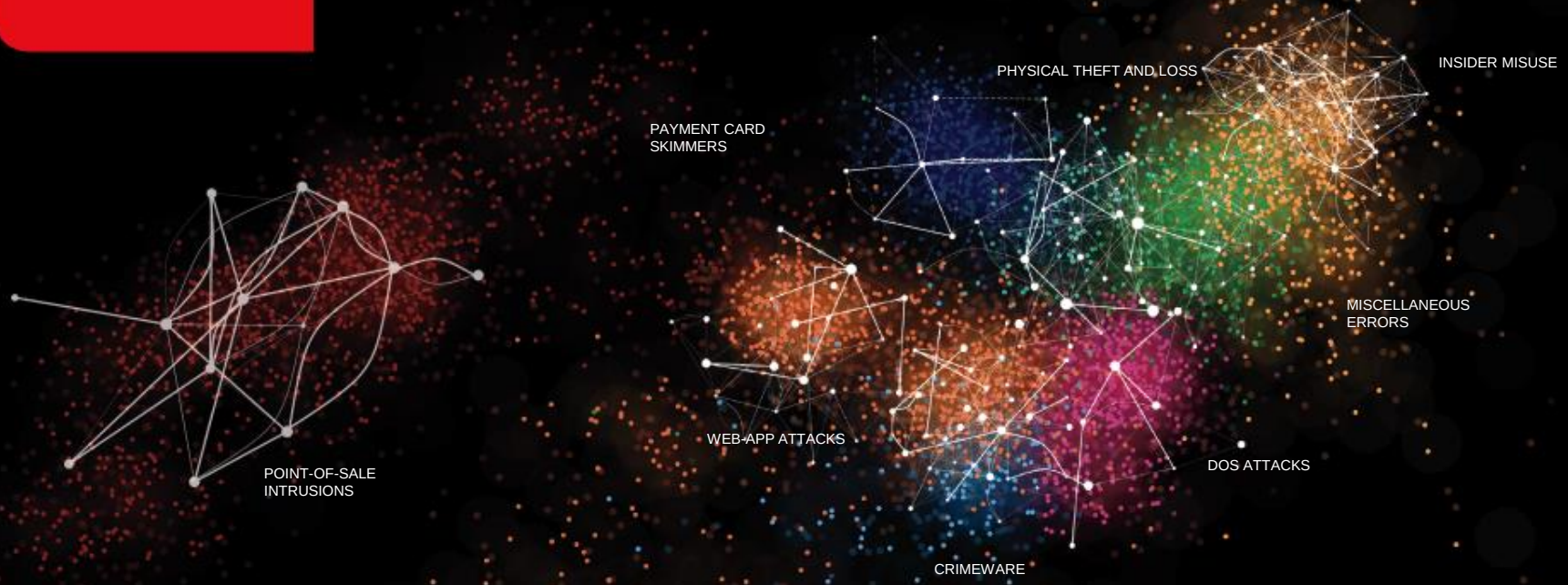
Credit/Debit/Payment Card Security and the Insurability of Large Retailers, …

Michael Carr, Argo Pro
Matt Prevost, ACE USA
Christopher Novak, Verizon Investigative Response

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.

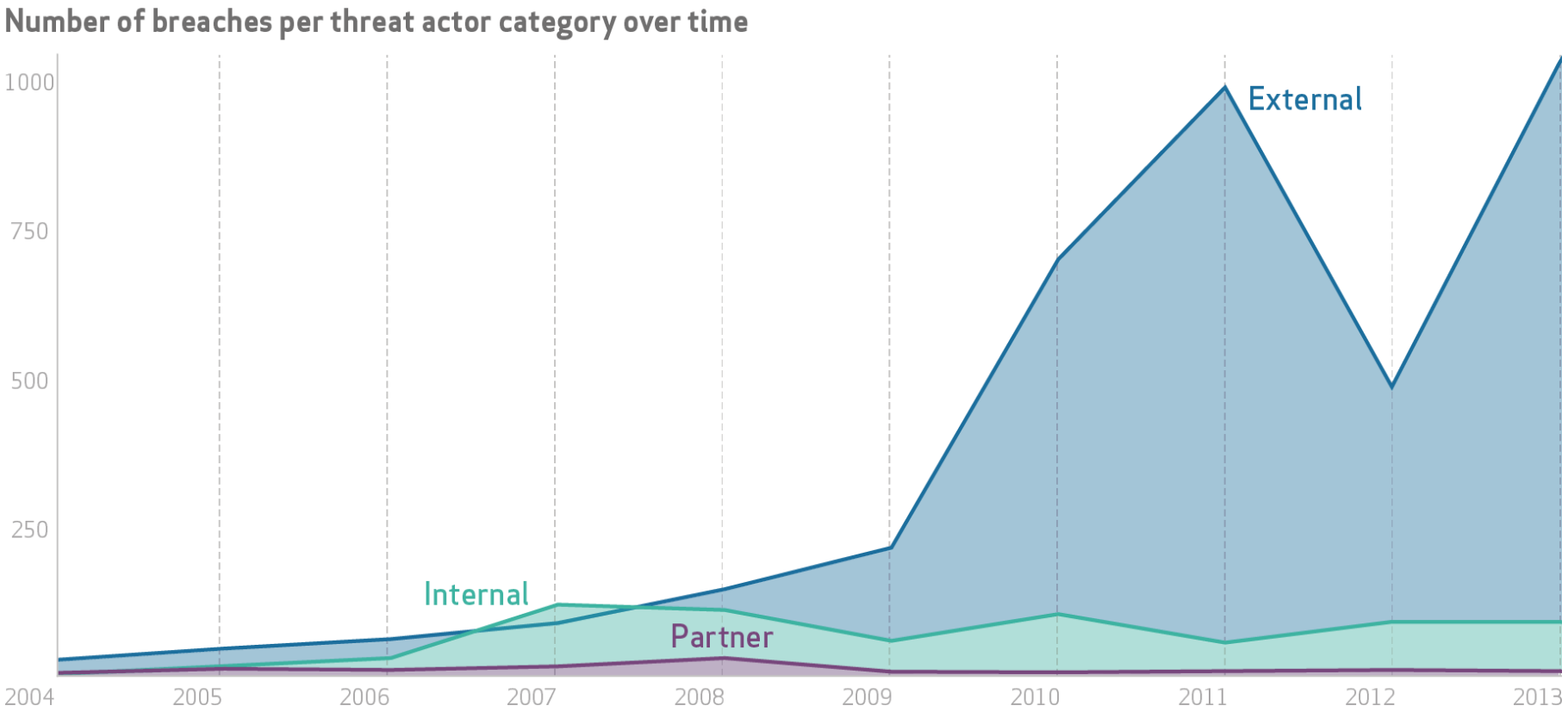
Conducted by Verizon with contributions from 50 organizations from around the world.

DBIR Identifies 9 attack patterns

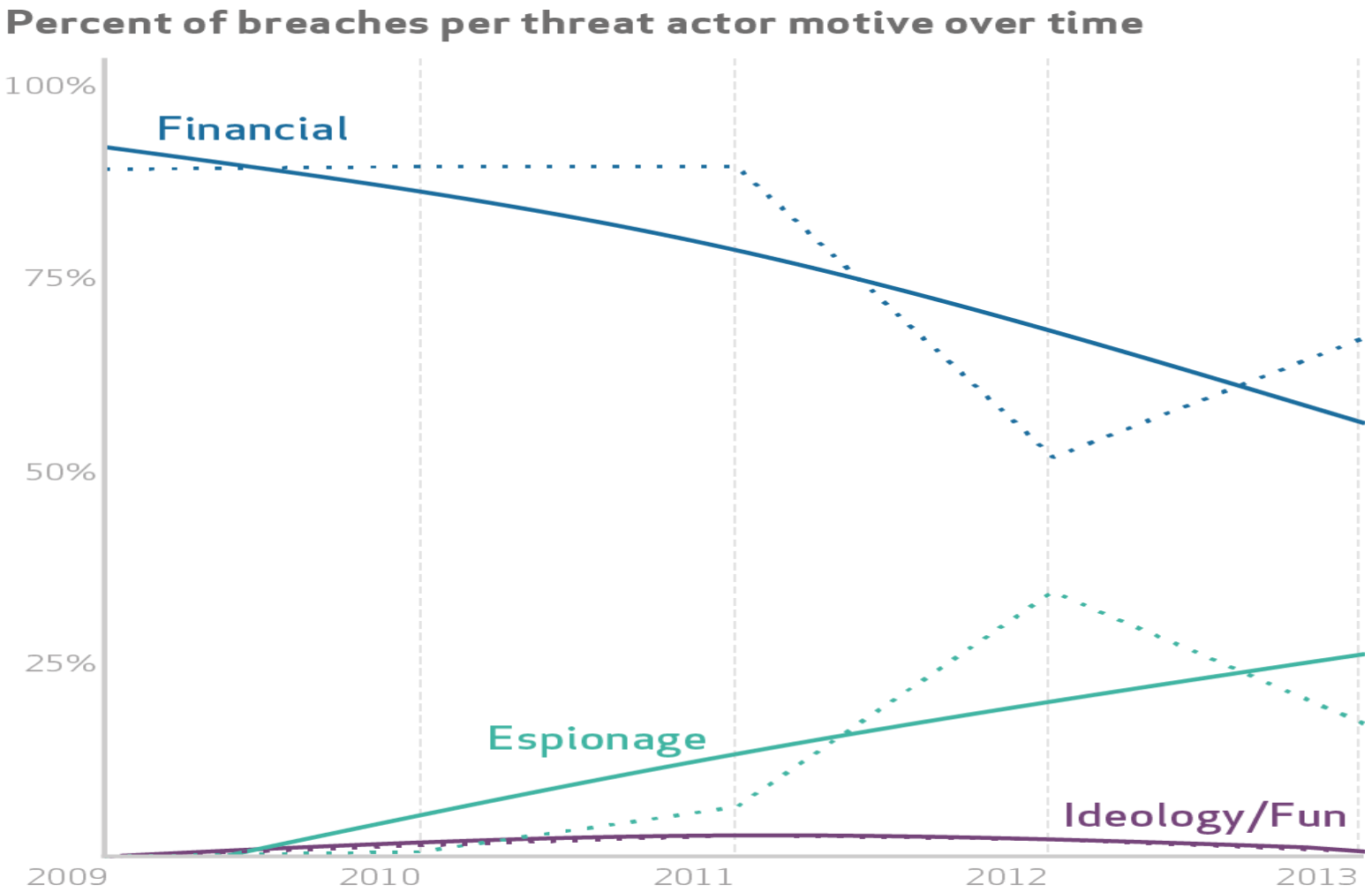
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING 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%

Who's behind the hacks and attacks?



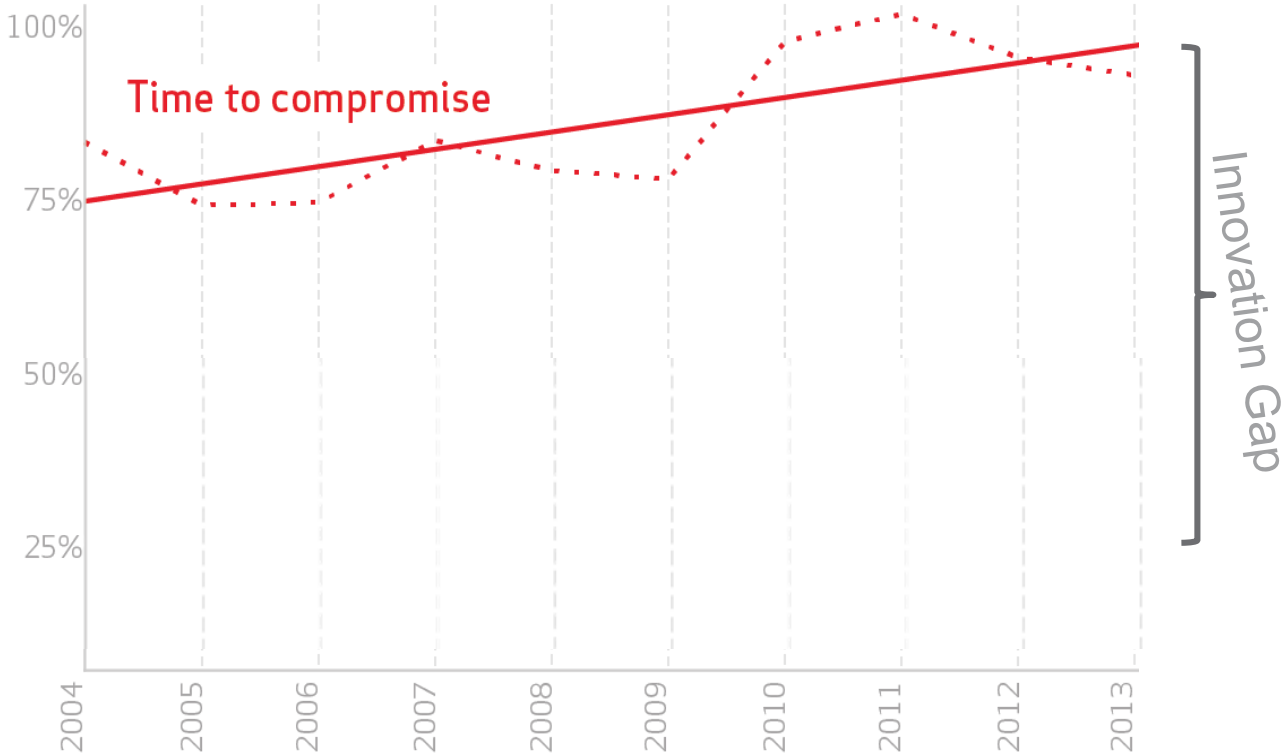
Threat Actor Motivations…



The Innovation Gap

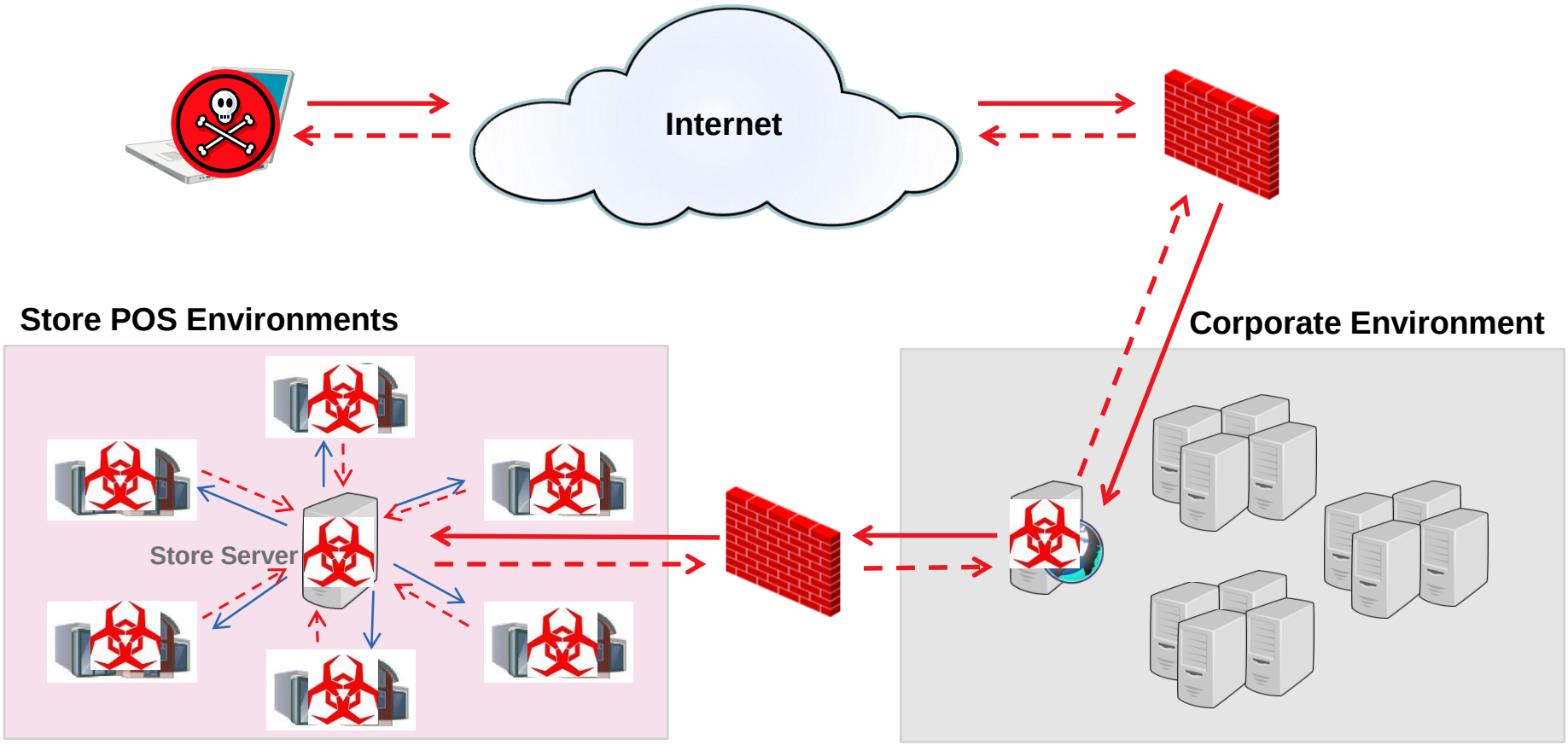
Time to Compromise versus Time to Discovery

- Time to compromise of days or less…
- Time to discovery of days or less…



The bad guys keep getting better—while the good guys struggle to keep up.

Case Study : RAM Scraper

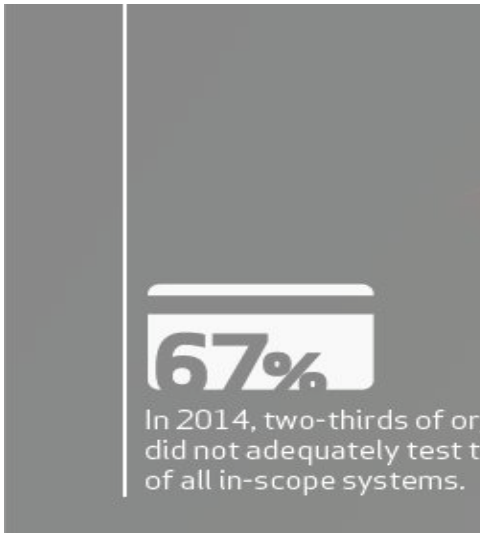


PCI Report 2015

0 IN TEN YEARS

Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach.

One of the criticisms of the PCI DSS, in common with any set of standards, is that focusing on compliance validation could actually be a distraction from achieving and maintaining genuine security. But for most companies the DSS provides a useful baseline. While validation is no assurance of security, not being compliant is pretty much a guarantee that you're not secure.



If you can take systems out of scope you can avoid the cost and effort of involving them in PCI DSS compliance activities, both in terms of regular activities (such as patching or vulnerability scans) and the annual assessment.

PCI Report 2015

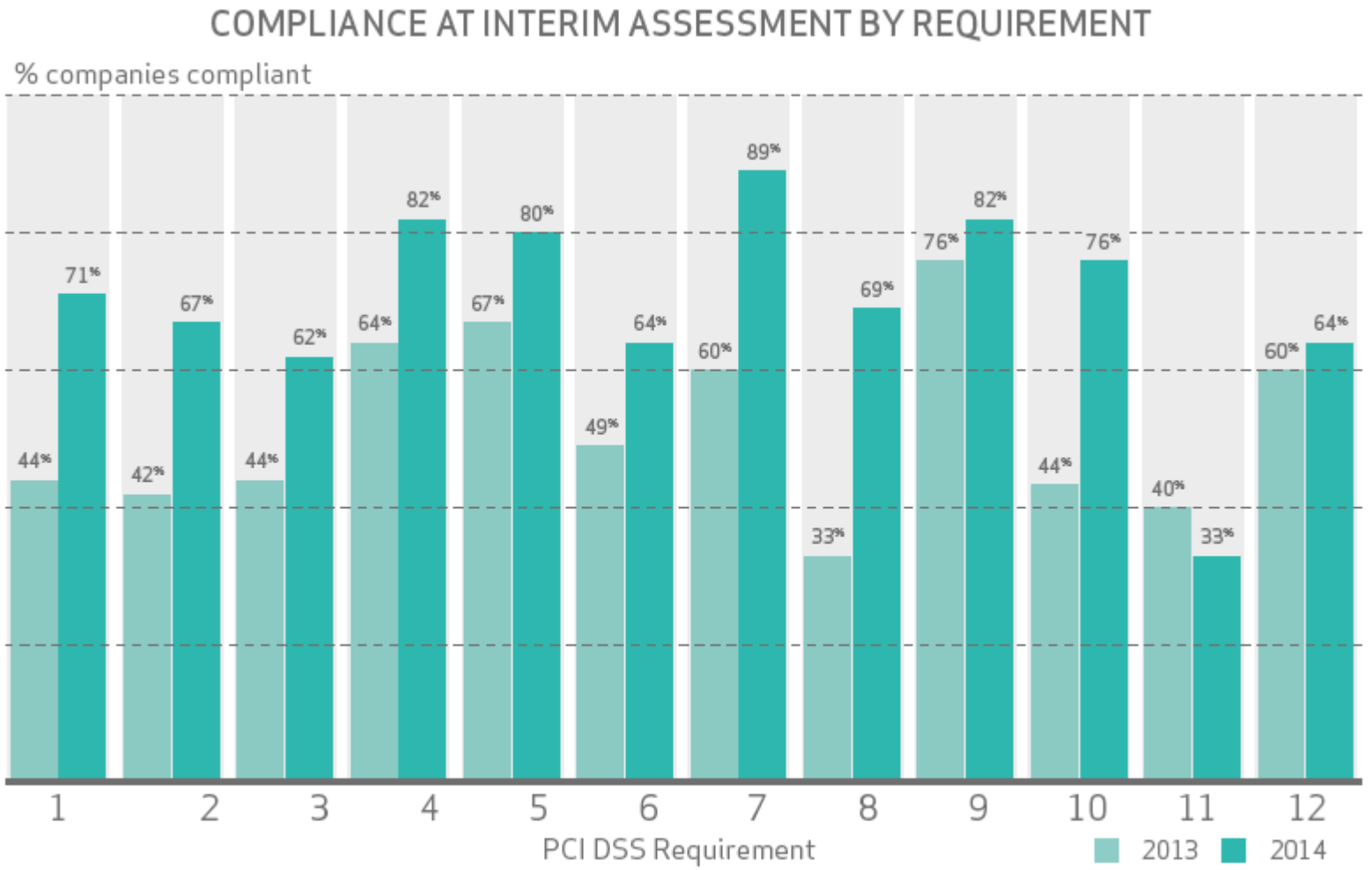


Figure 3: Compliance at interim assessment by Requirement, comparison of 2013 and 2014

PCI Report 2015

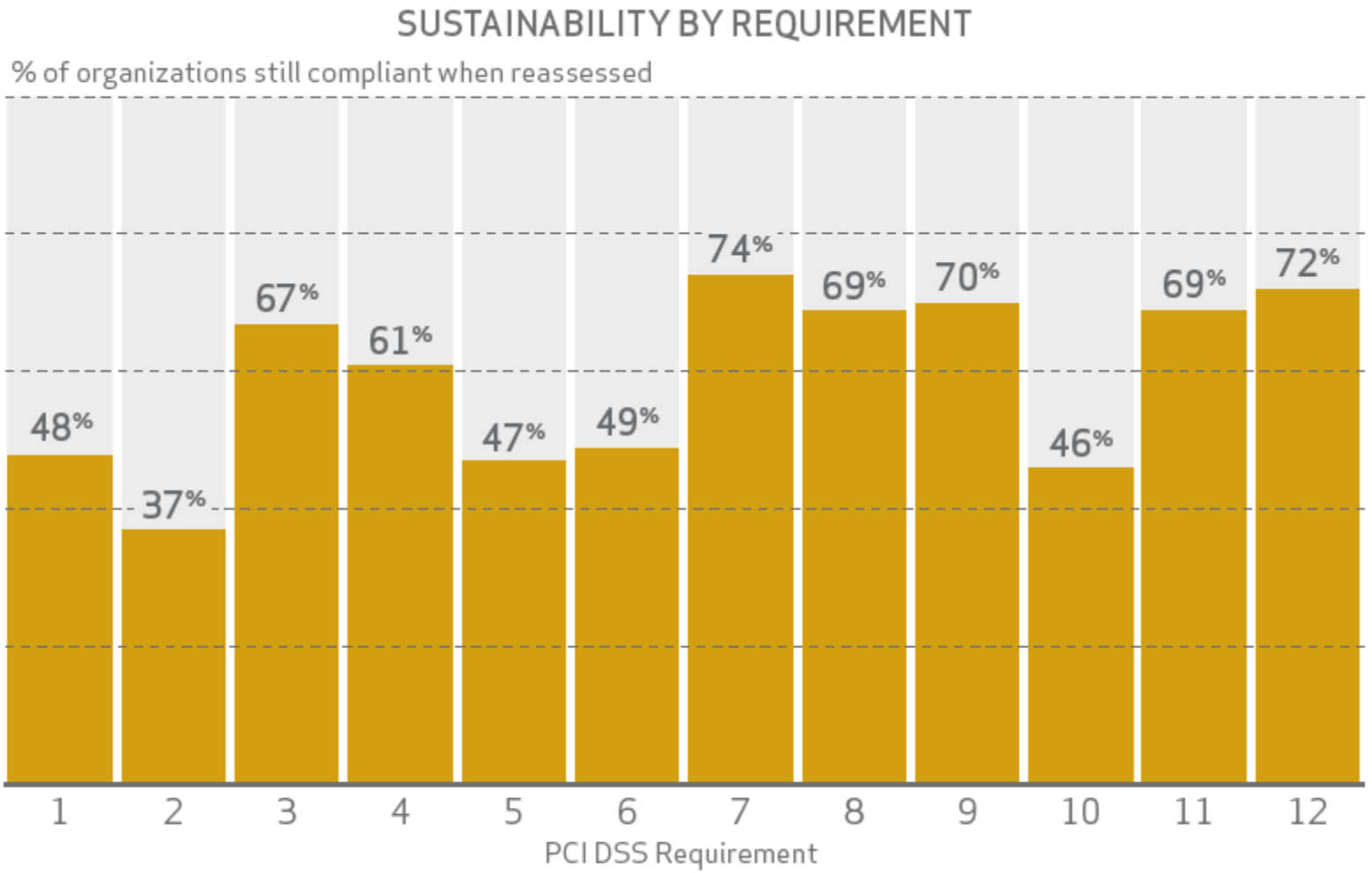


Figure 21: Number of companies compliant at interim assessment following successful FRoC, 2013–2014

PCI Report 2015

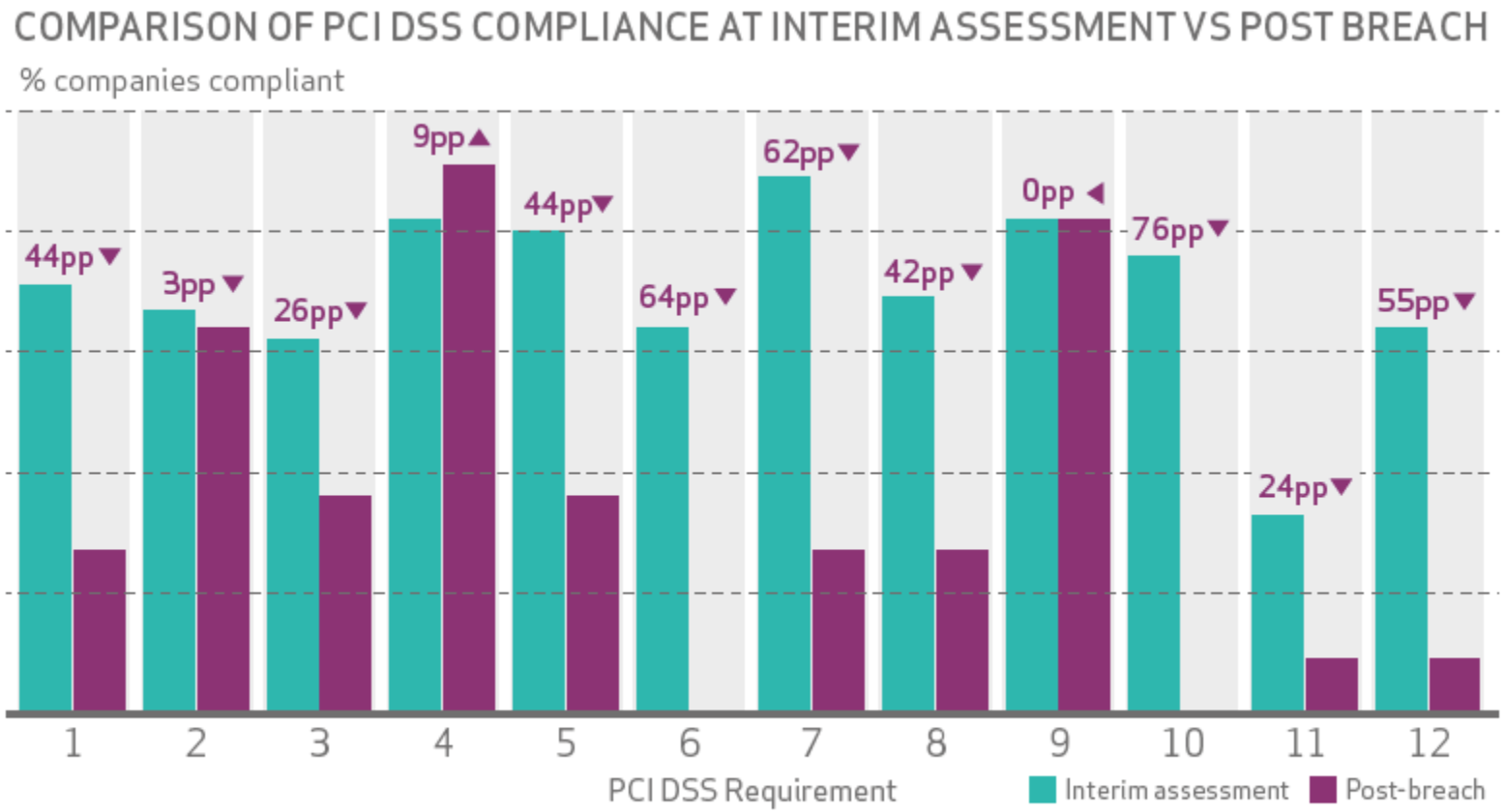


Figure 8: Compliance observed during QSA assessments and PFI post breach assessments, 2014 dataset

Coming soon… DBIR 2015!

Q&A / Discussion…

Sign up to get your advanced copy:

www.VerizonEnterprise.com/DBIR

Michael Carr, Argo Pro

Matt Prevost, ACE USA

Christopher Novak, Verizon Investigative Response