Deployment Strategies for Effective Encryption

Ben Rothke, CISSP, CISA
Information Security
Wyndham Worldwide Corp.
Deployment Strategies for effective encryption

- Encryption internals are built on complex mathematics and number theory.
- Your successful encryption program requires a CISSP, CISA and PMP, not necessarily a PhD.
- Effective encryption strategy requires **attention to detail**, **good design**, combined with good **project management** and **documentation**.
- Your encryption strategy must reflect this.
It’s 2013 – where’s the encryption?

- many roll-outs are nothing more than stop-gap solutions
- *Getting it done* often takes precedence over key management, documentation, processes, etc.
- many organizations lack required security expertise
- these and more combine to obstruct encryption from being ubiquitous
- adds up to a significant need for an effective encryption deployment strategy
3 steps to effective encryption

1. define your requirements
2. know where your sensitive data resides
3. create detailed implementation plans

► when implementing your encryption strategy, it’s imperative to remember that your encryption project, and information security is a **process, not a product.**
Encryption nirvana scenario

**Policy**
- Define Drivers
- Data Classification
- Policy Definition

**Strategy**
- Data Mapping
- Risk Modeling
- Control Gaps

**Deployment**
- Implementation
- Management
- Audit

**Initial Drivers**
- Business
- Technical
- Regulatory

**Effective Encryption**
Common deployment mistakes

- Thinking encryption projects are plug and play
  - until they have to deal with key management
  - don’t forget about legacy systems

- Going to a vendor too early
  - vendors sell hardware/software
  - you need requirements, project plans, implementation plans, etc.

- Not giving enough time to design and testing
  - an effective encryption roll-out takes time
  - requires significant details
  - you can’t rush this!
Encryption strategy

- mathematics of cryptography is rocket science
  - most aspects of information security, compliance and audit aren’t
- good computer security is attention to detail and good design, combined with effective project management
  - enterprise encryption strategy must reflect this
- not everyone will need encryption across the board
- policies need to be determined first as to what requires encryption
  - strategy of “let’s just encrypt everything” demonstrates confusion
Analyze your encryption needs

- protect data from loss and exposure
- prevent access to the system itself?
- does software need to access the files after encryption?
- data to be transported securely? via what means?
- how much user burden is acceptable?
- how strong does the encryption need to be?
- do you need to match the solution to the hardware?
- regulatory, contractual, organizational policy
- ask a lot of questions at this point!
  - and when you are done, ask a lot more
Drivers and requirements

► If you don’t know your drivers, you’re driving blind.

► Business
  ► customer trust
  ► intellectual property

► Technical
  ► AES, PGP, BitLocker, etc.
  ► mobile devices

► Regulatory
  ► PCI / SoX / EU / ISO-17799
  ► State data breach laws

Image source: http://www.whattofix.com/blog/archives/2008/05/peace-for-pachy.php
Documentation and policies

- Encryption **must** be supported by policies, documentation and a formal risk management program
  - shows work adequately planned and supervised
  - demonstrates internal controls studied and evaluated

- Policy must be
  - endorsed by management
  - communicated to end-users and business partners / 3rd-parties that handle sensitive data. If it can’t meet company’s policies, don’t give others access to the data
  - encryption responsibility should be fixed with consequences for noncompliance
Encryption processes

- Encryption is a process intensive endeavor
- Must be well-defined and documented
- If not implemented and configured properly, can cause system performance degradation, operational hurdles and locking yourself out of your own data
- Improperly configured encryption processes give false sense of security
  - Perception that confidentiality of sensitive information is protected when it’s not
It’s all about the data

- Identify all methods of data input/output
- storage media
  - smartphones, USB, laptops, removable, SSD, and more
- business partners and other third parties
- understand all applicable regulations and laws
- high-risk areas
  - laptops
  - wireless
  - data backups
  - others
Requirements analysis

► define business, technical, and operational requirements and objectives for encryption

► define policies, architecture, and scope of encryption requirements

► conduct interviews, review policy documents, analyze current and proposed encryption strategy to identify possible security gaps

► determine liabilities

► better requirements definition directly correlates to successful encryption program
Understand your encryption options

► **full-disk / host-based encryption (at rest)**
  ► data encrypted at creation, first possible level of data security

► **appliance-based**
  ► data leaves host unencrypted, then goes to dedicated appliance for encryption. Quickest to implement; but can be costly

► **storage device encryption**
  ► data transmitted unencrypted to storage device
  ► easiest integration into existing backup environments

► **tape**
  ► data encrypted on tape drive; easy to implement
  ► provides protection from both offsite and on-premise information loss

► **database**
  ► database encrypted tables inside the database, protected by native DBMS access controls
Key management (KM)

► Key management is a big deal; don’t underestimate it
► generation, distribution, storage, recovery and destruction of encryption keys
► encryption is 90% management and policy, 10% technology
► most encryption failures due to ineffective KM processes
► 80% of 22 SAP testing procedures related to encryption are about KM
► effective KM policy and design requires significant time and effort
Key management fundamentals

Ask lots of the fundamental questions:

► how many keys do you need?
► where are keys stored?
► who has access to keys?
► how will you manage keys?
► how will you protect access to encryption keys?
► how often should keys change?
► what if key is lost or damaged?
► how much key management training will we need?
► how about disaster recovery?
Immediate steps in the long-term encryption expedition

► prioritize based on specific requirements and compensating controls
► identify your most sensitive/confidential data and know where it resides
  ► organizations that don’t have an effective data classification program usually fail at their data encryption projects - *Gartner*
► know which regulatory mandates matter most
► leverage DLP to more effectively identify sensitive content that resides on the network and at the endpoint
There's a book for that
organizations that do not have an effective data classification program usually fail at their data encryption projects.

creating an effective deployment strategy is the difference between strong encryption and an audit failure.

encryption is about attention to detail, good design and project management.
Ben Rothke, CISSP CISA
Manager – Information Security
Wyndham Worldwide Corporation

www.linkedin.com/in/benrothke
www.twitter.com/benrothke
www.slideshare.net/benrothke