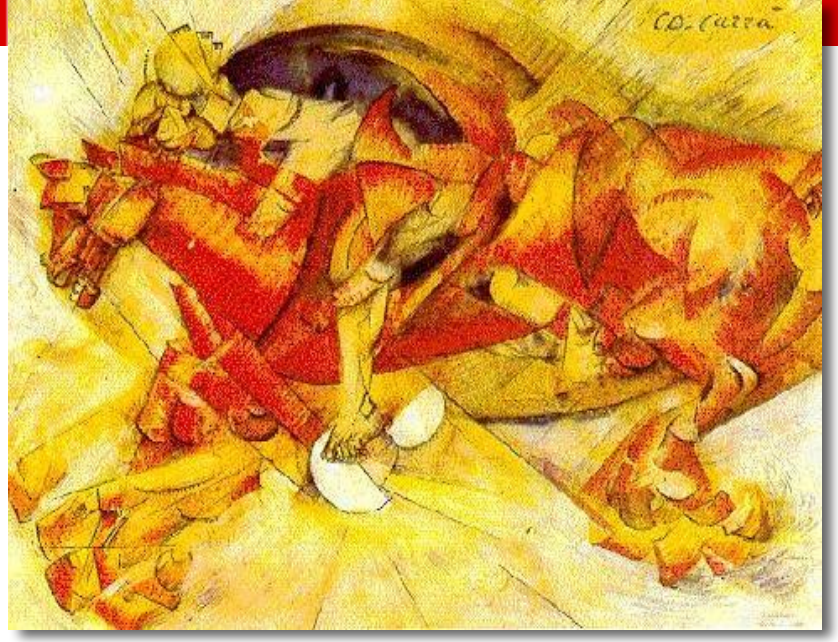


Information Assurance: Best Practices

Fiona Pattinson

Payment Security Training Conference - Beijing, China
Feb 28th, 2014

This is not a new problem

我非生而知之者，好古，敏以求之者也。

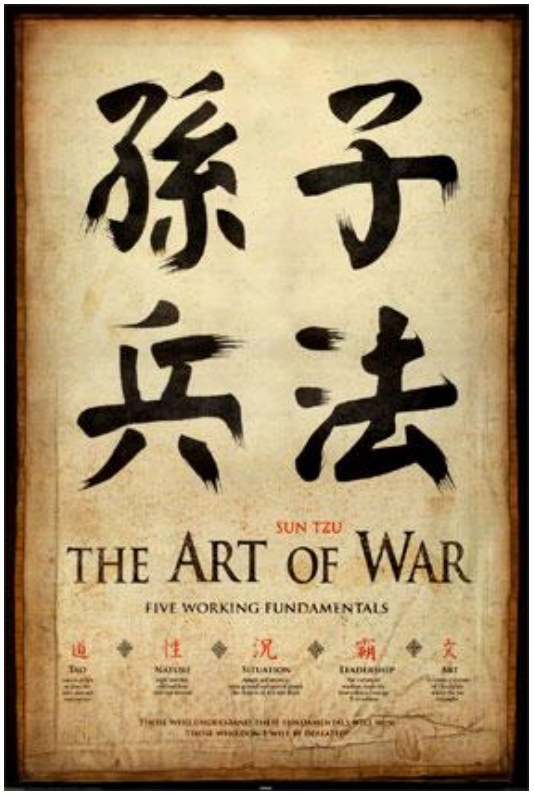
I am not one who was born in the possession of knowledge;

I am one who is fond of antiquity,
and earnest in seeking it there.

Threats

Vulnerabilities

Reducing risks



Ancient Information Assurance

Who told you?

What did they tell you?

When did they tell you?

Why did they tell you?

Was the information intended for you?

How did they get the information?

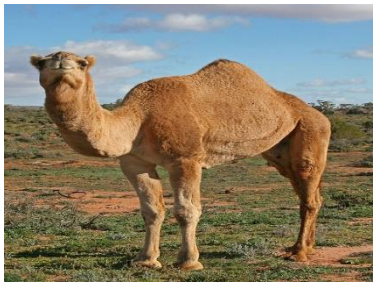
Do you have confidence in the information they gave you?

These are NOT new questions

From: http://nanrae.com/chinese-seals.html

Cylinder seal c1800 BC

Technology solutions are not new



=

=

=

MS 4631
Bulla-envelope with 11 plain and complex tokens inside.
Near East, ca. 3700-3200 BC

Identity solutions are not new

Ancient seal script	Simplified seal script	Mou seal script	Bird-and-insect script	Hanging-needle seal script	Regular script	"fiudie" seal script
This kind of seal script with an irregular and complicated structure was mainly used in the Warring States period(475 -221BC).	This script with neither too round nor too square characters was commonly used for the Qin and some Han seals (221BC-AD220).	As a major script for the Han seals, the Mou script modified characters with more curved strokes on the base of the Xiao seal script.	It is a kind of modification of seal script, which made characters in form of a bird, fish or insect.	This seal script was sometime used for private Chops of the Wei and Jin dynasties (220-420) with vertical strokes ended pointedly like a needle.	It is seldom seen in Han (206 BC~ AD 24) and Jin (265-420)Chops, but often in Song (960-1279) and Yuan (1271-1368) private Chops.	It first appeared in the Sui and Tang official Chops (581-907), and was continuously used for the Jin, Yuan, Ming and Qing (1115-1911) seals.
 Chun'an Jun (an oficial title)	 Jiao De (a person's name)	 Prince Guangling Seal	 Wu Yi (a person's name)	 Duck Xuancheng Seal	 Shang Qi Signature	 Pingding County Seal

Special terms for seals

From: http://nanrae.com/chinese-seals.html

Trust

Who issued them?

Who stands behind them?

Who trusts them?

Who has confidence in them?

Are they real?

© 2013 ParkPennies

Since ancient times we learned some very important characteristics of assurance

诚信

Good faith

Bona fides

absence of fraud or deception

Information Assurance Best Practices Today

新年快乐.

31 January 2014

18 February 2015

Wood Horse

Best Practices for Information Assurance in 2014

…did not change!

Who told you?

What did they tell you?

When did they tell you?

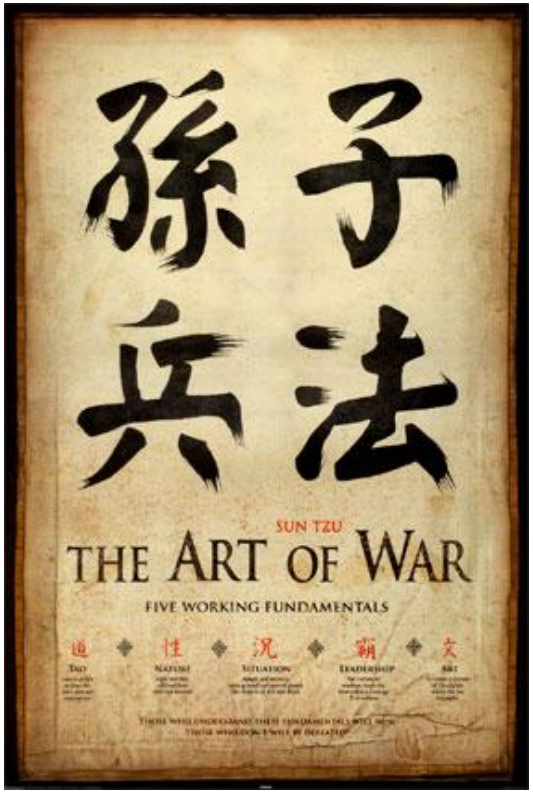
Why did they tell you?

Was the information intended for you?

How did they get the information?

Do you have confidence in the information they gave you?

Measurement



IV: Tactical Dispositions

軍形

善用兵者，修道而保法，故能為勝敗之政。

兵法：「一曰度，二曰量，三曰數，四曰稱，五曰勝；地生度，度生量，量生數，數生稱，稱生勝。」故勝兵若以鎰稱銖，敗兵若以銖稱鎰。勝者之戰民也，若決積水于千仞之谿，形也。

18: Measurement owes its existence to Earth;

Estimation of quantity to Measurement;

Calculation to Estimation of quantity;

Balancing of chances to Calculation; and

Victory to Balancing of chances.

Measurement

BITS

THE Open GROUP
Making standards work®

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

International
Organization for
Standardization

Example: PCI DSS

A merchant provides a Credit Card company with a PCI DSS report.
From the Credit Card company's point of view...

Q: Who told you? ***A: The merchant***

Q: What did they tell you? ***A: That they comply with the PCI DSS***

Q: When did they tell you? ***A: Within the last year***

Q: Why did they tell you? ***A: Because you mandate them to***

Q: Was the information intended for you? ***A: Yes***

Q: How did they get the information? ***A: From a trusted third party , following the PCI DSS standard***

Does the Credit Card Company have confidence in the information they have been given?

Example 2: PCI DSS

A merchant provides their customer with the same PCI DSS report.
From the customer's point of view…

Q: Who told you? *A: The merchant*

Q: What did they tell you? *A: That they comply with the PCI DSS*

Q: When did they tell you? *A: Within the last year*

Q: Why did they tell you? *A: Because they want to demonstrate that they are trust worthy*

Q: Was the information intended for you? *A: No*

Q: How did they get the information? *A: From a trusted third party , following the PCI DSS standard*

Does the customer have confidence in the information they have been given?

Example: FIPS 140-2

A developer points an integrator to the list of FIPS 140-2 validated modules, proudly showing that their module is listed...

Q: Who told you? ***A: The CMVP (US and Canadian govt)***

Q: What did they tell you? ***A: That they comply with their own FIPS 140-2 spec, and that the module may be legally procured by the US Government***

Q: When did they tell you? ***A: During the lifetime of the module***

Q: Why did they tell you? ***A: Because the program has a very high reputation and can be relied on even by those outside of the US government.***

Q: Was the information intended for you? ***A: No***

Q: How did they get the information? ***A: From a (mutually) trusted third party.***

Is the CMVP acting as a trusted assurance "broker"?

Measuring the assurance

Criteria	PCI-DSS (QSA)	PCI-DSS (SAQ)	O-TTPS	CC	FIPS 140-2
Independent 3rd Party assessment	☑	☒	☑	☑	☑
Program validation	☑	☒	☑	☑	☑
Tiered assurance for the assessment	☒ ☞ Risk based	☒ ☜ Risk based	☒	☑	☑
Regular risk assessment for the "assurance consumer" embodied in the standard	☑ 3-year	☑ 3-year	☑ TBD	☑ For each assess-ment	☒
Tiered assurance (Levels) for the subject of the assessment	☒	☒	☒	☑	☑
"assessment subject" promise: warrant & represent	☑	☑	☑	☒	☒

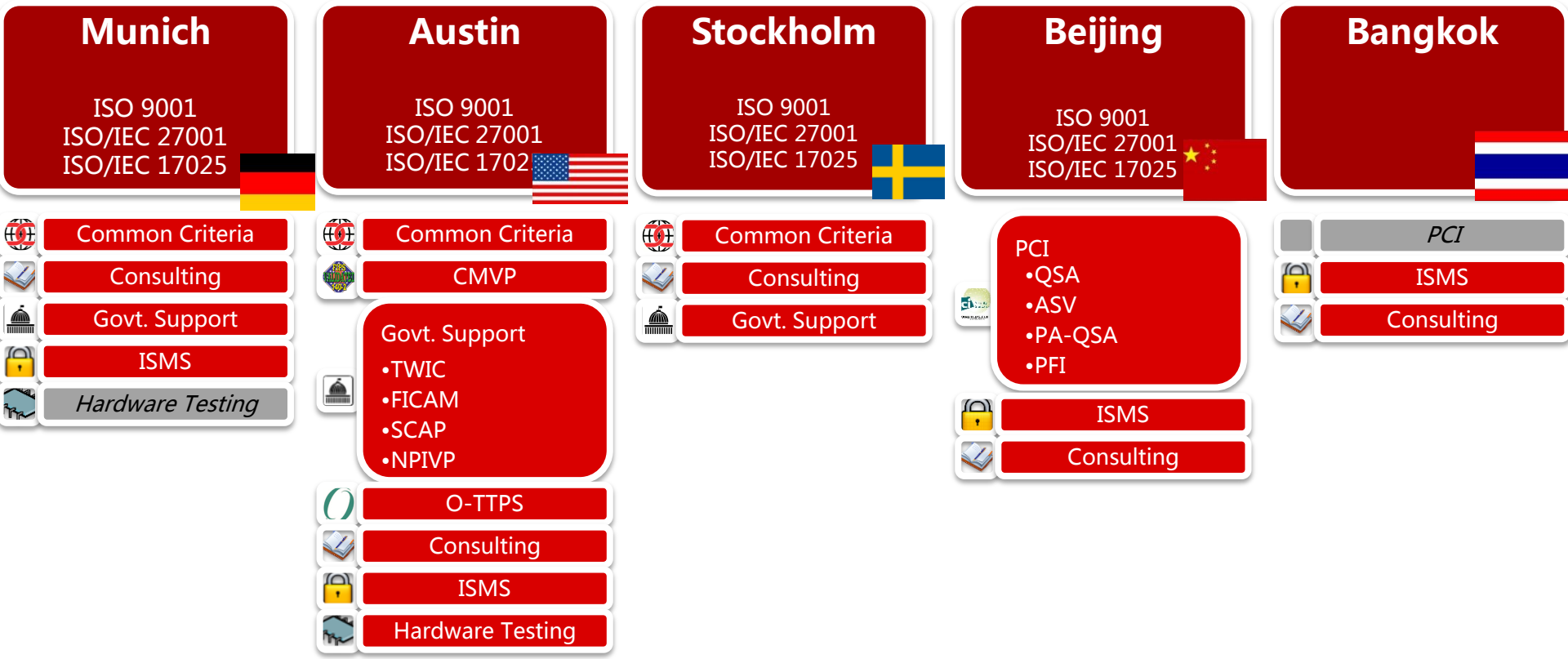
Combining Assurance

Example, the financial industry

Selecting assurance for the different components of their business based on risk

ISO/IEC 27001, CC, FIPS 140-2, PCI-DSS, PA-DSS

Globalization on security services



Trends and the Future

The demand for assurance is rising , the use of COTS ICT products grows seemingly logarithmically, the technology used by the products evolves and the threats to them evolve too.

The need to address high volume is a driver for the assurance programs:

e.g. PCI-DSS compliance programs tiered to meet the risks presented by high volume processors vs low volume processors.

- Shorter assessment times
- Reduced assessment costs

Trends and the Future

The need to address evolving technology and threats is a driver for the standards: For example In ISO/IEC JTC 1/SC 27, several study periods are underway including:

- Privacy Impact Assessment (PIA) Security evaluation of anti-spoofing techniques for biometrics
- Privacy seal programs
- PKI
- Clouds
- High Assurance
- Competence Requirements for security evaluators
- Operational testing of cryptographic modules in the environment

Summary

Information Assurance is NOT new.

Trust and confidence are very important issues

Today, measurement , and some trust and confidence comes through careful use of:

a) National and International Standards

b) The assurance programs utilizing the standards

问题