PERSONALITY PROFILING YOUR THIRD PARTIES FOR EFFECTIVE SUPPLIER MANAGEMENT

John Elliott
Data Protection Officer @ Large European Airline | Author @ Pluralsight
@withoufire
Hello

My name is ...

John

I am ...

ENTP
**ENTP**

- **E – Extroversion preferred to introversion:** ENTPs gain energy through interactions with people or objects in the outside world.

- **N – Intuition preferred to sensing:** ENTPs tend to be more abstract than concrete. They focus their attention on the big picture rather than the details first, and on future possibilities rather than immediate realities.

- **T – Thinking preferred to feeling:** ENTPs tend to value objective criteria above personal preference. When making decisions, they generally give more weight to logic than to social considerations.

- **P – Perception preferred to judgment:** ENTPs tend to withhold judgment and delay important decisions, preferring to "keep their options open" should circumstances change.
I should be good at ...

- Innovation
- Original thoughts
- Invention
- Visionary things
- Being a Lawyer (!)
I’m not awesome at ...

- Following through with detailed plans
- Thinking of the needs of other people
- Single tasking
- Responding well to authority....
Here’s my thought

Do third-party vendors have personalities?
Here’s my thought

and if they did, would that affect how we manage them?
This has nothing to do with compliance

Which third parties are most likely to lose data

What can I do to minimize this risk
Vendor / Supplier / 3rd Party risk is ...

**IMPACT**

- Inherent service risk: Independent of the vendor capabilities

**PROBABILITY**

- Vendor risk: DEPENDENT on the vendor capabilities
- Service architecture risk: Independent of the vendor capabilities
Vendor risk is ...

- Inherent service risk
- Vendor risk
- Service architecture risk

Impact

Probability

Quantified Qualitative Risk
Vendor risk is ...

- Inherent service risk
- Vendor risk
- Service architecture risk

**Impact**

**Probability**

- Quantified Qualitative Risk
- More Magic

- Contracts
- Documented advice and assistance
- Operational readiness targets
- Operational readiness assessment
- Ongoing assessment
Vendor risk is ...

There could be infinite variables here
Vendor risk is ...

There are less options here

- Documented advice and assistance
- Operational readiness targets
- Operational readiness assessment
- Ongoing assessment
Vendor risk is ...

- Standards
- Manuals
- Level of detail

- Self-assess
- Phone
- Audit
- Auto

- Documented advice and assistance
- Operational readiness targets
- Operational readiness assessment
- Ongoing assessment
Process

Could vendor personality affect

- Documented advice and assistance: OK
- Operational readiness targets: OK
- Operational readiness assessment: OK
- Ongoing assessments: OK
3-axis of supplier personalities

Knowledge

Able to execute

Intent to execute

Ignorant    Know
Unable      Able
Negative    Positive
## Vendor Personality Types

<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Ability</th>
<th>Intent</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know</td>
<td>Able</td>
<td>Positive</td>
<td>KAP: Dream supplier</td>
</tr>
<tr>
<td>Ignoreant</td>
<td>Able</td>
<td>Positive</td>
<td>IAP: Dunning Krugers</td>
</tr>
<tr>
<td>Ignoreant</td>
<td>Able</td>
<td>Negative</td>
<td>IAN: Bureaucrats</td>
</tr>
<tr>
<td>Ignoreant</td>
<td>Unable</td>
<td>Positive</td>
<td>IUP: Puppies</td>
</tr>
<tr>
<td>Ignoreant</td>
<td>Unable</td>
<td>Negative</td>
<td>IUN: Freddie Krugers</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Positive</td>
<td>KUP: Frustrators</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Negative</td>
<td>KUN: Theorists</td>
</tr>
<tr>
<td>Know</td>
<td>Able</td>
<td>Negative</td>
<td>KAN: Deceivers</td>
</tr>
</tbody>
</table>

**Legend:**
- **Know:** Fully aware of the situation and their ability to handle it.
- **Ignorant:** Unaware of either the situation or their ability to handle it.
- **Able:** Capable of handling the situation.
- **Unable:** Not capable of handling the situation.
- **Positive:** Intent is to support and collaborate.
- **Negative:** Intent is to avoid or deceive.
Documented advice and assistance: OK
Operational readiness targets: OK
Operational readiness assessment: OK
Ongoing assessments: OK

Could vendor personality affect
Process

Knowledge

- Know
- Ignorant

Documented advice and assistance
- Extensive+ follow up

Operational readiness targets
- high-level
- detailed

Operational readiness assessment
- self
- onsite

Ongoing assessments
- phone
- onsite
Process

Able to execute

Able

Unable

Documented advice and assistance

Operational readiness targets

Operational readiness assessment

Ongoing assessments

Able

Unable

Detailed

Self

Onsite

Phone

#RSAC

RSA Conference 2018
## Process

<table>
<thead>
<tr>
<th>Intent to execute</th>
<th>Documented advice and assistance</th>
<th>Operational readiness targets</th>
<th>Operational readiness assessment</th>
<th>Ongoing assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive</td>
<td></td>
<td></td>
<td>self</td>
<td>self</td>
</tr>
<tr>
<td>Negative</td>
<td></td>
<td>detailed</td>
<td>onsite</td>
<td>continuous</td>
</tr>
</tbody>
</table>
# Vendor Personality Types

<table>
<thead>
<tr>
<th>Know</th>
<th>Able</th>
<th>Intend</th>
<th>Docs &amp; assist</th>
<th>OR Targets</th>
<th>OR Assess</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>K\text{now}</td>
<td>A\text{ble}</td>
<td>P\text{ositive}</td>
<td>Self</td>
<td>Detailed</td>
<td>Onsite</td>
<td>Continuous</td>
</tr>
<tr>
<td>K\text{now}</td>
<td>A\text{ble}</td>
<td>N\text{egative}</td>
<td>Self</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
</tr>
<tr>
<td>K\text{now}</td>
<td>U\text{nable}</td>
<td>P\text{ositive}</td>
<td>Detailed</td>
<td>Onsite</td>
<td>Phone</td>
<td>Continuous</td>
</tr>
<tr>
<td>K\text{now}</td>
<td>U\text{nable}</td>
<td>N\text{egative}</td>
<td>Detailed</td>
<td>Onsite</td>
<td>Phone</td>
<td>Continuous</td>
</tr>
</tbody>
</table>
Vendor Personality Types

<table>
<thead>
<tr>
<th>Know</th>
<th>Able</th>
<th>Intend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know</td>
<td>Able</td>
<td>Positive</td>
</tr>
<tr>
<td>Know</td>
<td>Able</td>
<td>Negative</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Positive</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Negative</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Positive</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Negative</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Positive</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Negative</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Docs &amp; assist</th>
<th>OR Targets</th>
<th>OR Assess</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self</td>
<td>Self</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Continuous</td>
<td></td>
</tr>
<tr>
<td>Extensive+ follow up</td>
<td>Phone</td>
<td>Self</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
</tr>
<tr>
<td></td>
<td>Onsite</td>
<td>Continuous</td>
<td></td>
</tr>
</tbody>
</table>
Vendor Personality Types

<table>
<thead>
<tr>
<th>Know</th>
<th>Able</th>
<th>Intend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know</td>
<td>Able</td>
<td>Positive</td>
</tr>
<tr>
<td>Know</td>
<td>Able</td>
<td>Negative</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Positive</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Negative</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Positive</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Negative</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Positive</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Negative</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Docs &amp; assist</th>
<th>OR Targets</th>
<th>OR Assess</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extensive+ follow up</td>
<td>Detailed</td>
<td>Detailed</td>
<td>Self</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Self</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Phone</td>
<td>Phone</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Continuous</td>
<td>Continuous</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Onsite</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Phone</td>
<td>Phone</td>
</tr>
<tr>
<td>Detailed</td>
<td>Onsite</td>
<td>Continuous</td>
<td>Continuous</td>
</tr>
</tbody>
</table>
## Vendor Personality Types

<table>
<thead>
<tr>
<th>Know</th>
<th>Able</th>
<th>Intend</th>
<th>Docs &amp; assist</th>
<th>OR Targets</th>
<th>OR Assess</th>
<th>Ongoing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know</td>
<td>Able</td>
<td>Positive</td>
<td>Self</td>
<td>Self</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Know</td>
<td>Able</td>
<td>Negative</td>
<td>Detailed</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Positive</td>
<td>Onsite</td>
<td>Detailed</td>
<td>Continuous</td>
<td></td>
</tr>
<tr>
<td>Know</td>
<td>Unable</td>
<td>Negative</td>
<td>Detailed</td>
<td>Onsite</td>
<td>Continuous</td>
<td>Phone</td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Positive</td>
<td>Phone</td>
<td>Self</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ignorant</td>
<td>Able</td>
<td>Negative</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Positive</td>
<td>Onsite</td>
<td>Onsite</td>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>Ignorant</td>
<td>Unable</td>
<td>Negative</td>
<td>Onsite</td>
<td>Continuous</td>
<td>Continuous</td>
<td></td>
</tr>
</tbody>
</table>

Remember, this is just a model.
SO HOW CAN YOU ASSESS A VENDOR’S PERSONALITY?
Sniff test
External Ratings (also sniff test)

But beware of ...

<table>
<thead>
<tr>
<th>Know</th>
<th>Able</th>
<th>Negative</th>
</tr>
</thead>
</table>

SecurityScorecard
BIT SIGHT
UpGuard
Ask Open Questions

Make the vendor think

Demonstrate knowledge, ability or intent

Force deceitful declarations

Can not be completed by sales
Q. What do you see as the top three cyber threats to your business?
Q. How do you gain short-, medium- and long-term threat intelligence?
Q. What formal and informal information sharing networks are you members of?
Q. How many days of professional resource have been used in penetration testing and ‘red team’ tests or other similar assurance exercises in the past twelve months?
...What do you plan to do differently next year?
Q. How many people have more than 50% of their role allocated to cyber/information security responsibilities?
Ask open questions

...Do you think this is enough?
Q. How many person-days have you estimated would it take a malicious external attacker to breach your defenses and gain privileged access to critical systems?
...How quickly would you detect this type of intrusion into your network?
...How many intrusions have you detected in the past twelve months?
Q. What are the RPO, RQO and RTO for the systems that support the service you provide to us?
... When you last did a test what RTO, RPO and RQO did you achieve?
Q. Have you formally appointed a Data Protection Officer (DPO)? If so, who is this.
Ask open questions

... If so, who is this ...
Ask open questions

... and what are their qualifications ...

RSAConference2018
Q. What processes do you have in place to respond to Data Subjects who request their data in accordance with GDPR Article 15?
Q. How will you detect a ‘Personal Data Breach’?
What’s interesting?

Non-answers

We have ISO27001 and our CISO is awesome answers

Long answers
What’s interesting?

- This is far too confidential
- Everything is outsourced to XXX
- No one asked us this before
Summary ...

Inherent service risk
Vendor risk
Service architecture risk

IMPACT

Quantified Qualitative Risk

PROBABILITY

Contracts
Documented advice and assistance
Operational readiness targets
Operational readiness assessment
Ongoing assessment

Magic
More Magic
Summary...

Vendor Personality can determine the effort needed

- Inherent service risk
- Vendor risk
- Service architecture risk

IMPACT

PROBABILITY

Contracts
- Documented advice and assistance
- Operational readiness targets
- Operational readiness assessment

Ongoing assessment
Taking this back to the office

- Isolate the levers (approaches) you use to gain supplier assurance
  - Do you use operational readiness targets

- Can you save resources by profiling suppliers?
  - This exercise is not free

- Would it save compliance-related activities?

- Try a sample questionnaire on some suppliers
QUESTIONS

Or @withoutfire