The Road Less Traveled

War Stories from the Life of an Onsite Assessor

Jon Ehret

VP of Strategy & Risk - RiskRecon

riskrecon

mastercard

My Bio

Jon Ehret – VP, Strategy & Risk

- CISSP, CISA, CRISC
- Third party risk practitioner since 2004
- Co-founder and former President of the Third Party Risk Association
- Experience building and running third party risk programs in finance and healthcare

Jonathan.ehret@riskrecon.com

riskrecon
mastercard

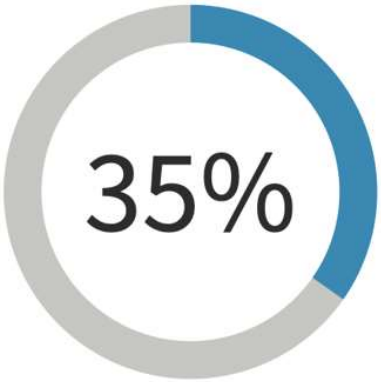
Two roads diverged in a wood, and I took the one less traveled by,
And that has made all the difference.

- Robert Frost

riskrecon
mastercard

The Onsite Assessment – The Road Less Taken

- Not widely used
  - In a RiskRecon study of over 150 TPRM programs, only 35% performed onsite assessments
  - Pretty much impossible during current environment
- Costly and time consuming
  - Can add weeks to onboarding time and drive review $$ up
- Don’t make sense for every vendor
  - I suggest your critical vendors or those vendors that cause concern
- Very valuable tool that can tell you things about your vendor no other tool can



riskrecon
mastercard

Does your questionnaire tell you about this??

Would it change your mind about doing business with them?

riskrecon
mastercard

War Stories From My Life as an Onsite Assessor

riskrecon
mastercard

Opportune timing

- Random mid-western company
- Facilities manager boasted about how their generators would fire up within 30 sec of a power outage
- 5 minutes after saying it….total power failure
  - Generator was up and running in roughly 20 sec
- Somewhat related….I had another IT Manager offer to cut the power to his building in order to prove resiliency.

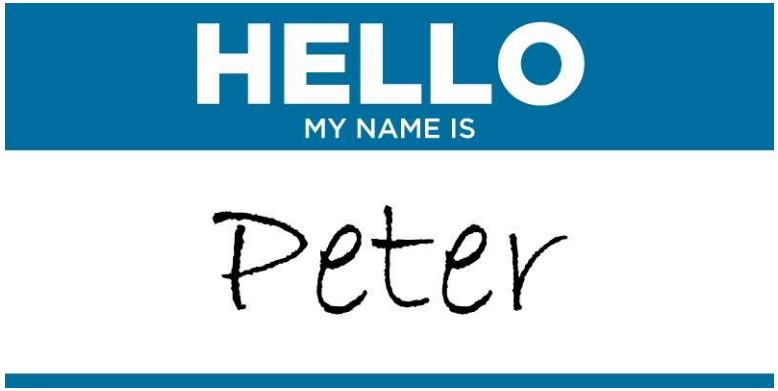
riskrecon
mastercard

But I like to see the blinky lights…

- Company's datacenter was in a glass room
- CEO stated that he liked to walk by and see all the lights blinking so he knew stuff was working
- Adjacent to datacenter was an exterior glass door
  - Opened up to a dark parking lot with no cameras

riskrecon
mastercard

Does Anyone Work Here??



- Silicon valley fintech startup, early 2000's
- Onsite visit to office space
- Decent size facility, but almost nobody present
- Office cubes labeled with white sheets of paper and the names handwritten in pen

riskrecon
mastercard

The Chatty Guy

- Mortgage collections agency, circa 2014
- For the most part normal onsite visit until…
  - Chief Compliance guy decided to sit in and introduce himself
  - Proceeded to talk about how he was all over YouTube being accused of unfair collections acts

riskrecon
mastercard

Waterfront Property

- Small mid western company, mid 2000's
- Onsite visit to data center revealed it was in the basement of facility
- Facility was only feet from bank of river
- Data center was below water level
- River had a history of flooding

riskrecon
mastercard

The Pony Express

- Actually more than one place!
- Answered via questionnaire that backups/media were securely transferred offsite
- In reality transferred via cardboard box
  - One stored them next to bed of CEO
  - One stored them in the box, on the floor of his garage in South Florida

riskrecon
mastercard

The Boiler Room

- Collection Agency
- Owner greeted me wearing a tracksuit with gold chains and chest hair
- Large open floor space with rows of card tables set up, PCs loosely sitting in place
- Operation could be torn down and rebuilt anywhere in city within 6 hours
- IT Manager was the guy who owned a PC the longest
  - Behind his desk was a bunch of “For Dummies” books.

riskrecon
mastercard

Disposable Buildings

- Major International Fintech, mid 2000's
- Their mail room had been exposed during the Anthrax scare in 2001
- To address, they made the mail room a modular building
  - Kept a spare building in back that could be dropped in by crane as needed

riskrecon
mastercard

Want to know more about RiskRecon

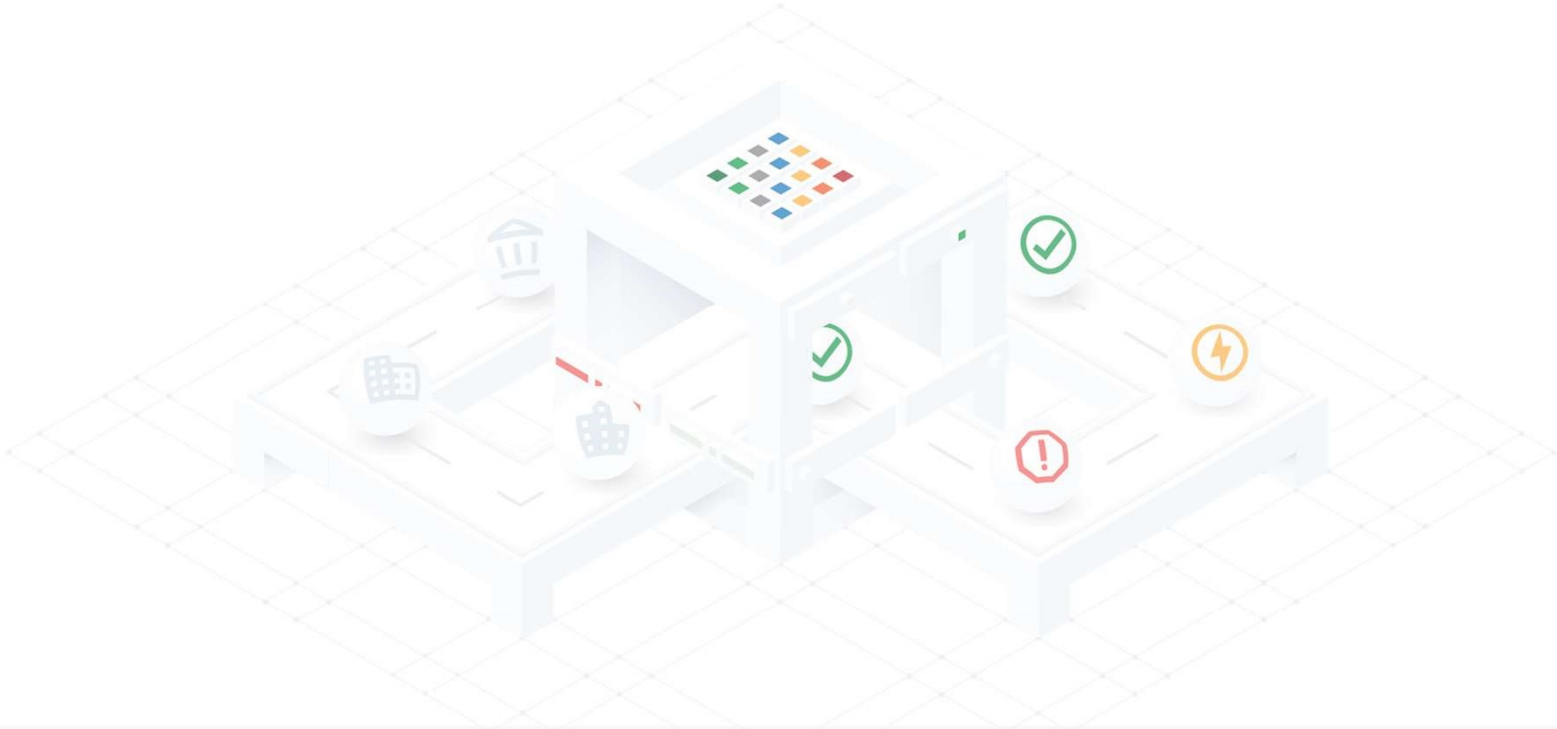
www.RiskRecon.com

Contact: sales@riskrecon.com

Resources

1) Know Your Risk Now – Free Risk Assessment Report https://www.riskrecon.com/know-your-risk
2) AWS Core Assessment Toolkit https://www.riskrecon.com/aws-assessment-toolkit
3) Third-Party Security Risk Management Playbook https://thirdpartyplaybook.com
4) Forrester Cybersecurity Risk Rating Solutions Wave Report https://bit.ly/riskrecon-forrester-wave
5) Ripples Across the Risk Surface Report https://www.riskrecon.com/ripples-across-the-risk-surface
6) Third-Party Risk Management Insights https://blog.riskrecon.com

riskrecon
mastercard



Thank you.

riskrecon
mastercard