

# 2013 Data Breach Investigations Report



Christopher Novak  
Director, Global Investigative Response  
June 4, 2013

PID#

# Data Breach Investigations Report (DBIR) Series

*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.*

Please download the full Data Breach Investigations Report:  
[www.verizonenterprise.com/DBIR/2013](http://www.verizonenterprise.com/DBIR/2013)

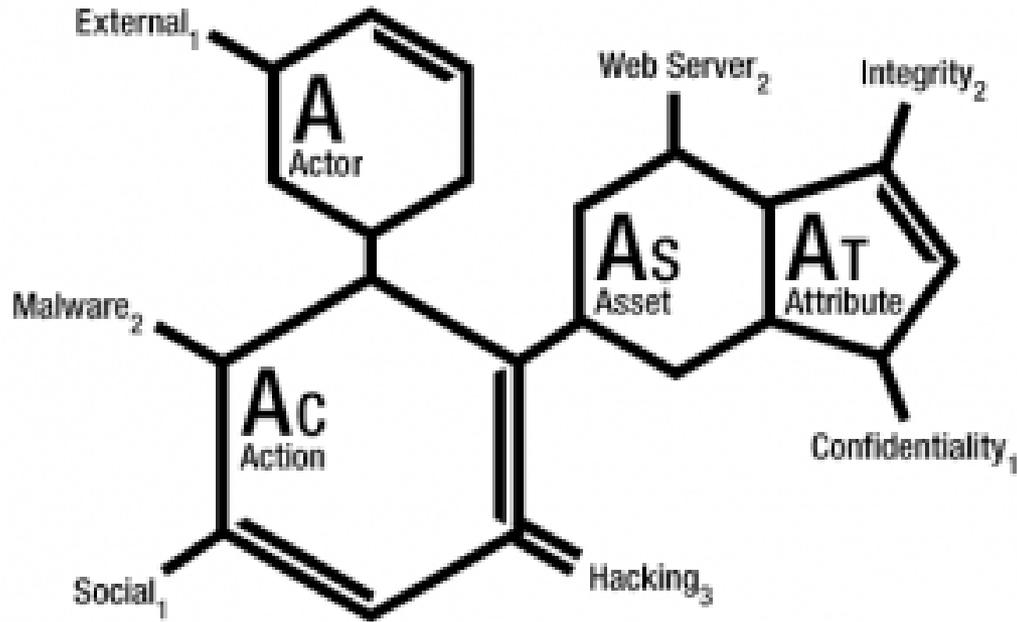
# 2013 Data Breach Investigations Report

19 global contributors  
47,000+ security incidents  
621 confirmed data breaches

A global study conducted by the Verizon RISK Team with cooperation from:



VERIS\* is a (open and free) set of metrics designed to provide a **common language for describing security incidents** (or threats) in a structured and repeatable manner.



**Actor** – Who did it?

**Action** – How'd they do it?

**Asset** – What was affected?

**Attribute** – How was it affected?

\*Vocabulary for Event Recording and Incident Sharing

# Threat Actor

Figure 10: Threat actor categories

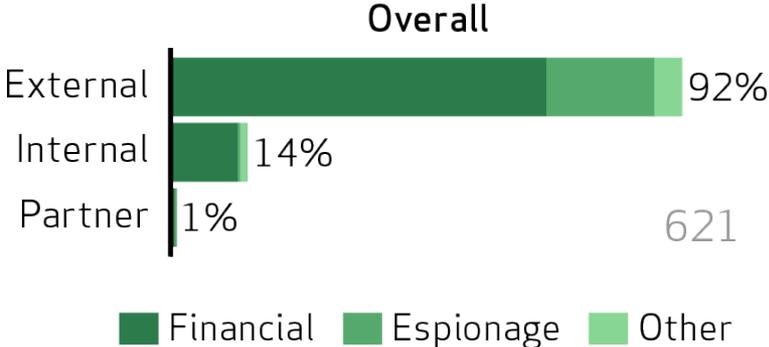
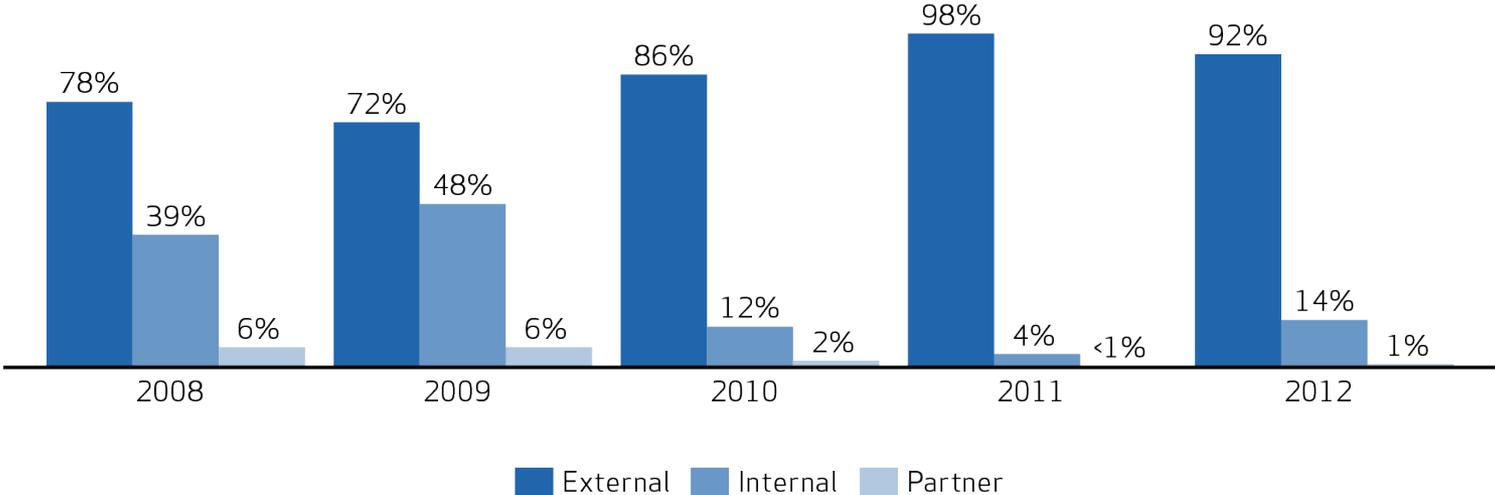
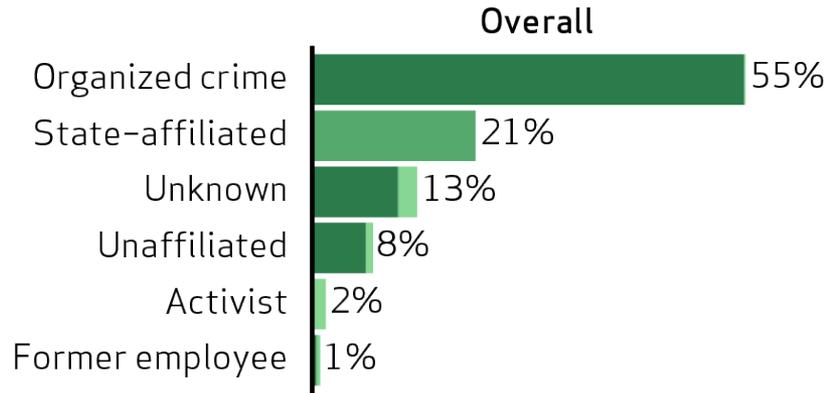


Figure 9: Threat actor categories over time

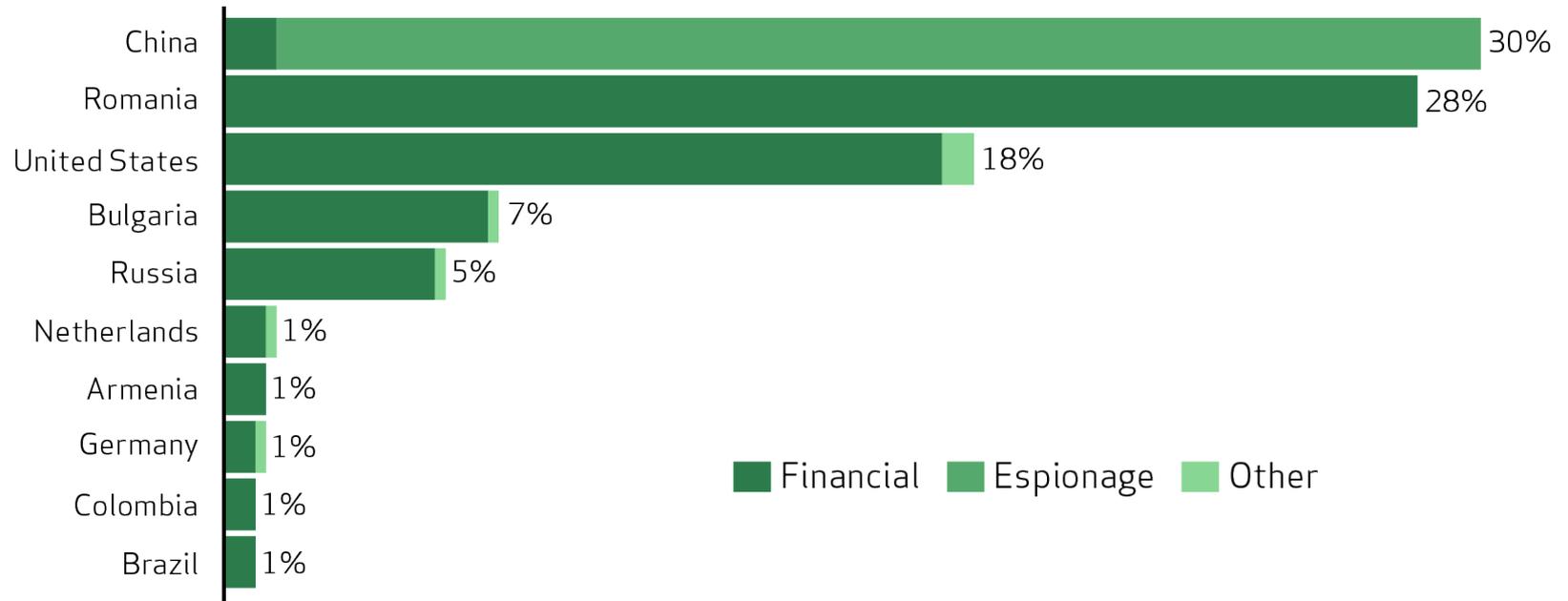


# Threat Actor

## Figure 12: Variety of external actor



## Figure 13: Origin of external actors: Top 10



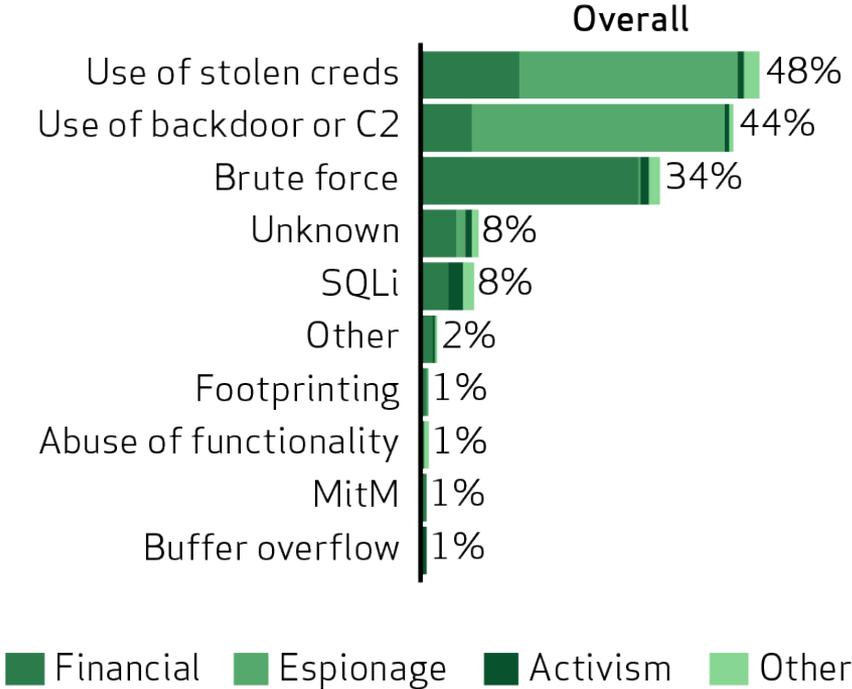
# Breach Count vs. Victim Industry & Size

1 to 100	1		2	10	1	79		5	18		14		3	1	3		3	38	6	2	7	193	
101 to 1,000				13		3	1	8	3		5		1	2	1			13	2	4	1	57	
1,001 to 10,000		1		7	1	3	22	10	12		6		1	2	1			2	1	2		71	
10,001 to 100,000		2		13	1	4		2	93		5				1					1		122	
More than 100,000	1	4		2					31		1					2		1				42	
Unknown				1		7	1	14	73	1	5		1				1	2	2	5	23	136	
<b>Total</b>	<b>2</b>	<b>7</b>	<b>2</b>	<b>46</b>	<b>3</b>	<b>96</b>	<b>24</b>	<b>39</b>	<b>230</b>	<b>1</b>	<b>36</b>		<b>6</b>	<b>5</b>	<b>6</b>	<b>2</b>	<b>4</b>	<b>56</b>	<b>11</b>	<b>14</b>	<b>31</b>	<b>621</b>	
	Agriculture (11)	Mining (21)	Utilities (22)	Construction (23)	Manufacturing (31)	Wholesale Trade (42)	Retail (44)	Transportation (48)	Information (51)	Finance (52)	Real Estate (53)	Professional (54)	Management (55)	Administrative (56)	Educational (61)	Healthcare (62)	Recreation (71)	Accommodation (721)	Food Services (722)	Other Services (81)	Public (92)	Unknown	<b>Total</b>

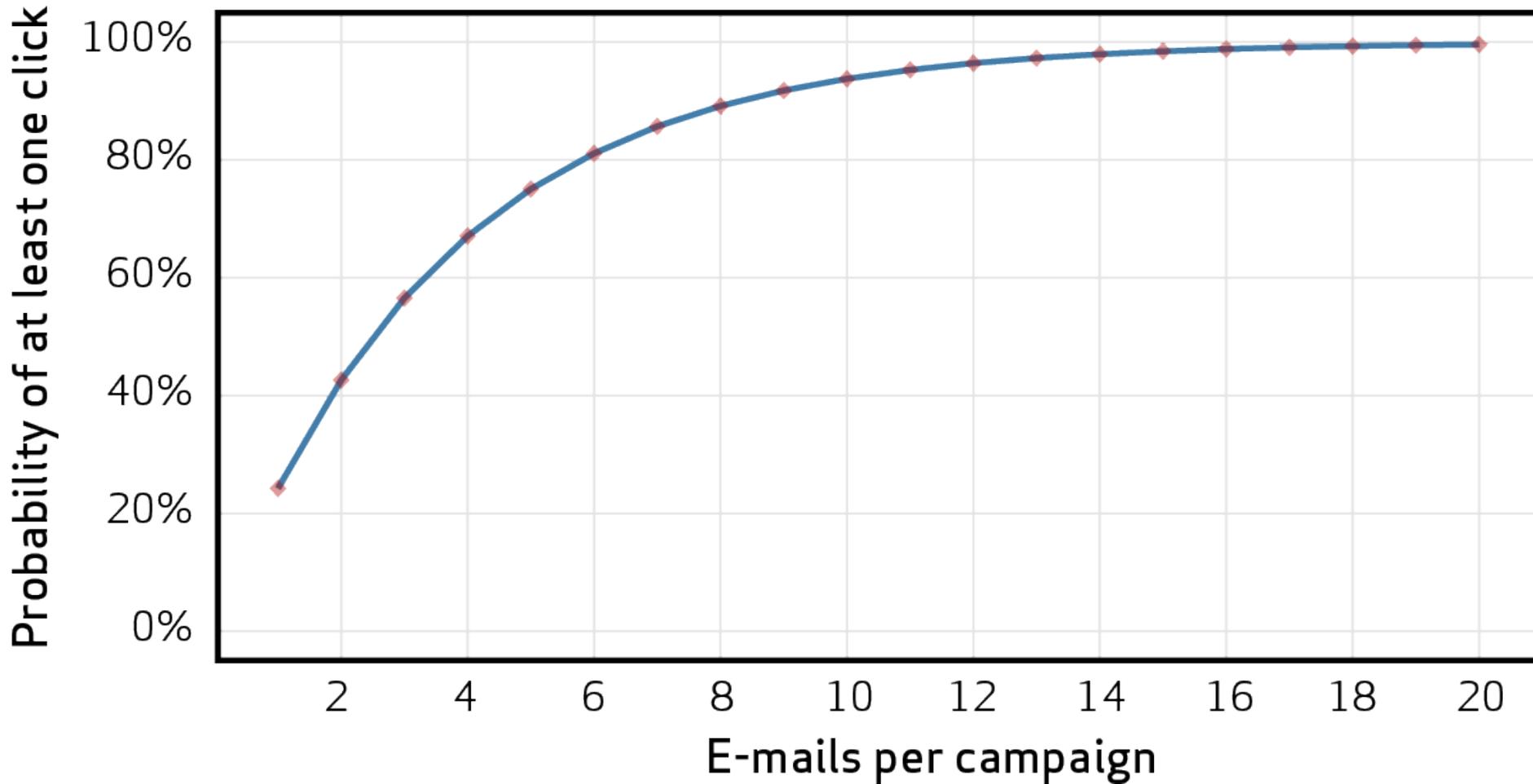
\* Industries based on [NAICS](#)

# Variety of Hacking Actions

Figure 23: Variety of hacking actions



# The Inevitability of “The Click”

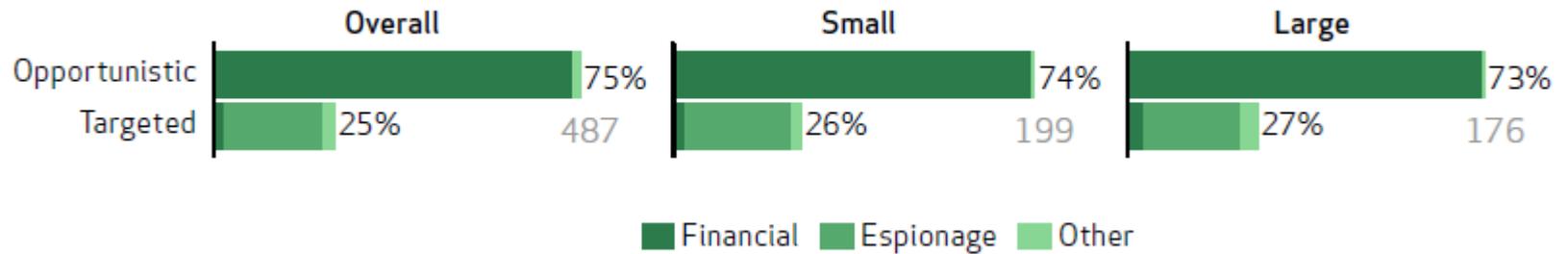


# Breach Count by Data Variety & Motive

Financial	376	37	100	47	1		2	7	10	6	1	13
Espionage	1	1	119	1	1	3	1	113	122	119		21
Activism	2		3	8	1			2	4			
Other	1	1	14	6			1	2	10			8
	Payment	Bank	Credentials	Personal	Medical	Classified	Copyrighted	System	Internal	Secrets	Other	Unknown

# Attack Targeting

Figure 38: Attack targeting



# Attack Difficulty

Figure 39: Difficulty of initial compromise

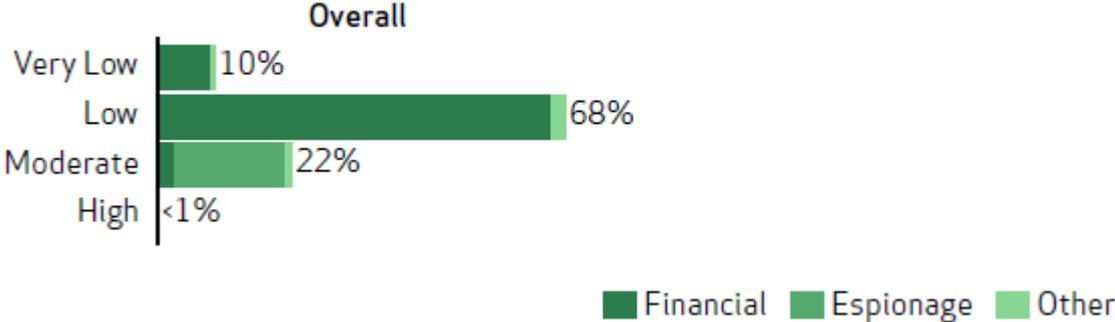
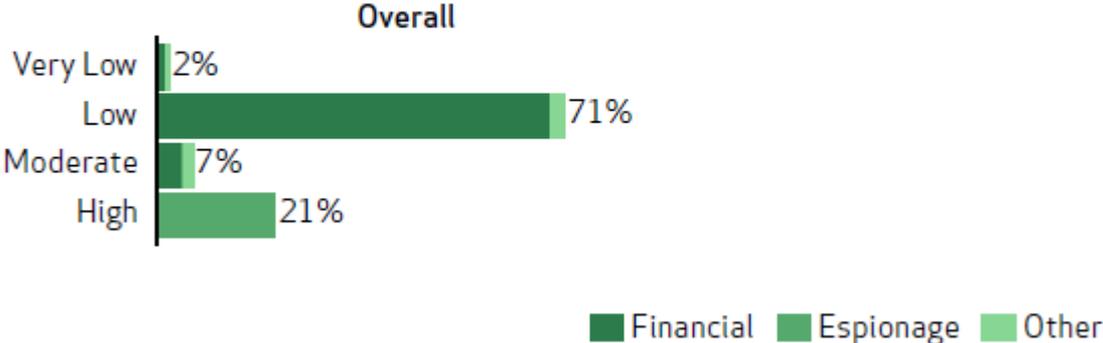
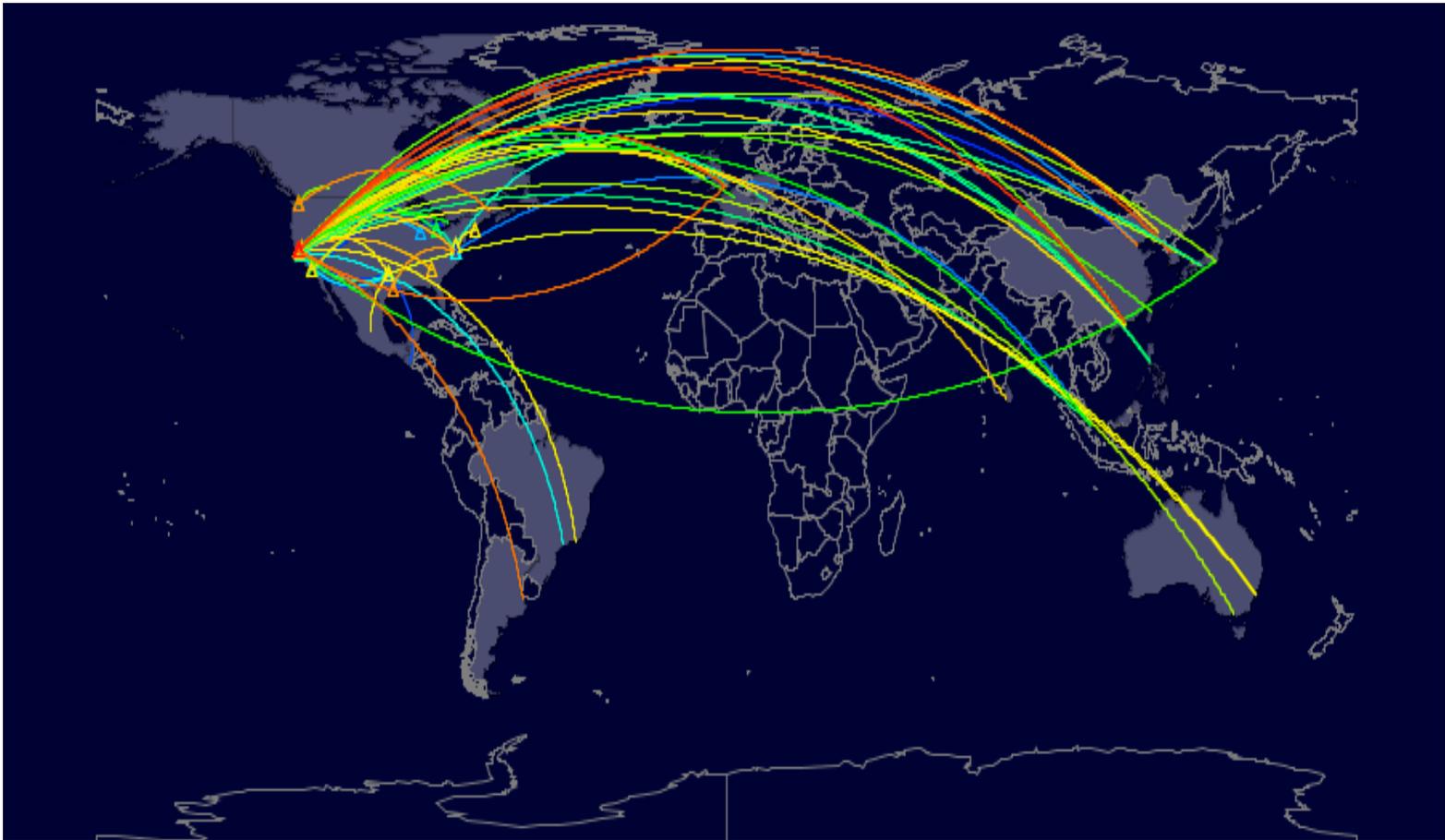


Figure 40: Difficulty of subsequent actions

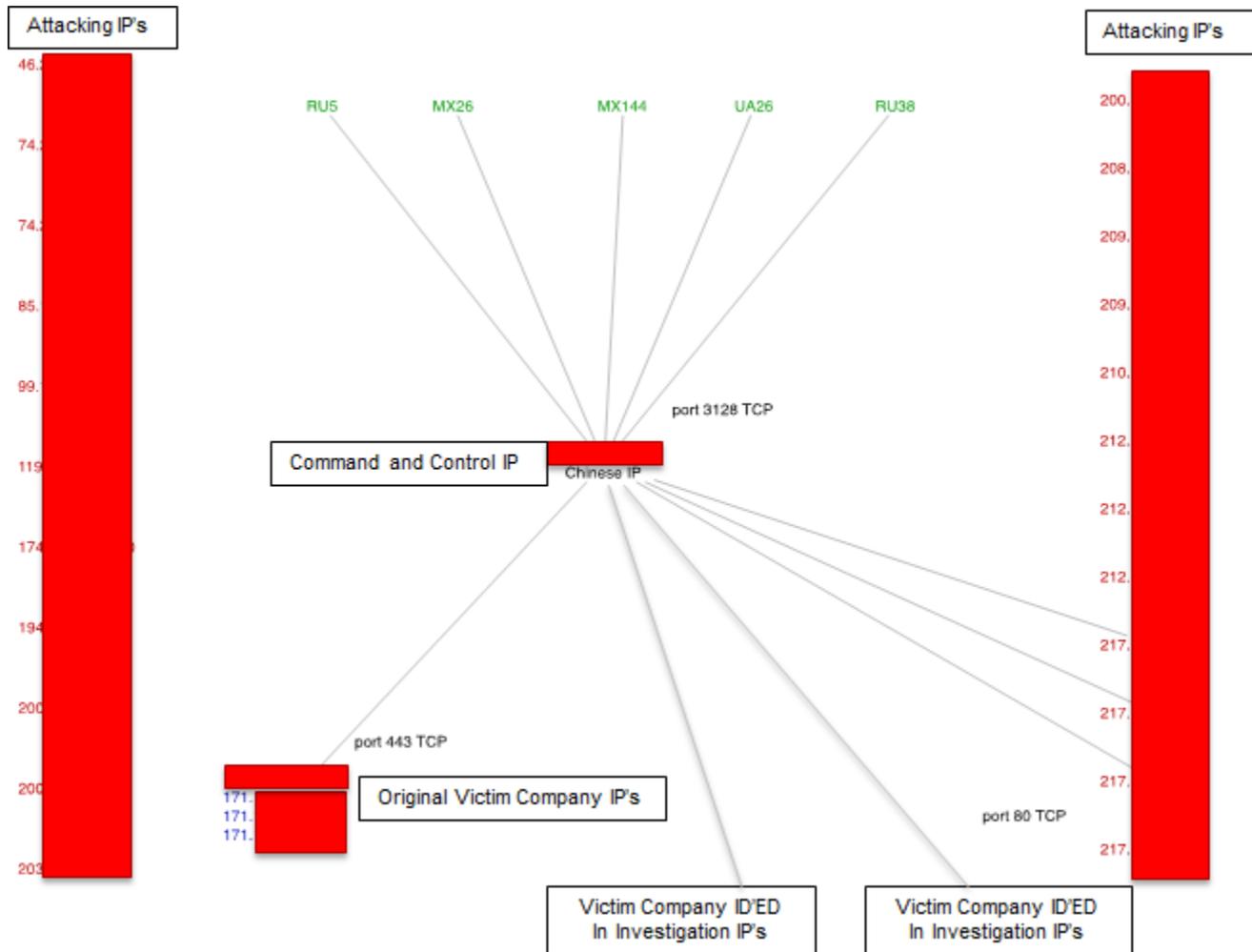


# Case Study – DDoS / Data Exfiltration



UDP Traffic with Victim US Corporation

# Case Study – DDoS / Data Exfiltration

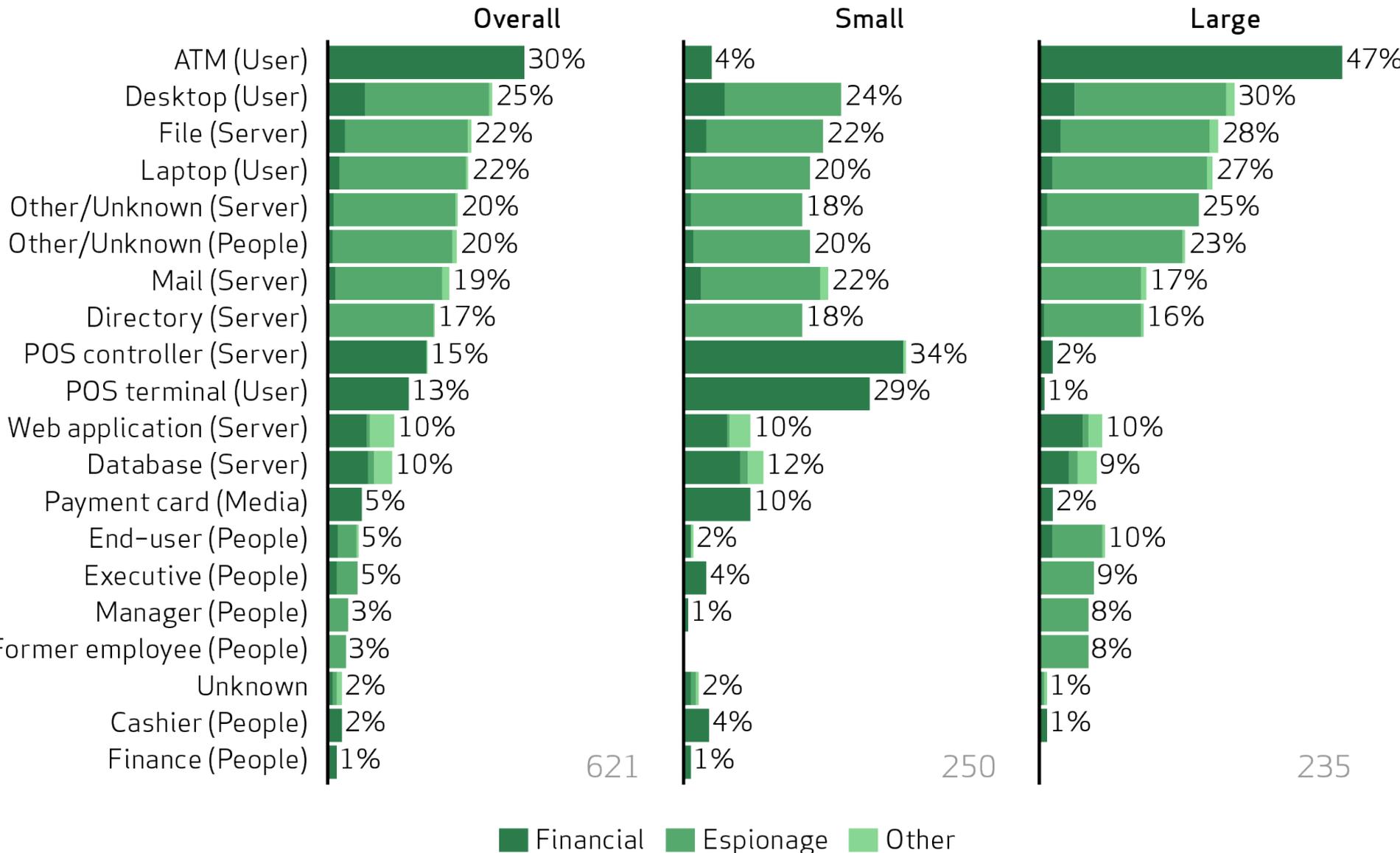


# Case Study – DDoS / Data Exfiltration

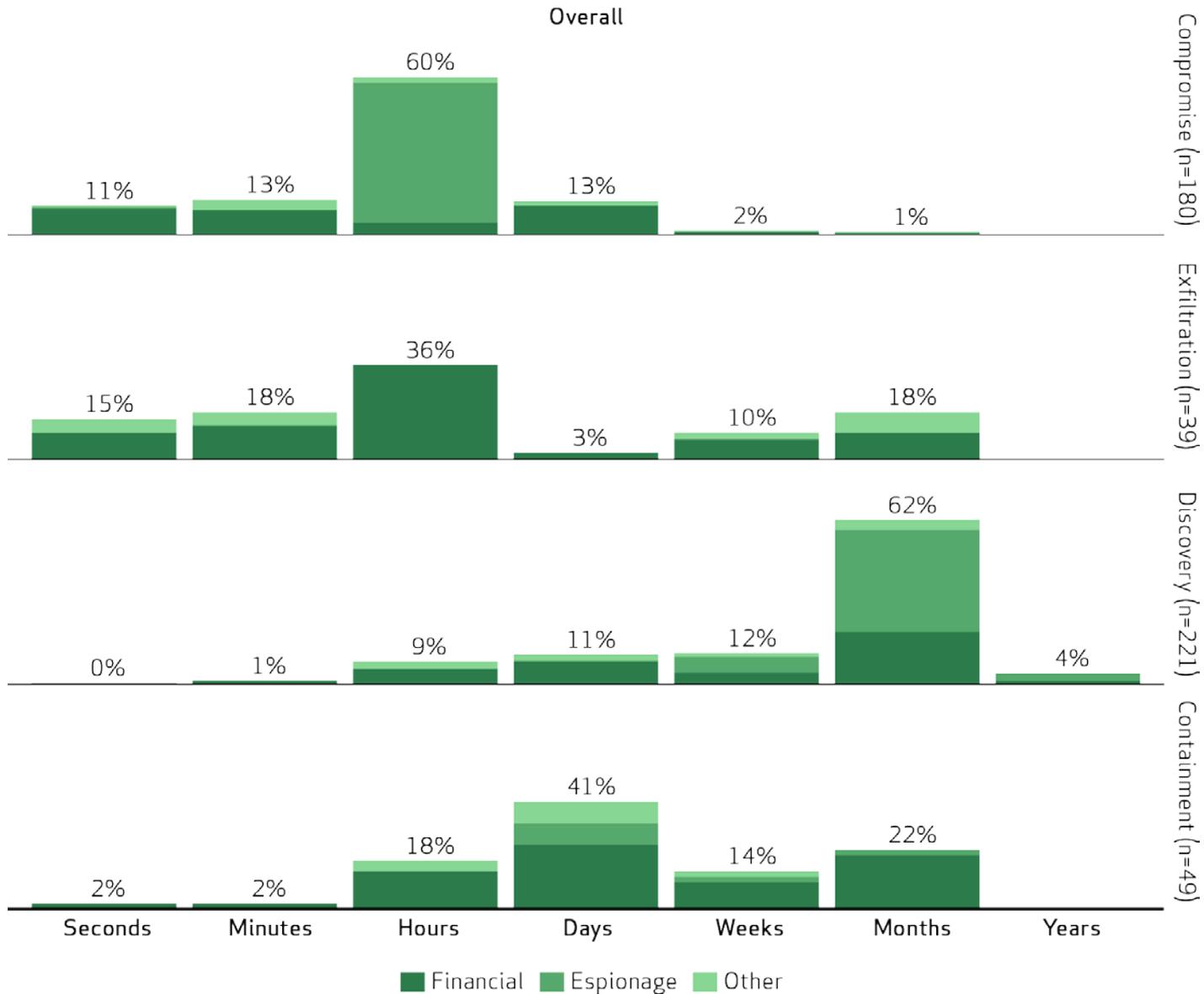


TCP Traffic with Victim US Corporation

# Variety of Compromised Assets

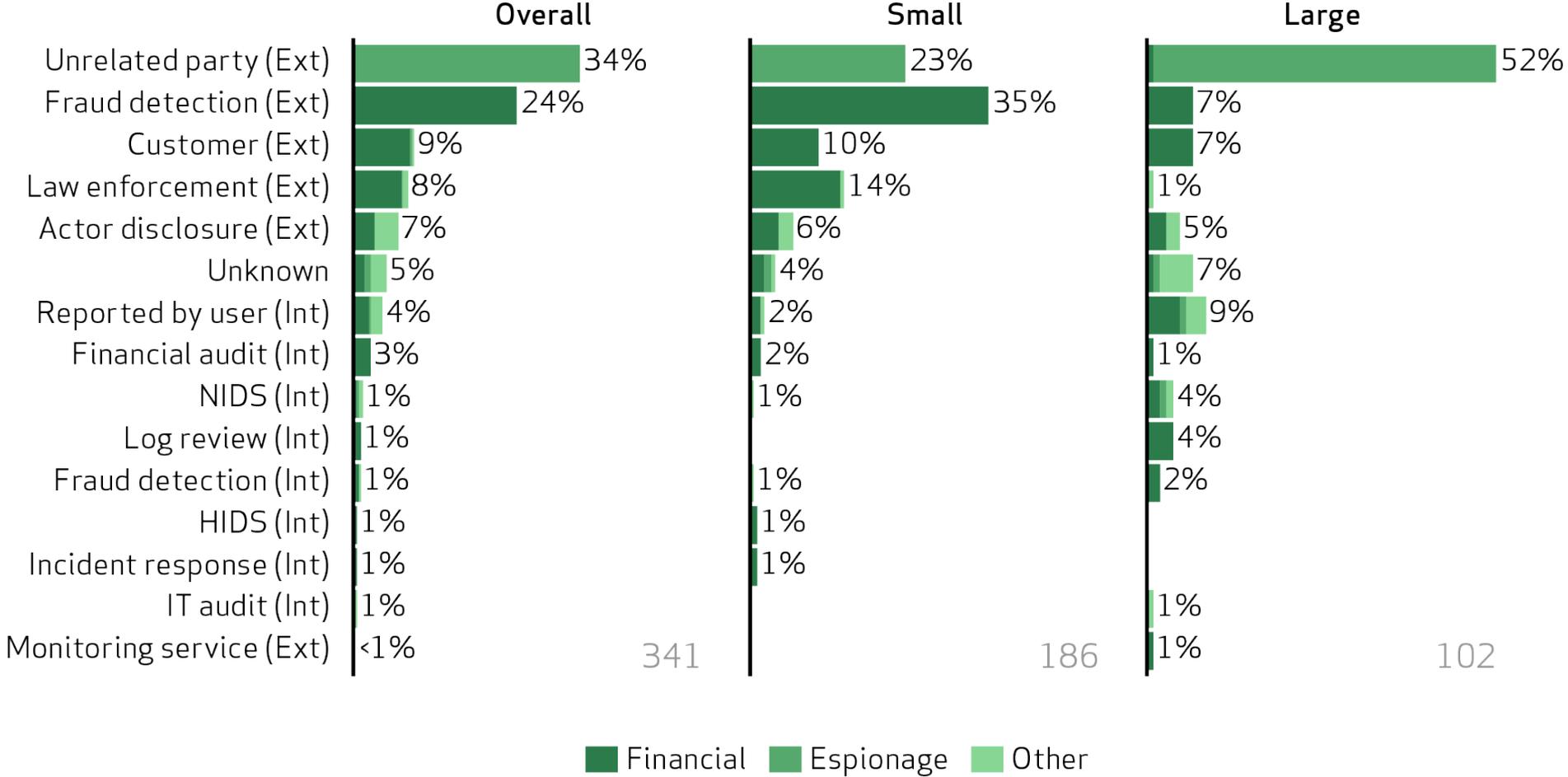


# Timespan of Events



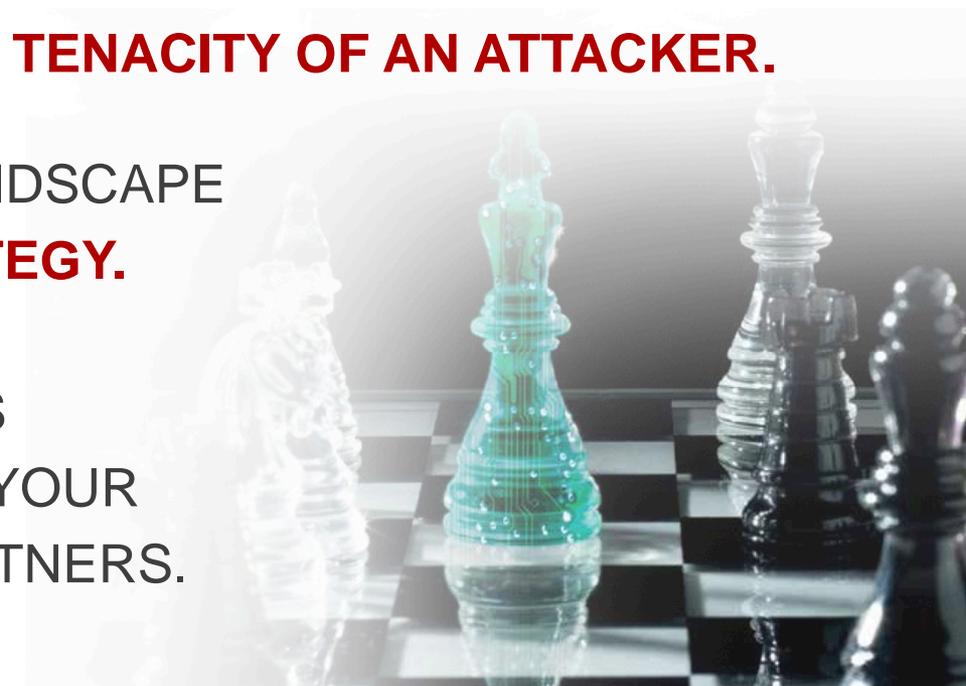
# Discovery Methods

Figure 44: Discovery methods



# Recommendations

- MAKE SECURITY A **COMPANY-WIDE EFFORT**; YOUR PEOPLE CAN BE **YOUR GREATEST ASSET** OR YOUR WEAKEST LINK.
- CREATE BETTER AND FASTER **DETECTION** THROUGH A MIX OF PEOPLE, PROCESSES, AND TECHNOLOGY.
- NEVER UNDERESTIMATE THE **TENACITY OF AN ATTACKER.**
- EVALUATE YOUR THREAT LANDSCAPE TO **PRIORITIZE A CYBER STRATEGY.**
- **DOWNLOAD** AND SHARE THIS KNOWLEDGE WITH PEOPLE IN YOUR ORGANIZATION AND YOUR PARTNERS.



# Recommendations

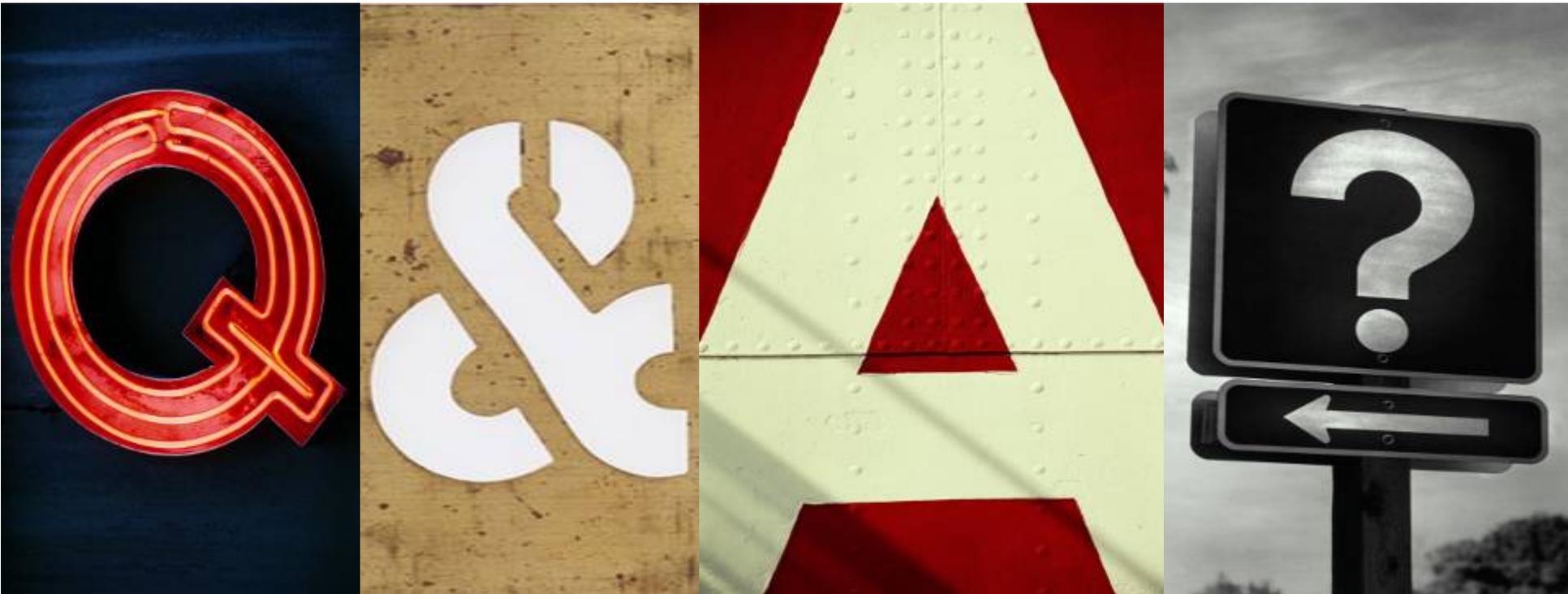
Figure 46: CCA’s Critical Security Controls mapped to common VERIS threat actions

		20 Critical Security Controls																				
		<a href="#">1</a>	<a href="#">2</a>	<a href="#">3</a>	<a href="#">4</a>	<a href="#">5</a>	<a href="#">6</a>	<a href="#">7</a>	<a href="#">8</a>	<a href="#">9</a>	<a href="#">10</a>	<a href="#">11</a>	<a href="#">12</a>	<a href="#">13</a>	<a href="#">14</a>	<a href="#">15</a>	<a href="#">16</a>	<a href="#">17</a>	<a href="#">18</a>	<a href="#">19</a>	<a href="#">20</a>	
Top VERIS Threat Actions	Tampering	•		•				•		•												
	Spyware		•	•	•	•							•									
	Backdoor**		•	•	•	•	•				•	•	•	•								
	Export data		•	•	•	•					•		•	•					•		•	
	Use of stolen creds							•		•	•		•									
	Capture stored data		•	•	•	•							•				•		•		•	
	Phishing		•	•	•	•				•				•	•							•
	C2		•	•	•	•	•					•	•	•	•							
	Downloader		•	•	•	•								•	•							
	Brute force				•		•	•			•	•		•	•	•	•	•				

\*\* BKDOOR includes the Malware threat actions of backdoor and command and control, along with the Hacking action that represents the use of backdoor and command and control channels.

# Questions & Answers

Please download the full Data Breach Investigations Report:  
[www.verizonenterprise.com/DBIR/2013](http://www.verizonenterprise.com/DBIR/2013)



*Christopher Novak*  
*Director, Global Investigative Response*  
+1-914-574-2805  
[chris.novak@verizon.com](mailto:chris.novak@verizon.com)