Phishing Freakonomics (aka “Picking Winners”)

Russell Butturini

Senior Information Security Architect, Top 20 CPA Firm

Defcon 27 Packet Hacking Village

(Not a picture of me)

-Senior security architect and head of all things IT security along with my governance and compliance dictatress at a top 20 CPA/financial services firm.

-@tcstoolhax0r on Twitter

-Presenter at various Bsides, Derbycon, PHV, etc.

-Occasionally releases poorly written Python code that does cool things.

-Everything said in this talk is mine and doesn’t represent the views of my employer.

Why give this talk?

-”Phishing always works”

-”Users are stupid”

-”People are the weakest link”

-”It only takes one”

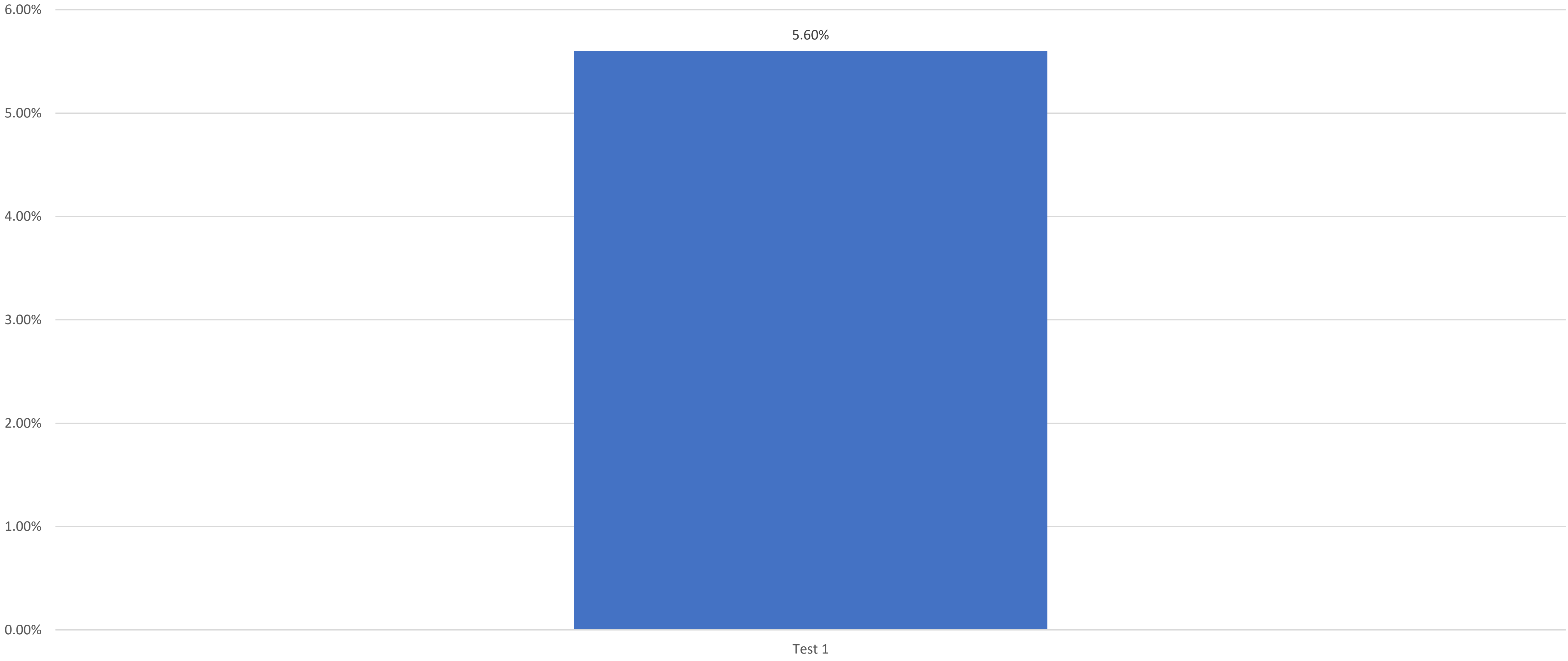
The Story

-No previous training and awareness program

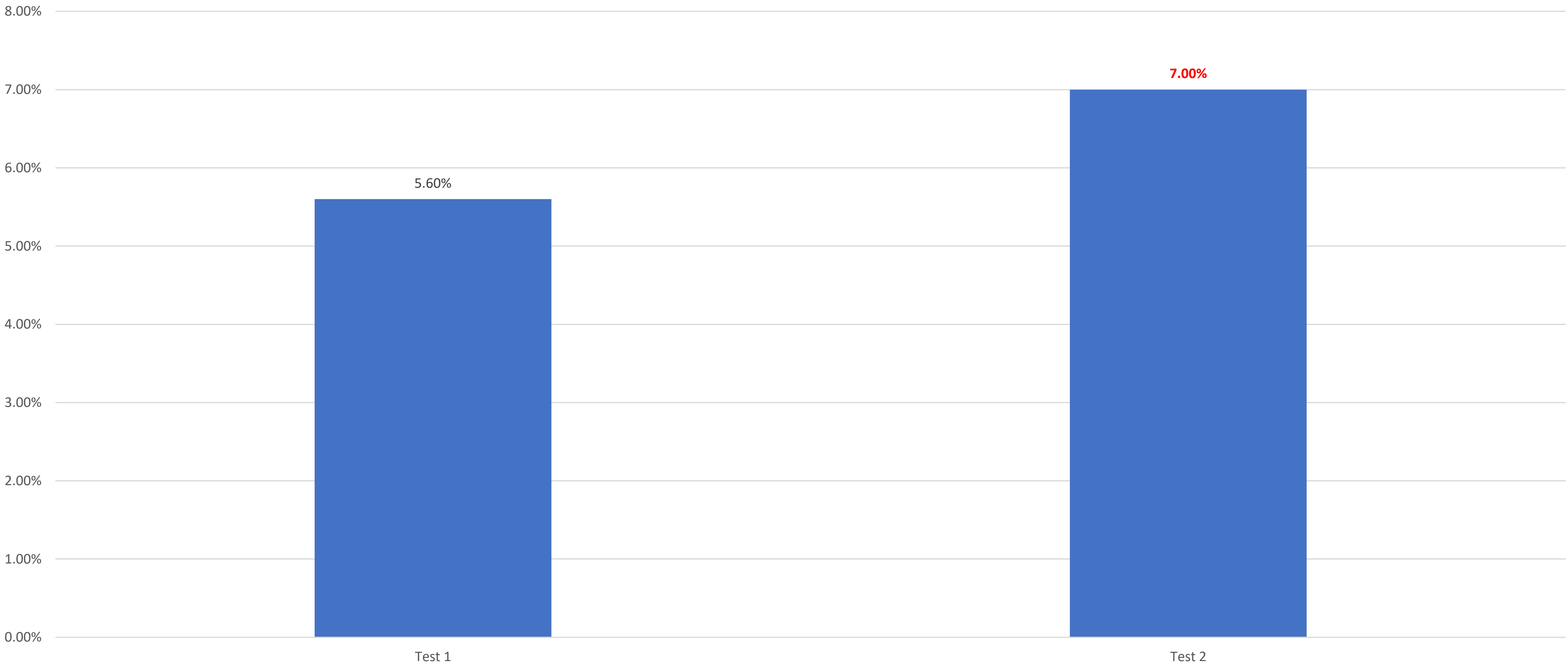
-Never done phish testing

-Unstructured reporting for email threats, lack of centralized security awareness resources for end users

The story



The story



A New Approach

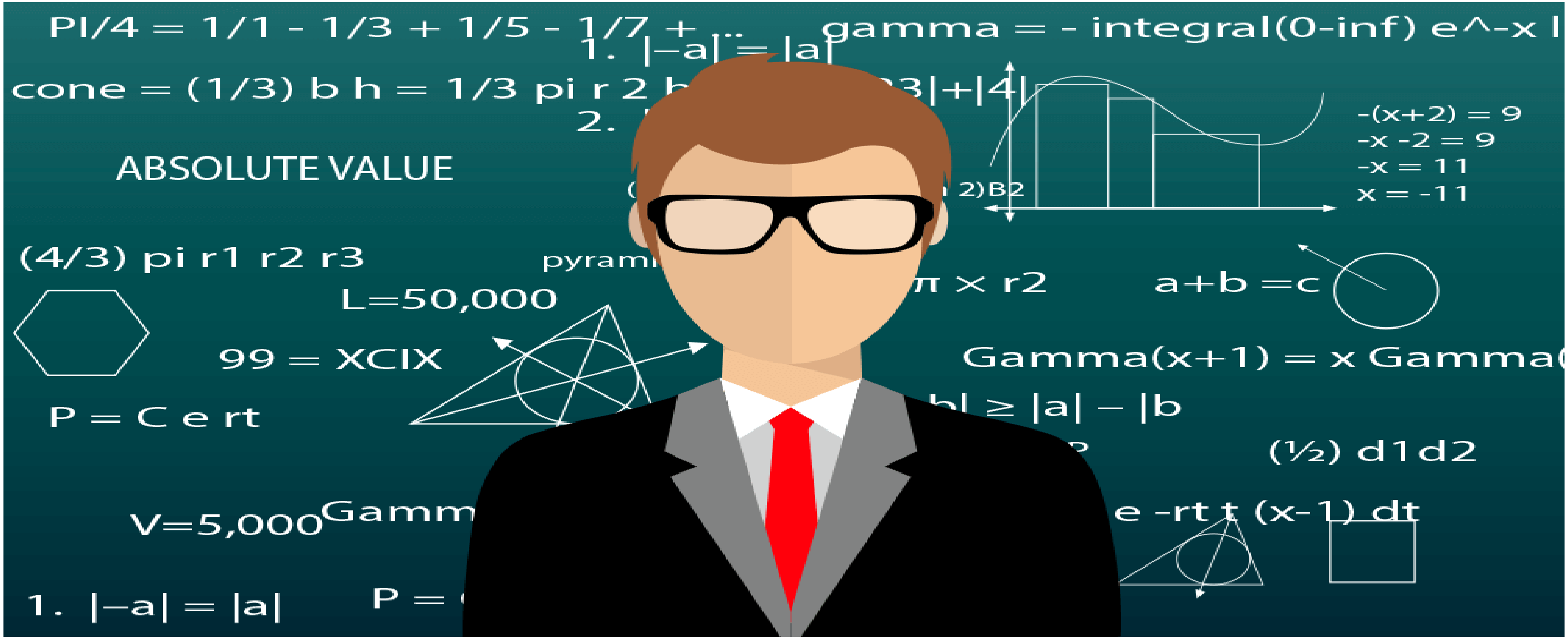
-Treat the problem like a software or code issue.

-Figure out why people are “vulnerable”.

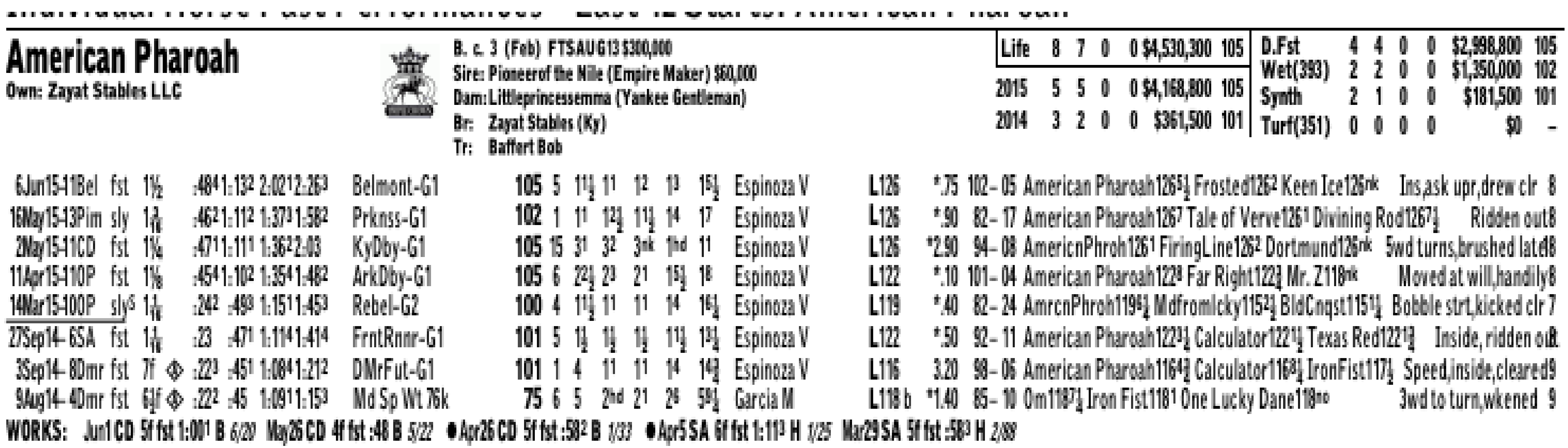
-How do we patch them???

-USE THE DATA IN FRONT OF US

Warning: Not a Data Scientist



I do this instead…



Individual Horse Past Performances – Last 12 Starts: American Pharoah

American Pharoah

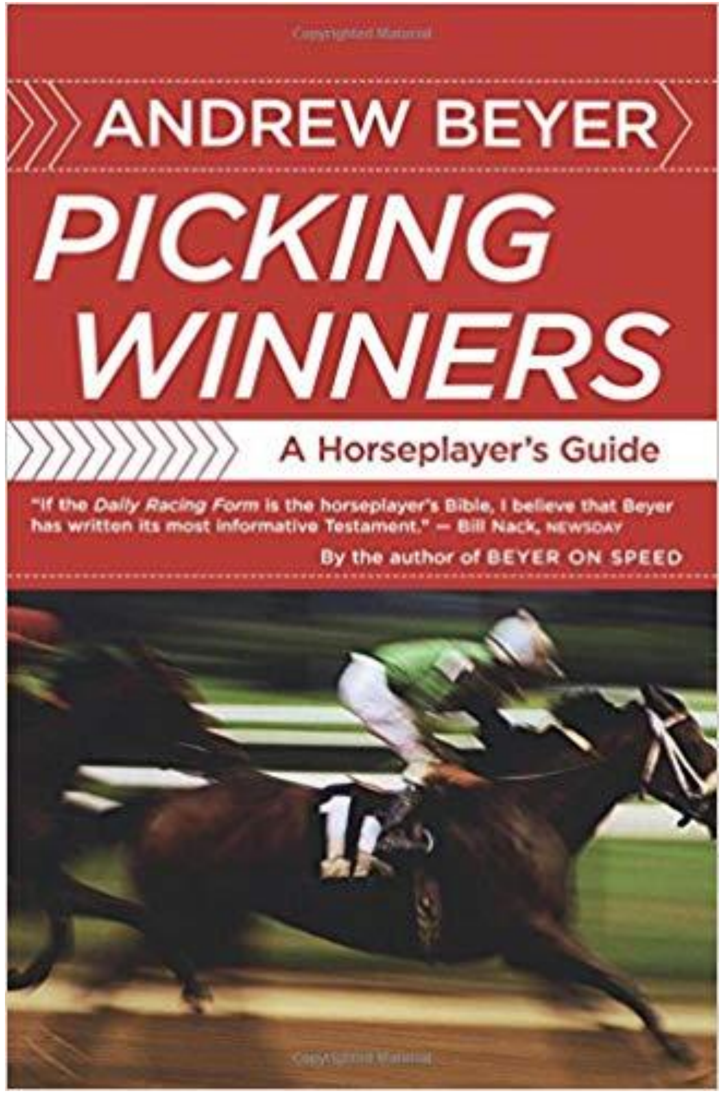
Own: Zayat Stables LLC

B. c. 3 (Feb) FTSAUG13 $300,000
Sire: Pioneerof the Nile (Empire Maker) $60,000
Dam: Littleprincessemma (Yankee Gentleman)
Br: Zayat Stables (Ky)
Tr: Baffert Bob

Life	8	7	0	0	$4,530,300	105	D.Fst	4	4	0	0	$2,998,800	105
							Wet(393)	2	2	0	0	$1,350,000	102
2015	5	5	0	0	$4,168,800	105	Synth	2	1	0	0	$181,500	101
2014	3	2	0	0	$361,500	101	Turf(351)	0	0	0	0	$0	–

6Jun15-11Bel	fst	$1\frac{1}{2}$		$:48^4$	$1:13^2$	$2:02^1$	$2:26^3$	Belmont-G1	105	5	$1^{1\frac{1}{2}}$	1^1	1^2	1^3	$1^{5\frac{1}{2}}$	Espinoza V	L126	*.75	102– 05	American Pharoah126$^{5\frac{1}{2}}$ Frosted126^2 Keen Ice126^{nk}	Ins,ask upr,drew clr	8
16May15-13Pim	sly	$1\frac{3}{16}$		$:46^2$	$1:11^2$	$1:37^3$	$1:58^2$	Prknss-G1	102	1	1^1	$1^{2\frac{1}{2}}$	$1^{1\frac{1}{2}}$	1^4	1^7	Espinoza V	L126	*.90	82– 17	American Pharoah126^7 Tale of Verve126^1 Divining Rod126$^{7\frac{1}{2}}$	Ridden out	8
2May15-11CD	fst	$1\frac{1}{4}$		$:47^1$	$1:11^1$	$1:36^2$	2:03	KyDby-G1	105	15	3^1	3^2	3^{nk}	1^{hd}	1^1	Espinoza V	L126	*2.90	94– 08	AmericnPhroh126^1 FiringLine126^2 Dortmund126^{nk}	5wd turns,brushed late	18
11Apr15-11OP	fst	$1\frac{1}{8}$		$:45^4$	$1:10^2$	$1:35^4$	$1:48^2$	ArkDby-G1	105	6	$2^{2\frac{1}{2}}$	2^3	2^1	$1^{5\frac{1}{2}}$	1^8	Espinoza V	L122	*.10	101– 04	American Pharoah122^8 Far Right122$^{\frac{3}{4}}$ Mr. Z118^{nk}	Moved at will,handily	8
14Mar15-10OP	sly^S	$1\frac{1}{16}$		$:24^2$	$:49^3$	$1:15^1$	$1:45^3$	Rebel-G2	100	4	$1^{1\frac{1}{2}}$	1^1	1^1	1^4	$1^{6\frac{1}{4}}$	Espinoza V	L119	*.40	82– 24	AmrcnPhroh119$^{6\frac{1}{4}}$ Mdfromlcky115$^{2\frac{1}{4}}$ BldCnqst115$^{1\frac{1}{4}}$	Bobble strt,kicked clr	7
27Sep14- 6SA	fst	$1\frac{1}{16}$		:23	$:47^1$	$1:11^4$	$1:41^4$	FrntRnnr-G1	101	5	$1^{\frac{1}{2}}$	$1^{\frac{1}{2}}$	$1^{\frac{1}{2}}$	$1^{1\frac{1}{2}}$	$1^{3\frac{1}{4}}$	Espinoza V	L122	*.50	92– 11	American Pharoah122$^{3\frac{1}{4}}$ Calculator122$^{1\frac{1}{2}}$ Texas Red122$^{1\frac{3}{4}}$	Inside, ridden out	8
3Sep14- 8Dmr	fst	7f	◈	$:22^3$	$:45^1$	$1:08^4$	$1:21^2$	DMrFut-G1	101	1	4	1^1	1^1	1^4	$1^{4\frac{3}{4}}$	Espinoza V	L116	3.20	98– 06	American Pharoah116$^{4\frac{3}{4}}$ Calculator116$^{8\frac{1}{4}}$ IronFist117$^{\frac{1}{2}}$	Speed,inside,cleared	9
9Aug14- 4Dmr	fst	$6\frac{1}{2}$f	◈	$:22^2$	:45	$1:09^1$	$1:15^3$	Md Sp Wt 76k	75	6	5	2^{hd}	2^1	2^6	$5^{9\frac{1}{4}}$	Garcia M	L118 b	*1.40	85– 10	Om118$^{7\frac{1}{2}}$ Iron Fist118^1 One Lucky Dane118^{no}	3wd to turn,wkened	9

WORKS: Jun1 CD 5f fst 1:00^1 B *6/20* May26 CD 4f fst :48 B *5/22* ●Apr26 CD 5f fst :58^2 B *1/33* ●Apr5 SA 6f fst 1:11^3 H *1/25* Mar29 SA 5f fst :58^3 H *2/88*



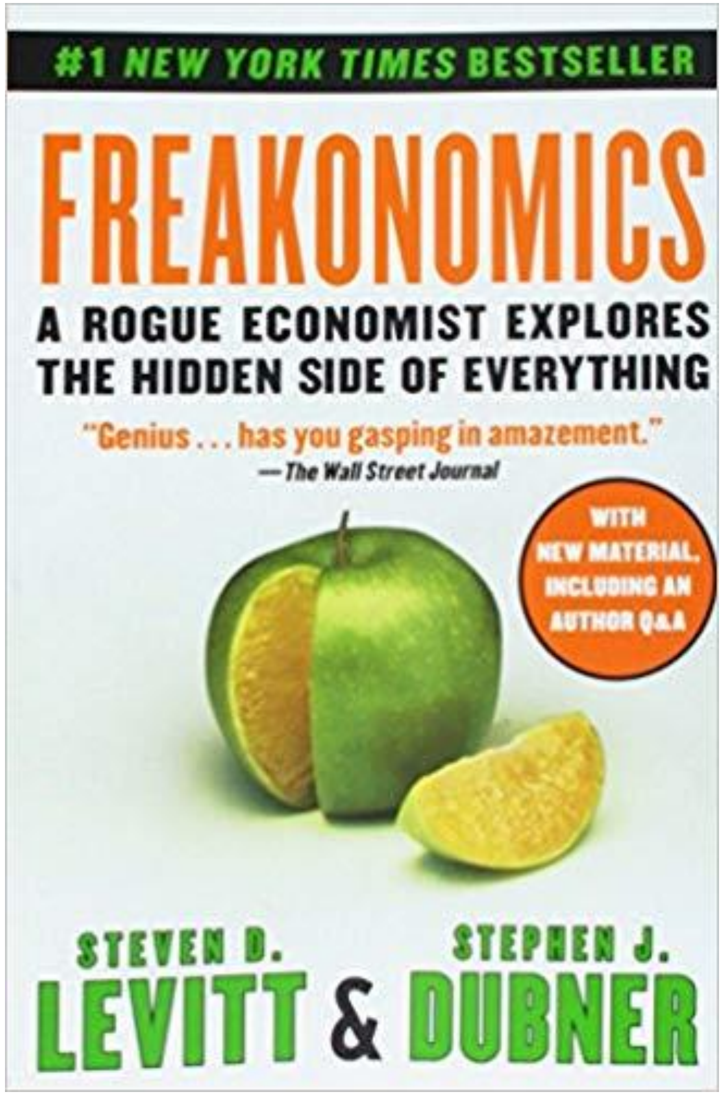
ANDREW BEYER

PICKING WINNERS

A Horseplayer's Guide

"If the *Daily Racing Form* is the horseplayer's Bible, I believe that Beyer has written its most informative Testament." — Bill Nack, NEWSDAY

By the author of BEYER ON SPEED



#1 NEW YORK TIMES BESTSELLER

FREAKONOMICS

A ROGUE ECONOMIST EXPLORES THE HIDDEN SIDE OF EVERYTHING

"Genius . . . has you gasping in amazement."
—*The Wall Street Journal*

WITH NEW MATERIAL, INCLUDING AN AUTHOR Q&A

STEVEN D. LEVITT & STEPHEN J. DUBNER

Key Questions

-Can we use various data points ("angles") to predict which users have a higher likelihood of falling victim to a phishing attack than others?

-Are there seemingly unrelated factors that should be examined to find patterns of phishing failures?

HUMAN NATURE
DO NOT CLIMB, PLAY ON, AND AROUND PIPE
SUMMED UP IN ONE PICTURE

Data Points

-10 years of phishing test results and training data from 3 different large environments.

-Phishing related security incidents

-HR data

-Survey results

-Miscellaneous data

-Sample size of ~3,200 fails; not all correlations had the same amount of data

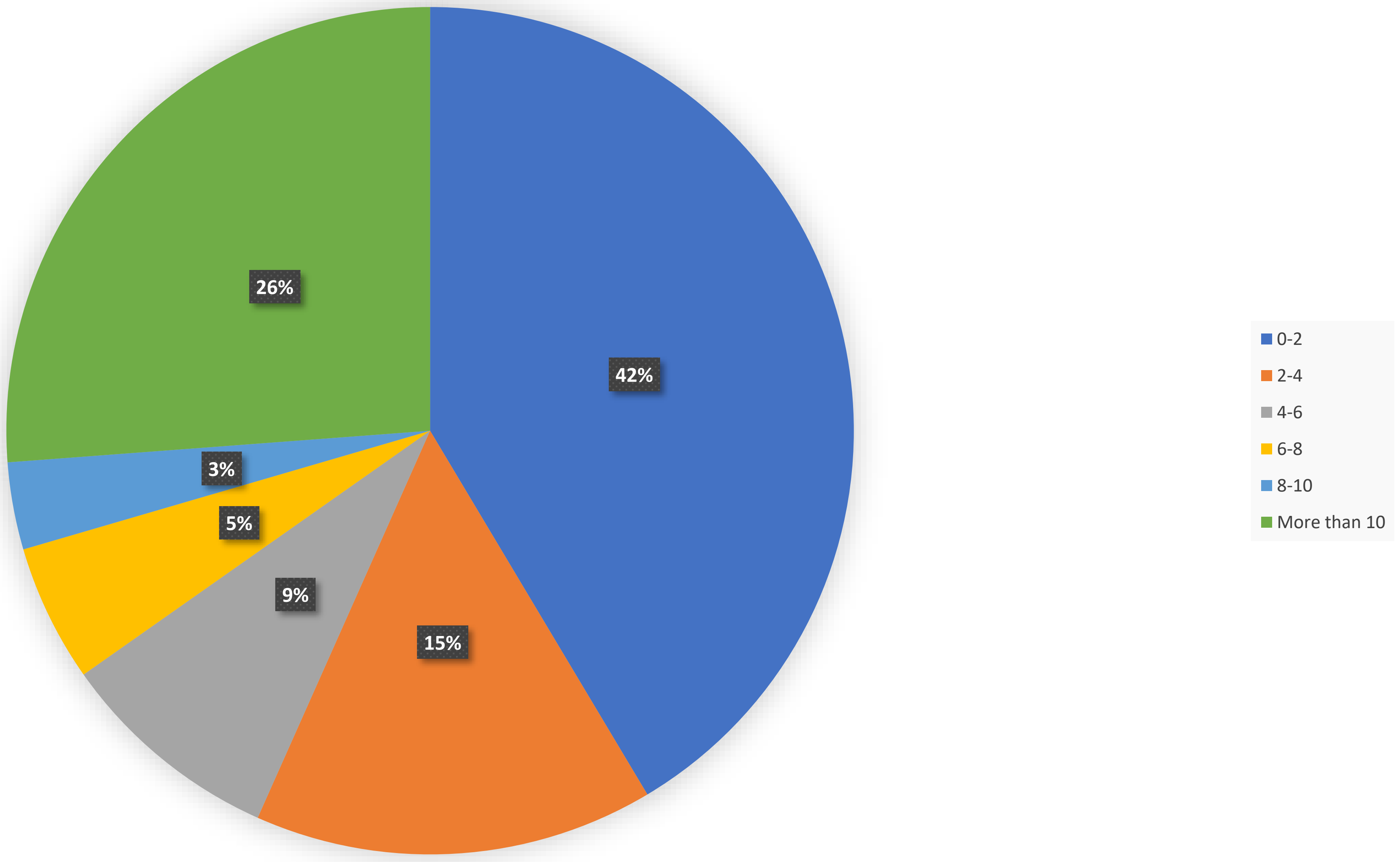
Elasticsearch/Kibana

-**FREE**

-Allowed for analyzing dissimilar events with different data points quickly.

-Simple to populate using Python

Failures by Years of Experience



-Subdividing the 10+ group further, 40% of the failures came from 22+ years of experience.

-New grads explained spikes….Timing changes risk!

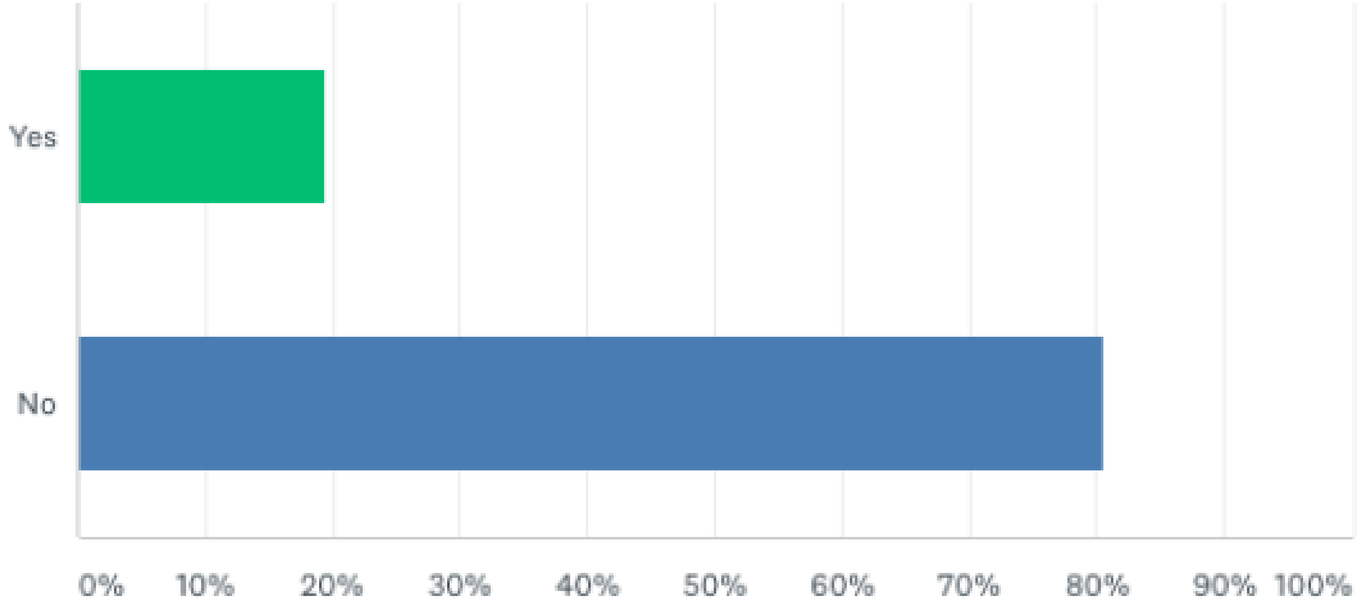
Action: Have office managers work with “elderly” colleagues and new hires to ensure they not only complete but understand security awareness. Add additional content to new hire training.

Survey

-Did you previous employer conduct security awareness training or phishing tests?

-Do you feel internal mass communications (i.e. emails from IT, HR, benefits) are easy to identify as legitimate?

Did your previous employer conduct security awareness training or phishing tests?



-Not enough employers are investing time in training people!!!

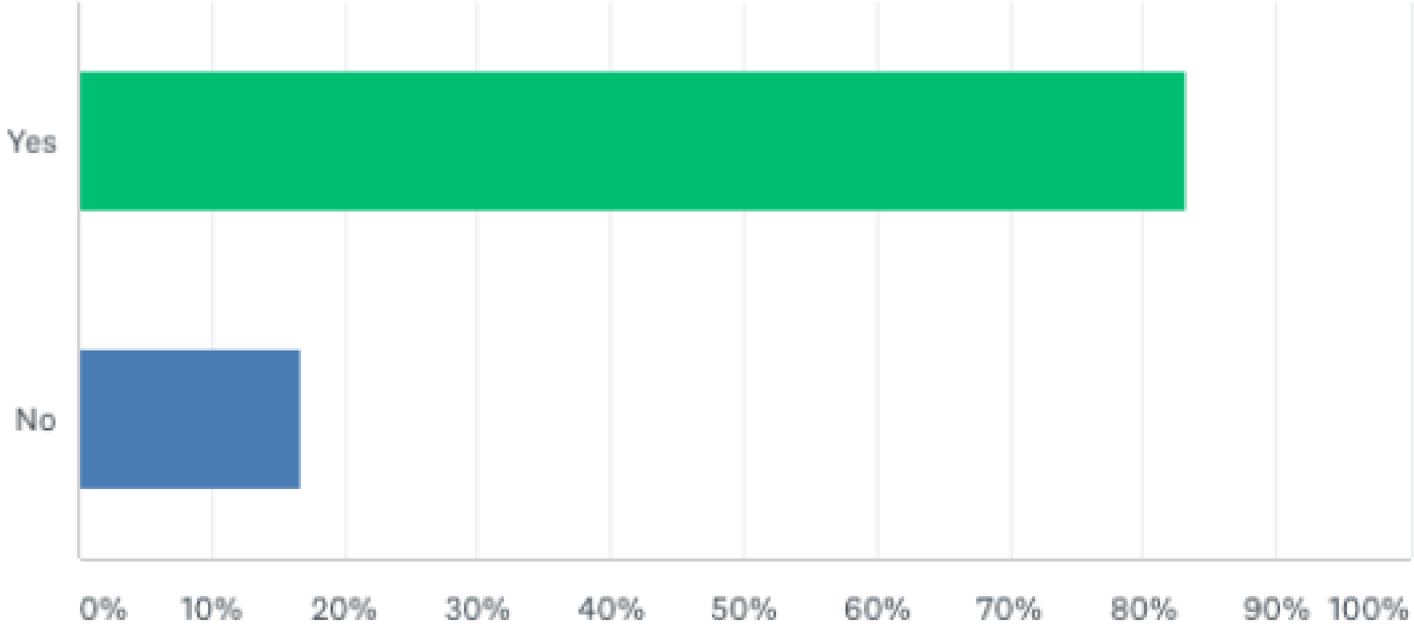
-One round of training may not be enough.

Action: Continue to aggregate data and track participation in training programs to improved results at an individual level.

Failures by Category

Category	Failure Percentage
Human Resources	19.8%
IT	13.2%
Online Services (email notifications, file sharing, etc.)	10.9%
Coupons	7.1%
Business and Financial Services	6.3%

Do you feel internal mass communications (i.e. emails from IT, HR, benefits) are easy to identify as legitimate?

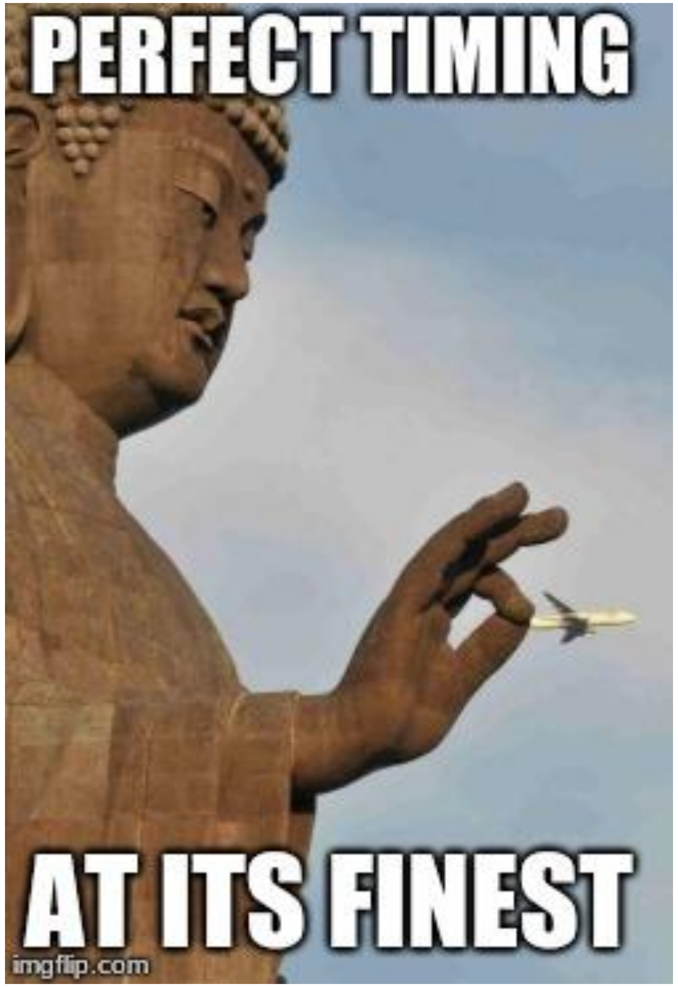


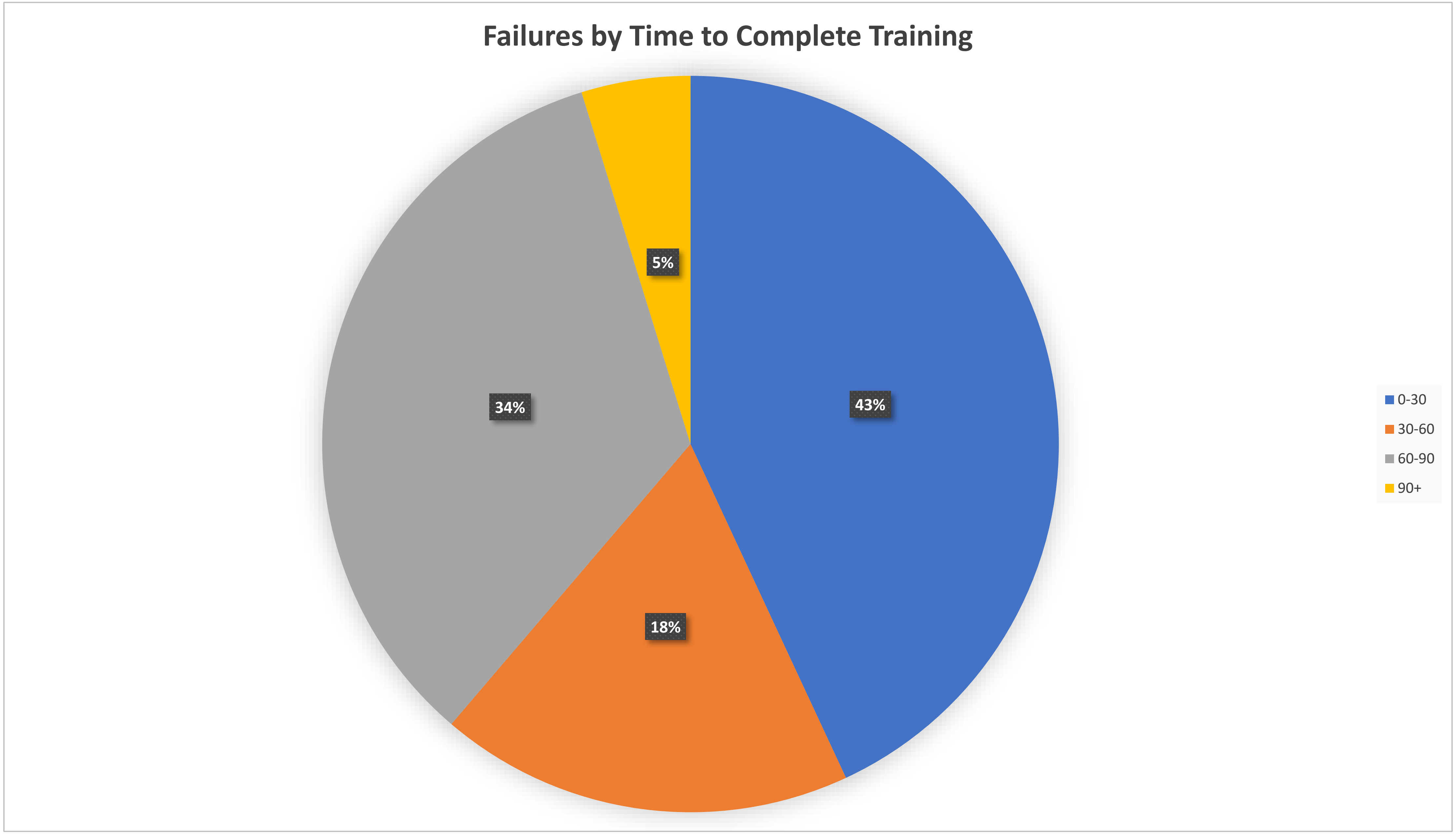
-Huge disconnect between the employees and corporate communications.

(i.e. They don’t know what they don’t know)

Action: Work with corporate marketing to develop a standardized look and feel for mass communications all departments can use.

Timing



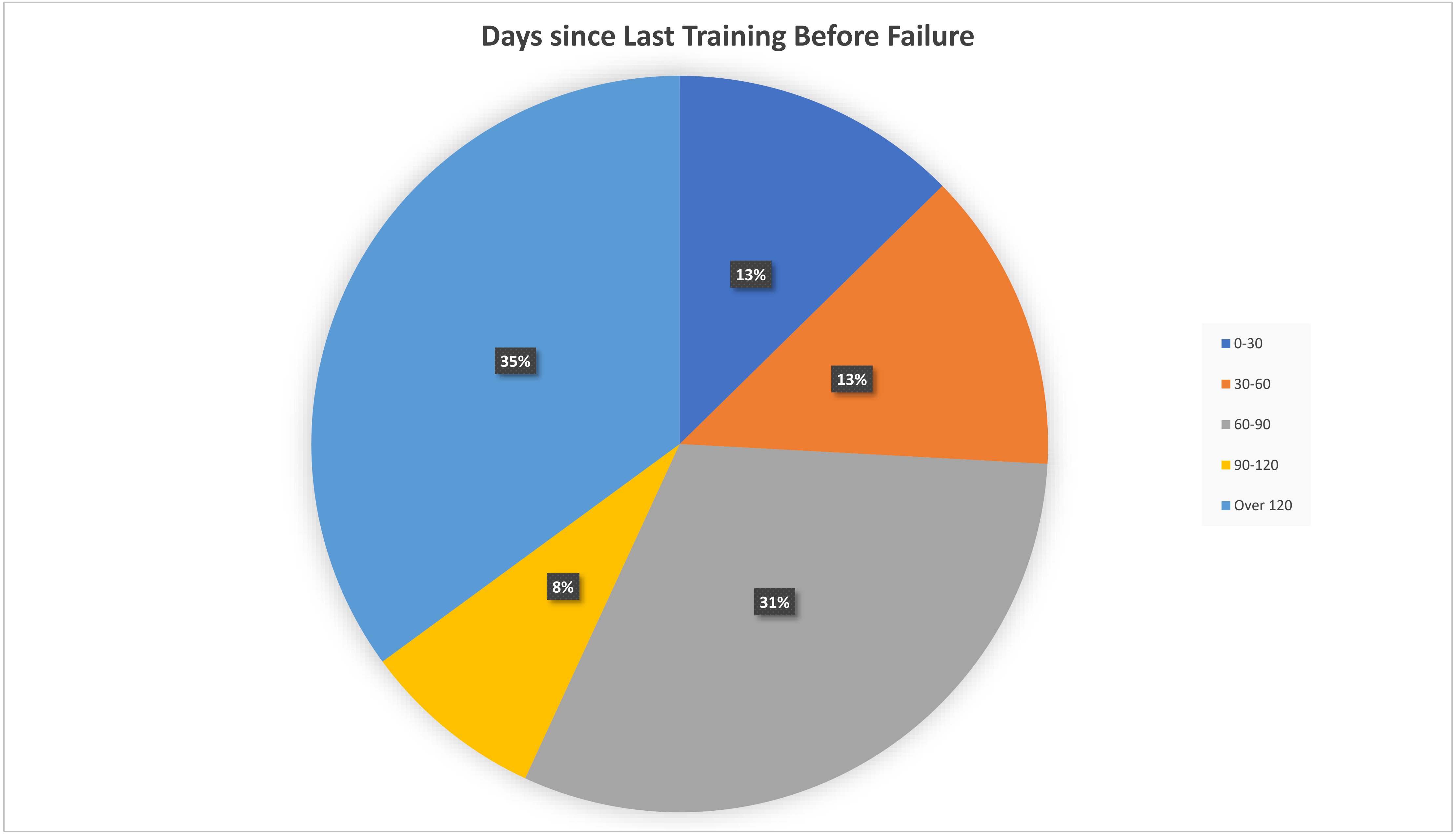


Failures by Time to Complete Training

-Completing the training early doesn’t mean it was effective.

-People who wait for the right time to do awareness training and maximize its value are the least risky.

Action: Communicate better with staff around training reminders. Don’t make them feel rushed to complete it. If a busy time is coming up, encourage staff to complete beforehand.



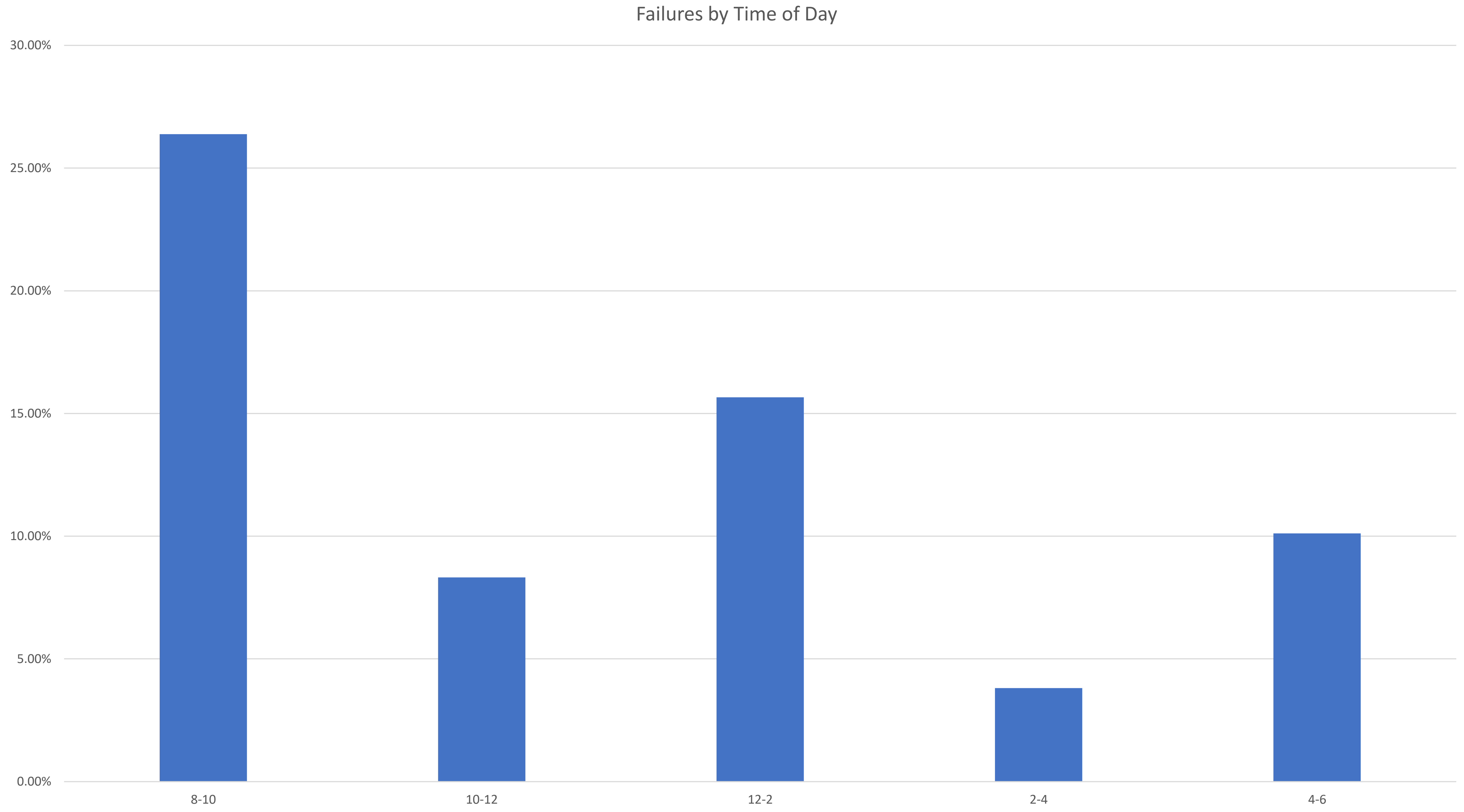
Days since Last Training Before Failure

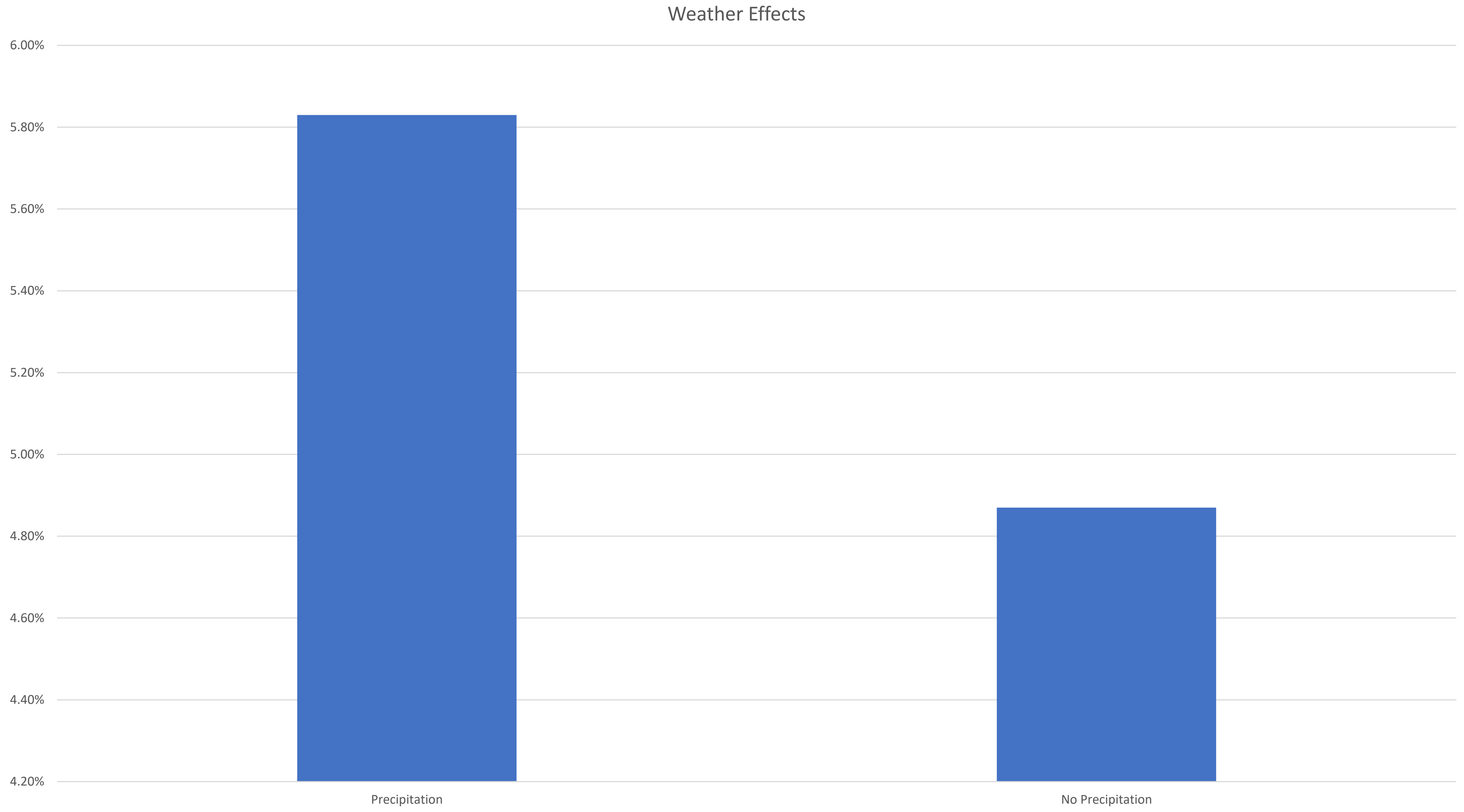
-Training effects last about 60 days!

-Less frequent reinforcement = More fail.

Action: Provide frequent reinforcement. Evaluate doing multiple small trainings throughout the year vs. one large annual training.

Environmental Factors/Weird Stuff


Failures by Time of Day
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
8-10
10-12
12-2
2-4
4-6


Weather Effects
6.00%
5.80%
5.60%
5.40%
5.20%
5.00%
4.80%
4.60%
4.40%
4.20%
Precipitation
No Precipitation

A few more thoughts…

-Make contact human and personal

-Avoid shaming at all costs

-Contests don’t work

-Always accentuate the positive

Results

-Haven’t implemented everything yet, but still saw a nearly 2% improvement from the previous “bad” test to the next test.

-Not enough data accrued yet to decide if this is coincidental or a hard result.

-Informal, anecdotal feedback has been **VERY positive!**

That’s it!

-Thanks to PHV for having me and thanks to all of you!

-@tcstoolhax0r on Twitter

-Slides will be up at github.com/tcstool later

-Questions?