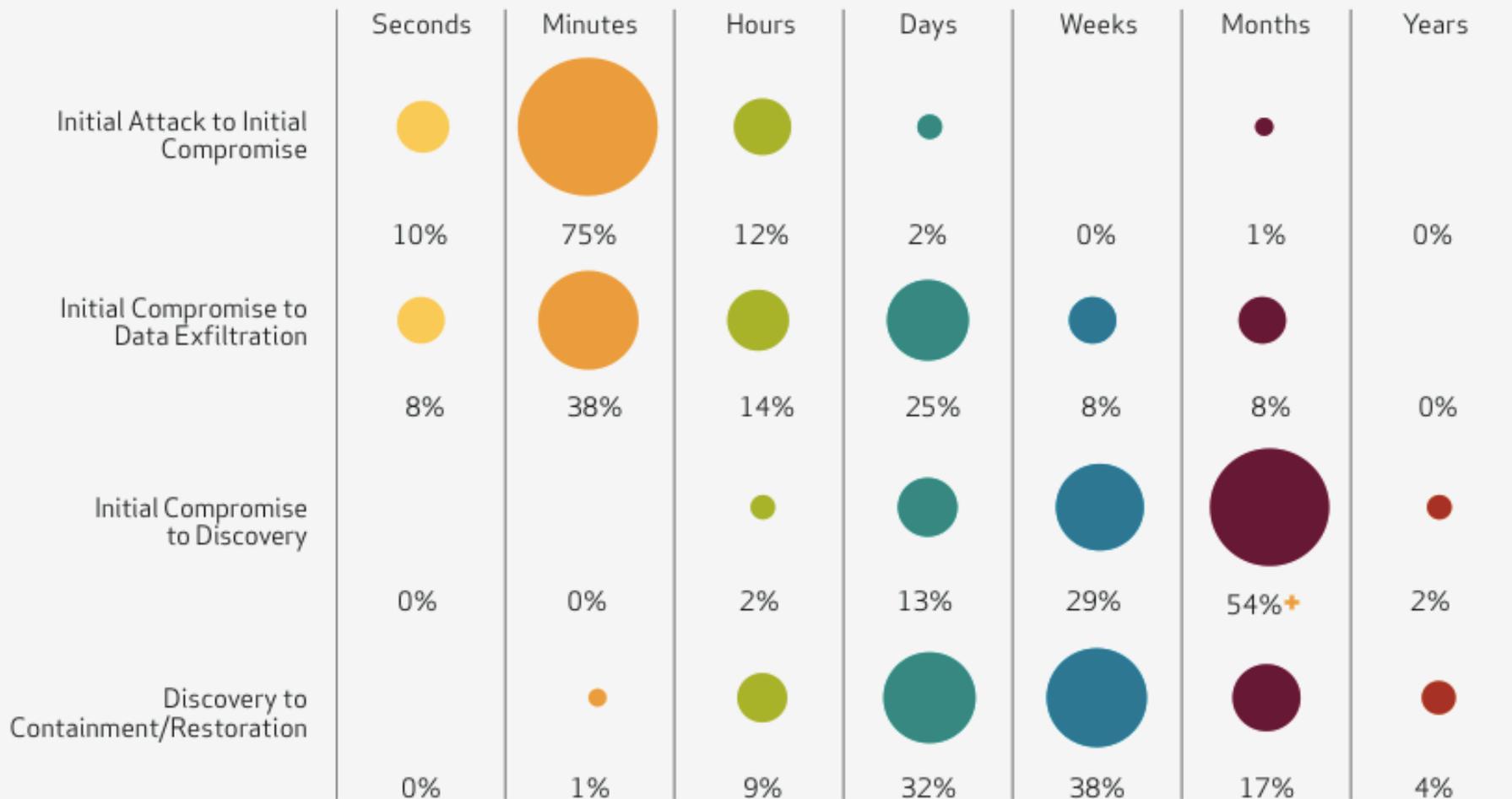
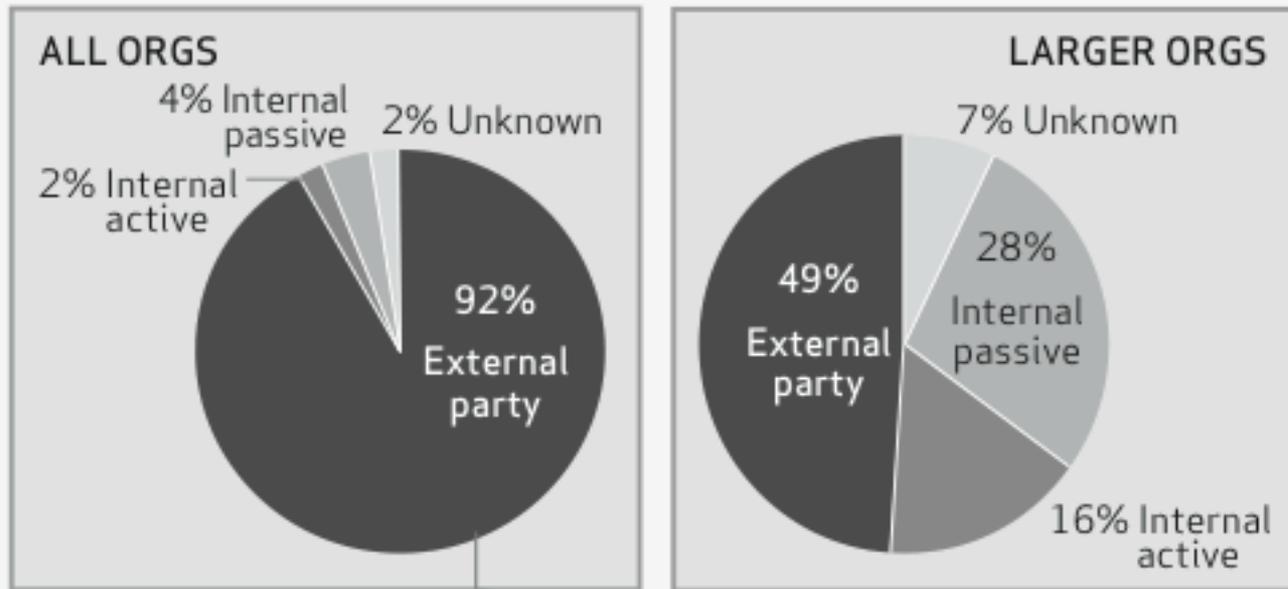


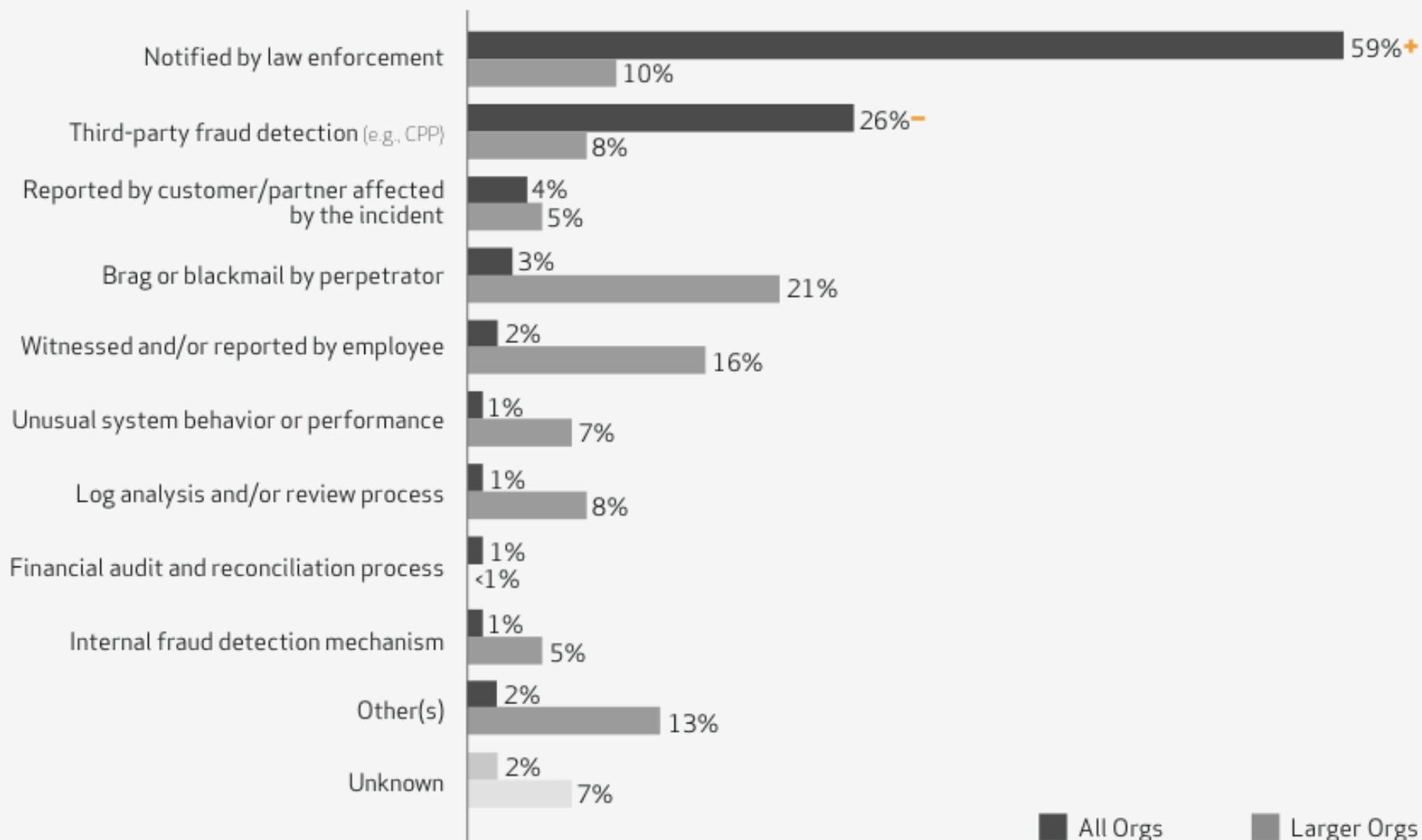
Figure 44. Simplified breach discovery methods by percent of breaches





Breach Discovery

Figure 45. Breach discovery methods by percent of breaches





Collective Intelligence Framework

