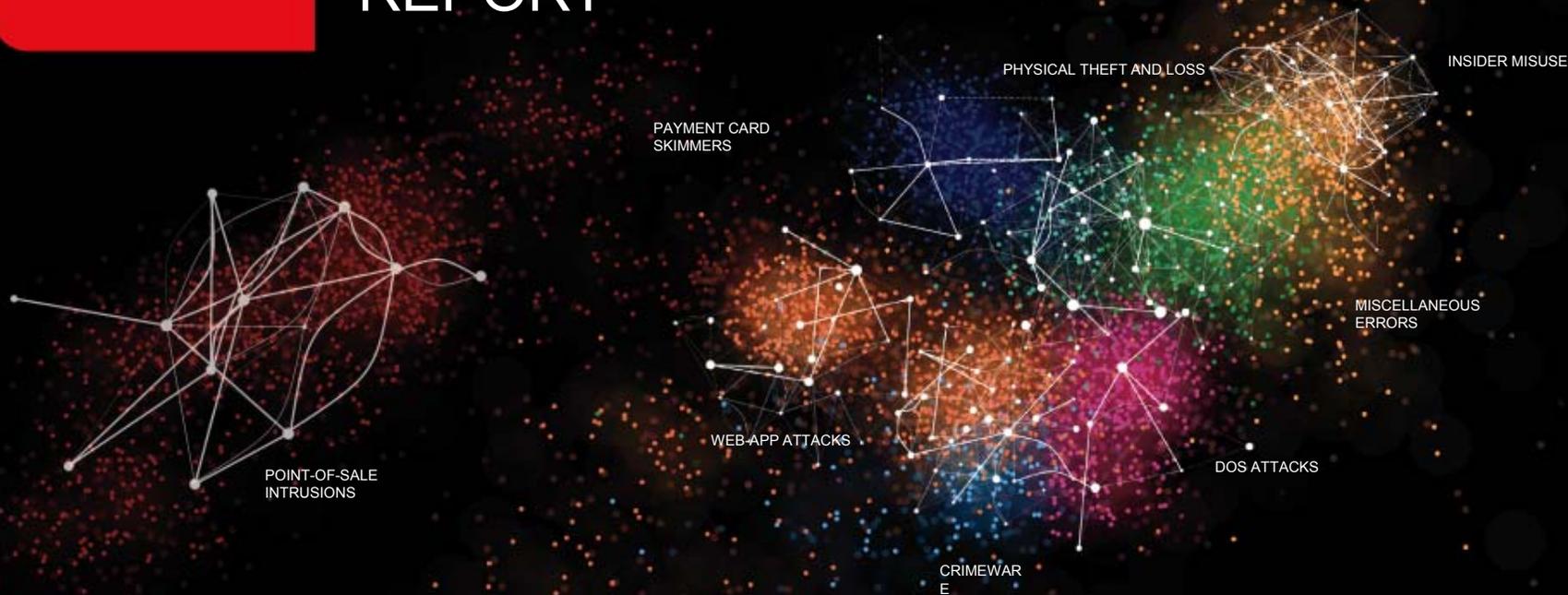




2014 DATA BREACH INVESTIGATIONS REPORT



92%

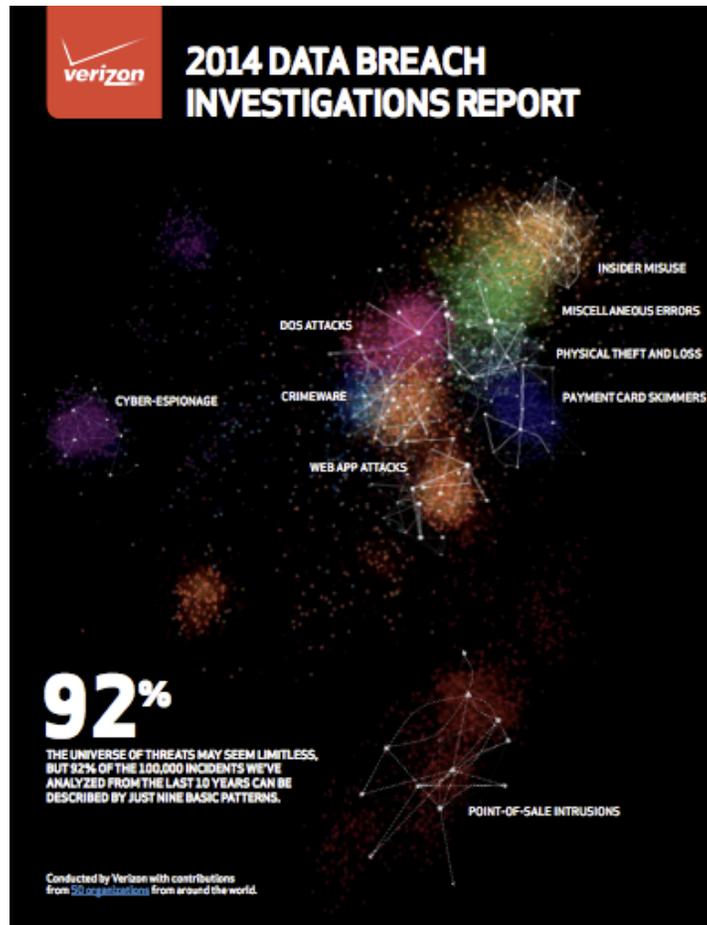
THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATERNS.

CYBER-ESPIONAGE

Conducted by Verizon with contributions from 50 organizations from around the world.



Welcome to the Data Breach Investigations Report, 2014



50
CONTRIBUTING GLOBAL ORGANIZATIONS

1,367
CONFIRMED SECURITY BREACHES

63,437
SECURITY INCIDENTS

95
COUNTRIES REPRESENTED



50 contributors from around the world





DBIR 2014 Contributors

CSIRTS

- CERT Insider Threat Center
- CERT Polska/NASK
- CERT-EU European Union
- CERT.PT
- Computer Emergency Response team of Ukraine (CERT-UA)
- Computer Incident Response Center Luxembourg (CIRCL), National CERT, Luxembourg
- CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI)
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- Irish Reporting and Information Security Service (IRISS-CERT)
- OpenCERT Canada
- US Computer Emergency Readiness Team (US-CERT)

CYBER CENTERS

- Centre for Cyber Security, Denmark
- Council on CyberSecurity
- Defense Security Service (DSS)
- European Cyber Crime Center (EC3)
- National Cybersecurity and Integration Center (NCCIC)
- Netherlands National Cyber Security Centre (NCSC-NL)

FORENSIC PROVIDERS

- Deloitte and Touche LLP
- G-C Partners, LLC
- Guidance Software
- S21sec
- Verizon RISK Team

INFOSEC PRODUCT AND SERVICE PROVIDERS

- Akamai
- Centripetal Networks, Inc.
- FireEye
- Kaspersky Lab
- Malicious Streams
- McAfee, part of Intel Security
- ThreatGRID, Inc.
- ThreatSim
- Verizon DoS Defense
- WhiteHat Security

ISACS

- Center for Internet Security (MS-ISAC)
- Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- Financial Services ISAC (FS-ISAC)
- Public Transit ISAC (PT-ISAC)
- Real Estate ISAC (RE-ISAC)
- Research & Education ISAC (REN-ISAC)

LAW ENFORCEMENT AGENCIES

- Australian Federal Police (AFP)
- Cybercrime Central Unit of the Guardia Civil (Spain)
- Danish National Police, NITES (National IT Investigation Section)
- Dutch Police: National High Tech Crime Unit (NHTCU)
- Policía Metropolitana (Argentina)
- Policía Nacional de Colombia
- US Secret Service

OTHER

- Anonymous contributor
- Commonwealth of Massachusetts
- Identity Theft Resource Center
- Mishcon de Reya
- VERIS Community Database (VCDB)
- Winston & Strawn



Countries Represented

Figure 1.
Countries represented in combined caseload



Countries represented in combined caseload (in alphabetical order): Afghanistan, Albania, Algeria, Argentina, Armenia, Australia, Austria, Azerbaijan, Bahrain, Belarus, Belgium, Bosnia and Herzegovina, Botswana, Brazil, Brunei Darussalam, Bulgaria, Cambodia, Canada, Chile, China, Colombia, Congo, Croatia, Cyprus, Czech Republic, Denmark, Egypt, Ethiopia, Finland, France, Georgia, Germany, Greece, Hong Kong, Hungary, India, Indonesia, Iran, Islamic Republic of, Iraq, Ireland, Israel, Italy, Japan, Jordan, Kazakhstan, Kenya, Korea, Republic of, Kuwait, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Macedonia, the former Yugoslav Republic of, Malaysia, Mali, Mauritania, Mexico, Moldova, Republic of, Montenegro, Morocco, Mozambique, Nepal, Netherlands, New Zealand, Oman, Pakistan, Palestinian Territory, Occupied, Peru, Philippines, Poland, Portugal, Qatar, Romania, Russian Federation, Saudi Arabia, Singapore, Slovakia, Slovenia, South Africa, Spain, Switzerland, Taiwan, Province of China, Tanzania, United Republic of, Thailand, Turkey, Turkmenistan, Uganda, Ukraine, United Arab Emirates, United Kingdom,

Source: verizonenterprise.com/DBIR/2014



Security Incident vs. Data Breach

Number of security incidents by victim industry and organization size

Industry	Total	Small	Large	Unknown
Accommodation [72]	212	115	34	63
Administrative [56]	16	8	7	1
Agriculture [11]	4	0	3	1
Construction [23]	4	2	0	2
Education [61]	33	2	10	21
Entertainment [71]	20	8	1	11
Finance [52]	856	43	189	624
Healthcare [62]	26	6	1	19
Information [51]	1,132	16	27	1,089
Management [55]	10	1	3	6
Manufacturing [31,32,33]	251	7	33	211
Mining [21]	11	0	8	3
Professional [54]	360	26	10	324
Public [92]	47,479	26	47,074	379
Real Estate [53]	8	4	0	4
Retail [44,45]	467	36	11	420
Trade [42]	4	3	0	1
Transportation [48,49]	27	3	7	17
Utilities [22]	166	2	3	161
Other [81]	27	13	0	14
Unknown	12,384	5,498	4	6,822
Total	63,437	5,819	47,425	10,193

Number of security incidents with confirmed data loss by victim industry and organization size

Industry	Total	Small	Large	Unknown
Accommodation [72]	137	113	21	3
Administrative [56]	7	3	3	1
Construction [23]	2	1	0	1
Education [61]	15	1	9	5
Entertainment [71]	4	3	1	0
Finance [52]	465	24	36	405
Healthcare [62]	7	4	0	3
Information [51]	31	7	6	18
Management [55]	1	1	0	0
Manufacturing [31,32,33]	59	6	12	41
Mining [21]	10	0	7	3
Professional [54]	75	13	5	57
Public [92]	175	16	26	133
Real Estate [53]	4	2	0	2
Retail [44,45]	148	35	11	102
Trade [42]	3	2	0	1
Transportation [48,49]	10	2	4	4
Utilities [22]	80	2	0	78
Other [81]	8	6	0	2
Unknown	126	2	3	121
Total	1,367	243	144	980

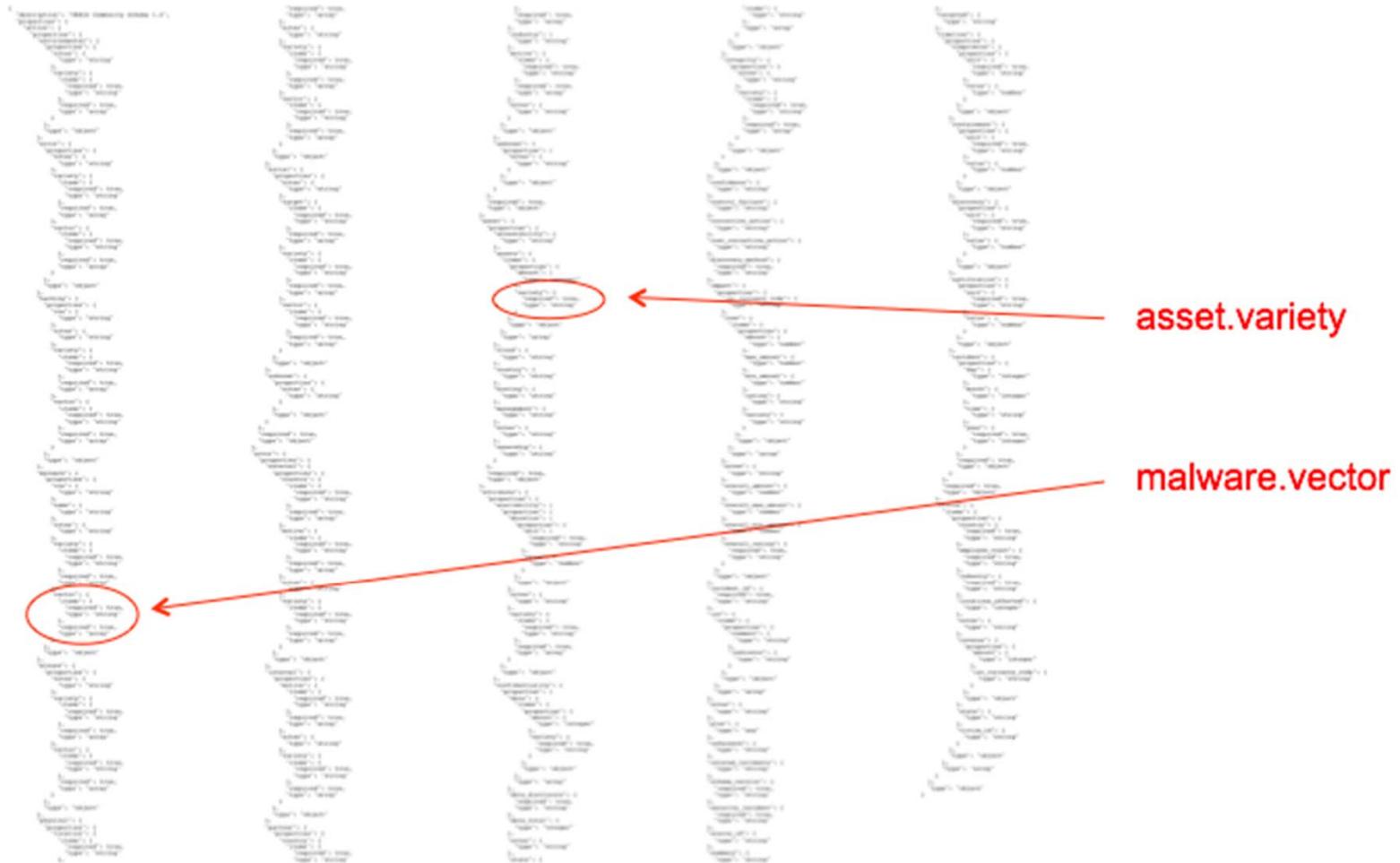


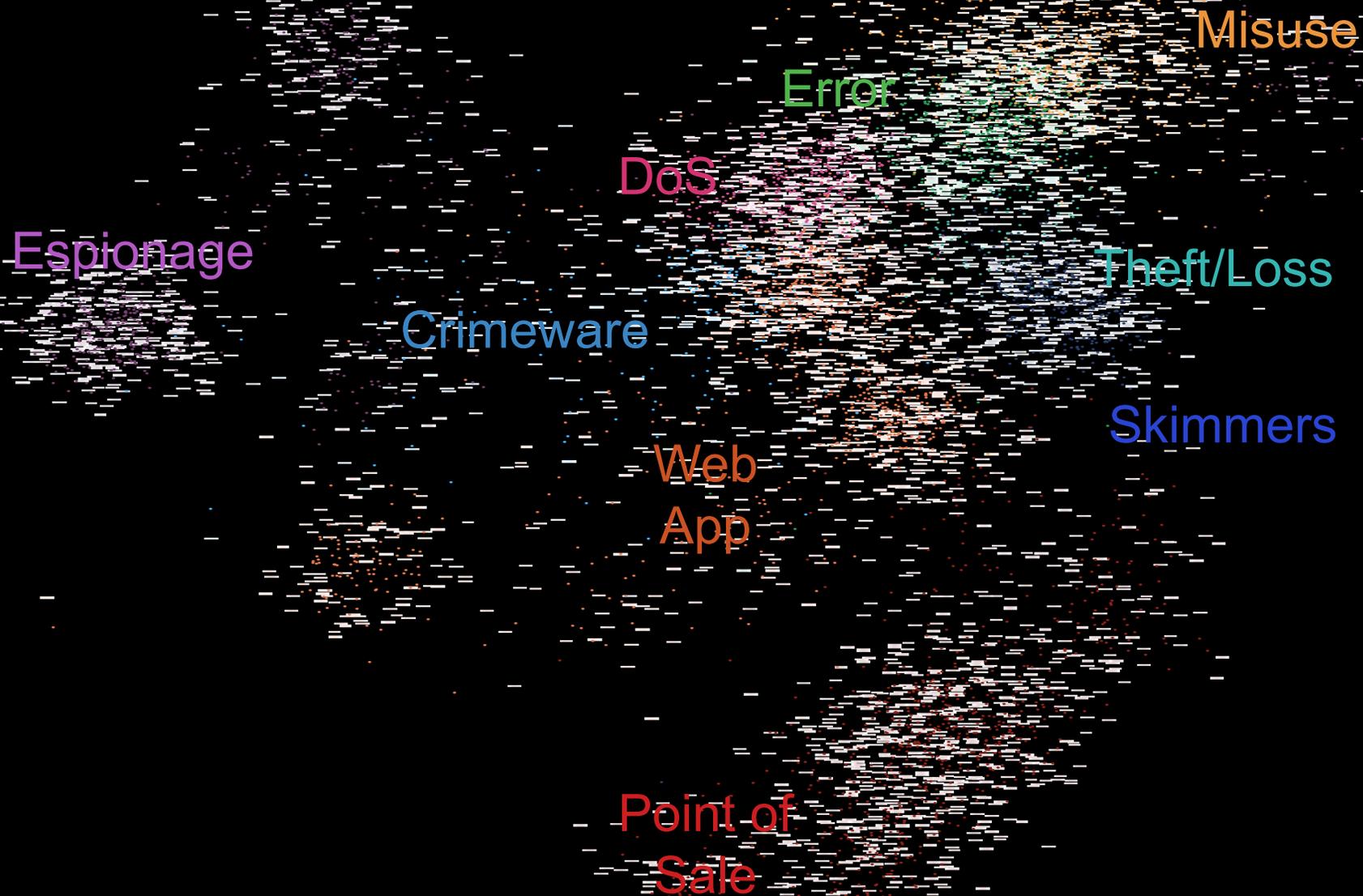
Criticisms of past DBIRs

1. Lacks info on breach impact or cost
2. Findings skewed by “stuff I don’t care about”
 - e.g., “I don’t have POS/ATMs” or “I’m a manufacturer.”
3. Not enough “root cause” analysis and recommendations not specific enough



The “DNA” of Security Incident



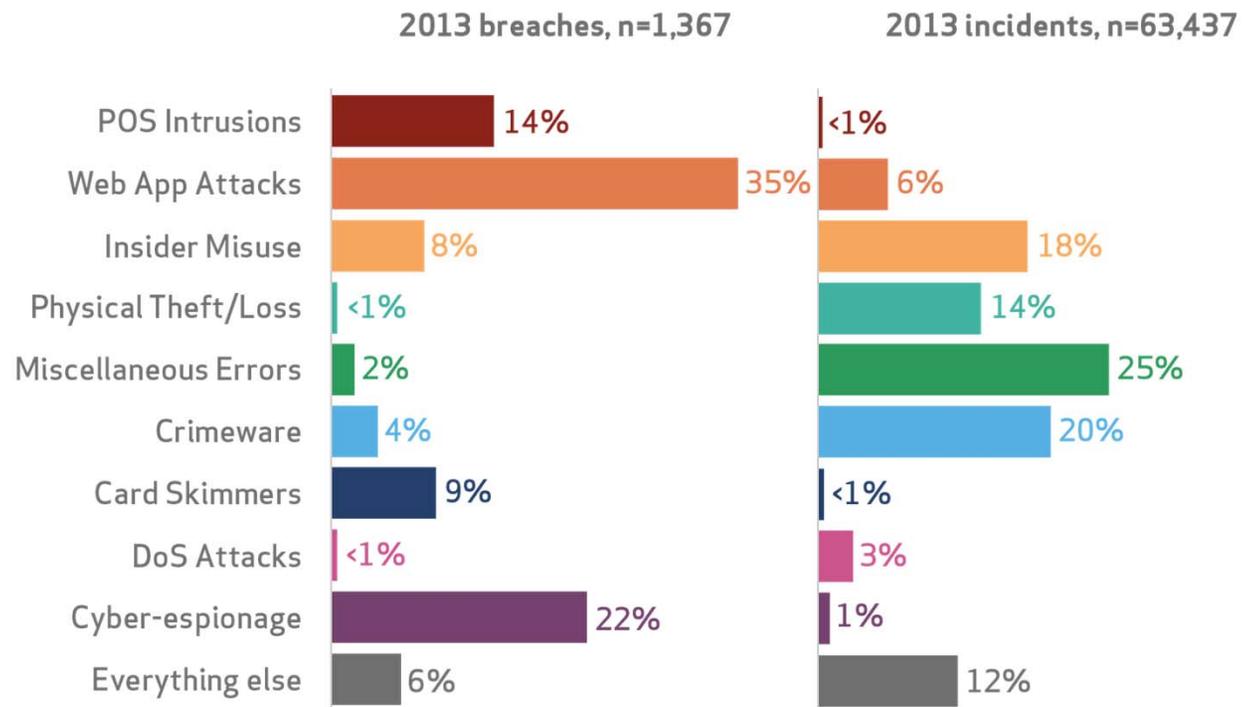


9 Incident Classification Patterns



Pattern Frequency

Figure 16.
Frequency of incident classification patterns



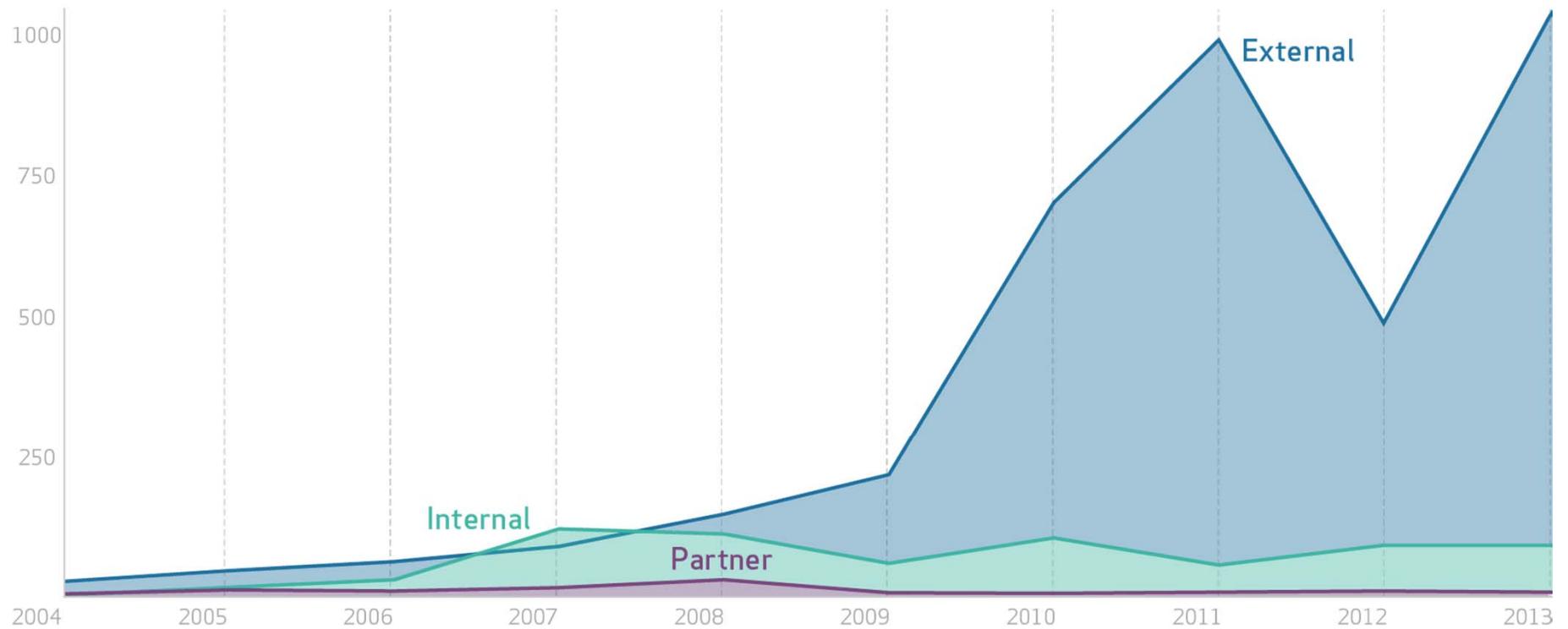
Source: verizonenterprise.com/DBIR/2014

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%



External Actors

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

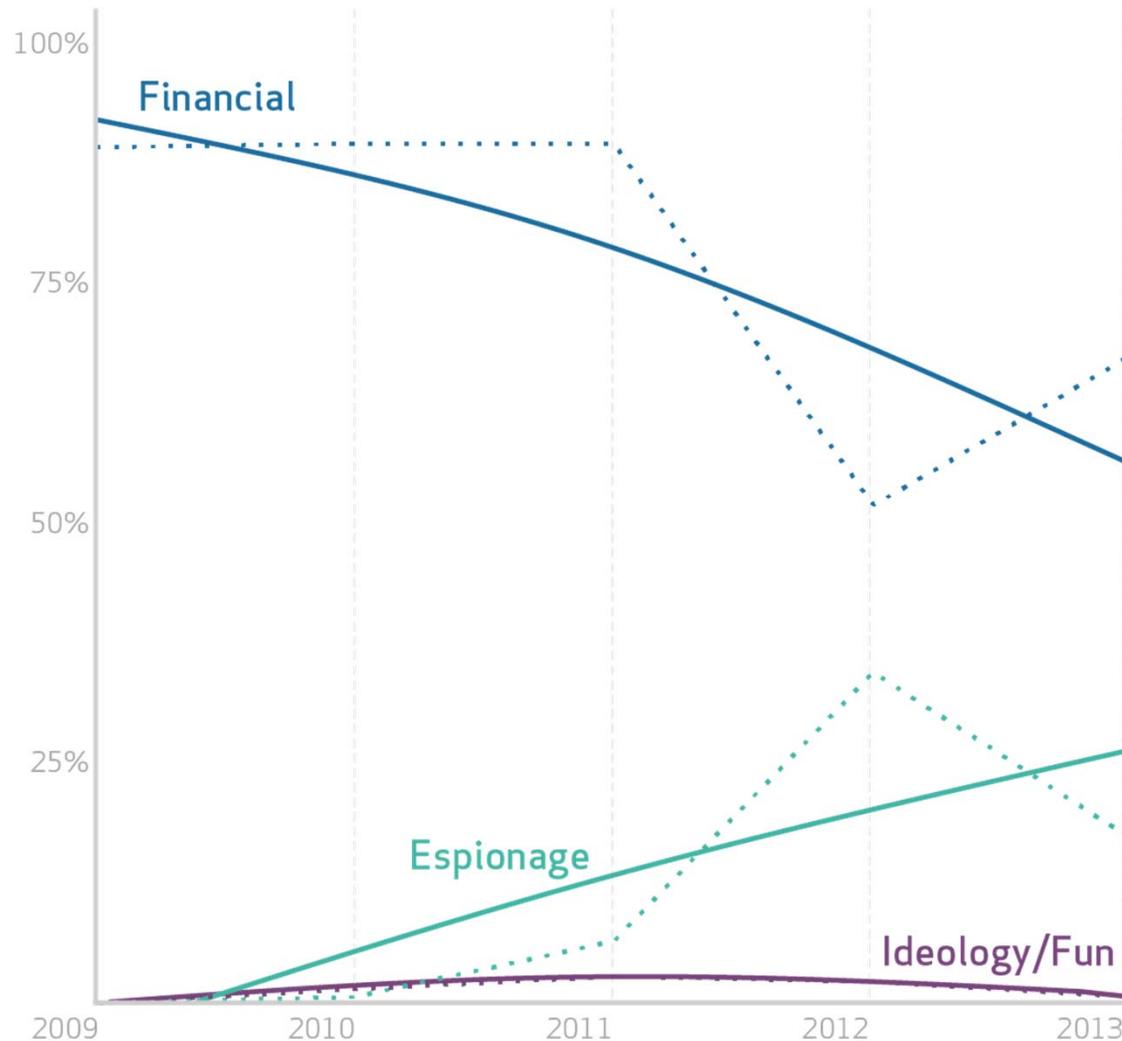


Source: verizonenterprise.com/DBIR/2014



External Actor: Motive

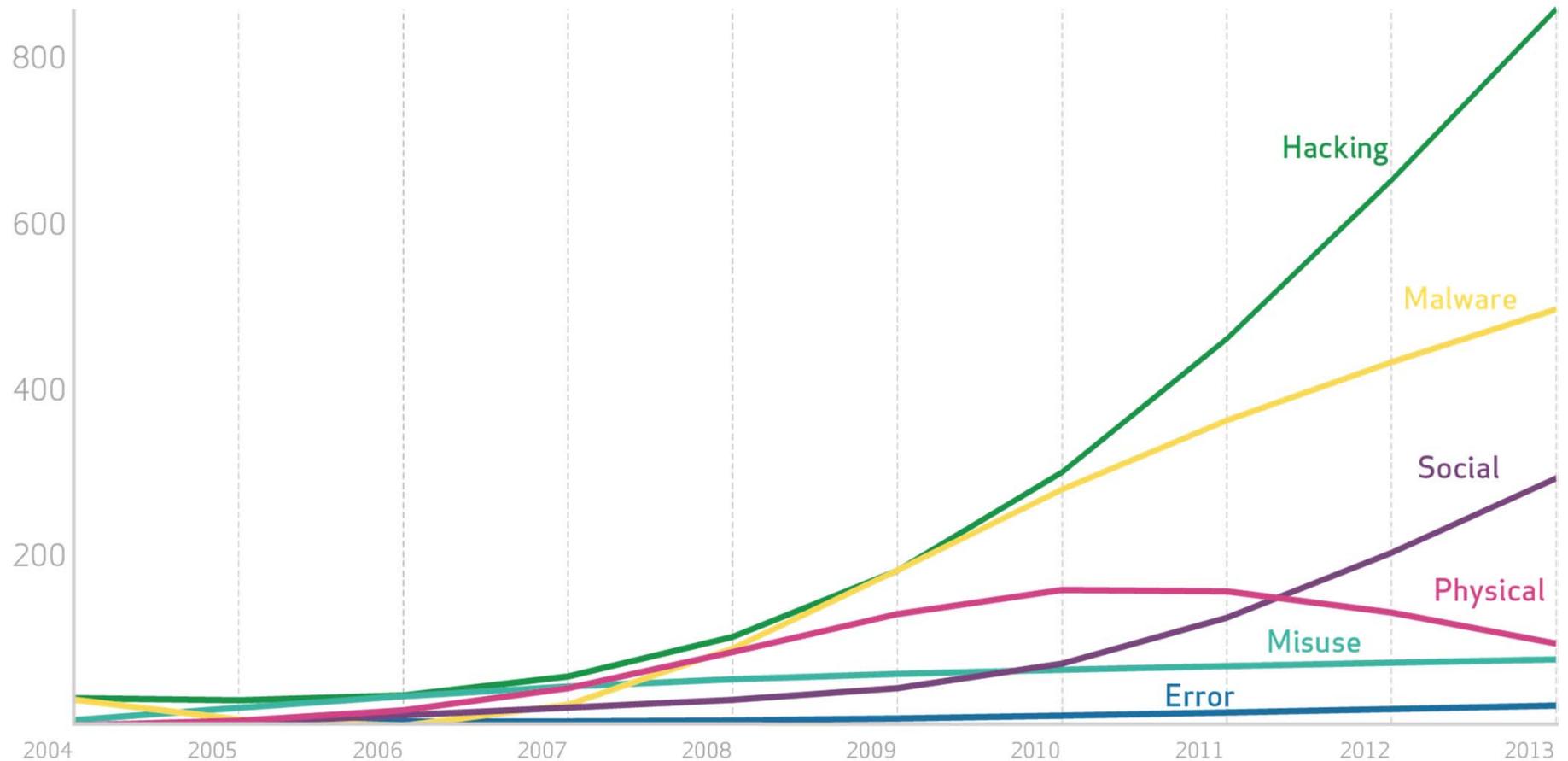
Percent of breaches per threat actor motive over time





Actions over Time

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

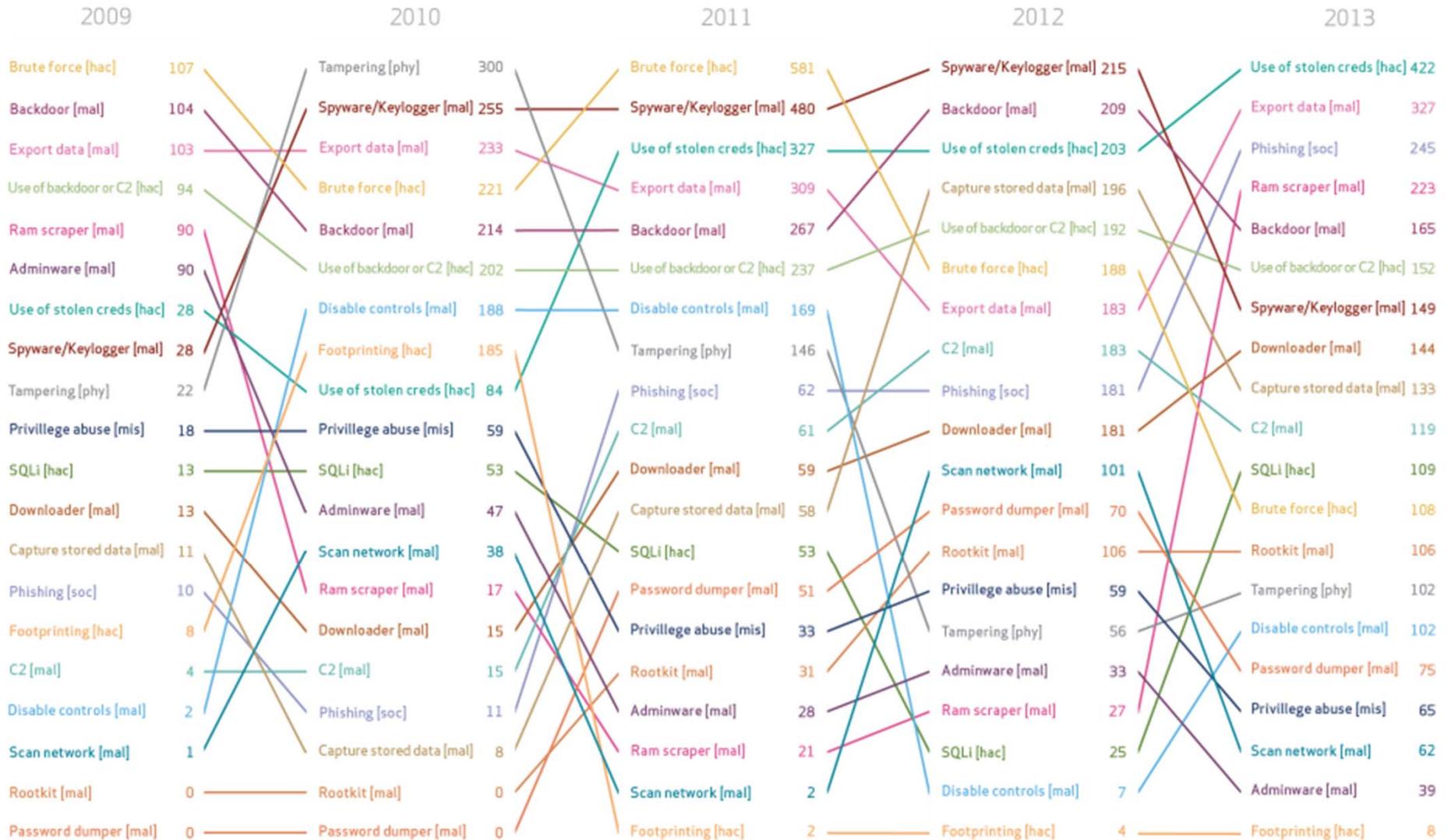


Source: verizonenterprise.com/DBIR/2014



5 Years of Threat Actions:

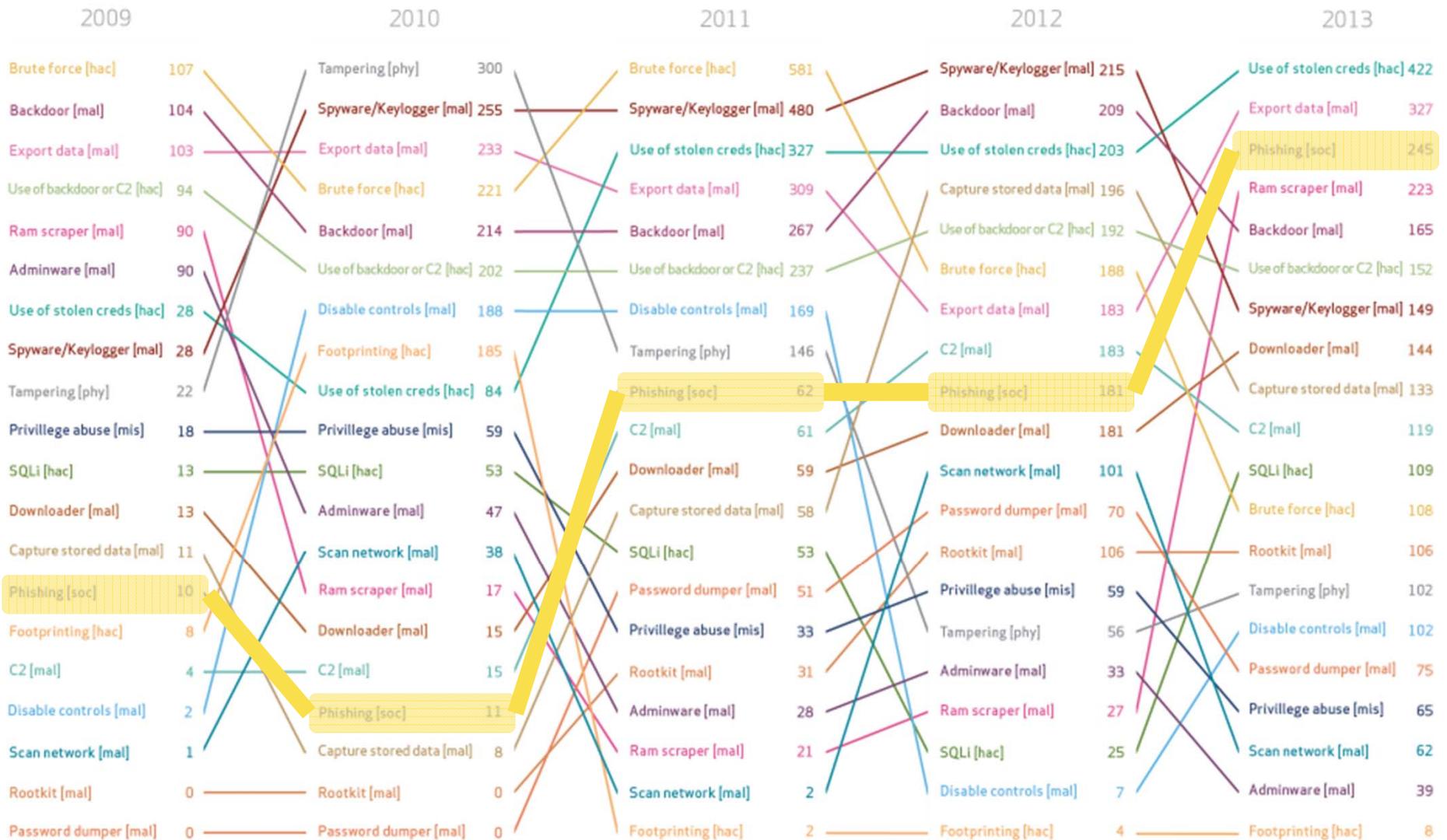
Top 20 varieties of threat actions over time





5 Years of Threat Actions: Phishing

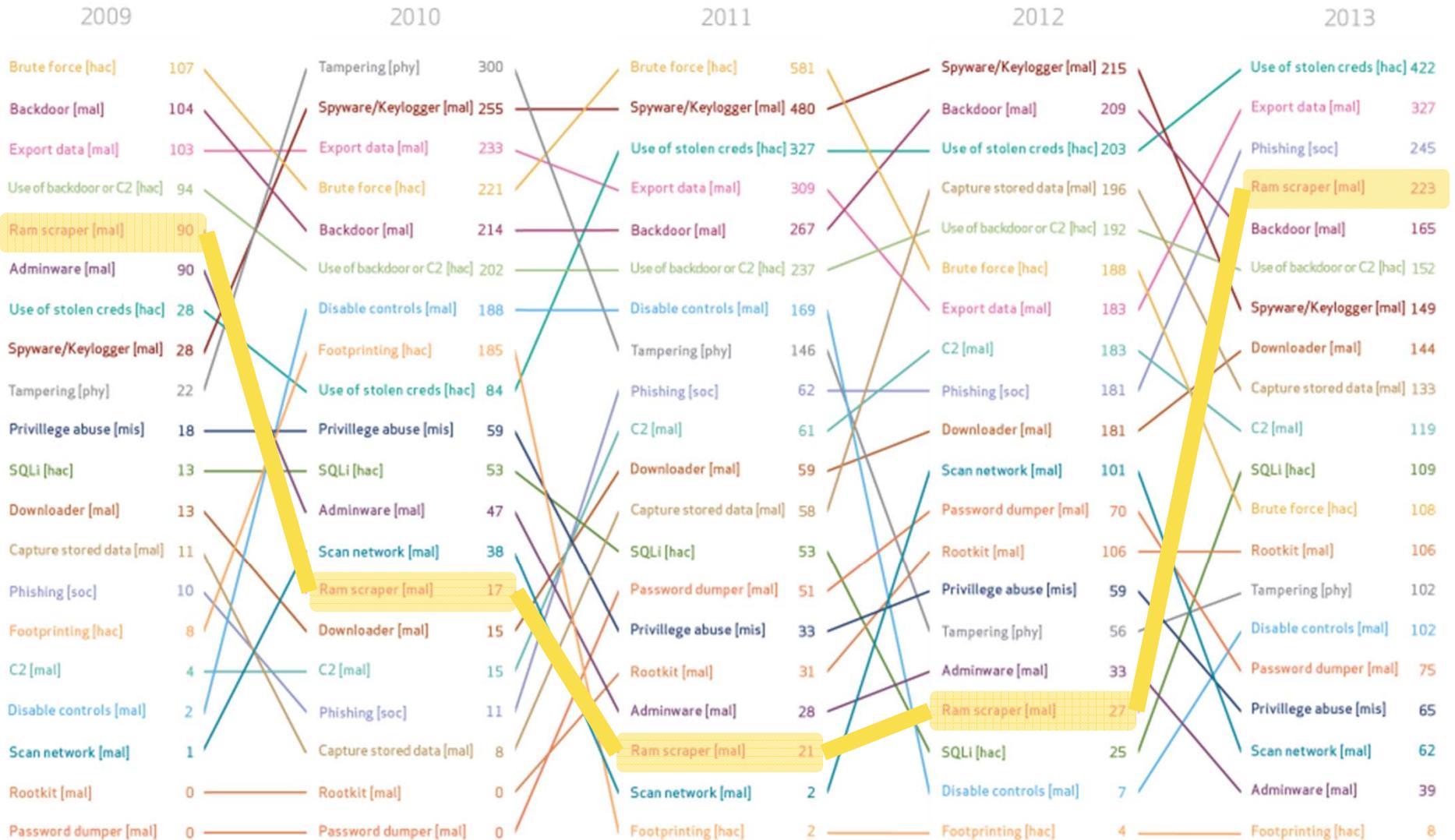
Top 20 varieties of threat actions over time





5 Years of Threat Actions: RAM Scrapers

Top 20 varieties of threat actions over time





5 Years of Threat Actions: RAM Scrapers and Keyloggers

Top 20 varieties of threat actions over time

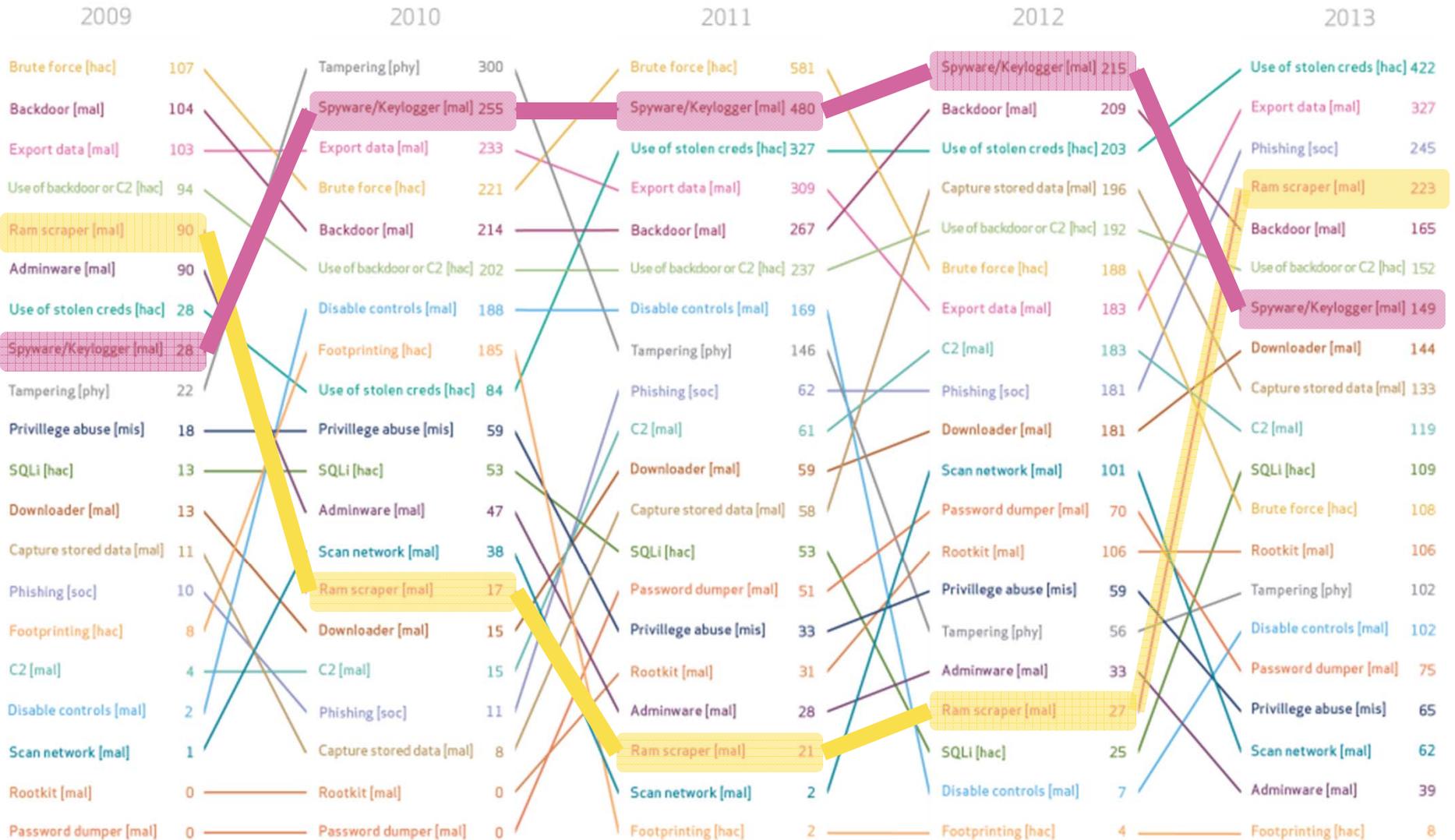
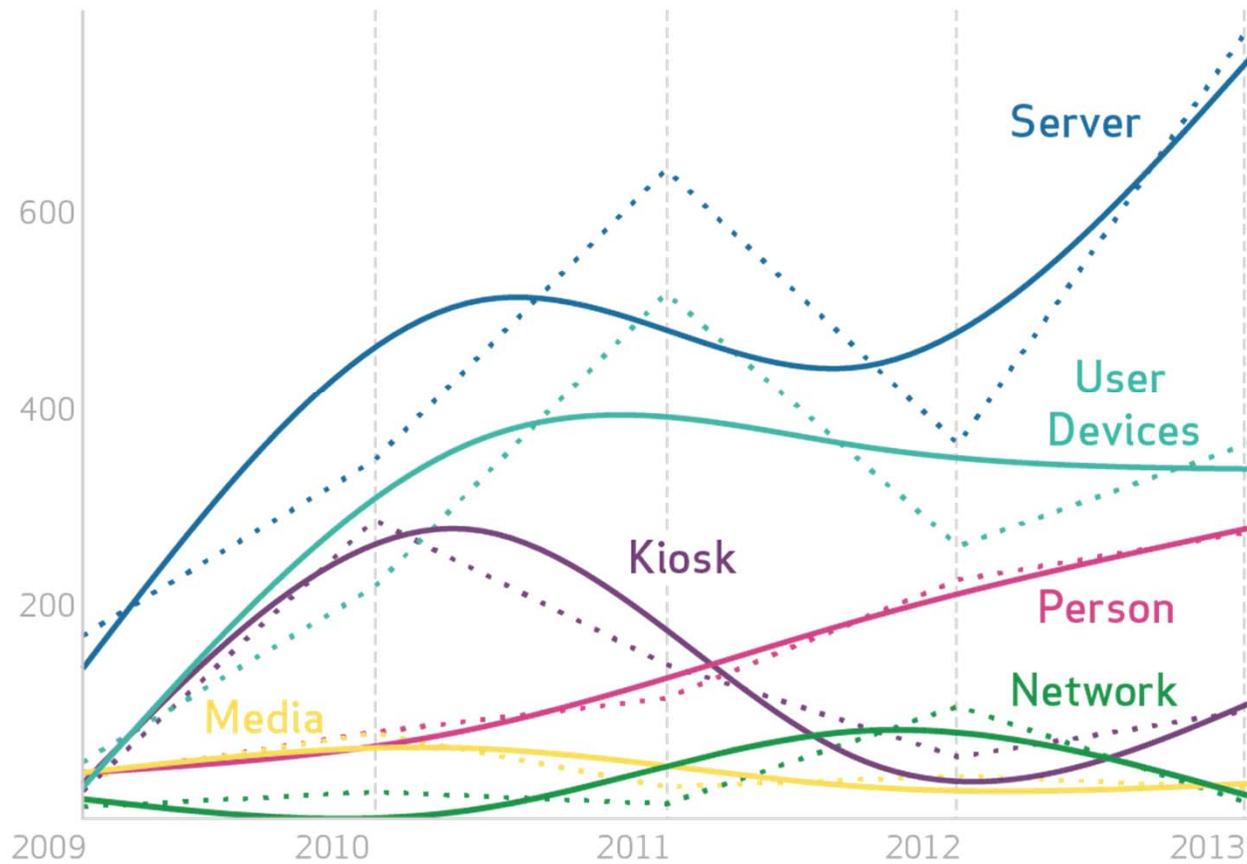




Figure 11.
Number of breaches per asset category over time

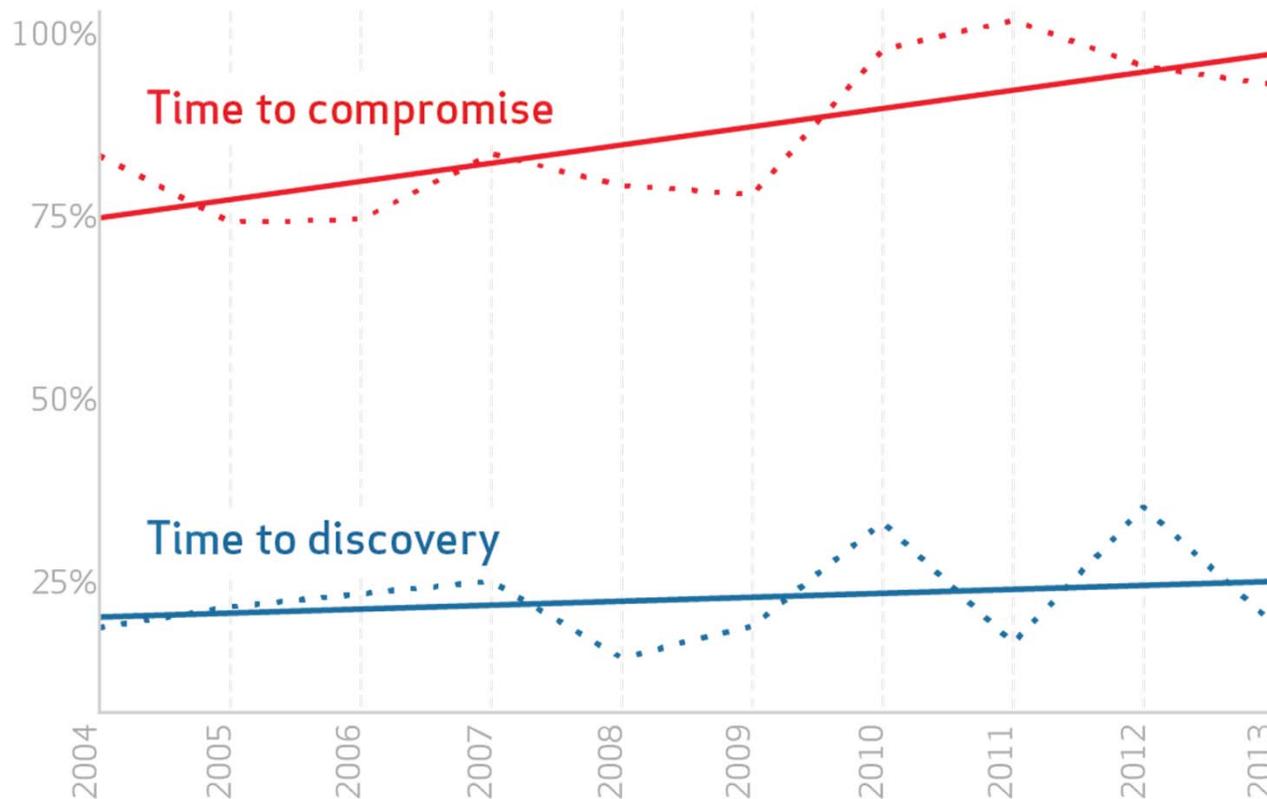


Source: verizonenterprise.com/DBIR/2014



Time to Compromise vs. Time to Discovery

Figure 13.
Percent of breaches where time to compromise (red)/time to discovery (blue) was days or less

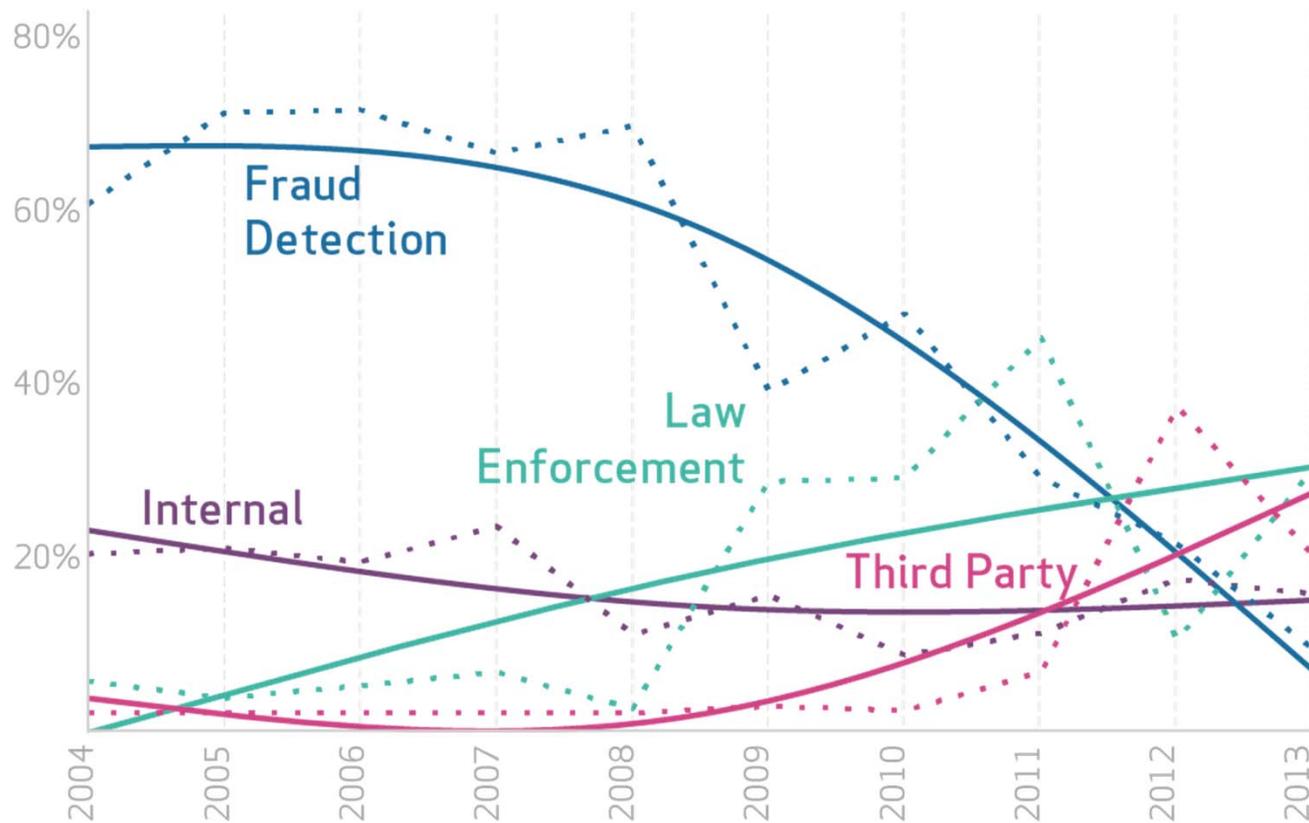


Source: verizonenterprise.com/DBIR/2014



Discovery Methods

Figure 14.
Breach discovery methods over time



Source: verizonenterprise.com/DBIR/2014



Conclusions & Recommendations

Critical Security Controls (SANS Institute)		POS Intrusions	Web App Attacks	Insider Misuse	Physical Theft/Loss	Misc Errors	Craneware	Card Skimmers	Cyber-espionage	DoS Attacks
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								●	
Restricted Access	11.2	●								
	11.5	●								
	11.6	●								
Limited Admin	12.1	●		●						
	12.2	●		●						
	12.3	●								
	12.4	●								
	12.5	●								
Boundary defense	13.1						●		●	
	13.7	●	●				●		●	
	13.10	●								
Audit Logging	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 69.
Critical security controls mapped to incident patterns.

Based on recommendations given in this report.



Conclusions & Recommendations

Critical Security Controls (SANS Institute)	Accommodation [22]	Administrative [56]	Construction [23]	Education [61]	Entertainment [21]	Finance [52]	Healthcare [62]	Information [51]	Management [55]	Manufacturing [31,3]	Mining [21]	Other [61]	Professional [54]	Public [92]	Real Estate [53]	Retail [44,45]	Trade [42]	Transportation [48,4]	Utilities [22]
Software Inventory	2.4																		
Standard Configs	3.1																		
	3.2																		
Malware Defenses	3.8																		
	5.1																		
	5.2																		
Secure Development	5.6																		
	6.4																		
	6.7																		
Backups	6.11																		
	6.2																		
Skilled Staff	9.4																		
	11.2																		
Restricted Access	11.5																		
	11.6																		
	12.1																		
Limited Admin	12.2																		
	12.3																		
	12.4																		
	12.5																		
Boundary defense	13.1																		
	13.7																		
	13.10																		
Audit Logging	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																		

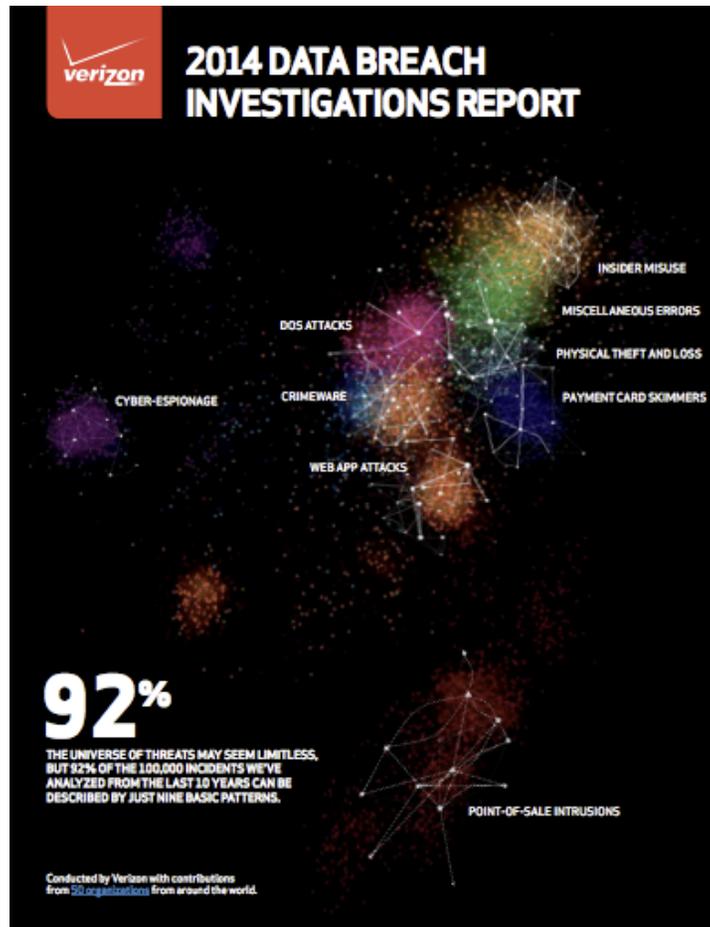
Figure 70.
Prioritization of critical security controls by industry.

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.



Questions?



Christopher Novak
Managing Principal
Verizon RISK Team
chris.novak@verizon.com