RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: SEM-T02C

Failing Forward: An Innovation Model Applied to Risk Management

My-Ngoc Nguyen (Pronounced Menop Wynn)

CEO/Principal and Certified Instructor
Secured IT Solutions and SANS

Can you tell us…have we been compromised or breached?

Image from www.executive-transitions.net

OH NO!!!!!

Image from Friends

But should we be concerned?

Images from TLC, dawn.com, and picswe.com

But should we be concerned?

Images from TLC, dawn.com, and picswe.com

What do you think our risks are?

Image from www.executive-transitions.net

What is their meaning of risk in their question?

- Used for various meanings
  - Risk for rain (Probability)
  - Going fast on a twisty road is risky (Dangerous)
- Likelihood x Impact
- Threat x Vulnerability x Impact or Asset?
- Threat x Vulnerability

©2014 Secured IT Solutions, LLC

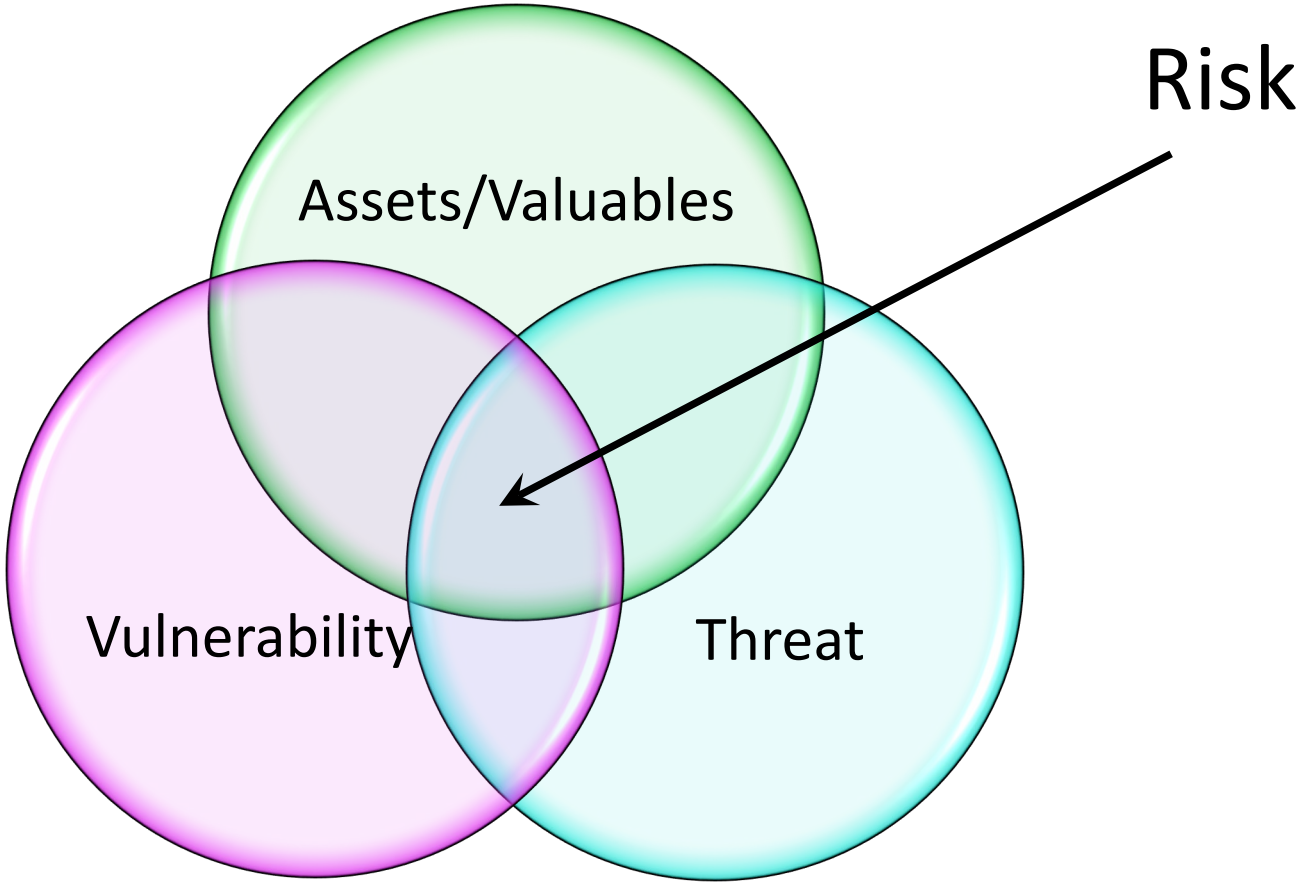
To manage your risk…

Know it, then

- Accept,
- Mitigate,
- Reduce, or
- Transfer

But do they know it (risk)?

Image from www.executive-transitions.net


Risk
Assets/Valuables
Vulnerability
Threat

"If you have everything to do, you do nothing" - Alan Paller, SANS

Yet, we want to do everything because we don't want to fail.


FAILURE

What do we think when we hear this word?

Why does it have such a negative connotation?

Probably because this is engrained in us as kids

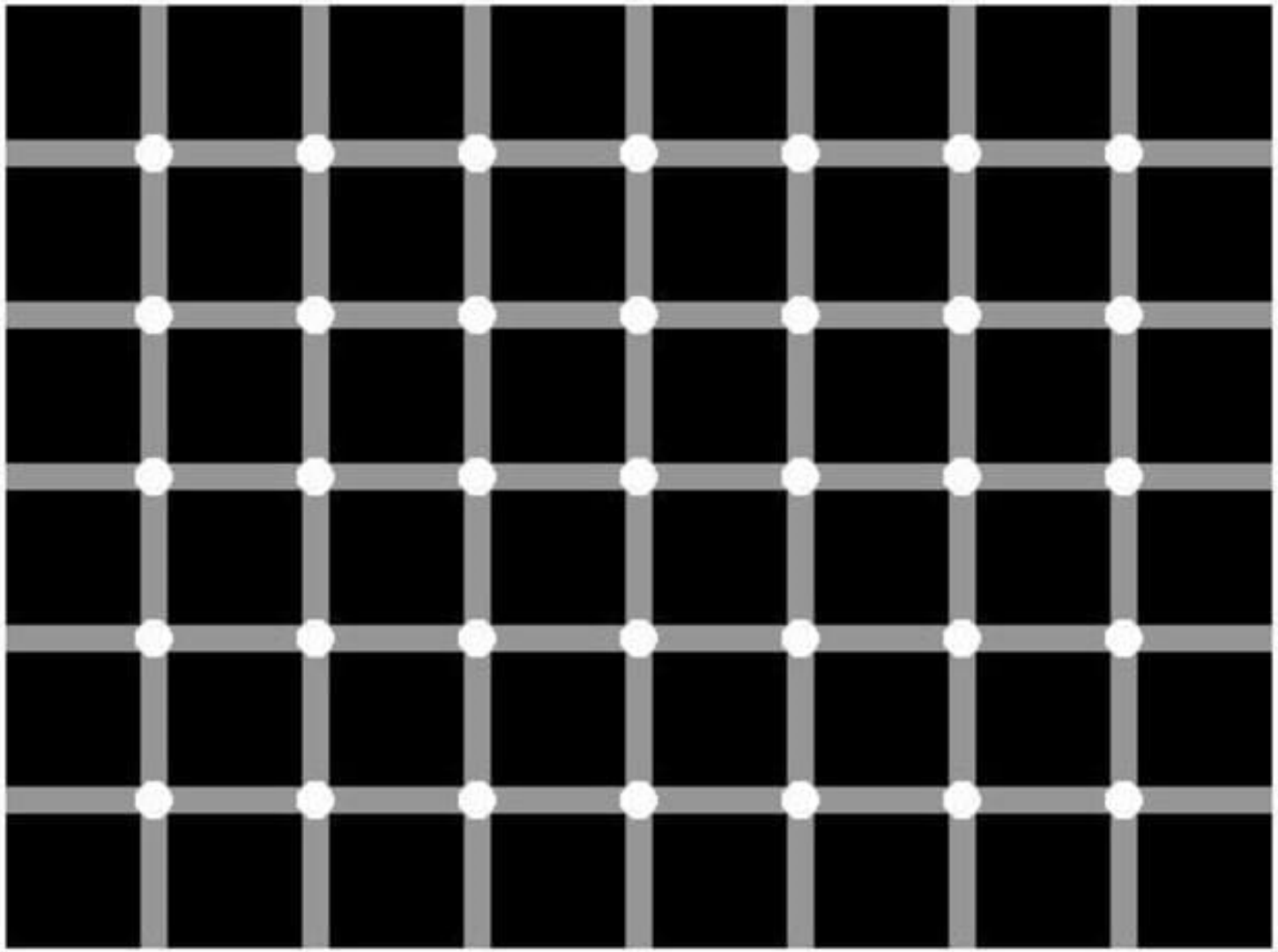
Does the fear of failing and failure stop us from trying and doing things?

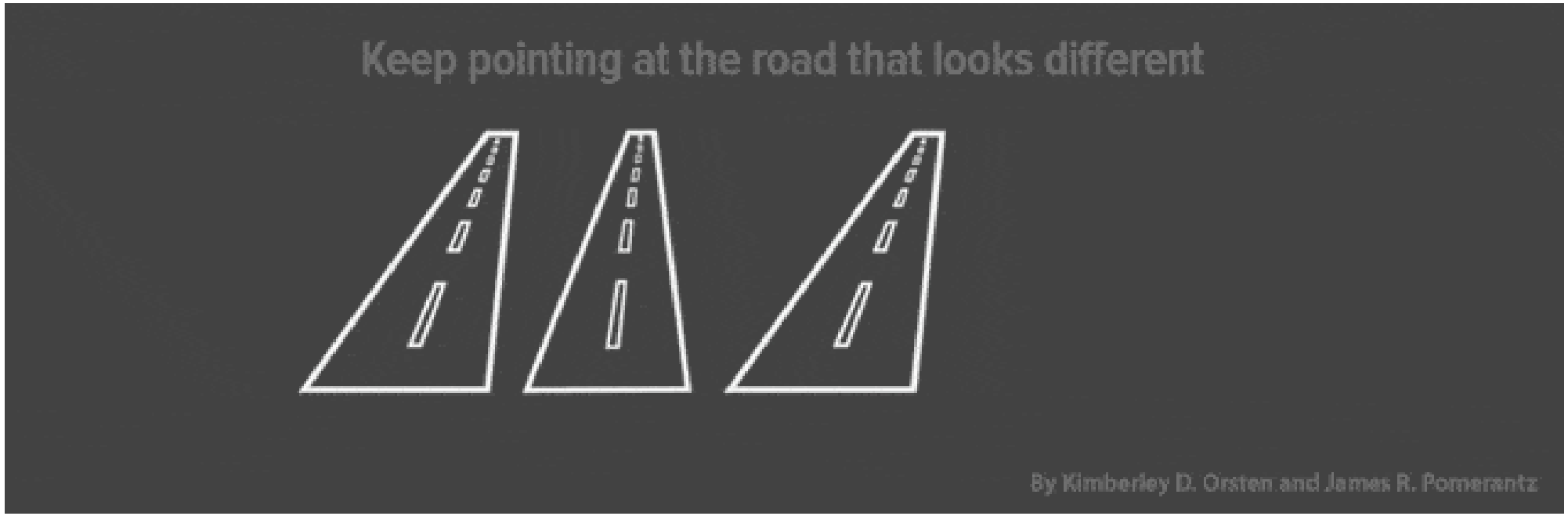
How many black dots do you count?

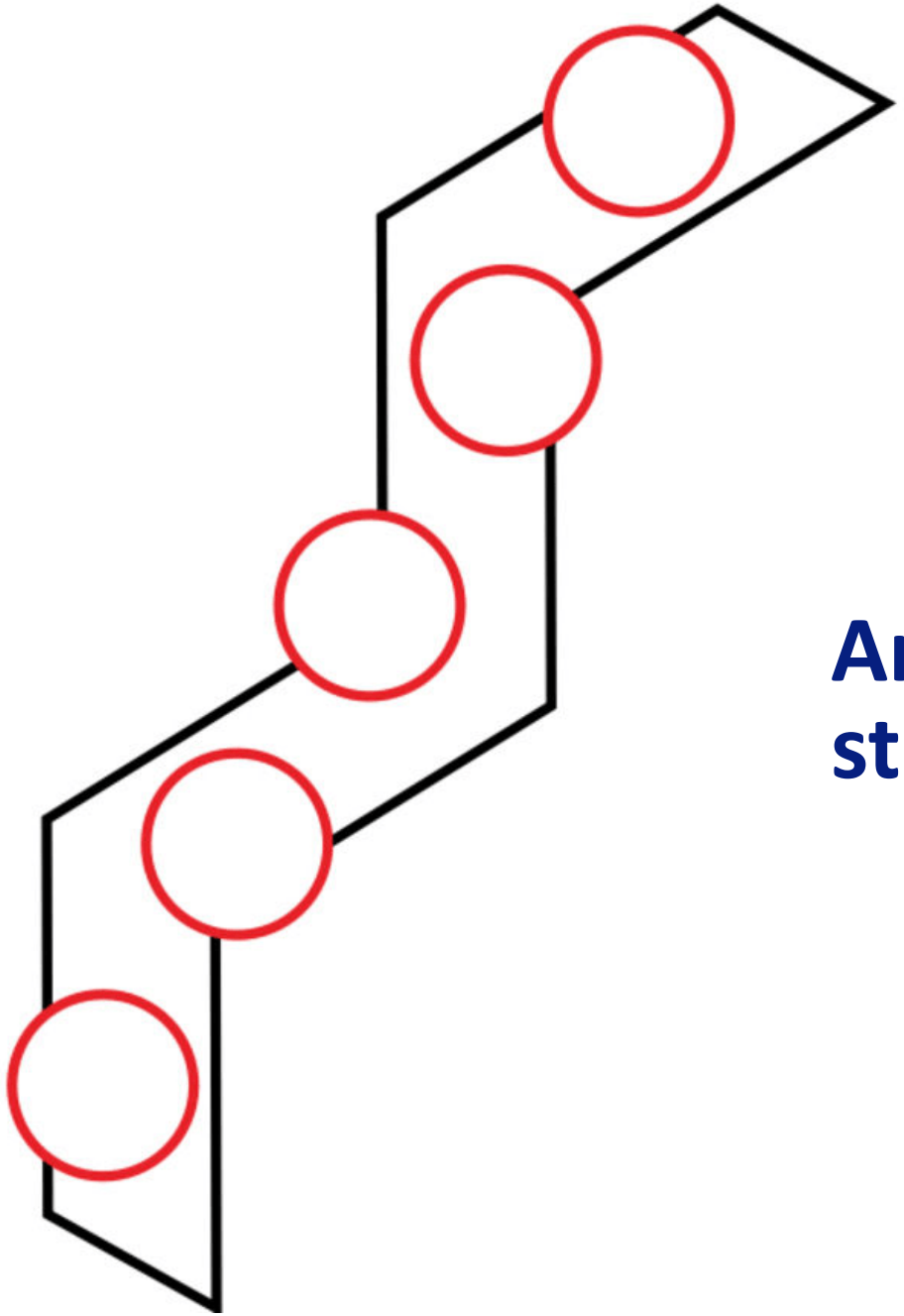
35?

15?

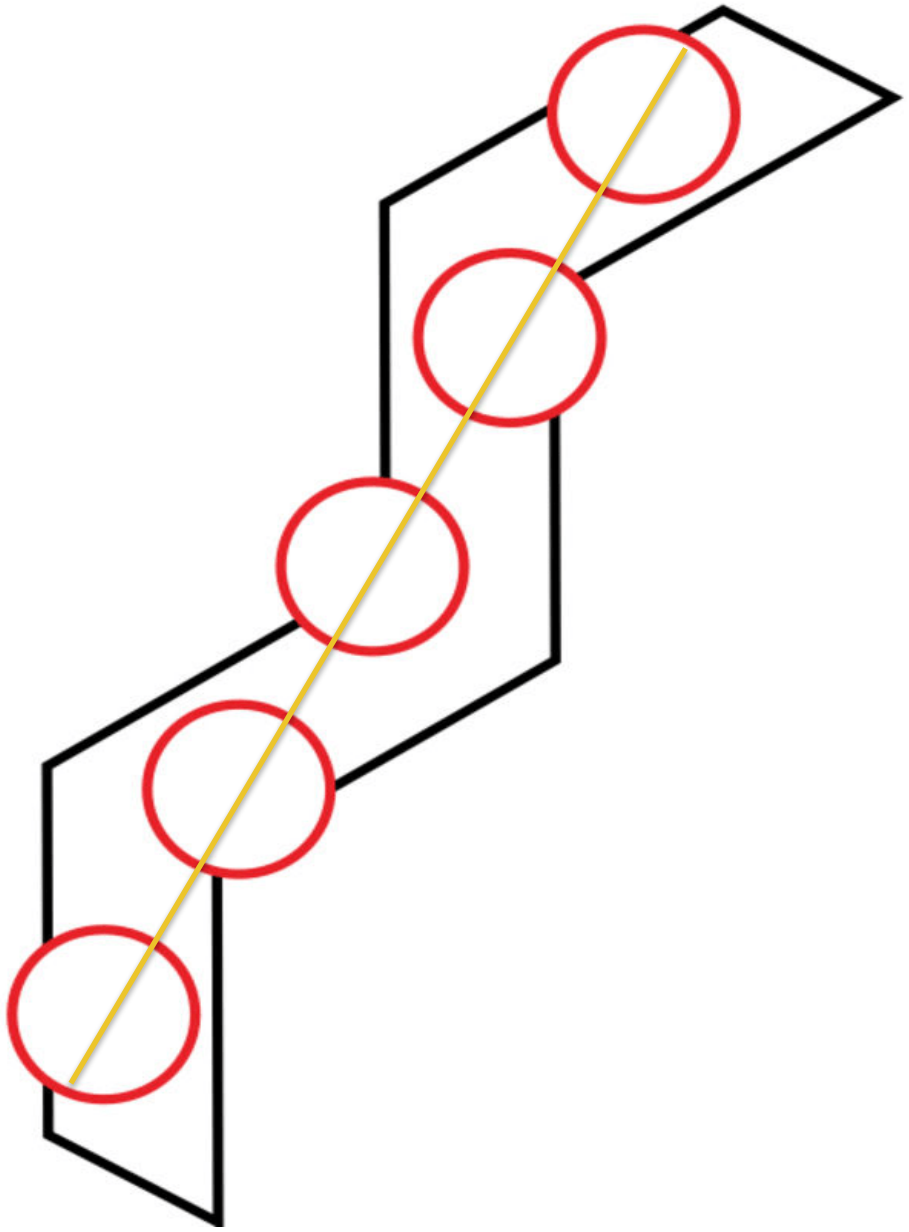
20?



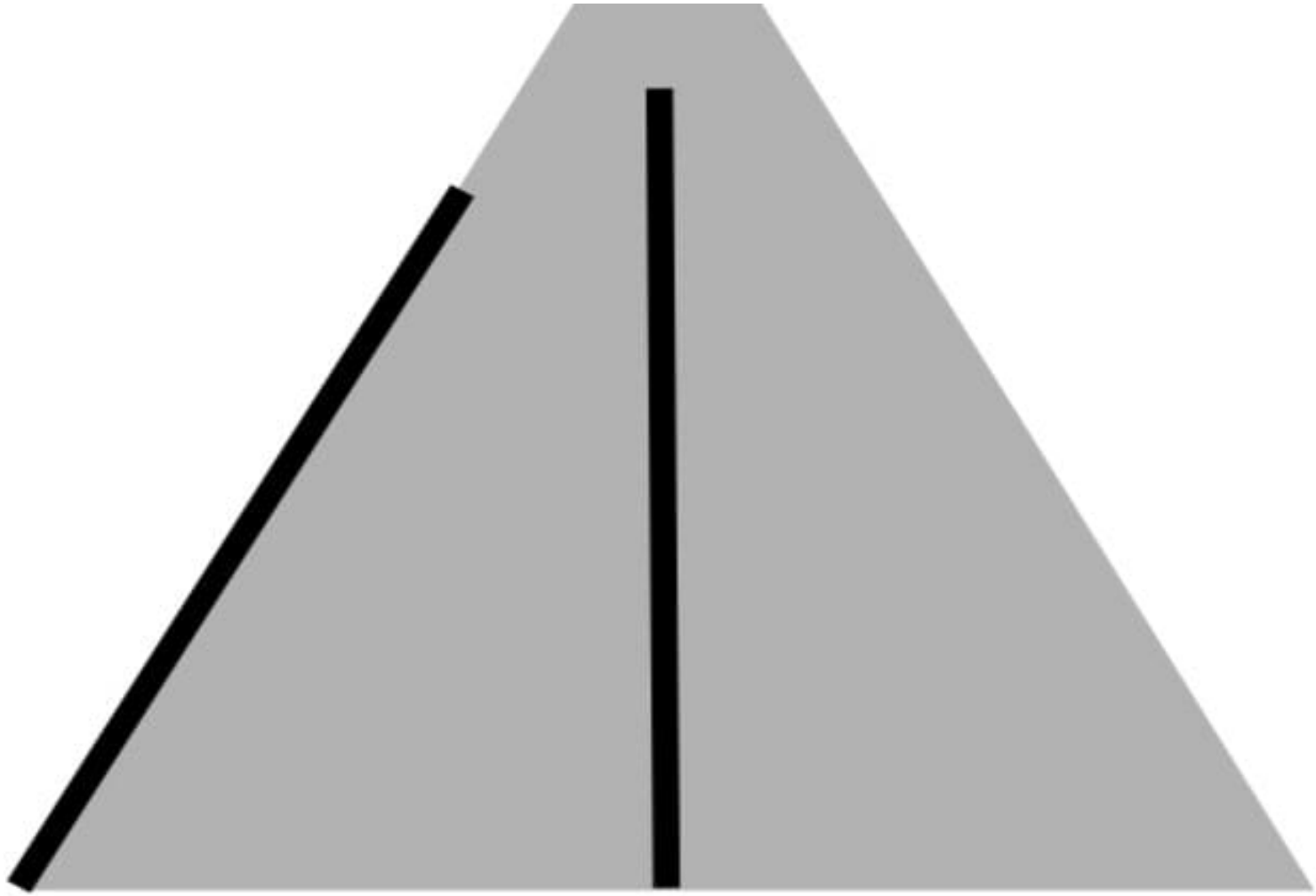

Keep pointing at the road that looks different
By Kimberley D. Orsten and James R. Pomerantz



Are these circles in a straight line?



Which black line is longer?



What's the feeling we get from

Failure

- What does failure mean to us when it comes to cyber security?
  - Incident? Breached?
  - Fined – compliance?

Does it mean… being one of these firms?

Organizations with Massive Data Breaches

- Yahoo (2016 / 2013): Initially thought 1 Billion but was 3 Billion – Oct 2017
- Yahoo (2016 / 2014): 500 Million
- Marriott (2018): 500 Million
- Adult Friend Finder (2016): 412.2 Million
- eBay (2014): 145 Million
- Equifax (2017): 143.5 Million
- Heartland Payment Systems (2009): 134 Million
- Target (2013): 110 Million
- Tk-TJ Max (2007): 94 Million
- JP Morgan Chase (2014): 83 Million
- Anthem (2015): 80 Million
- Sony Play Station (2011): 77 Million
- Home Depot (2014): 56 Million
- RSA (2011): 40 Million
- Adobe (2013): 38 Million
- Ashley Madison (2015): 32 Million
- Office of Personnel Management (2015): 21.5 Million
- American Medical Collection Agency for Quest and LabCorp (2019): 11.9 Million + 7.7 Million: total 19.6 Million

SECUREDIT SOLUTIONS

Source: USA Today, Business Insider, and CSO

OR does it mean… being victim to


VIRUS
INTRUDER
CRACKER
SPYWARE
PASSWORD
IDENTITY
UNSAFE
CODE
THEFT
HACKER

https://www.rt.com/news/china-blames-us-hacking-051/


© Gao xiaowen – Imaginechina

Images from: IBTimes UK, Security Magazine, RT

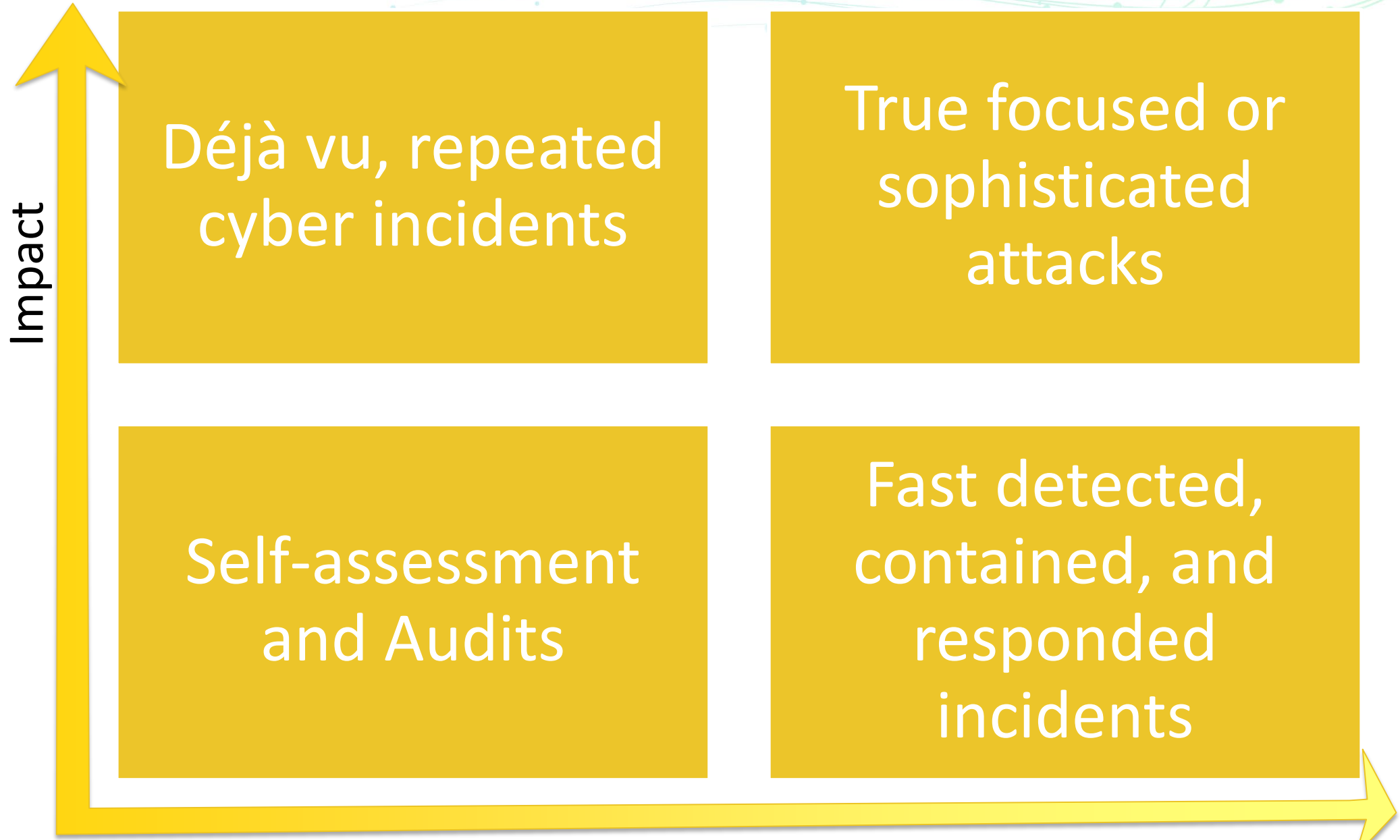
What does failure mean when it comes to compliance?


You're
Fired!

Types of Cyber Security Activities in Security Ops

- Incidents:
  - Repeated
    - An incident that the organization previously experienced
    - An incident that was experienced from another victim
    - An incident that was headlined
  - Fast detected, contained, and responded
  - Truly targeted and sophisticated
- Audits
- Self-assessments

© Secured IT Solutions. 2015 All Rights Reserved.



SECUREDIT SOLUTIONS

RSAConference2019 Asia Pacific & Japan

© Secured IT Solutions. 2015 All Rights Reserved.

It's bad to fail our audits, assessment, or pen tests.

WRONG!

FAIL OFTEN AND FAST

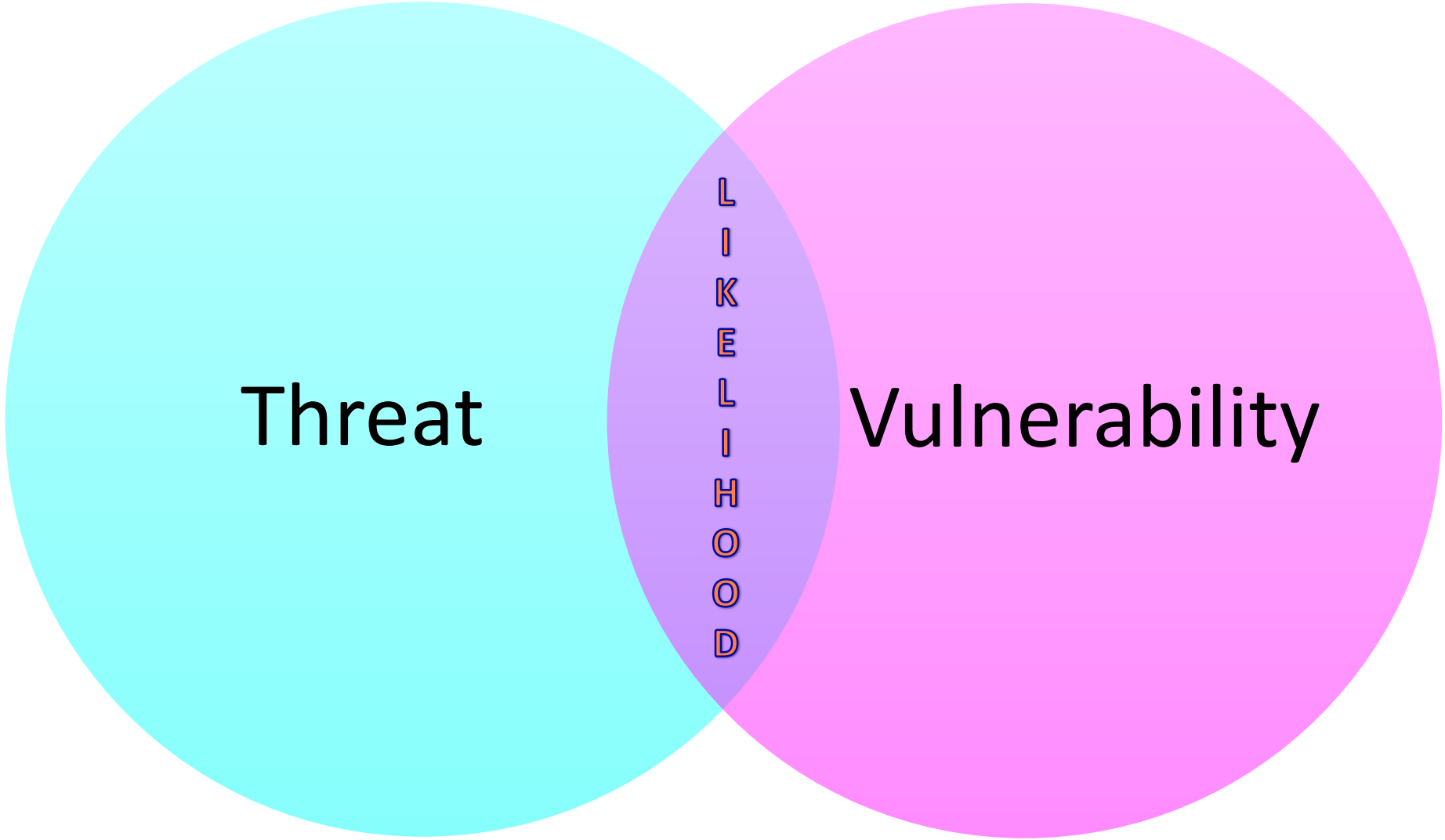
- Fail often and grow (learn fast – fail forward)
  - Ok to fail pen tests
  - Ok to fail audits
    Ok to fail assessments
  - Learn to be able to respond fast
    - Improves the meantime for detection and response

Pass the audits and become like:

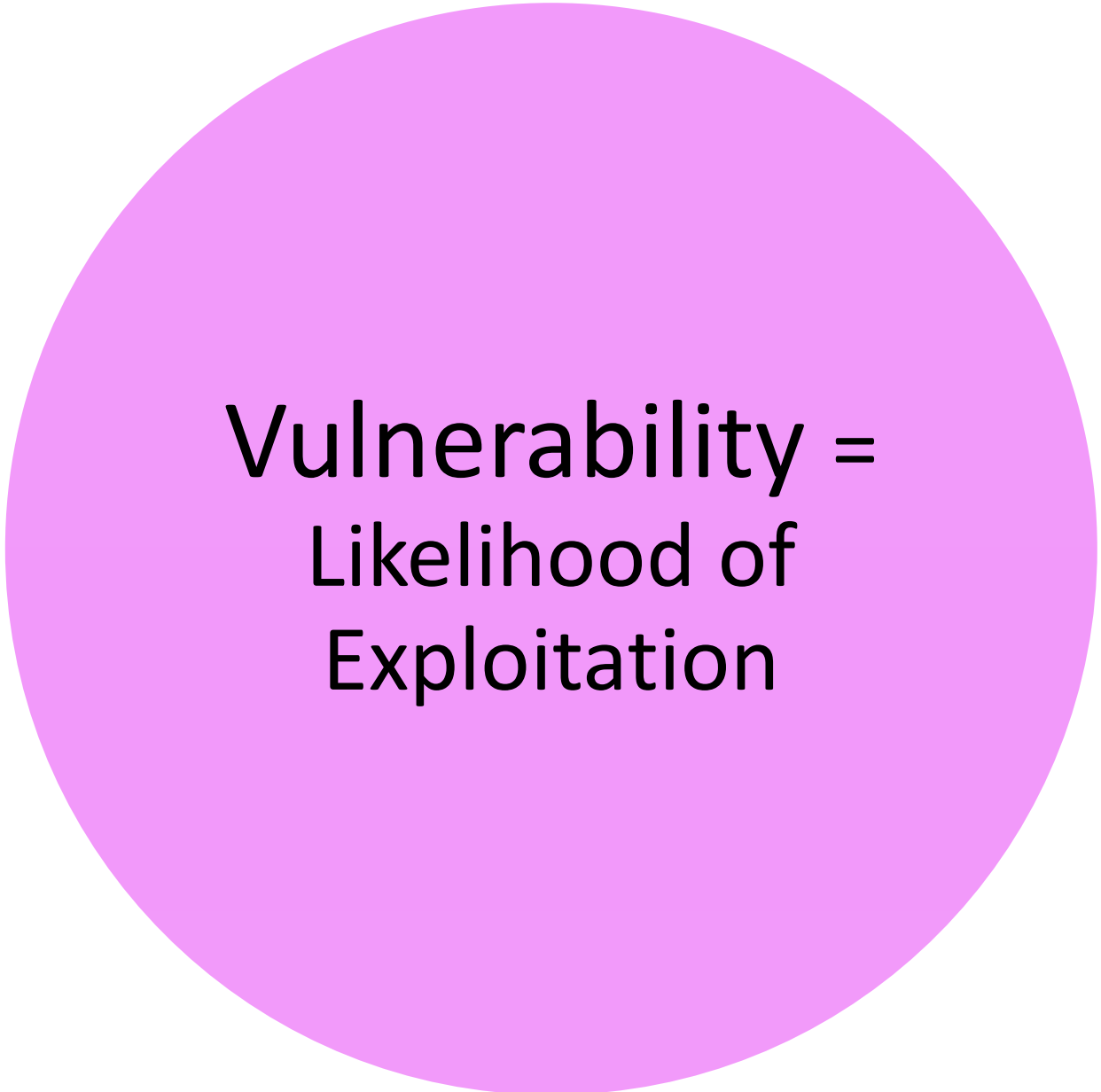
- Yahoo (SOX)
- eBay (SOX)
- Heartland Payment Systems (PCI)
- Target (PCI)
- Tk-TJ Max (PCI)
- JP Morgan Chase (GLBA, PCI, SOX, etc.)
- Anthem (HIPAA)
- Sony Play Station (PCI)
- Home Depot (PCI)

Risk = Likelihood x Impact

Risk – Overall Likelihood



Likelihood of Exploitation



Organizations with Massive Data Breaches

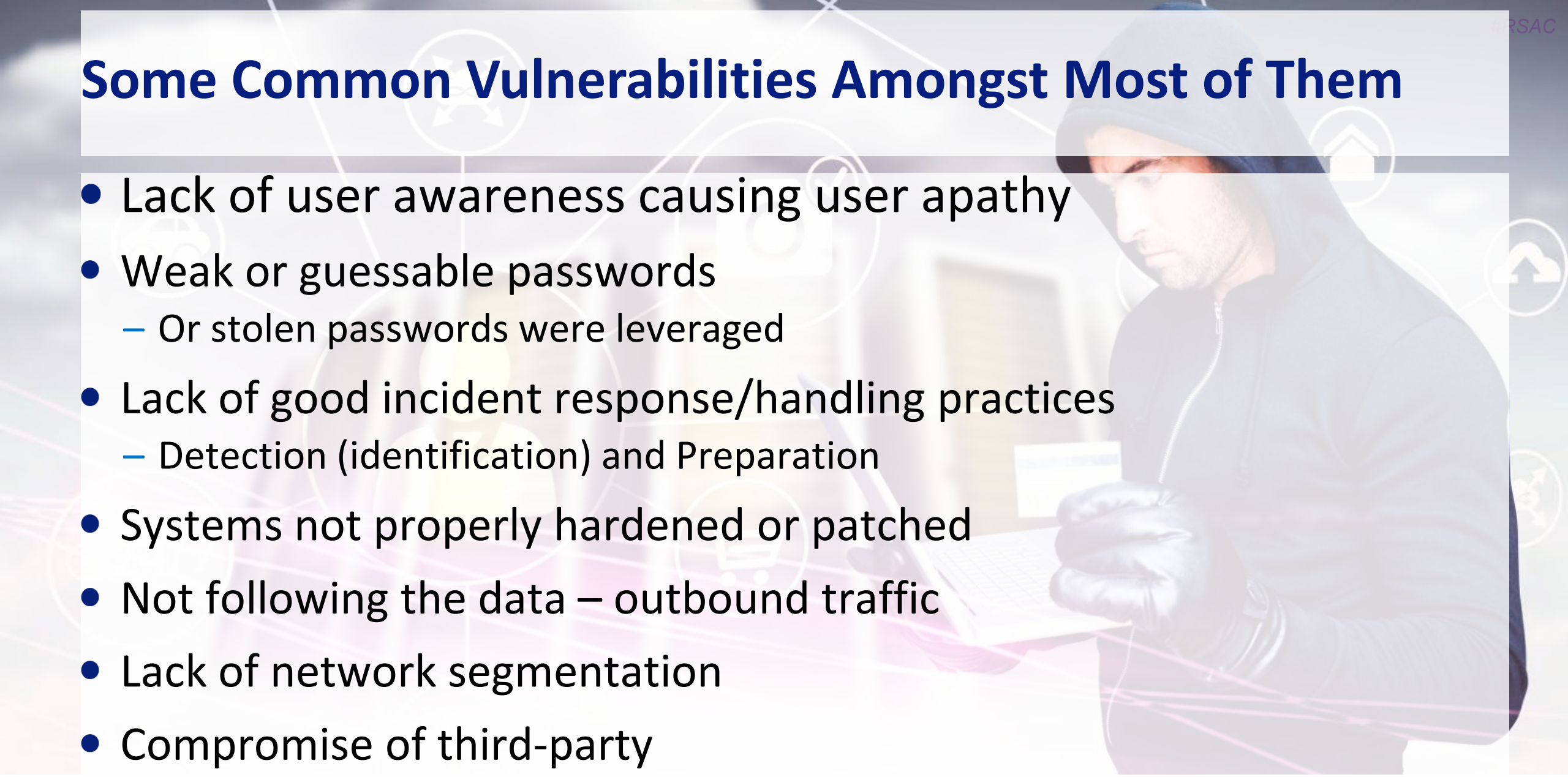
- Yahoo (2016 / 2013): Initially thought 1 Billion but was 3 Billion – Oct 2017
- Yahoo (2016 / 2014): 500 Million
- Marriott (2018): 500 Million
- Adult Friend Finder (2016): 412.2 Million
- eBay (2014): 145 Million
- Equifax (2017): 143.5 Million
- Heartland Payment Systems (2009): 134 Million
- Target (2013): 110 Million
- Tk-TJ Max (2007): 94 Million
- JP Morgan Chase (2014): 83 Million
- Anthem (2015): 80 Million
- Sony Play Station (2011): 77 Million
- Home Depot (2014): 56 Million
- RSA (2011): 40 Million
- Adobe (2013): 38 Million
- Ashley Madison (2015): 32 Million
- Office of Personnel Management (2015): 21.5 Million
- American Medical Collection Agency for Quest and LabCorp (2019): 11.9 Million + 7.7 Million: total 19.6 Million

SECUREDIT SOLUTIONS

Source: USA Today, Business Insider, and CSO

Some Common Vulnerabilities Amongst Most of Them

- Lack of user awareness causing user apathy
- Weak or guessable passwords
  - Or stolen passwords were leveraged
- Lack of good incident response/handling practices
  - Detection (identification) and Preparation
- Systems not properly hardened or patched
- Not following the data – outbound traffic
- Lack of network segmentation
- Compromise of third-party



Target

- November 2013
- 110 million card holder data
- Cost of breach was over $250 million + $10 million for class action lawsuit (April 2015)
- Attackers uploading their card-stealing malicious software to a small number of cash registers within Target stores
- Network credentials were stolen from a third-party HVAC vendor
- U.S. Department of Justice notified the retailer about the breach in mid-December
- Did not respond to FireEye's alerts from Nov. 30 and more from Dec. 2
  - Did not configure system for auto-block

Ashley Madison

A screenshot from the Ashley Madison data dump.

- July 2015
- Hacked by the Impact Team
  - 32 million Ashley Madison users
  - The 9.7 gigabytes of information released by the hackers included credit card information, names, billing details and home addresses
  - less than a month before that episode, Ashley Madison executives seemed very keen on completing a series of internal security assessments, audits and security awareness training exercises for employees.

Ashley Madison – 100 popular passwords

Password	Times used
123456	120,511
12345	48,452
password	39,448
default	34,275
123456789	26,620
qwerty	20,778
12345678	14,172
abc123	10,869
p***y	10,683
1234567	9,468
696969	8.801
ashley	8,793

Password	Times used
football	7,872
baseball	7,710
f**kyou	7458
111111	7,048
1234567890	6,572
ashleymadison	6,213
password1	5,959
madison	5,219
a**hole	5,052
superman	5,023
mustang	4,865
harley	4,815
654321	4,729

Password	Times used
123123	4,612
hello	4,425
monkey	4,296
000000	4,240
hockey	4,191
letmein	4,140
11111	4,077
soccer	3,936
cheater	3,908
kazuga	3,871
hunter	3,869
shadow	3,831
michael	3,743
121212	3,713
666666	3,704

Password	Times used
iloveyou	3,671
qwertyuiop	3,599
secret	3,522
buster	3,402
horny	3,389
jordan	3,368
hosts	3,295
zxcvbnm	3,280
asdfghjkl	3,174
affair	3,156
dragon	3,152
987654	3,123
liverpool	3,087
bigd**k	3,058
sunshine	3,058
yankees	2,995

Password	Times used
asdfg	2,981
freedom	2,963
batman	2,935
whatever	2,882
charlie	2,860
f**koff	2,794
money	2,686
pepper	2,656
jessica	2,648
asdfasdf	2,617
1qaz2wsx	2,609
987654321	2,606
andrew	2,549
qazwsx	2,526
dallas	2,516
55555	2,501
131313	2,498

Password	Times used
abcd1234	2,489
anthony	2,487
steelers	2,470
asdfgh	2,468
jennifer	2,442
killer	2,407
cowboys	2,403
master	2,395
jordan23	2,390
robert	2,372
maggie	2,357
looking	2,333
thomas	2,331
george	2,330
matthew	2,298
7777777	2,294
amanda	2,273

Password	Times used
summer	2,263
qwert	2,263
princess	2,258
ranger	2,252
william	2,245
corvette	2,237
jackson	2,227
tigger	2,224
computer	2,212

Equifax

- Reported Sept 2017
  - Breached discovered in July 2017
  - Unrelated breach in March 2017
- Compromised personal information of 143 million US citizens and approximately 693,665 UK citizens (initial thought 400k)
- Exploited through a Apache Struts flaw with patch released in March 2017
  - Equifax acknowledged that they were aware of this vulnerability at that time

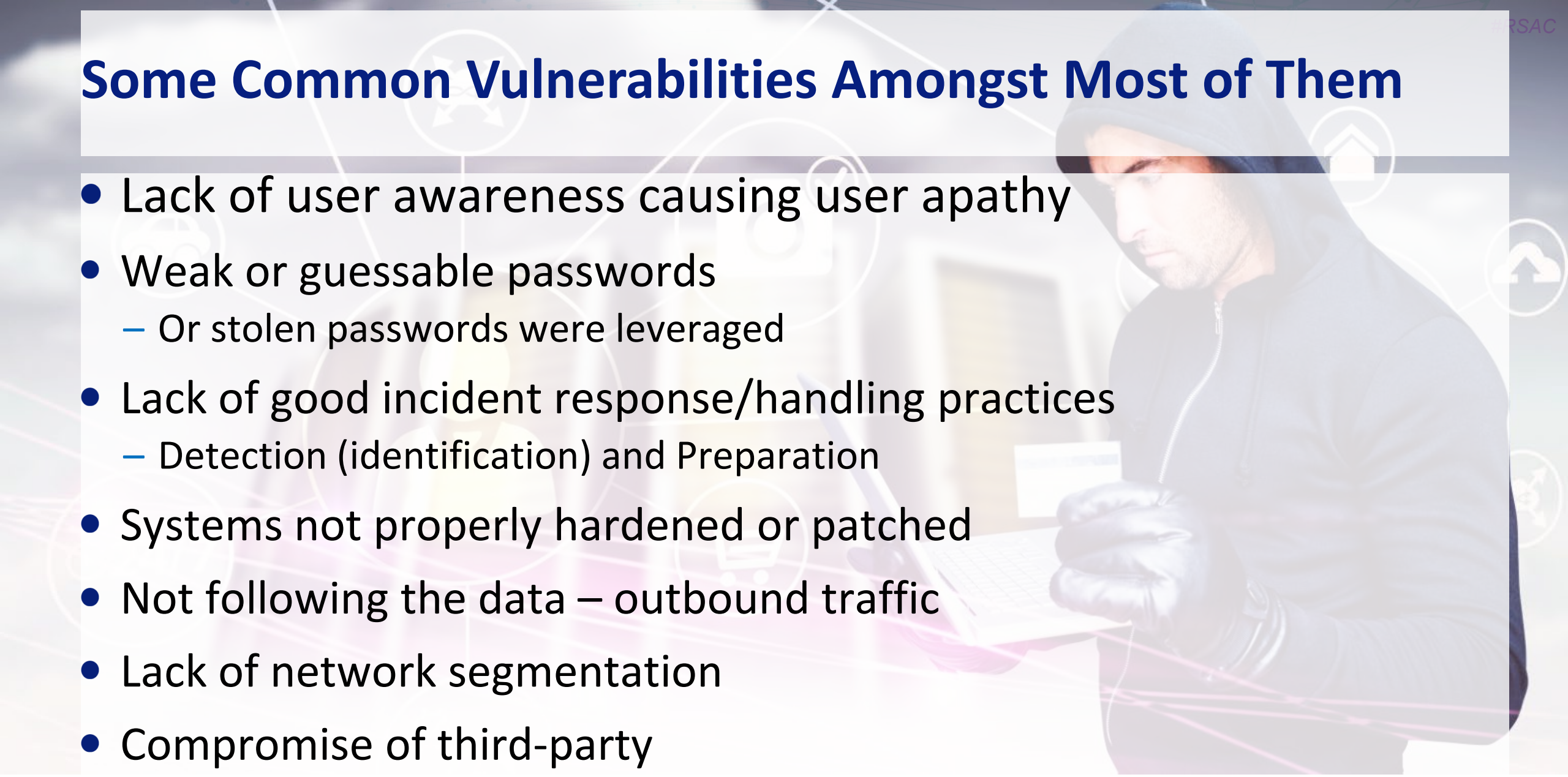
Equifax

- Insecure practices/criticism:
  - Found CISO was a music major after it was disclosed that CIO and CISO left company immediately after public report
  - Directed customers to wrong site used to phish visitors to that site
    - set up www.equifaxsecurity2017.com
    - company's official Twitter account responded to customer inquiries by apparently directing them to a fake phishing site called www.securityequifax2017.com.

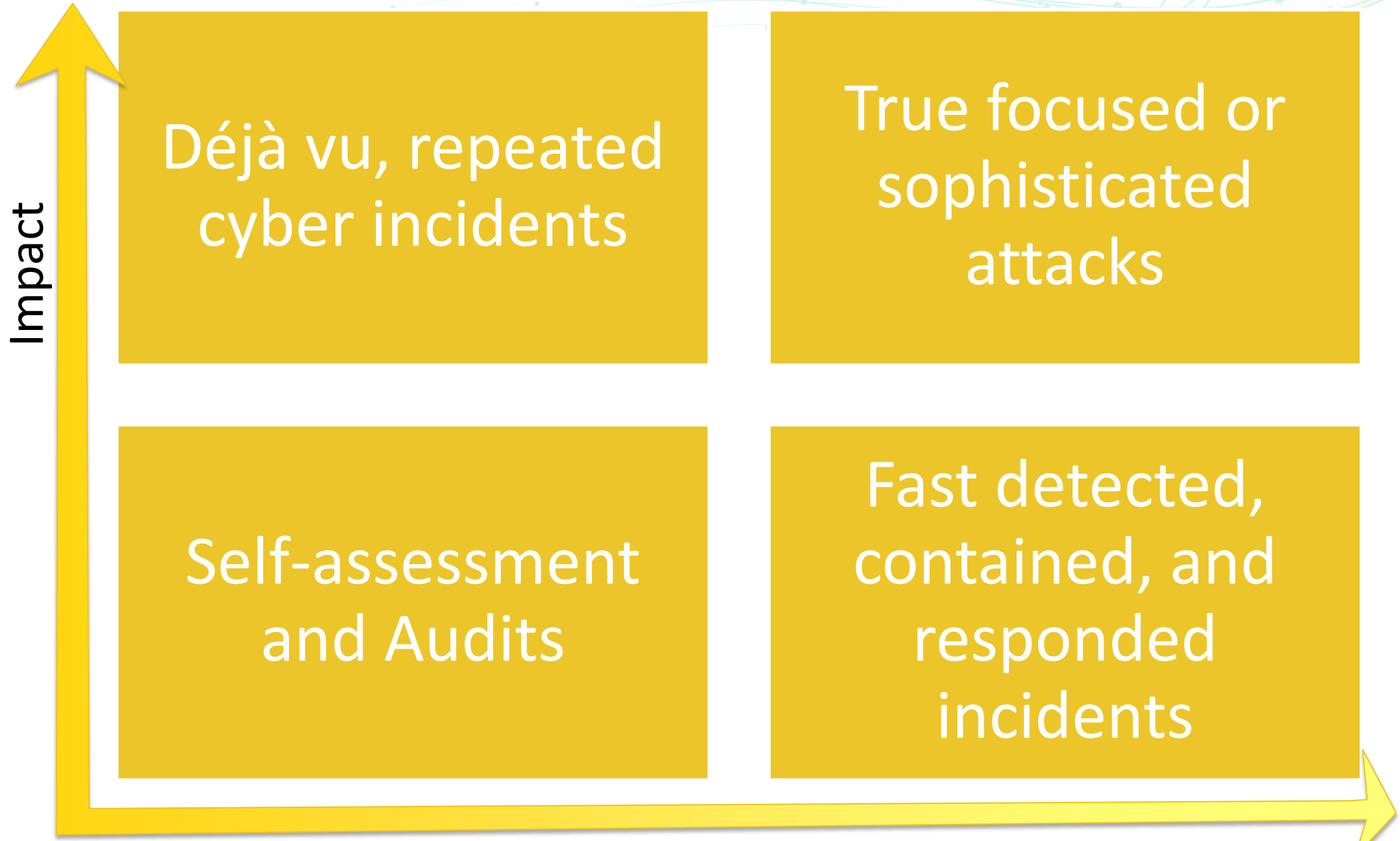
Marriott

- November 2018, reported the discovery of their breach that occurred four years ago in July of 2014
- 500 million consumer records: payment information, names, mailing addresses, phone numbers, email addresses, and passport numbers.
- Just incurred GDPR fines of £99 million
- Intrusion vectors not yet identified.

Some Common Vulnerabilities Amongst Most of Them



- Lack of user awareness causing user apathy
- Weak or guessable passwords
  - Or stolen passwords were leveraged
- Lack of good incident response/handling practices
  - Detection (identification) and Preparation
- Systems not properly hardened or patched
- Not following the data – outbound traffic
- Lack of network segmentation
- Compromise of third-party



SECUREDIT SOLUTIONS

RSAConference2019 Asia Pacific & Japan

© Secured IT Solutions. 2015 All Rights Reserved.

SECUREDIT SOLUTIONS

RSAConference2019
Asia Pacific & Japan

© Secured IT Solutions. 2015 All Rights Reserved.

The concept of failing fast and often

- Book Art and Fear by David Bayles and Ted Orland
- Ceramic class split into 2 groups and provided 2 different grading criteria
  - Group 1 was graded on **quantity** of pots they produce while Group 2 was graded on **quality** pot
  - Group 1 ended up producing the best work in quality (technical and artistic sophistication)

An example of a company succeeding by experiencing many failures in the last 10-15 years.

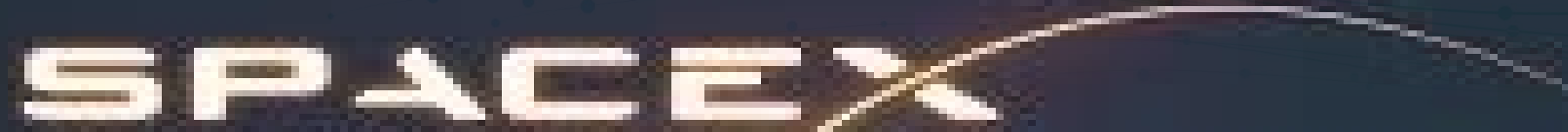
- became the first privately funded group to put a payload in Earth orbit, in 2008.
- launching unmanned cargo vehicles to the International Space Station (ISS) and
- has $4.2 billion in contracts from NASA alone and its recent success in cracking the defense contract business

SPACEX

- March 2019: SpaceX launched its first Crew Dragon on a Falcon 9 rocket
  - This launch is just the start of a SpaceX flight test to demonstrate to NASA that new Crew Dragon spacecraft is ready to carry astronauts.

"It's been 17 years. We still haven't launched anyone yet, but hopefully we will later this year," Musk said of SpaceX. "So, that will definitely be the culmination of a long dream for a lot of people, me and other people at SpaceX, for sure. Can't wait.“

Space.com



17 years that included failures

Failures experienced

- **2006** The first SpaceX launch fails just 33 seconds after lift-off. Cause: a rusty nut.
- **2007** The engines shut down prematurely and the rocket fails to reach orbit. SpaceX is 0 for 2.
- **2008** SpaceX's first payload for NASA; payload ended up in the sea instead. This third failure almost killed the company. It was saved—just a day after the crash—by billionaire Peter Thiel, the company's first outside investor.

Failures experienced

- September 2013: Hard impact on ocean
- April 2014: 1st Soft Water Landing
- July 2014: 2nd Soft Water Landing but breaks apart after landing
- August 2014: Engine Sensor Failed – Rocket blew up on air
- September 2014: Ran out of liquid oxygen
- January 2015: Ran out of hydraulic fuel
- April 2015: Stick throttle valve

Dec 2015 first Successful Landing

- Jan 2016: Landing leg collapsed
- March 2016 Landing burned failed

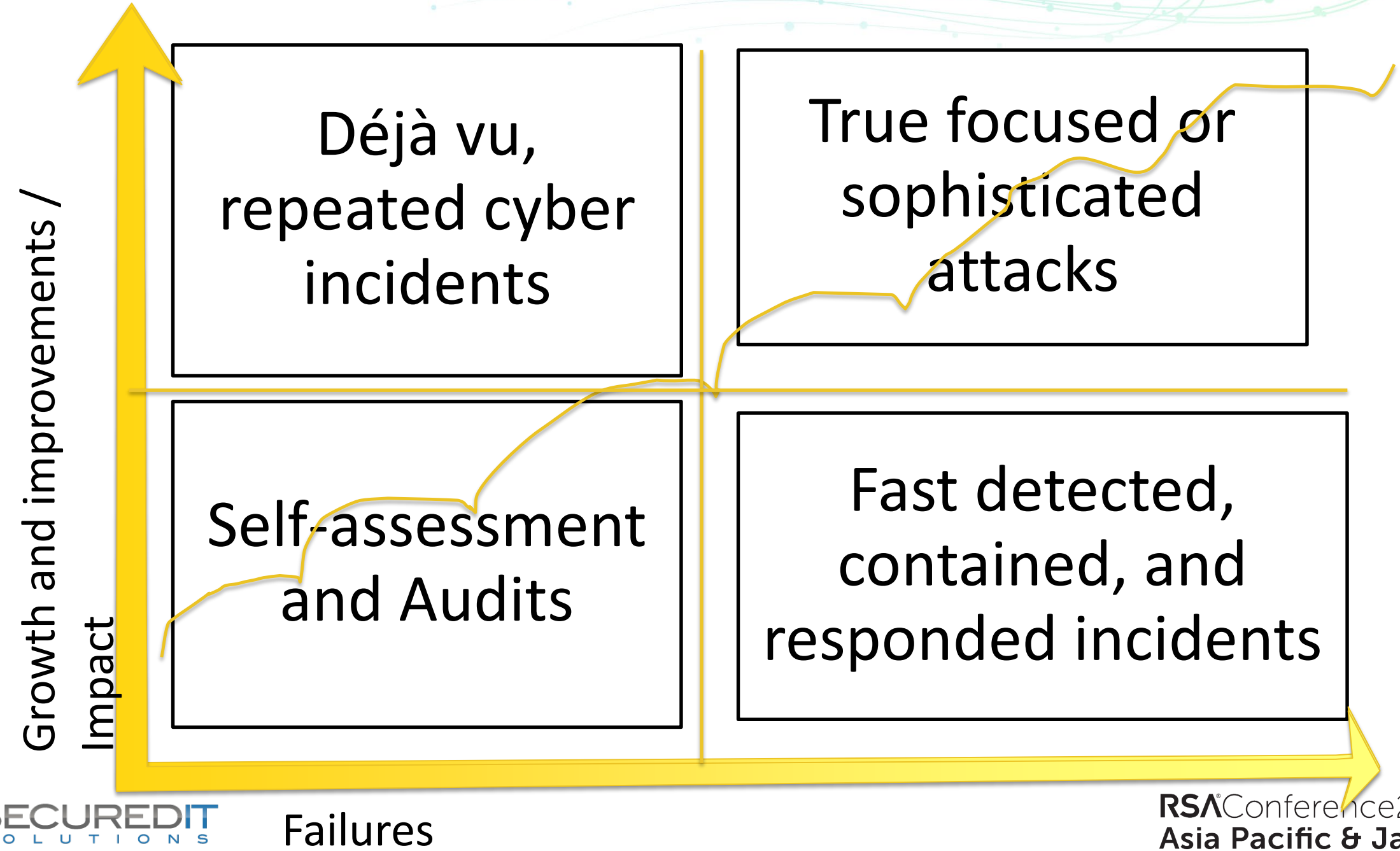
April 2016: First successful drone ship landing

- May 2016 Radar glitch and Leg broke
- June 2016: Ran out of propellant

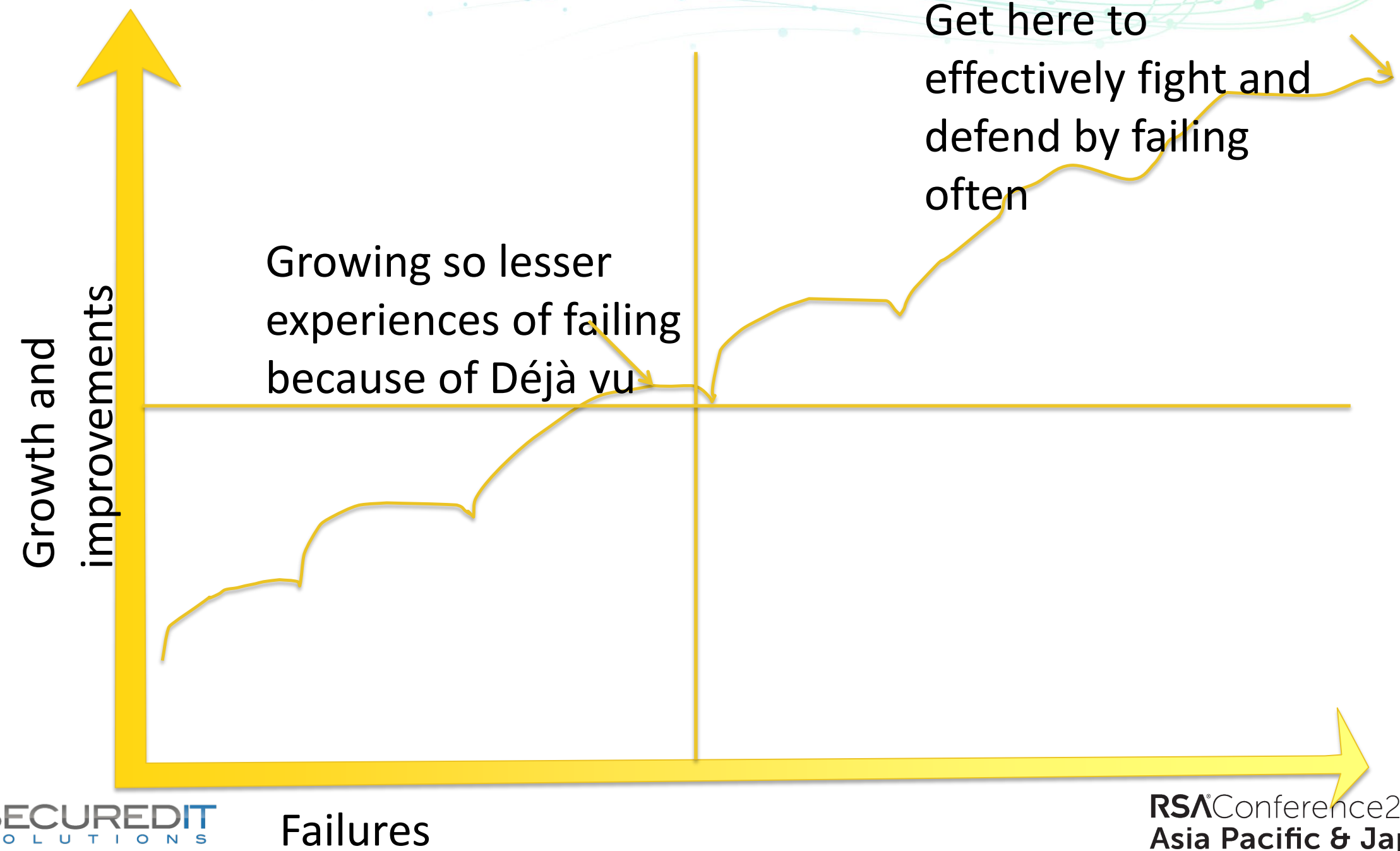
March 2017: First launch and landing of a reused first stage.

SECUREDIT SOLUTIONS

© Secured IT Solutions. 2015 All Rights Reserved.



© Secured IT Solutions. 2015 All Rights Reserved.



SECUREDIT SOLUTIONS

RSAConference2019 Asia Pacific & Japan

© Secured IT Solutions. 2015 All Rights Reserved.

Learning from failures not easy

- Learning is not instantaneous or automatic
  - People feel grief which obstructs our ability to learn from failure
    - People need to have the feeling
    - But you need to not allow the grief of the loss affect the inability to learn from a failures
    - Make the most of failures
  - Emotionally capable organization
    - Don’t desensitize failures

How to foster learning from failures?

- Use every opportunity
  - Quantity over Quality
- Focus on the right and calculated failures.

  Tailoring the easy-to implement failing forward suggestion from Fail Fast, Fail Often
  - Identify the impacts

How to foster learning from failures? cont.

- Identify the impacts
- Reverse thinking: look at ways you can fail
  - Drives process improvement and maturity
  - Drives Offensive Defense
- Do it anyways: Get out there and give it a try
  - Ex. No repercussion for blocking sites for an hour
    - Case study with watering hole

How to foster learning from failures? cont.

- Fail Forward: use exploratory action to learn and discover
  - Threat Intelligence
- Find the next challenge: Seek out the next opportunity to reach your limits.
  - Threat Hunting

– **Succeed!!**


Failure is a Stepping Stone to Success
Tony Robbins

"Apply"

- This session broke down components of risks and how an innovated model can be used for risk management to enable cyber security warriors (of all roles – leadership and self contributors) to adapt to continuous evolving threats
- Next week you should:
  - Identify areas of opportunities to fail fast and learn within your organization.
  - Level set and work on managing expectations with your management in regards to audits, assessments, and benchmarking.

"Apply"

- In the first three months following this presentation you should:
  - Evaluate what type of assessments your organization have gone through over the past 6 month to a year.
  - Then see where you failed in those assessments and whether those failures were embraced and lessons were learned as well as improvements were made.
- Within six months you should:
  - Select a set of security assessments to use to gain experience and be ok with failing
  - Measure your progress from embracing this model and seeing how it impacted your risks.
  - Ask yourself; "Is failing forward happening?"

Sources

- Times.com
- Fortune.com
- Verizon DBIR and DBD
- Fail Fast, Fail Often *How Losing can help you win.* By: Ryan Babineaux, Ph.D and John Krumboltz, Ph.D
- Timeline.com
- Forbes.com
- “How Not to Land an Orbital Rocket Booster” Youtube compilation
- Art and Fear by: Ted Orland and David Waylon

Questions???

My-Ngoc Nguyen

Email: myngocn@SecITSol.com

Phone: (702) 608-0437

Web: SecuredITSolutions.com

Location: 6795 Edmond Street

Las Vegas, NV 89118