

The Compliance Hangover

NIST Key Management Workshop
June 9, 2009

Brian Tokuyoshi
Product Marketing Manager
PGP Corporation



Compliance!



Data Breaches!

3

Compliance and
protection from
data breaches
are not the
drivers for
Enterprise Key
Management

4

It's causing the
problem.

5

The Aftermath of Compliance & Data Breaches

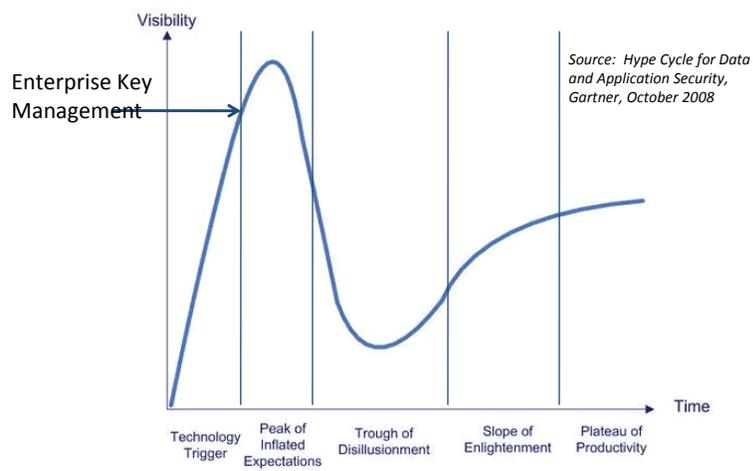
- Tight deadlines place emphasis on the goal, without considering the ramifications about the path taken
- Compliance only talks about getting the data encrypted, not how fast it should be decrypted. That's e-discovery.
- The coming hangover
 - Key Management is often done poorly
 - No overall strategy
 - Government agencies and DAR
 - Enterprise is next
- Deploying encryption without a plan to manage keys is a major driver for enterprise key management

6

Best Practices

- 1 Survey and catalog existing data
- 2 Plan your long term encryption requirements
- 3 Develop an enterprise policy on keys
- 4 Deploy a framework to manage encryption
- 5 Deploy data protection solution
- 6 Tackle the next project

Gartner Hype Cycle



Conclusions

- Applications tend to make poor key management systems
- For a lot of end-user organizations, it's going to get worse before it gets better
- Customers need to start thinking about processes for security, not just the technology
- Compliance initiatives should emphasize getting the administration done right