Hyperion Focus 16

Mixing security with EPM, what could possibly go wrong?

John Pegrum

Infratects (UK)

My background in EPM Infrastructure.

- 2006 – 2007 Hyperion Senior Infrastructure Consultant
- 2007 – 2010 Oracle Principal EPM Infrastructure Consultant
- 2010 – Now Infratects UK EPM Senior Infrastructure Consultant
- My role includes technical EPM architecture & design, implementation, migration, upgrades, troubleshooting and Security.
- I've held Microsoft MCSE, Citrix CCEA and VMware VCP certifications and am a Certified Ethical Hacker.

INFRATECTS

Today's Agenda

- Is security of EPM systems taken seriously?
- Traditional approach to EPM security?
- Who's responsible for security?
- Security considerations with EPM.
- Drawbacks of securing EPM.
- Further considerations.
- A weak link?
- Security challenges at clients
- Information Security policies and EPM
- Data classification.
- Corporate InfoSec policy compliance
- Industry standard InfoSec policy compliance
- Compliance everywhere!

INFRATECTS

Is security of EPM systems taken seriously?

- Based on my own experience there has traditionally been little or no effort to secure EPM platforms. This is strange given the business sensitive nature of the data especially HFM.

- EPM naturally has a large surface-attack area with multiple connection points. An almost perfect target?

- Securing EPM can be a time consuming process with multiple patches, server hardening, encryption & firewalling required and as such is often de-scoped from EPM implementations.

Traditional approach to EPM security?

- Latest EPM patches applied at time of implementation.
- Latest Windows updates applied prior to EPM installation.
- EPM patches applied only on a need (often reactive) basis.
- Windows updates often disabled.
- Testing EPM service security rarely done (if at all) however it's incorrectly assumed to be secure.
- One of the limitations of this approach is leaving temporary or permanent gaps in security coverage.

Who's responsible for security?

- It’s hidden in the name.
- Sec **U R** ity
- This is not entirely accurate, the CEO of the company will have overall responsibility and will most likely delegate accordingly.
- However we **all** have a role to play in ensuring that everything we do works to maintain security.

Security considerations with EPM.

- Encrypt or not?
- Do we harden the EPM service?
- Do we vulnerability scan the EPM service? (**If not why not?**)
- Do we penetration test EPM? (**If not why not?**)
- How will we resolve issues highlighted via the vulnerability / penetration testing results?
- If we patch a Middleware component will EPM still work and will it be supported by Oracle?
- How often do we re-visit the security of the EPM service?

Drawbacks of securing EPM.

- Retro-fitting security features (such as end to end SSL) in to an existing EPM deployment can be challenging.
- Securing an EPM platform can add to the overall system management overhead (complexity, troubleshooting, testing). TCO may go up as a result.
- Some EPM components may not be fully secured. (Full SSL and HFM 11.1.2.4).
  Gaps in security start to appear.
- Applying patches may require re-running a Penetration Test to ensure that the security issue has been addressed and no new holes have emerged.
  Close one security loophole and inadvertently open two more?
- Patching Oracle middleware tier with the latest patches may cause issues with EPM and may not be officially supported by Oracle (**ALWAYS** check with Oracle via a SR!)

Further considerations.

- SSL does not automatically secure the EPM platform, it encrypts the communications channel but not the points of entry.
- To fully secure EPM would require various hardening including encrypting JDBC connections, IIS*, OHS, WebLogic, Win32 clients, encrypting the RDBMS, segregating the tiers, log aggregation, alerting and daily review
- This is can be time consuming and would require revisiting on a regular basis.
- More importantly this full securing exercise would need to be done under a corporate security requirement else the likelihood of it happening are pretty remote.

* Not for HFM in EPM 11.1.2.4 however DRM, EPMA & HSF still require IIS.

INFRATECTS

A weak link?

- By not pro-actively patching EPM, Oracle Middleware or the host OS, the EPM service will invariably become a weak link.
- Partial patching or running with old patches can lead to a false sense of security and is almost as bad as not patching at all.
- Security is only as strong as the weakest link in the chain. If you're planning to secure the EPM system, secure it to a recognised security level, do not adopt a pick and mix approach. This is even more critical if cloud hosting!
- DO NOT BE THE WEAKEST LINK.

Security challenges at clients

Clients encounter multiple challenges within the organisation when implementing or running EPM services including:

- Patching EPM and Oracle Middleware to a level that the company Information Security team are comfortable with.
- Maintaining the EPM service especially when OS-level and EPM patches are applied (*Well it worked in Development when we tried it!*)
- Compliance with corporate-wide information security policies
- Compliance with industry-wide information security standards

Information Security policies and EPM

- Company Information Security policies will dictate how the EPM platform **will** be secured, often EPM configuration requirements can come in to conflict of these policies. (Anti-Virus and Windows UAC are good examples)

- Security drivers may include changes in corporate InfoSec policy or a security event.

- Maintaining security is an constantly moving target.

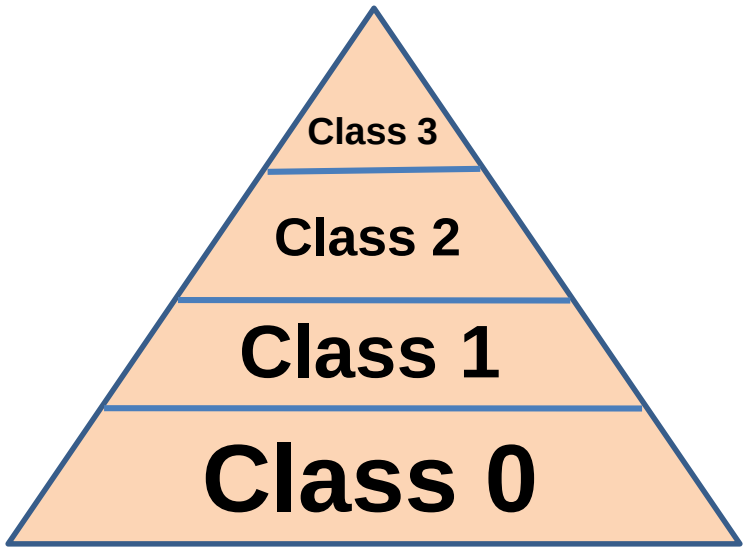
- Security should be at the very heart of the EPM platform and not an after thought.

- One example of a InfoSec policy is Data Classification.

Data classification.

Defining what data classification level the Oracle EPM data sits at within the organisation will often dictate what level of security & related polices apply.

- **Class 0 Public data**
  No damage.
- **Class 1 Sensitive Data.**
  Damage caused if made publicly available.
- **Class 2 Private data.**
  Serious damage if made publicly available.
- **Class 3 Confidential / Proprietary.**
  Exceptionally grave damage caused if made public.



Corporate InfoSec policy compliance

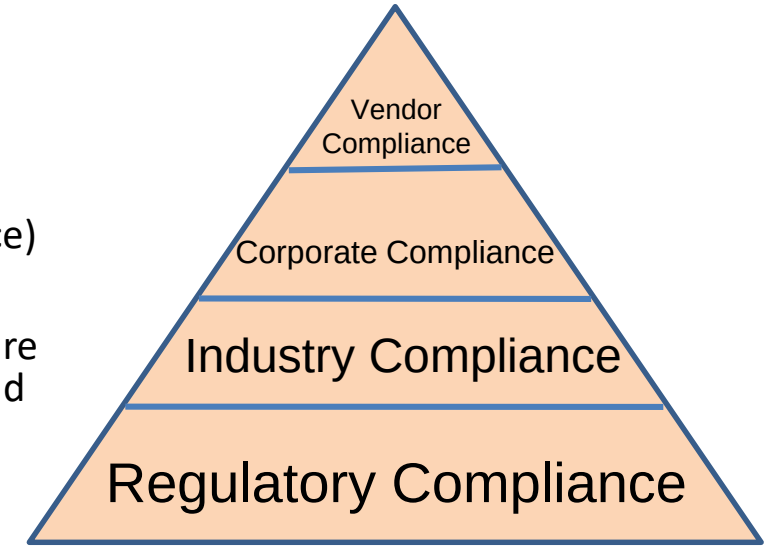
- Company executives are increasingly sensitive to ensuring that they implement and enforce an effective Information Security strategy across the enterprise.
- Security waivers are becoming more difficult to obtain.
- InfoSec policy compliance fast becoming part of internal audit.

Industry standard InfoSec policy compliance

- Industry InfoSec standards often mandate compliance with defined policies and audit these accordingly. Failing to comply even once could lead to losing certification.

Compliance everywhere!

- **Vendor Compliance.** Will **WANT** to adhere to in order to be supported (pre-reqs, supported versions)*
- **Corporate Compliance.** We **SHOULD** adhere as closely as possible (keeping in mind Vendor Compliance)
- **Industry Compliance.** We **WILL** to adhere to ensure that we maintain good standing within our industry and follow industry best-practices.
- **Regulatory Compliance.** We **MUST** adhere to. Severe penalties and other repercussions typically follow should infractions occur.



** Does not include EULA and Licence compliance – as these are both taken as MUST adhere to.*

INFRATECTS

What I've talked about today.

- How security is perceived and how it's traditionally been implemented with EPM.
- The security considerations around patching EPM and some of the inherent issues.
- How Information Security policies are forcing how clients implement and maintain EPM to change.
- How vendor, corporate, industry and regulatory compliance can all affect the EPM service.

Summary

Security will never go away, don’t fight it! Work with the InfoSec team to address potential security and compliance issues .

Take an active interest in how best to protect YOUR EPM service.

DO NOT BE THE WEAK LINK.

Thank you all.

John Pegrum

john.pegrum@infratects.com

INFRATECTS

Hyperion Focus 16

Thank you