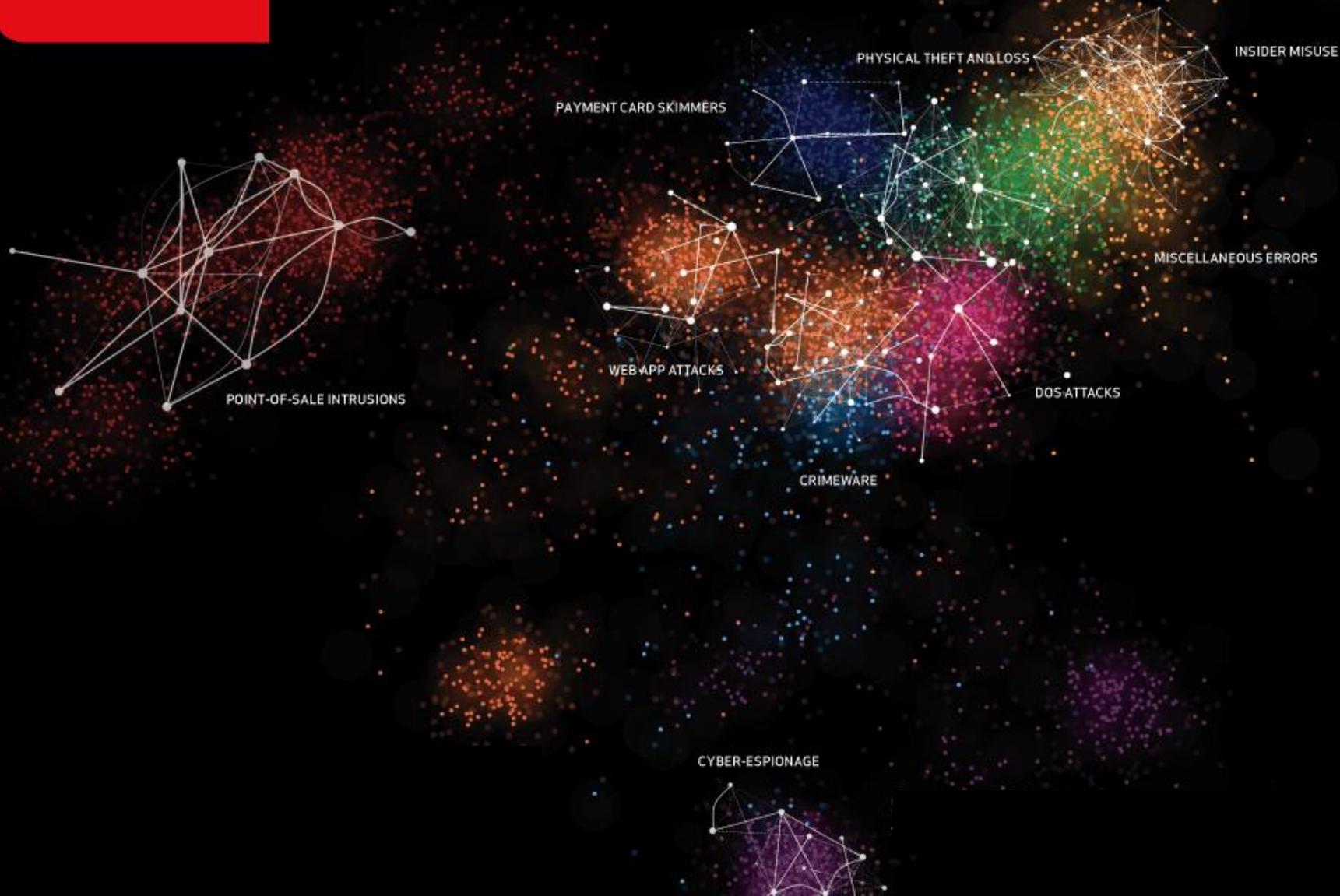




2014 DATA BREACH INVESTIGATIONS REPORT





Incidents that 50 global contributors investigated form the basis of the research

Mishcon de Reya



Deloitte.



Homeland Security



AFP AUSTRALIAN FEDERAL POLICE



CENTER FOR INTERNET SECURITY



PT-ISAC

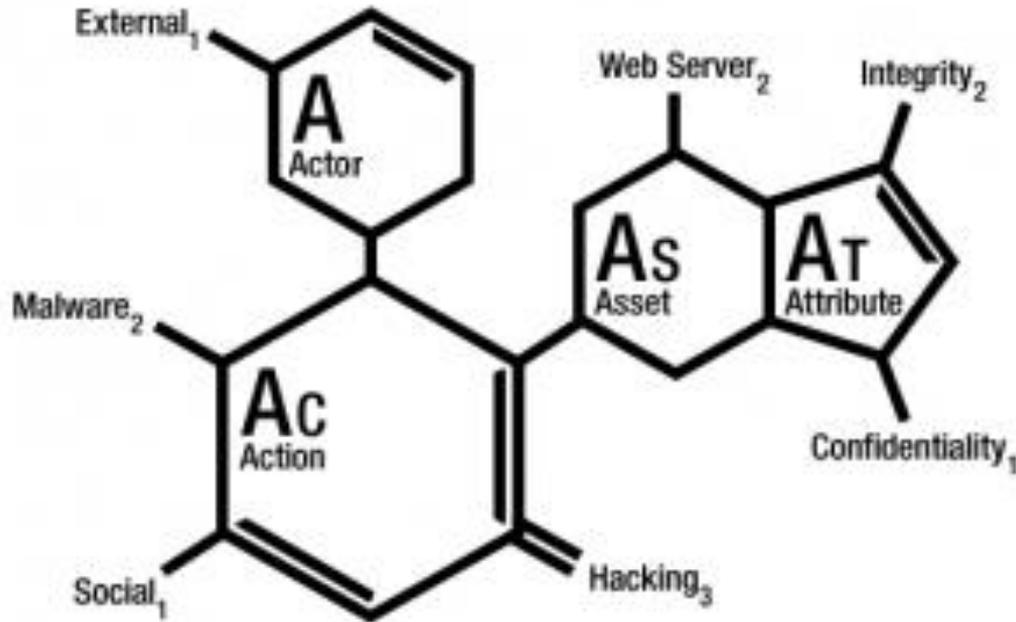


US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM





The DBIR uses the VERIS framework for data collection and analysis



Actor – Who did it?

Action – How'd they do it?

Asset – What was affected?

Attribute – How was it affected?

Documentation, classification examples, enumerations: <http://veriscommunity.net/>

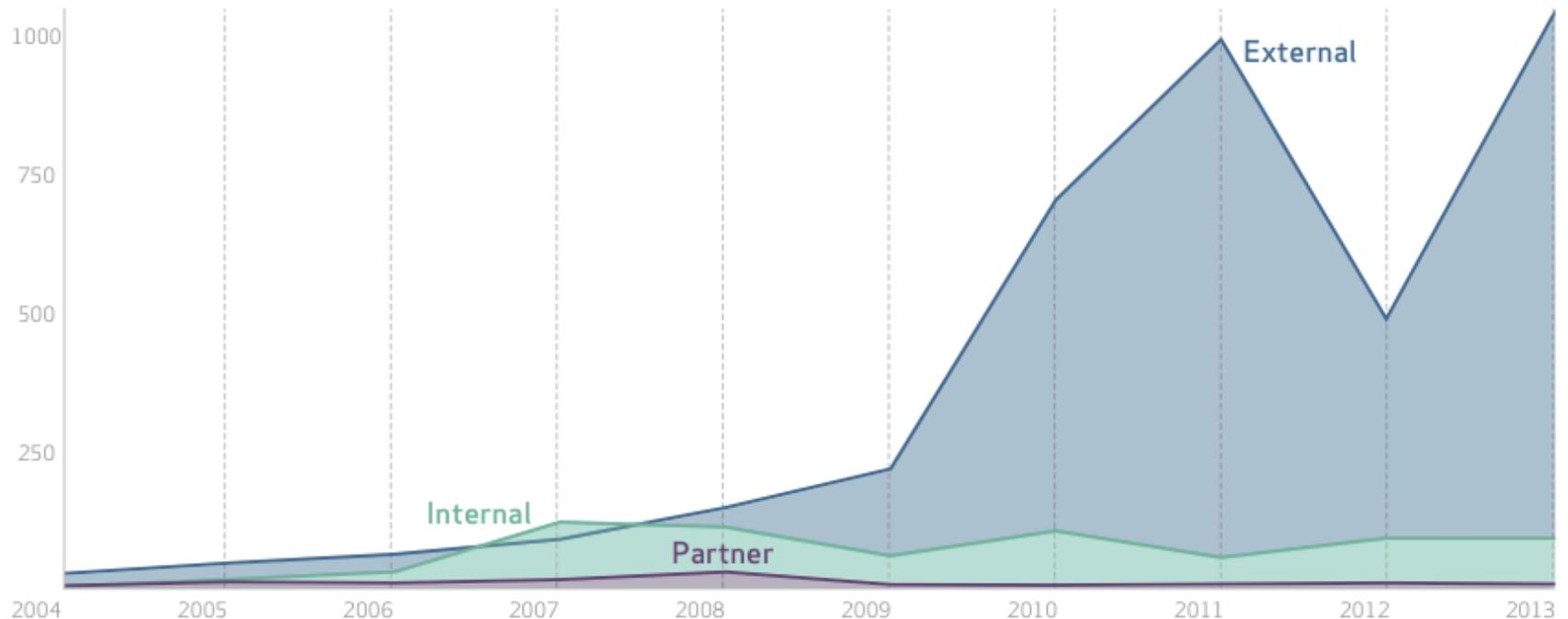


A decade of data breaches



Internal and partner threat actors are fairly consistent; external ones are increasing

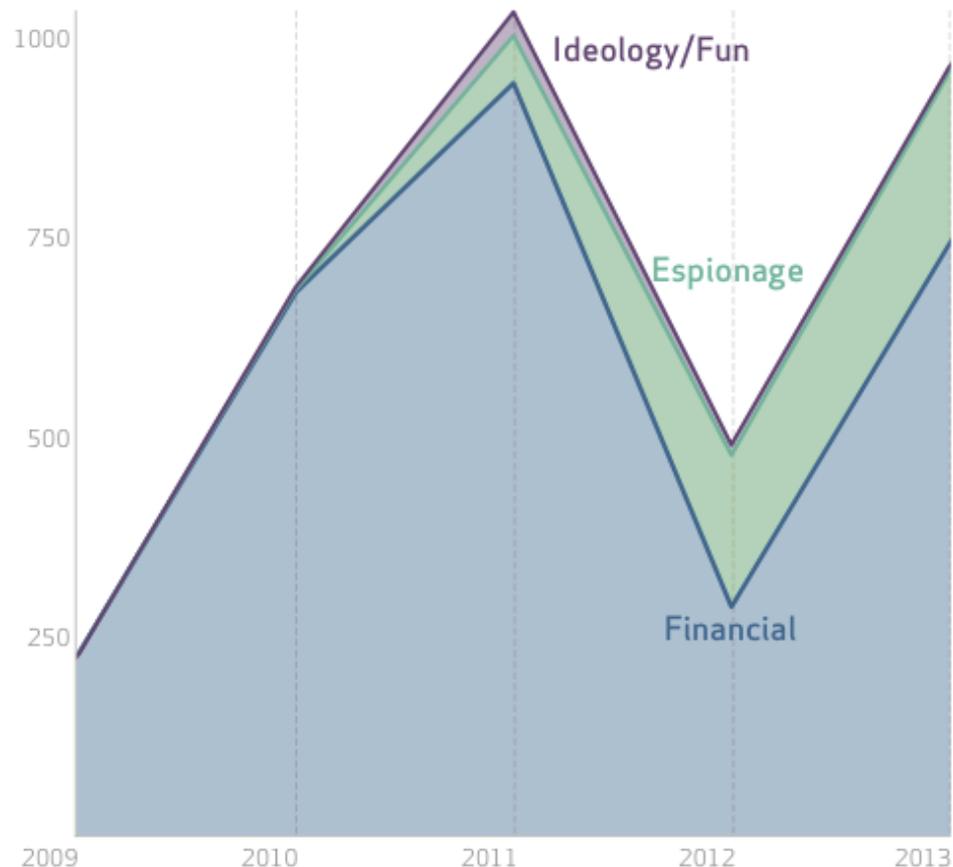
Figure 4.
Number of breaches per threat actor category over time





Espionage-motivated incidents increase; possibly due to increased visibility

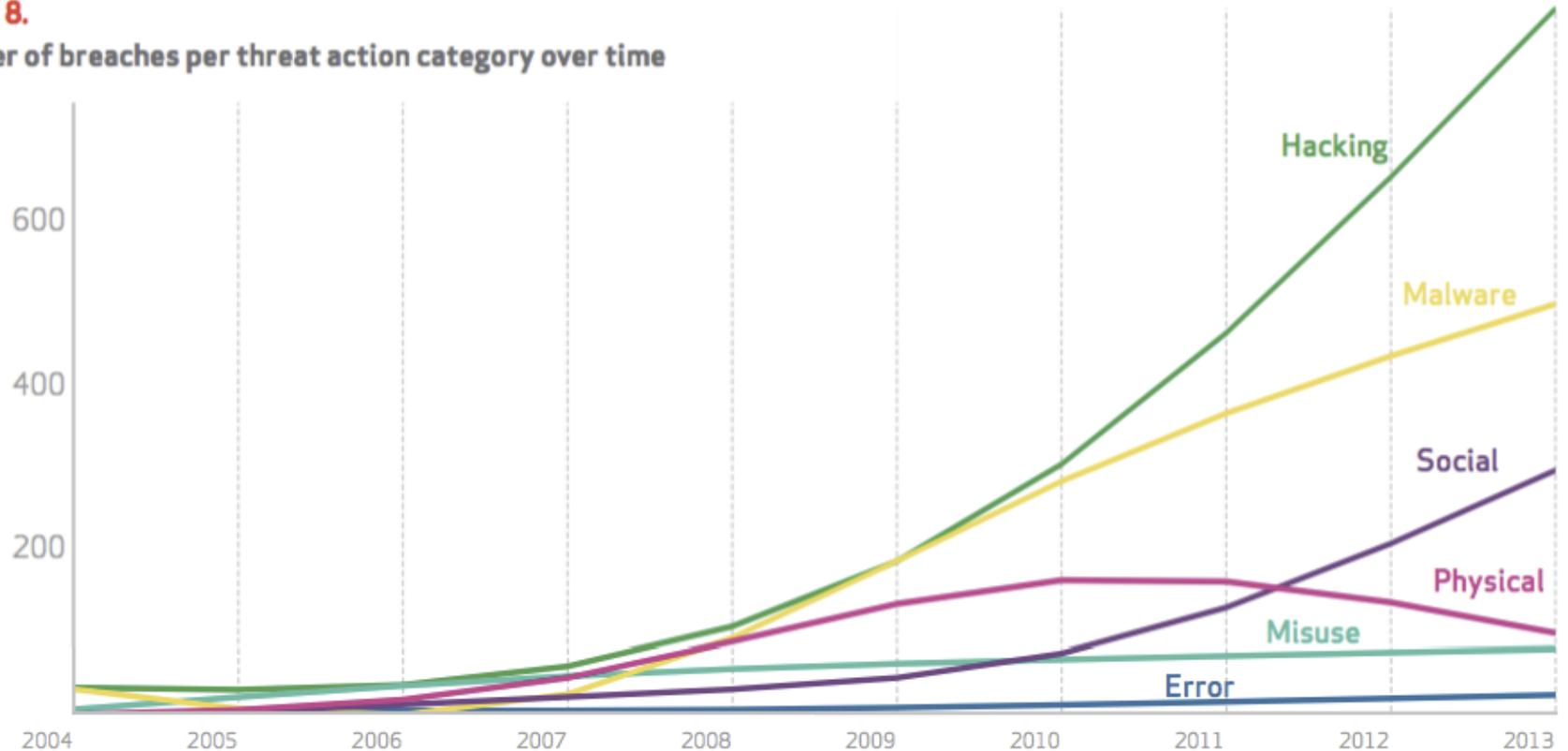
Figure 7.
Number of breaches per threat actor motive over time





Increased threat diversity reflects both better sharing and real trends

Figure 8.
Number of breaches per threat action category over time

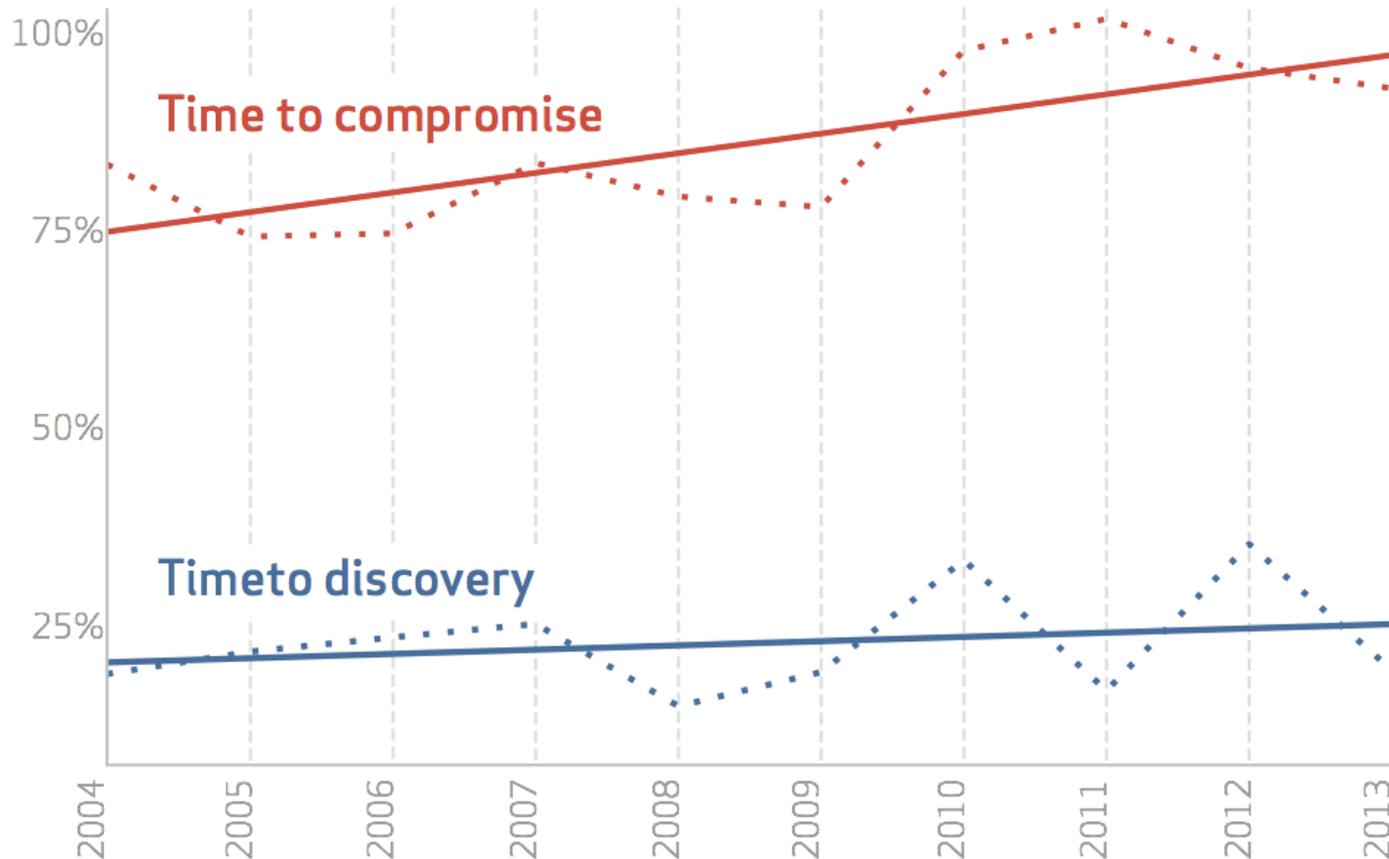




Attackers are faster than defenders, and the gap is widening

Figure 13.

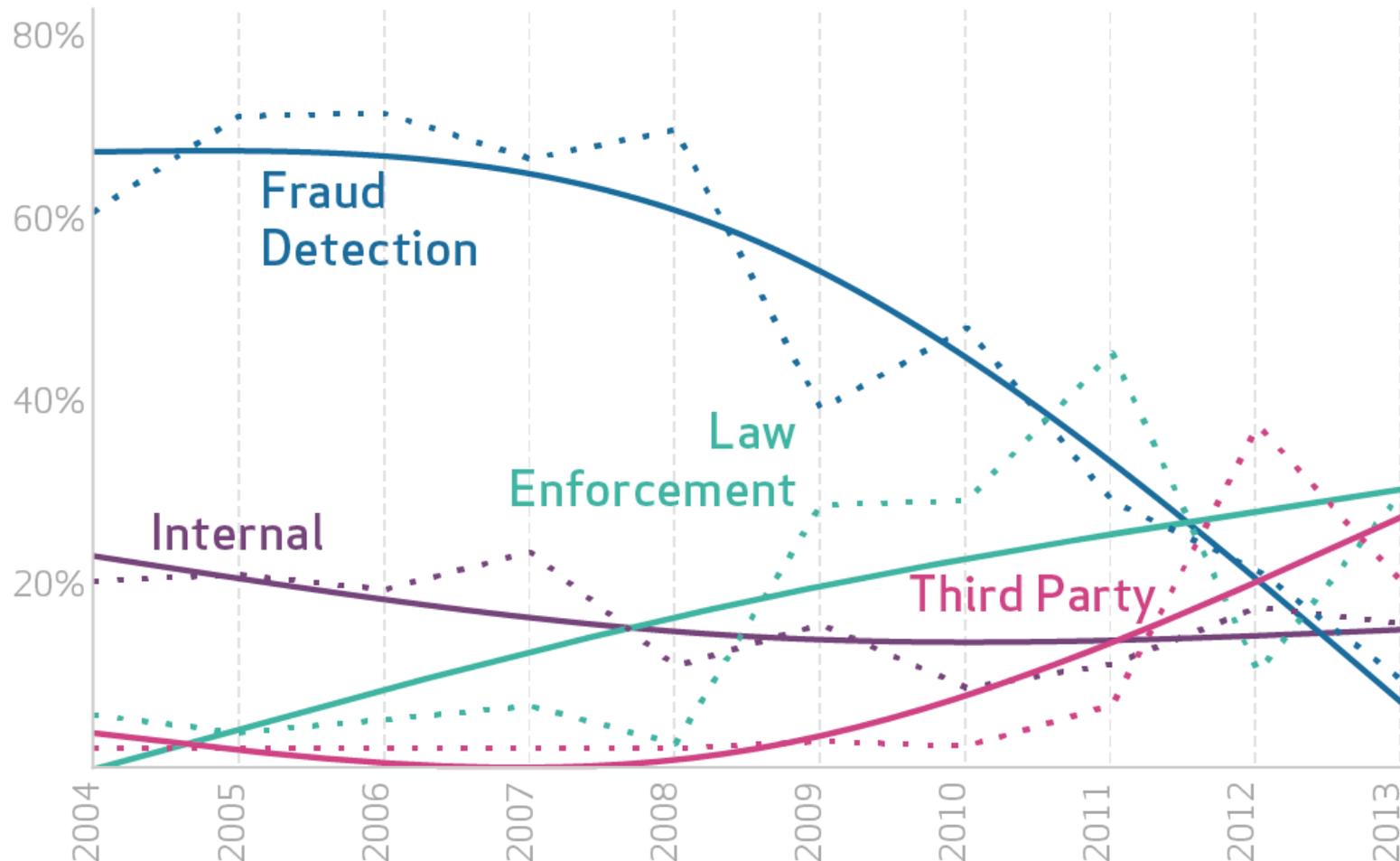
Percent of breaches where time to compromise (red)/time to discovery (blue) was days or less





Law enforcement and third parties detect breaches more often; internal is still poor

Figure 14.
Breach discovery methods over time



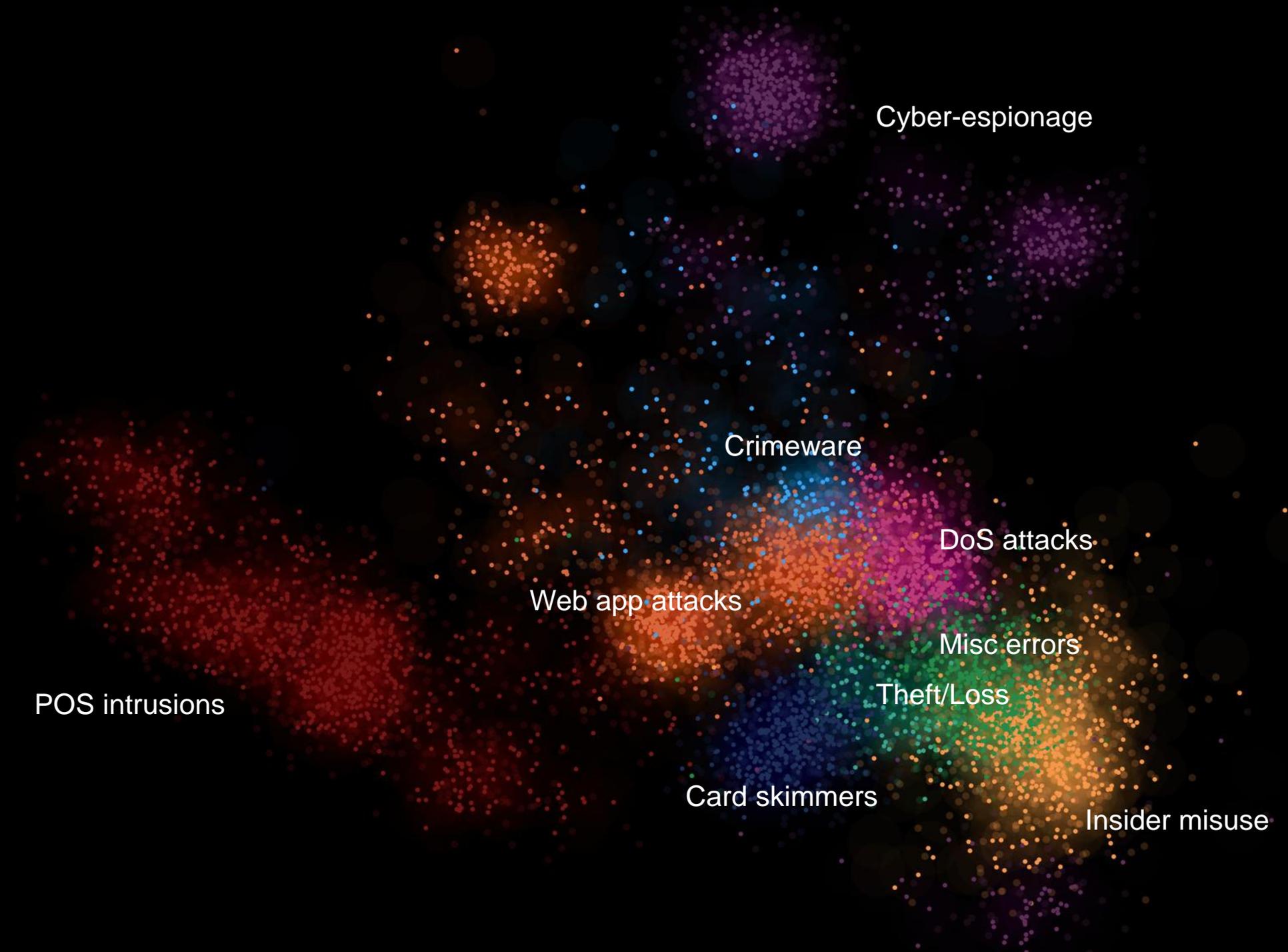


2014: specific patterns for specific recommendations



Last year, we noticed most breaches fit into patterns

111	<i>POS smash-and-grab</i>
190	<i>Physical ATM</i>
+ 120	<i>Assured Penetration Technique</i>
421	
+ 621	<i>Total Breaches</i>
68%	



POS intrusions

Web app attacks

Card skimmers

Crimeware

Cyber-espionage

DoS attacks

Misc errors

Theft/Loss

Insider misuse



The frequency of patterns in an industry supports specific recommendations

Figure 19.
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUSION	WEB APP ATTACK	INSIDER MISUSE	THEFT/LOSS	MISC. ERROR	CRIMEWARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPIONAGE	EVERYTHING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%



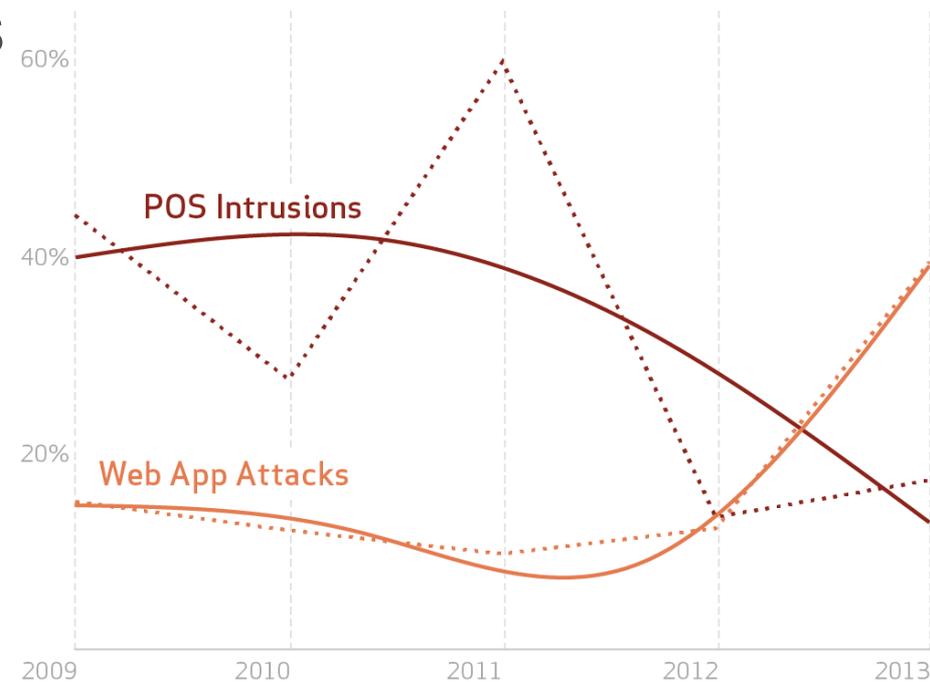
Point of Sale (POS) Intrusions



Point of Sale Intrusion Key Findings

- Overall frequency is actually declining
- Brute forcing remote access to POS still primary intrusion vector
- Increased frequency of RAM scraping malware (versus key logging)
- Recommendations:
 - Restrict remote access, mixed use
 - Enforce password policies
 - Deploy AV
 - Network segmentation
 - Network monitoring
 - 2-factor authentication

Figure 20.
Comparison of POS Intrusions and Web App Attacks
incident classification patterns, 2011-2013





Web App Attacks



Web App Attacks Key Findings

- Common motivations are ideology/fun and financial
- Discovery is typically external and slow
- Most attacks exploit weak input validation or use stolen credentials
- Compromising content management systems for DDoS use was common
- Recommendations:
 - 2-factor authentication
 - Rethink CMS
 - Validate inputs
 - Enforce lockout policies
 - Monitor outbound connections

Figure 26.

External actor motives within Web App Attacks (n=1,126)

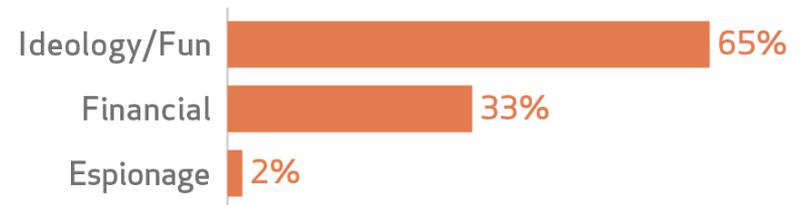
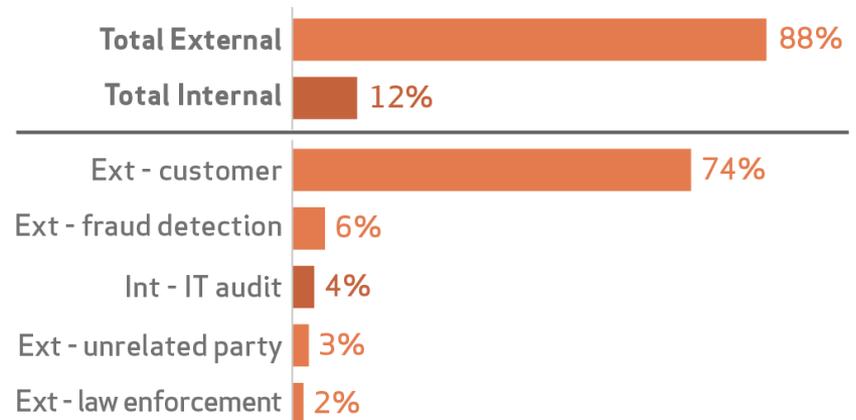


Figure 27.

Top 10 discovery methods for financially motivated incidents within Web App Attacks (n=122)





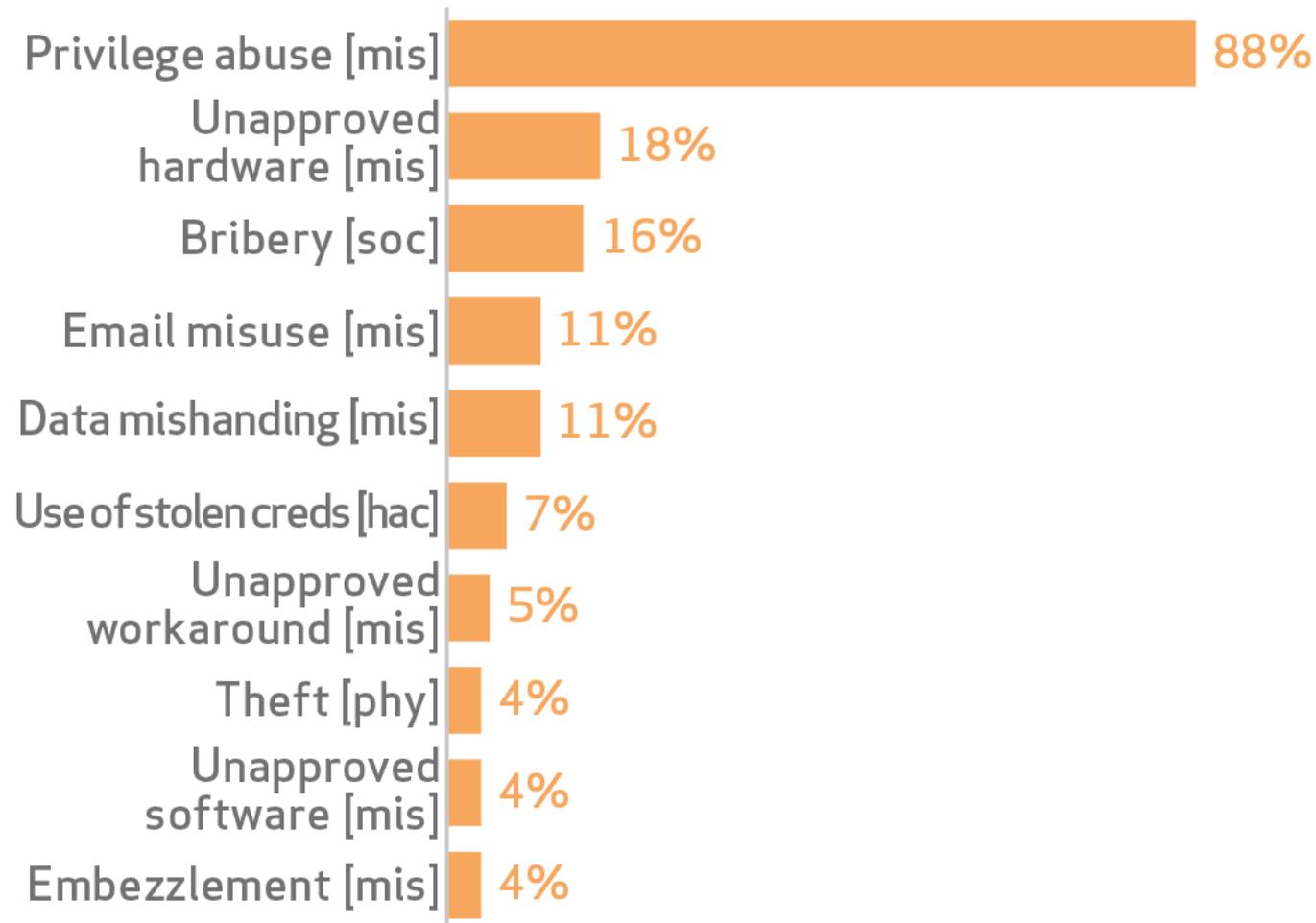
Insider and privilege misuse



Most insider misuse activity abuses trust necessary to perform normal duties

Figure 30.

Top 10 threat action varieties within Insider Misuse (n=153)

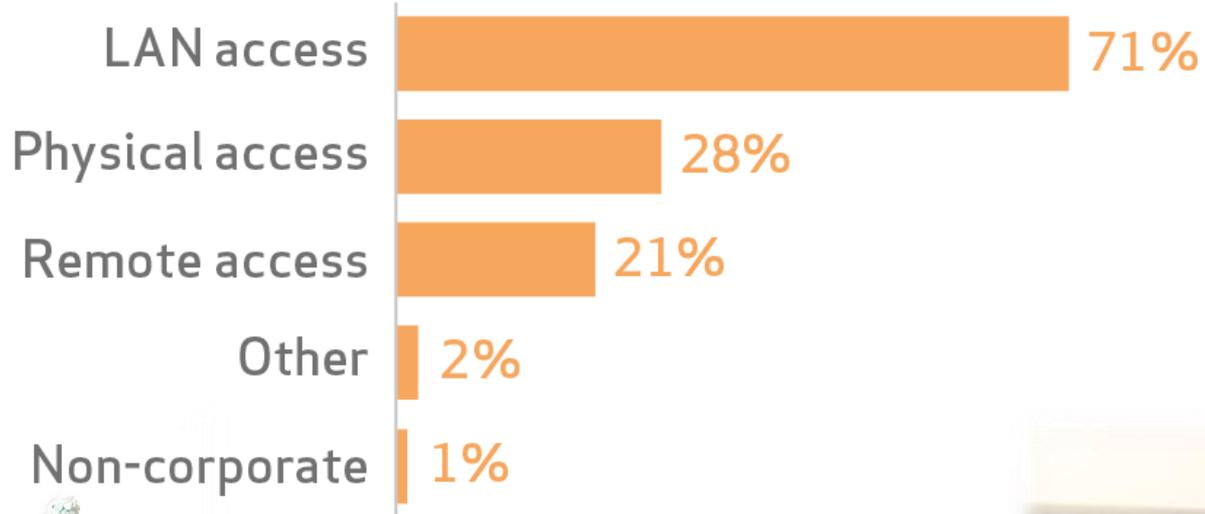




Most incidents happen at the victim organization

Figure 31.

Vector for threat actions within Insider Misuse (n=123)

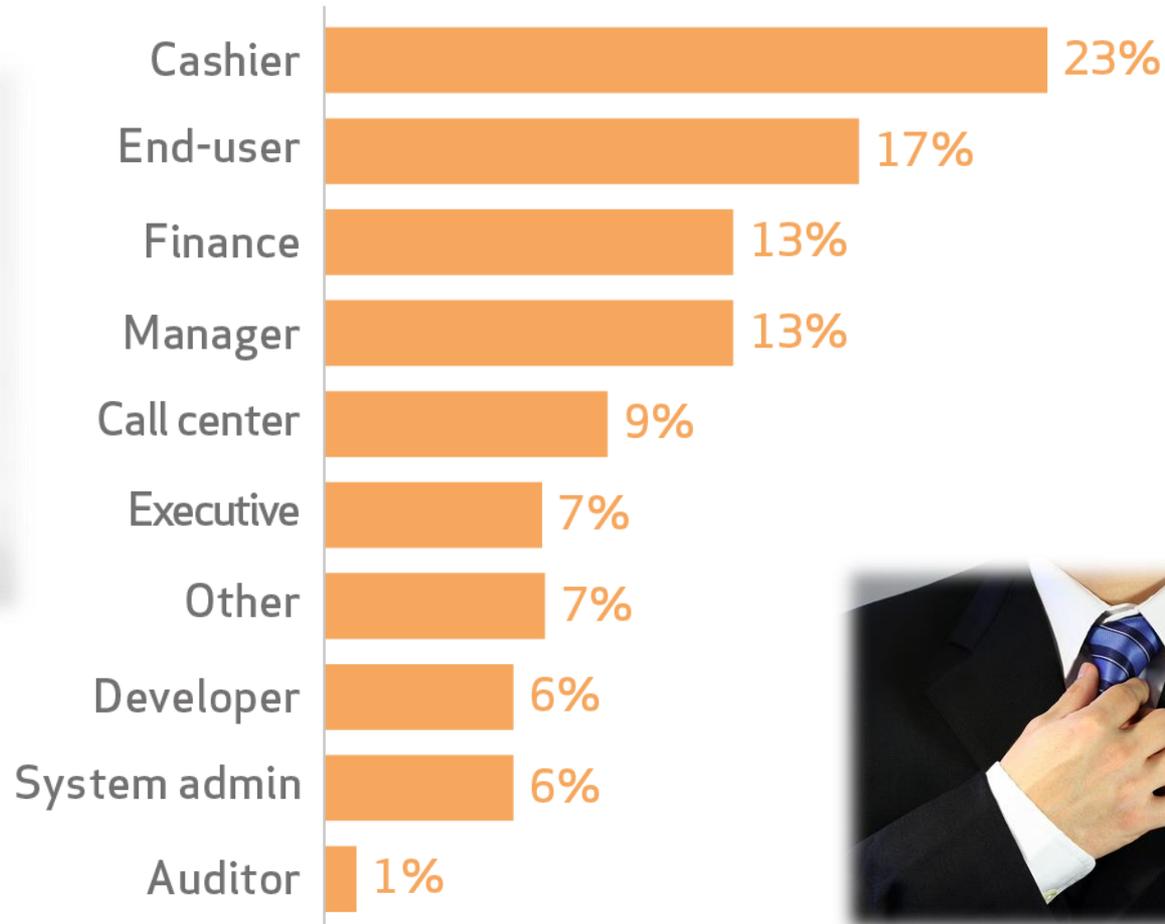




Internal actors include more managers and executives than in prior years

Figure 32.

Top 10 varieties of internal actors within Insider Misuse (n=99)

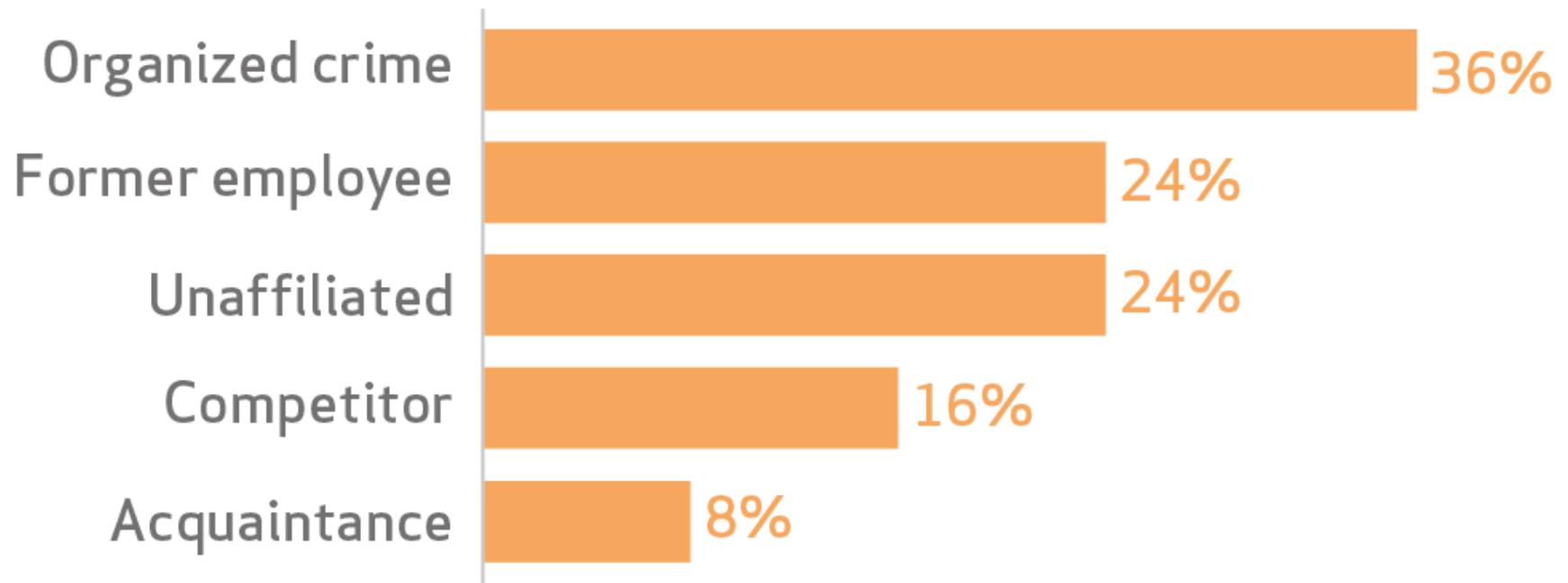




External actors bribe, exploit known access, and solicit information

Figure 33.

Variety of external actors within Insider Misuse (n=25)

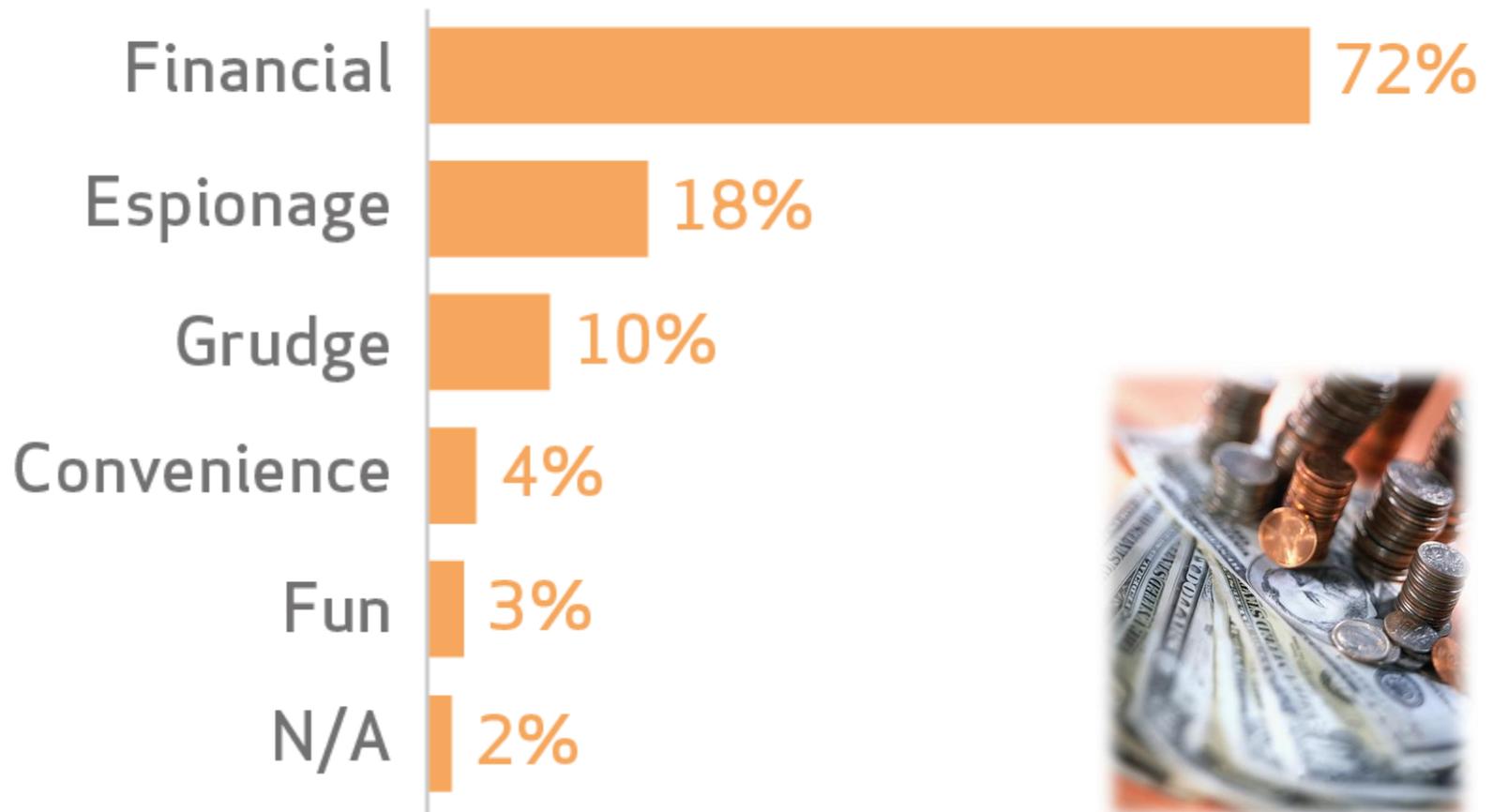




Motivation is primarily financial, with some espionage (to benefit a competitor)

Figure 34.

Actor motives within Insider Misuse (n=125)

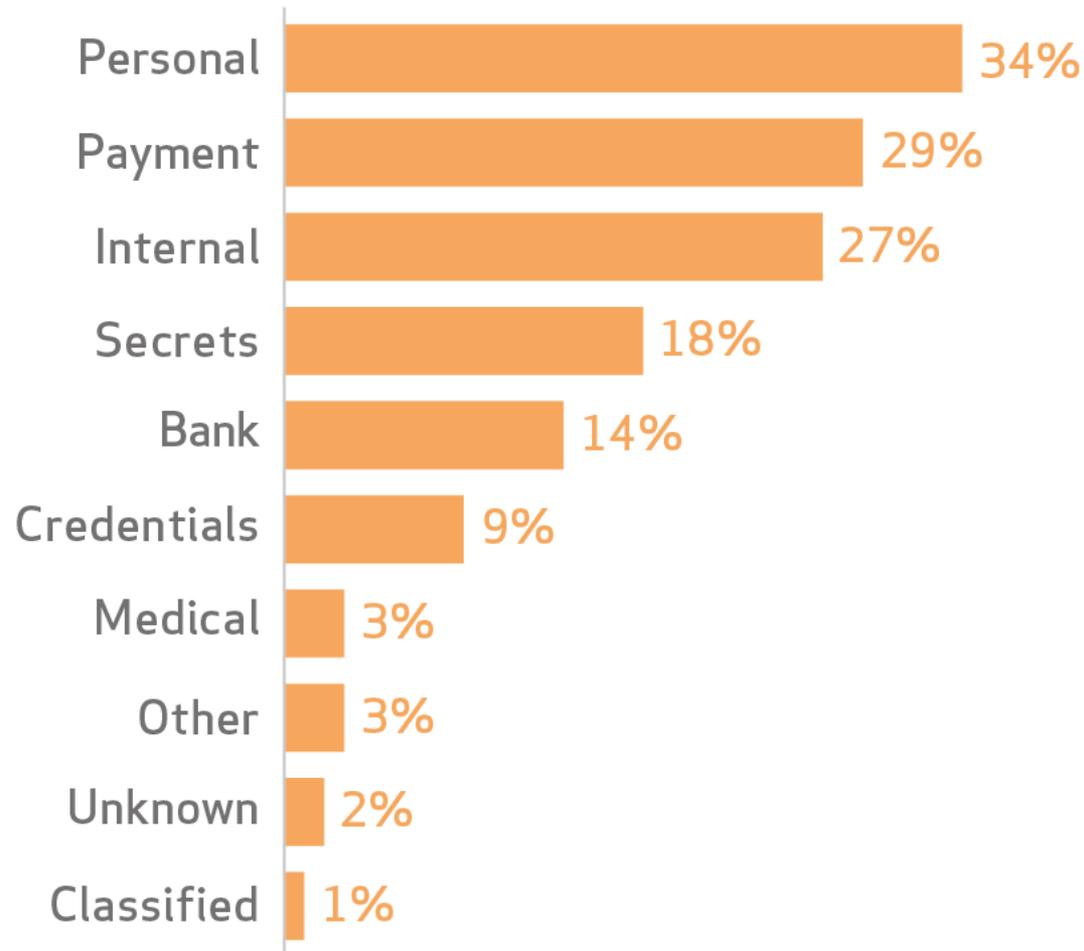




The varieties of data at risk are diverse

Figure 35.

Variety of at-risk data within Insider Misuse (n=108)

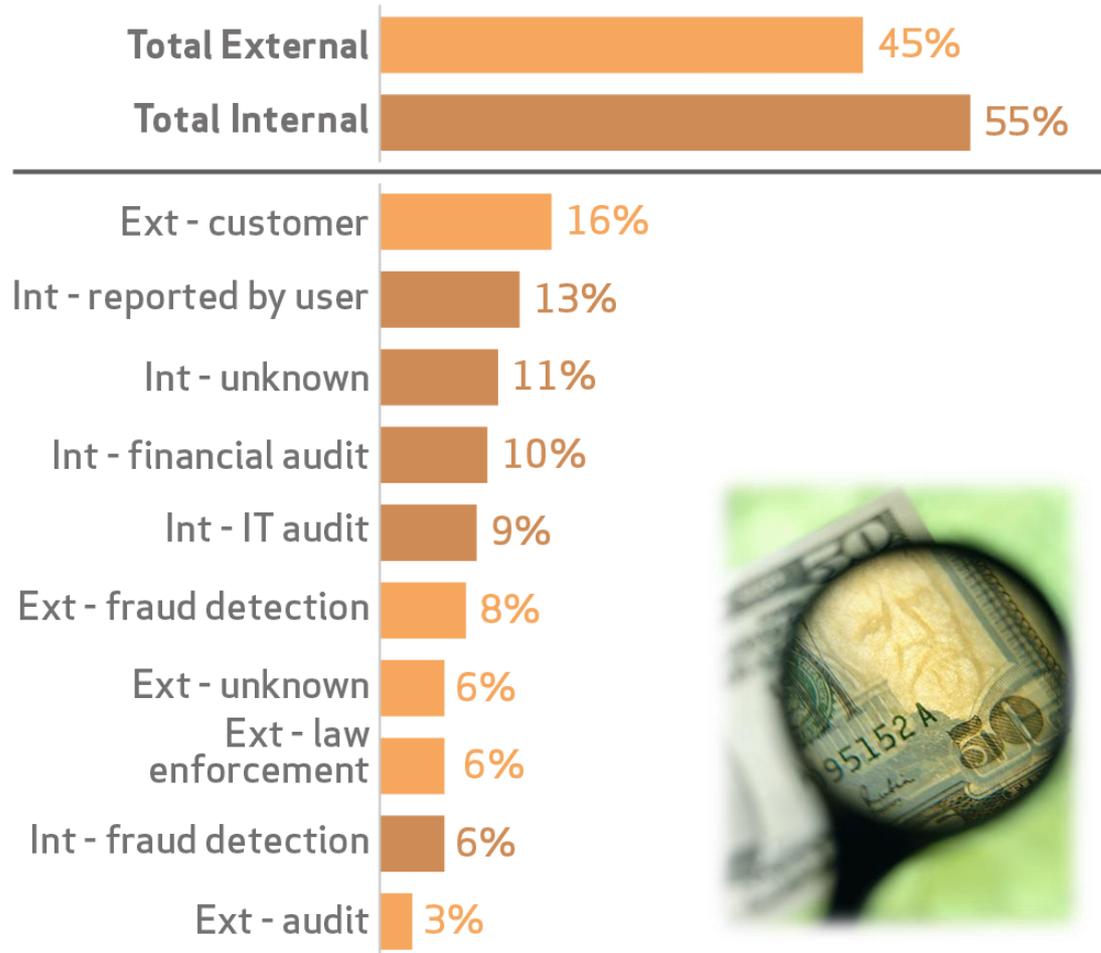




Internal detection is unusually common for insider and privilege misuse

Figure 37.

Top 10 discovery methods within Insider Misuse (n=122)

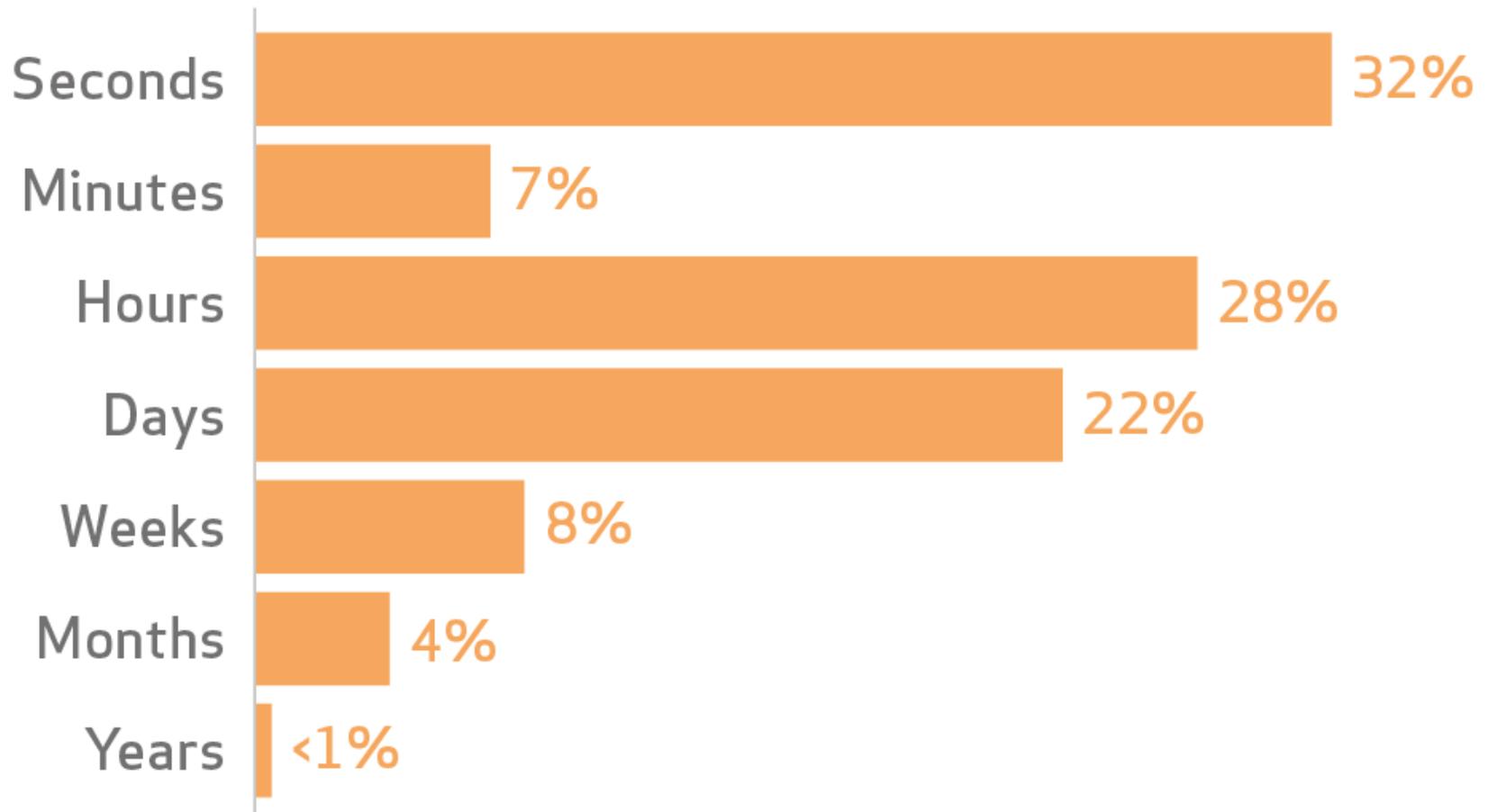




Discovery time is also unusual: many were discovered within days

Figure 38.

Discovery timeline within Insider Misuse (n=1,017)





Recommended controls for insider and privilege misuse

- Know your data and who has access to it
- Review user accounts
- Watch for data exfiltration
- Publish audit results



Physical Theft and Loss

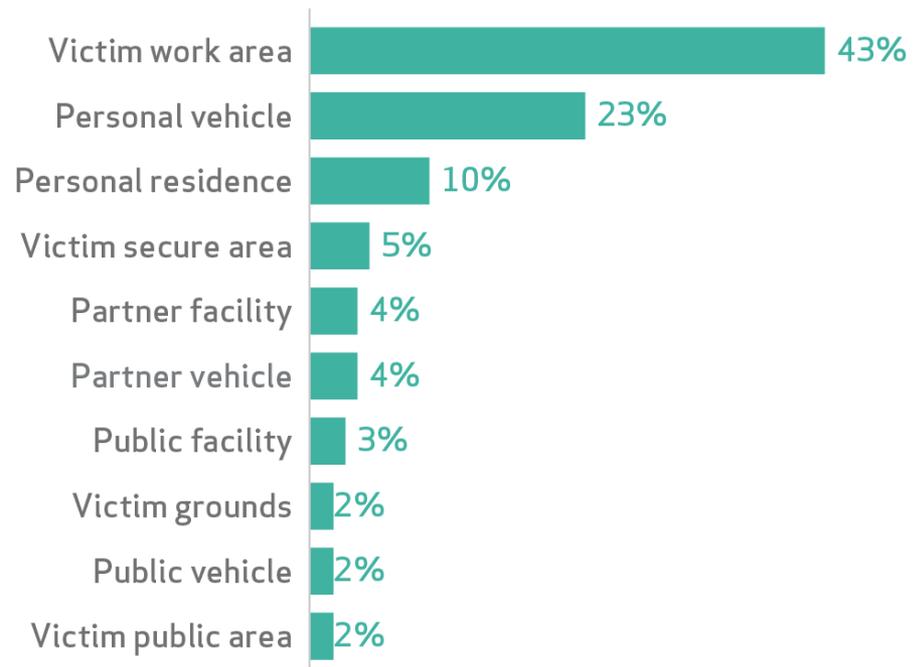


Physical Theft and Loss Key Findings

- Assets are stolen more often from offices than vehicles or residences
- Loss is reported more frequently than theft (15:1)
- More losses and thefts are reported because of disclosure regulations than fraud
- Data varieties at risk are mostly personal and medical
- Recommendations:
 - Encrypt devices
 - Keep them with you
 - Back them up
 - Lock them down
 - Use unappealing tech

Figure 40.

Top 10 locations for theft within Theft/Loss (n=332)



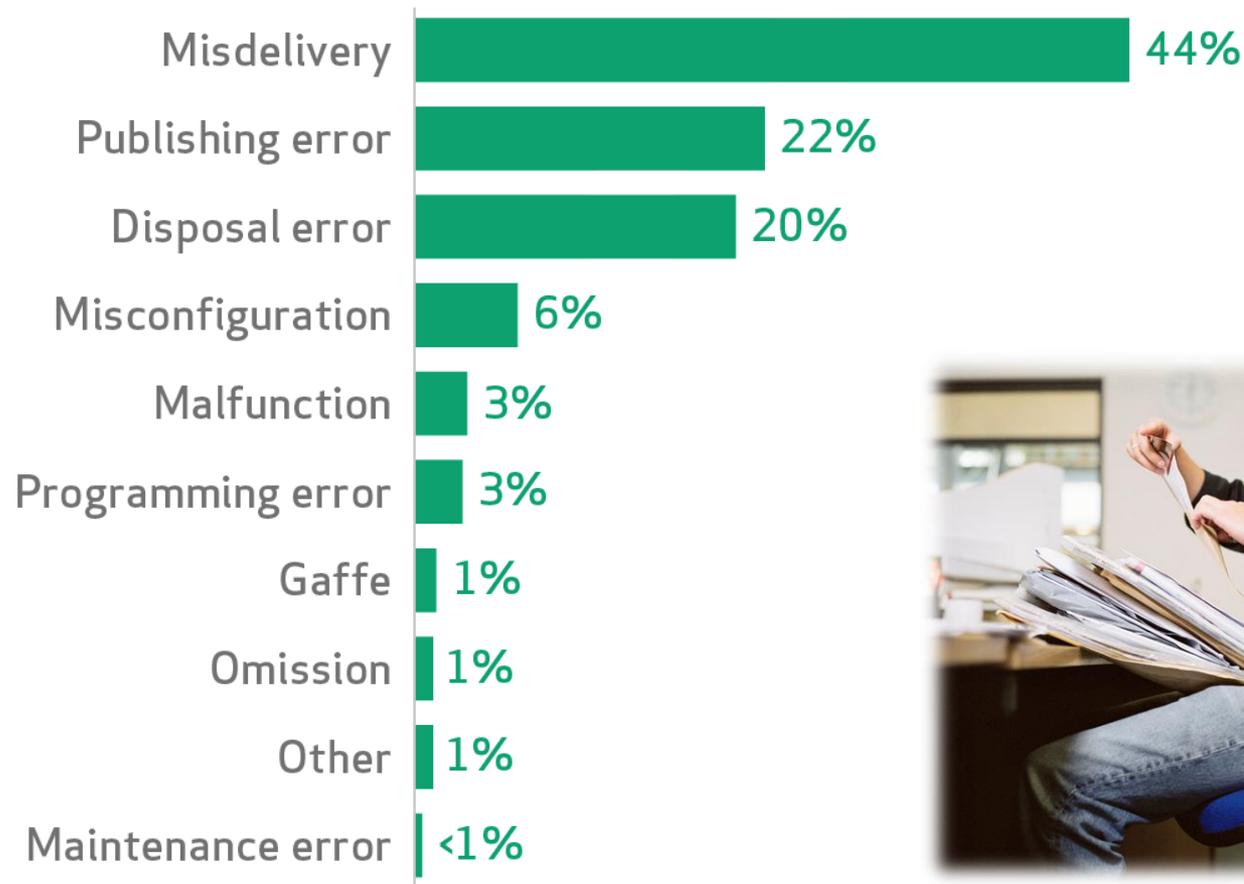


Miscellaneous errors



Highly repetitive processes involving sensitive data are particularly error prone

Figure 43.
Top 10 threat action varieties within Miscellaneous Errors
(n=558)





Discovery typically takes a long time, and it's external about two-thirds of the time

Figure 45.
Discovery and containment timeline within Miscellaneous Errors

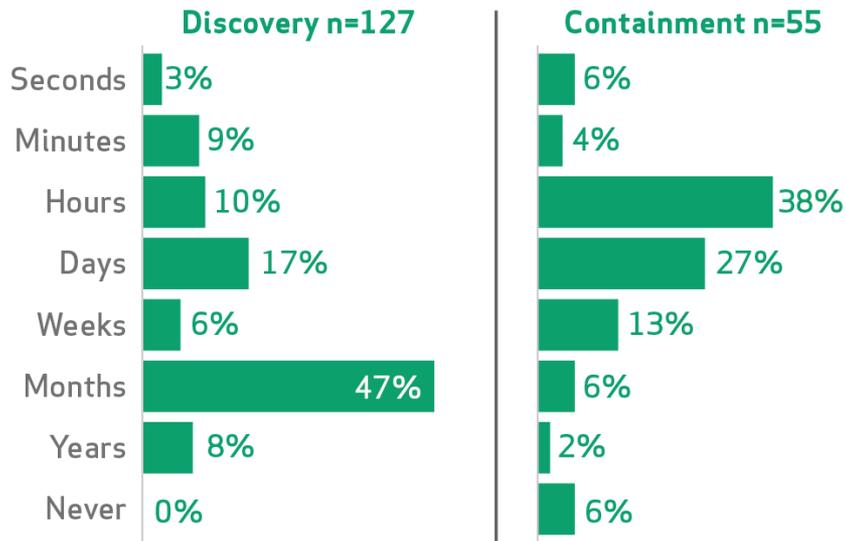
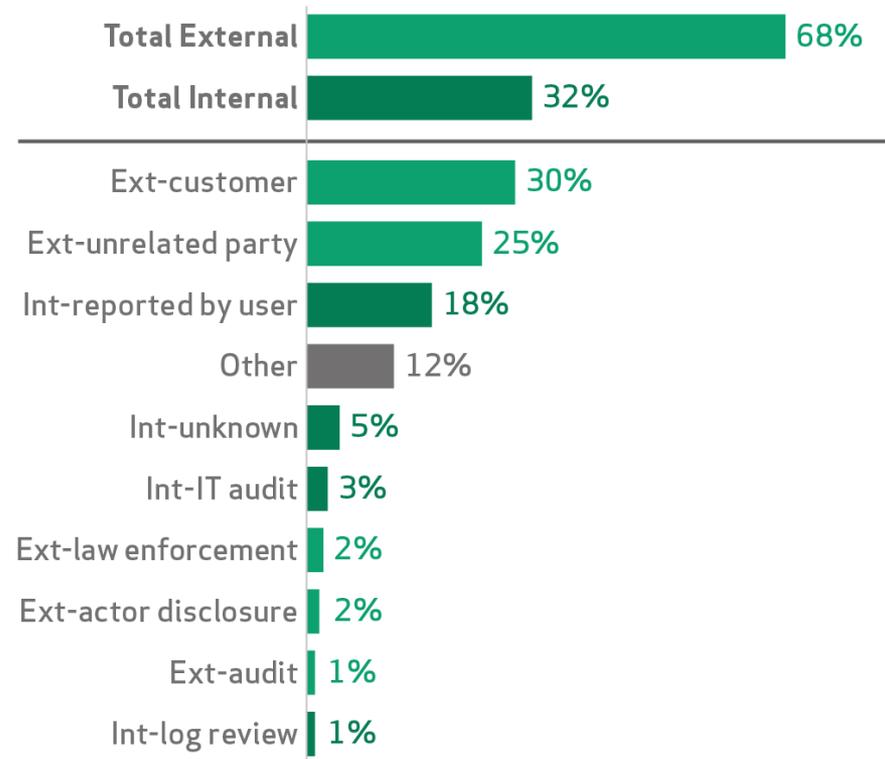


Figure 46.
Top 10 discovery methods for Miscellaneous Error incidents (n=148)





Recommended controls for miscellaneous errors

- Consider Data Loss Prevention (DLP) software
- Tighten processes around posting documents
- Spot-check large mailings
- IT disposes of all information assets (and test them)



Crimeware

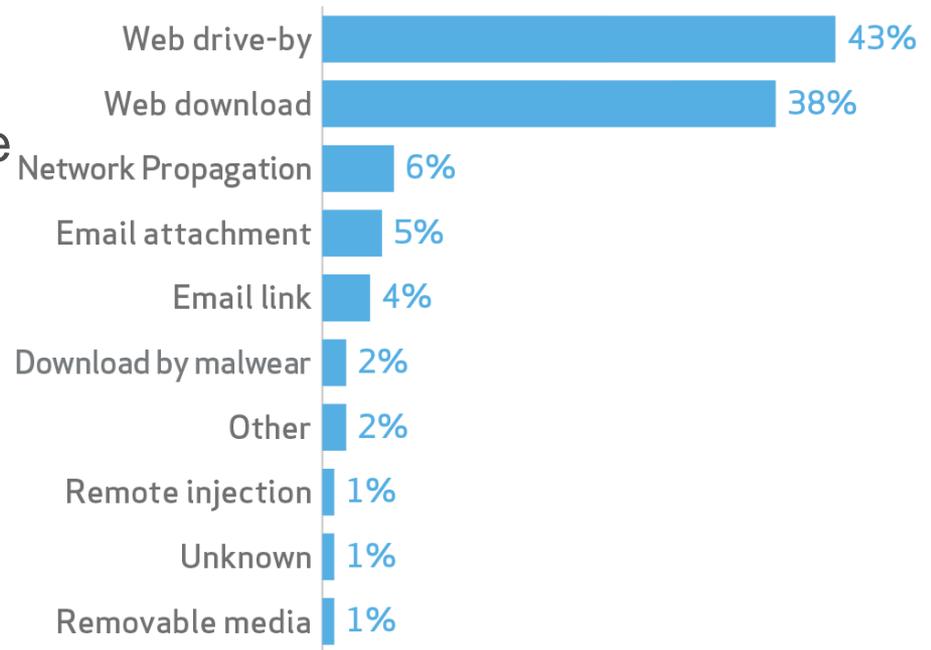


Crimeware Key Findings

- Web downloads and drive-bys are the most common infection vectors
- Primary goal is usually to gain control of systems for illicit uses like stealing credentials, DDoS attacks, and spamming
- Recommendations:
 - Keep browsers up to date
 - Disable Java in the browser
 - 2-factor authentication
 - System configuration change monitoring
 - Leverage threat feeds

Figure 48.

Top 10 vectors for malware actions within Crimeware (n=337)





Payment card skimmers



Payment card skimmers key findings

- Most actors are Eastern European
- Most assets are ATMs
- More highly skilled criminals now collect data via Bluetooth or SIM cards with remote caching and tampering alerts
- Recommendations:
 - Tamper-resistant terminals
 - Tamper evident controls
 - Watch for tampering
 - Protect your PIN
 - Avoid unusual-looking terminals
 - Report unusual observations

Figure 53.

Origin of external actors within Card Skimmers (n=40)

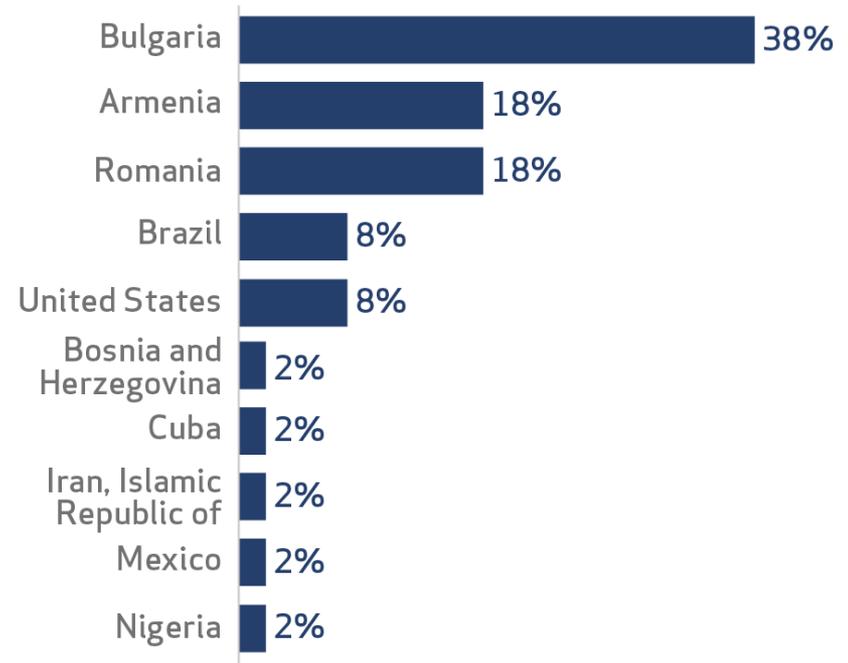


Figure 54.

Assets affected within Card Skimmers (n=537)





Cyber espionage



Certain industries saw far more cyber espionage than others

Figure 56.
Number of incidents by victim industry and size within Cyber-espionage

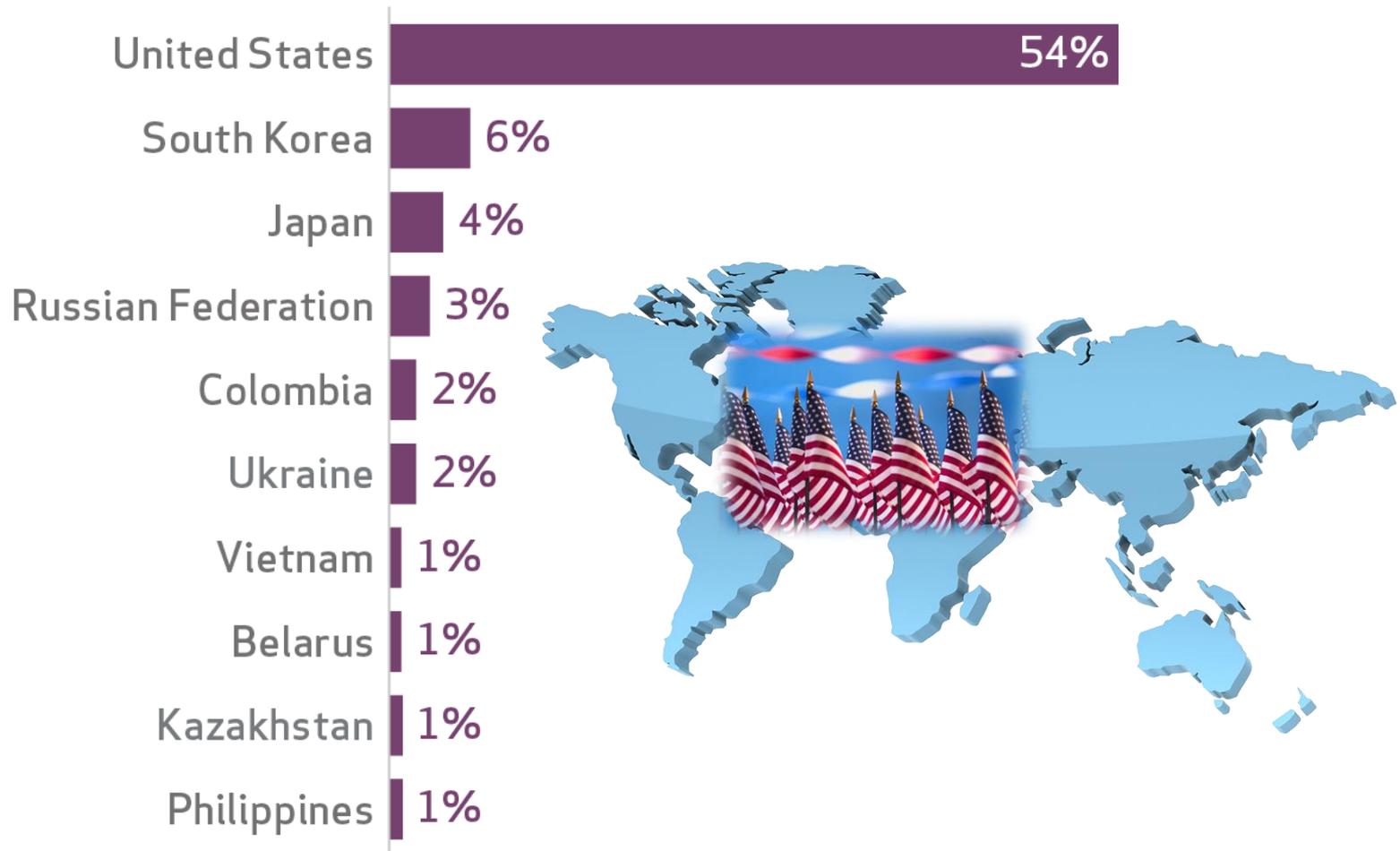
Industry	Total	Small	Large	Unknown
Administrative [56]	2	1	1	0
Construction [23]	1	0	0	1
Education [61]	2	1	1	0
Finance [52]	3	0	2	1
Healthcare [62]	2	1	0	1
Information [51]	11	2	2	7
Management [55]	2	1	1	0
Manufacturing [31,32,33]	81	5	17	59
Mining [21]	5	0	2	3
Professional [54]	114	11	5	98
Public [92]	133	20	19	94
Real Estate [53]	1	1	0	0
Retail [44,45]	1	0	1	0
Transportation [48,49]	5	1	3	1
Utilities [22]	8	0	1	7
Other [81]	5	5	0	0
Unknown	135	0	3	132
Total	511	49	58	404



About half of our sample is U.S. victims, but visibility on others is increasing

Figure 57.

Victim country within Cyber-espionage (n=470)

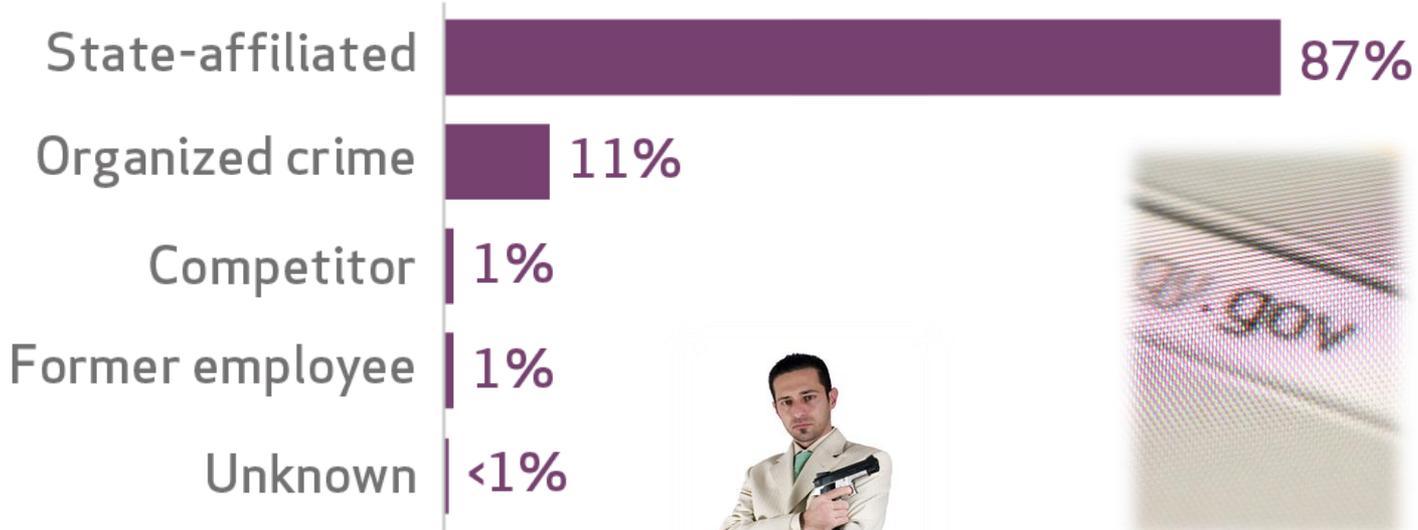




Most actors are state affiliated, but a significant minority are not

Figure 58.

Variety of external actors within Cyber-espionage (n=437)

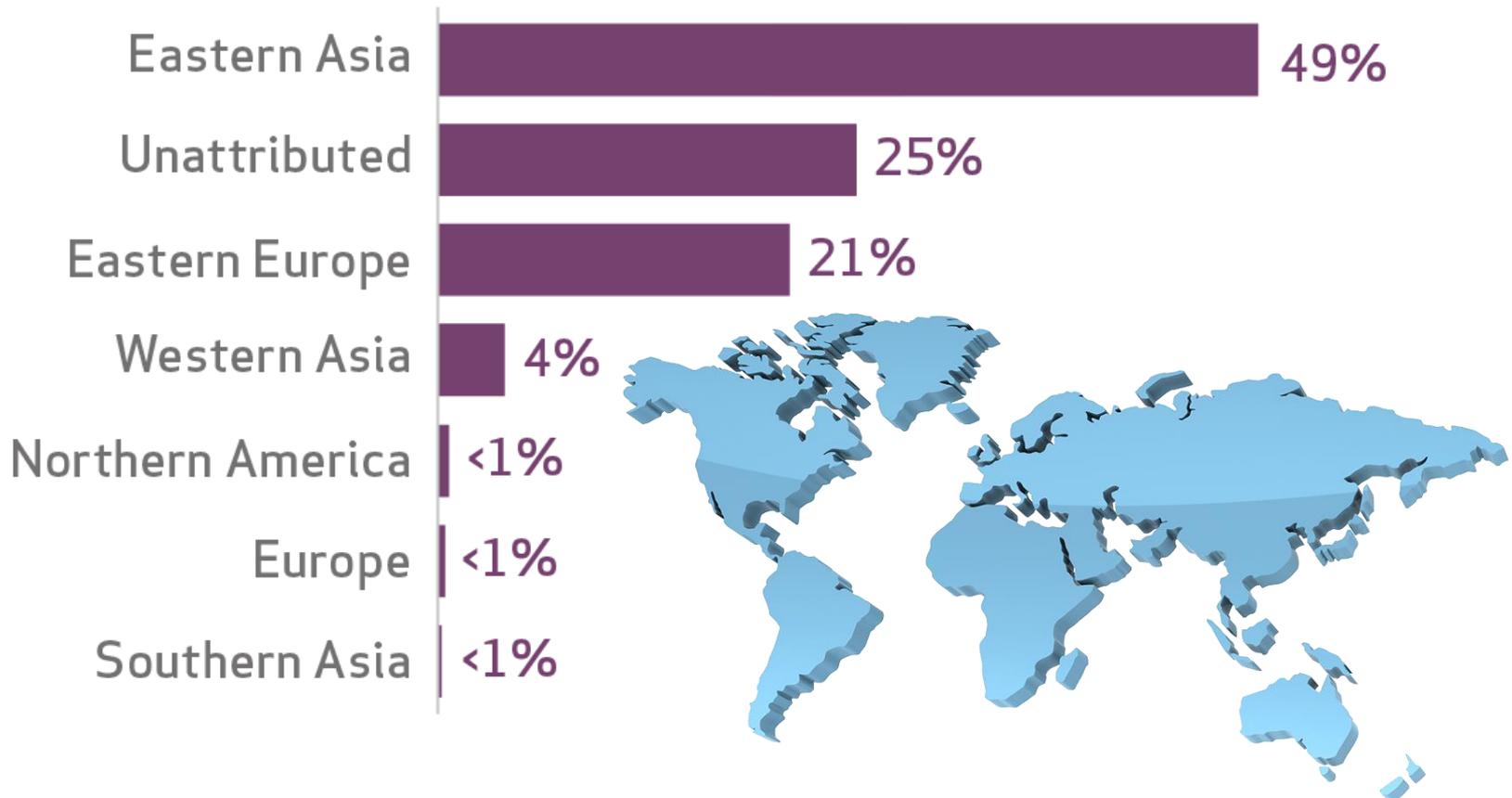




More data about non-eastern-Asia actors reflects more, better research

Figure 59.

Region of external actors within Cyber-espionage (n=230)

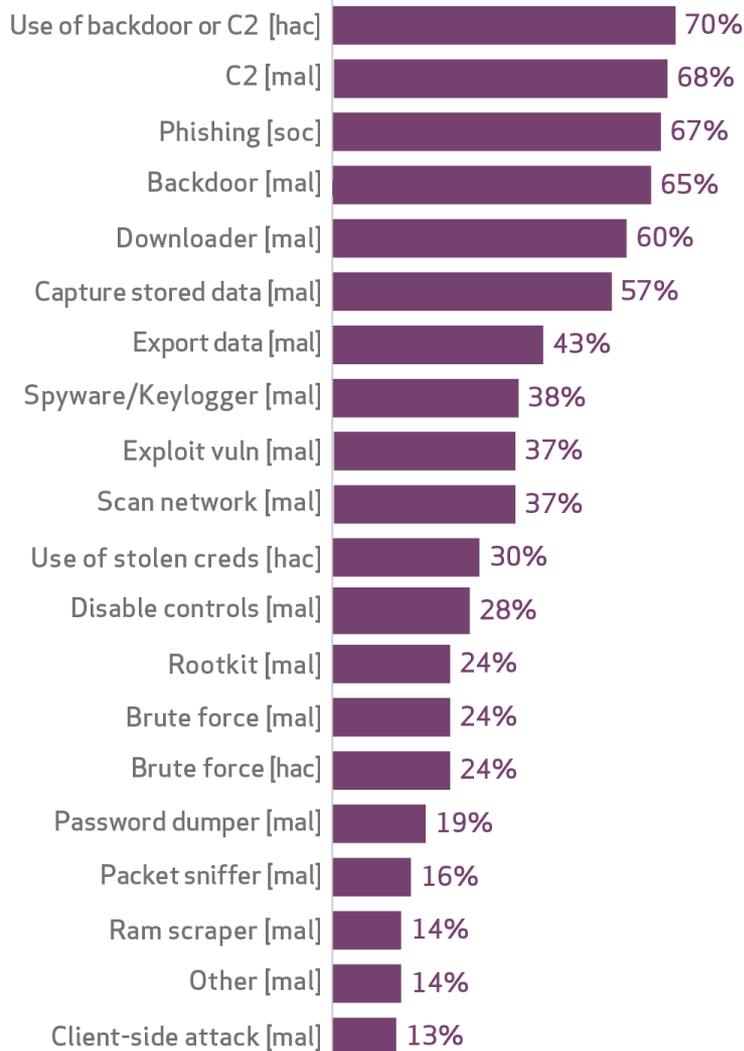




Cyber espionage involves a much wider range of tools than other patterns

Figure 60.

Top threat action varieties within Cyber-espionage (n=426)

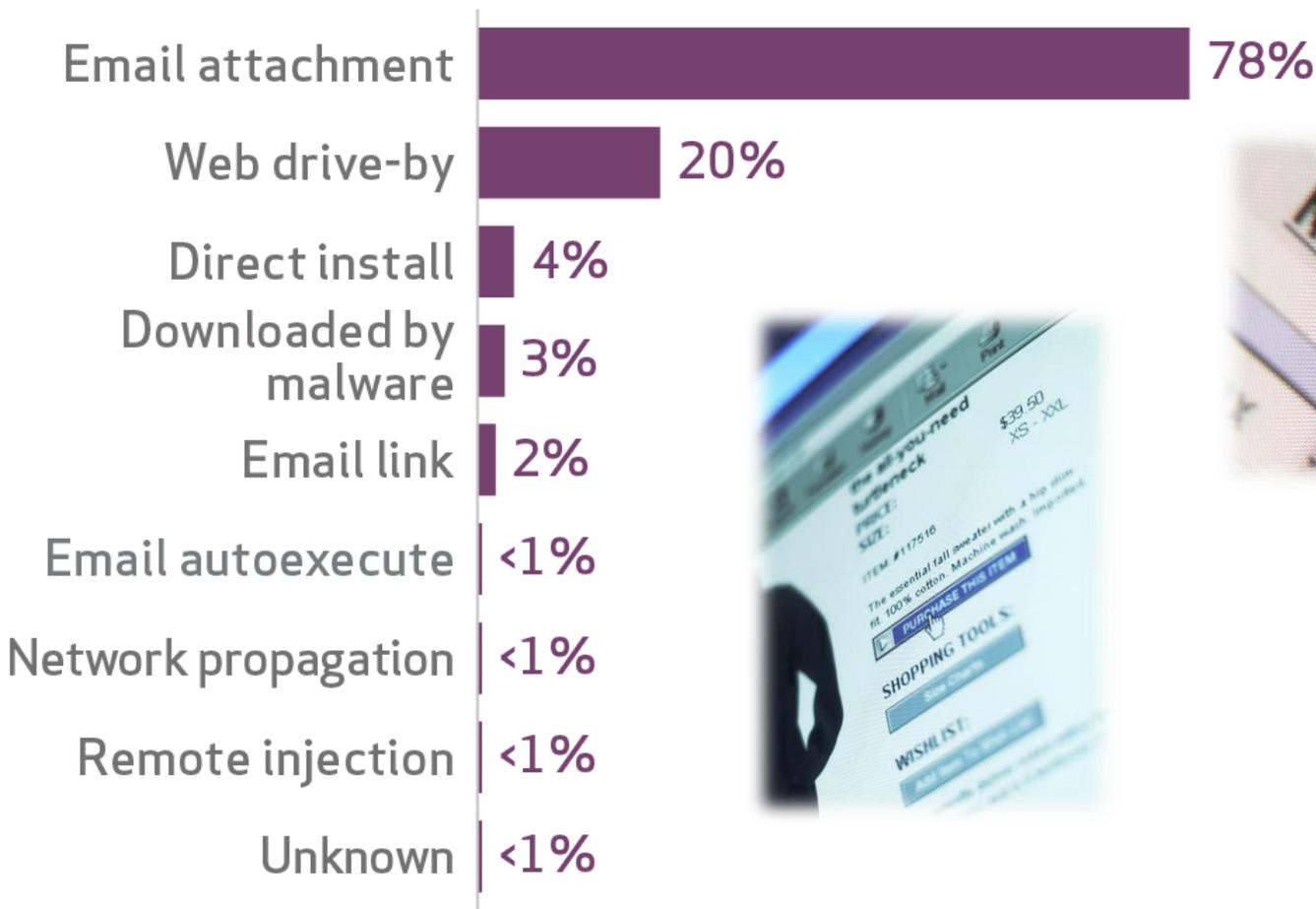




But there are relatively few ways attackers gain access to victims

Figure 61.

Vector for malware actions within Cyber-espionage (n=329)

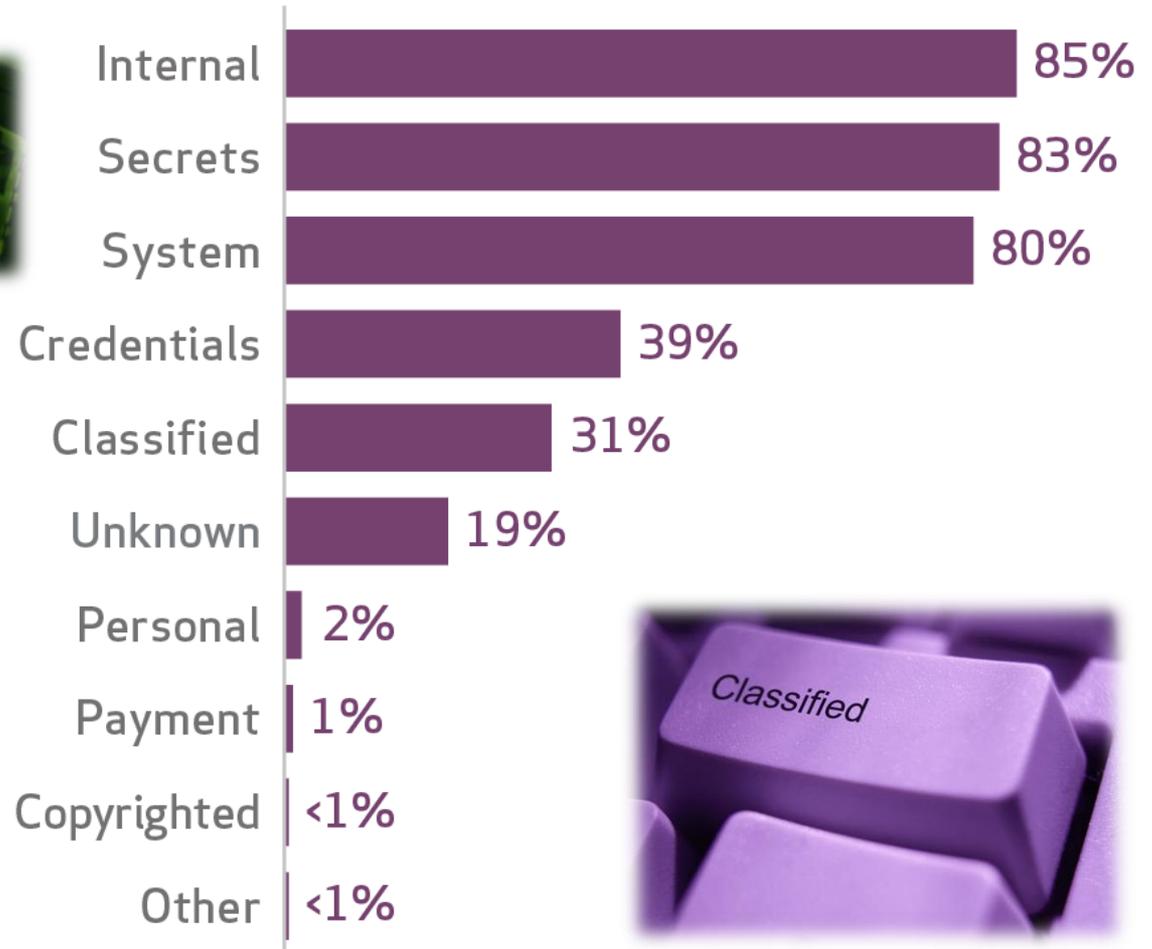




Attackers compromise sensitive data they're after and credentials along the way

Figure 62.

Variety of at-risk data within Cyber-espionage (n=355)





Discovery methods and times leave a lot of room for improvement

Figure 63.

Top 10 discovery methods within Cyber-espionage (n=302)

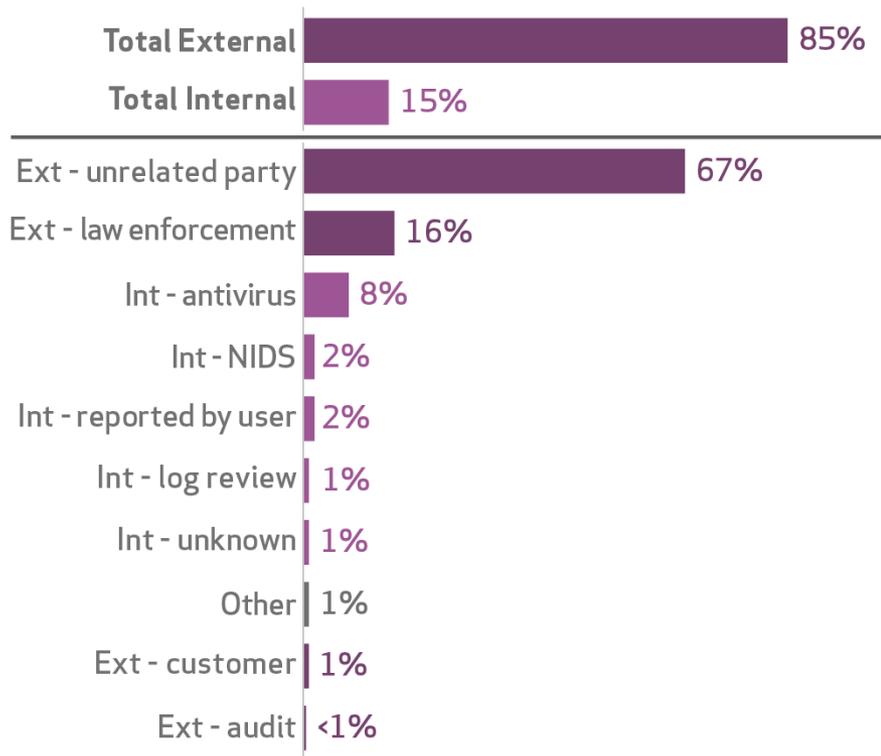
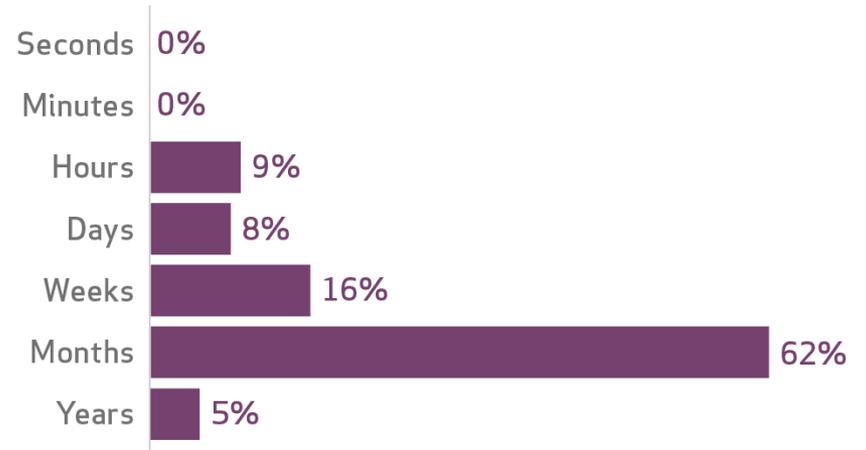


Figure 64.

Discovery timeline within Cyber-espionage (n=101)





Recommended controls for cyber espionage

- Patching
- Anti-virus
- User training
- Network segmentation
- Good logging
- Break the delivery-exploitation-installation chain
- Spot C2 and data exfiltration
- Stop lateral movement inside the network



Denial of Service Attacks



Denial of Service Attacks Key Findings

- Using compromised CMSs continued
- DNS reflection attacks increased
- Izz ad-Din al-Qassam Cyber Fighters (QCF) was responsible for a significant number of attacks
- There was little hard evidence of DoS attacks to distract from fraud
- Recommendations:
 - Basic practices of patching, turning off unneeded services
 - Isolate key assets on the network
 - Make preparations for anti-DDos service
 - Ask ISPs about upstream capacity



So what?

Figure 69. Critical security controls mapped to incident patterns. Based on recommendations given in this

Critical Security Controls (SANS Institute)	POS Intrusions	Web App Attacks	Insider Misuse	Physical Theft/Loss	Misc errors
Software Inventory	2.4				
Standard Configs	3.1				
	3.2	●			
	3.8				
Malware Defenses	5.1	●			
	5.2	●			
	5.6				
Secure Development	6.4	●			
	6.7	●			
	6.11	●			
Backups	8.1			●	
Skilled Staff	9.3			●	
	9.4				
	11.2				
Restricted Access	11.5	●			
	11.6	●			
	12.1	●	●		
Limited Admin	12.2		●		
	12.3	●	●		
	12.4	●			
Boundary defense	12.5	●			
	13.1				
	13.7	●	●		
Audit Logging	13.10	●			
	13.14	●			
	14.5	●			
Identity Management	16.1		●		
	16.12		●		
	16.13		●		
Data Loss Prevention	17.1			●	
	17.6		●		●
	17.9		●		●
Incident Response	18.1				
	18.2				
	18.3				
Network Segmentation	19.4				

Figure 70.

Prioritization of critical security controls by industry. Based on frequency of incident patterns within each industry and recommendations for each pattern given in this report. The shading is relative to each industry.

Critical Security Controls (SANS Institute)	Accommodation [7]	Administrative [56]	Construction [23]	Education [61]	Entertainment [71]	Finance [52]	Healthcare [62]	Information [51]	Management [55]	Manufacturing [31]	Mining [21]	Other [81]	Professional [54]	Public [92]	Real Estate [53]	Retail [44,45]	Trade [42]	Transportation [48]	Utilities [22]
Software Inventory	2.4																		
Standard Configs	3.1																		
	3.2																		
	3.8																		
Malware Defenses	5.1																		
	5.2																		
	5.6																		
Secure Development	6.4																		
	6.7																		
	6.11																		
Backups	8.1																		
Skilled Staff	9.3																		
	9.4																		
	11.2																		
Restricted Access	11.5																		
	11.6																		
	12.1																		
Limited Admin	12.2																		
	12.3																		
	12.4																		
Boundary defense	12.5																		
	13.1																		
	13.7																		
Audit Logging	13.10																		
	13.14																		
	14.5																		
Identity Management	16.1																		
	16.12																		
	16.13																		
Data Loss Prevention	17.1																		
	17.6																		
	17.9																		
Incident Response	18.1																		
	18.2																		
	18.3																		
Network Segmentation	19.4																		



Additional information is available

- Download: www.verizonenterprise.com/dbir
- VERIS: www.veriscommunity.net
- Email: DBIR@verizon.com
- Twitter: [@vzdbir](https://twitter.com/vzdbir) and hashtag [#dbir](https://twitter.com/hashtag/dbir)
- Blog: <http://www.verizonenterprise.com/security/blog/>