



# Vendor Survey of Assurance Practices

ACSAC 2008  
Works In Progress Session

Sean Barnum  
Principal Consultant  
sbarnum@digital.com

Jeremy Epstein  
Principal Consultant  
jepstein@digital.com



digital

Software Confidence. Achieved.

www.digital.com  
info@digital.com  
+1.703.404.9293

# What do vendors really do?

- *What* do they do to increase assurance?
- *Who* does assurance within the company?
- *Why* do they invest in assurance?
- *When* did they start assurance?



## Vendor participation summary

Vendor	K	H	M	W	F	B	S	R
Size	Large	Large	Small	Medium	Small	Large	Large	Large
Security	No	Yes	Yes	Yes	Yes	No	No	No

### Size:

- Small <US\$100M/year
- Medium >US\$100M, <US\$1B/year
- Large >US\$1B/year

### Security:

- Yes – company's products are *predominantly* security (firewalls, IDS, PKI, anti-virus)
- No – company's products are not predominantly security (business software, network infrastructure, network management, DBMS)

*All of the large companies in the survey have some security and some non-security products; classification by predominance*

## Results – “what” questions

<i>Vendor</i>	<i>Training?</i>	<i>Design reviews?</i>	<i>Pentesting?</i>	<i>Source analysis?</i>	<i>Dynamic testing?</i>
M	Informal	Informal	Internal & external	Manual	Yes
W	Formal & refresher	Not a focus	Internal, external, & customers	Proprietary tools	Yes
F	Informal & seminars	Performed by developers	Extensive internal, some external	Manual & proprietary tools	Yes
H	Formal	Informal	Internal, external & customers	Company-wide automated	Yes
B	Formal, extensive	Workshop with experts	Internal but discouraged	Company-wide automated	Yes
S	Seminars	Workshop with experts	Field only	Manual, simple tools	Minimal
K	Formal, mandatory	Performed by security expert	Varies by product	Varies by product, some automated	Yes
R	Minimal	Minimal	Not internal, but attacked by hackers	Primary focus – before every check-in	Minimal



## Results – “why” questions

<i>Vendor</i>	<i>Customer expectations</i>	<i>Fear of publicity</i>	<i>Explicit requests</i>
M	Primary	Secondary	Minor
W	Primary	Minor	Govt only (Common Criteria)
F	Primary	Yes – “don’t be viewed like Microsoft”	Occasional
H	Secondary	Primary	Govt only (Common Criteria)
B	Secondary	Minor	Primary
S	Secondary	Primary – “CNN moment”	Govt only (Common Criteria)
K	Primary	Secondary	Minor
R	Primary	Minor	Govt only (Common Criteria)



# Conclusions

- Software vendors are aware of the risks of insecure software, and are frequently motivated by fear to minimize the security vulnerabilities in their products.
- Few non-government customers explicitly ask for software assurance, but vendors believe that it's an unspoken expectation.
- Common Criteria was mentioned by nearly all vendors, and all but two felt it was a paperwork exercise that had almost no impact on the assurance of their products.
- Techniques used to gain assurance vary among vendors, but nearly all agree that developer training is one of the most valuable uses of limited resources.
- All agree that penetration testing has its limitations, it is still helpful as a way to know how good or bad a product is.
- Source code analysis is still early in the acceptance phase, both because tools are expensive and difficult to use effectively.
- Dynamic testing, including fuzzing, seems to be more cost-effective.

# What's next?

- Extensions to the survey
  - Please encourage vendors to contact me to participate!
- Future surveys for other industry segments?
  - Embedded systems?
  - Financial institutions (affected by OCC & PCI requirements)?
  - Online merchants?
  - SaaS vendors?
  - Integrators (more likely to be influenced by govt standards)?
- How will vendors use this information?
  - Will it encourage those behind the curve to catch up?
  - Will it provide excuses for those in the middle to continue?
  - Will it cause those at the front to reduce spending?
  - Following “industry norms” is a good defense against lawsuits...





# Vendor Survey of Assurance Practices

**Sean Barnum**

Principal Consultant  
sbarnum@cigital.com

**Jeremy Epstein**

Principal Consultant  
jepstein@cigital.com



**cigital**

Software Confidence. Achieved.

[www.cigital.com](http://www.cigital.com)  
[info@cigital.com](mailto:info@cigital.com)  
+1.703.404.9293