



Preventing Information Leakage?

Scott Shepard
Principal Consultant
GlassHouse Technologies

 **GLASSHOUSE**

Scott.Shepard@GlassHouse.com



Agenda

- Objective: Effectively design and implement framework, with processes and tools to protect the organization from data leakage
- Changing security environment
- Defining a new security strategy
- Case study
 - Data-Centric security strategy
 - Enhanced security controls



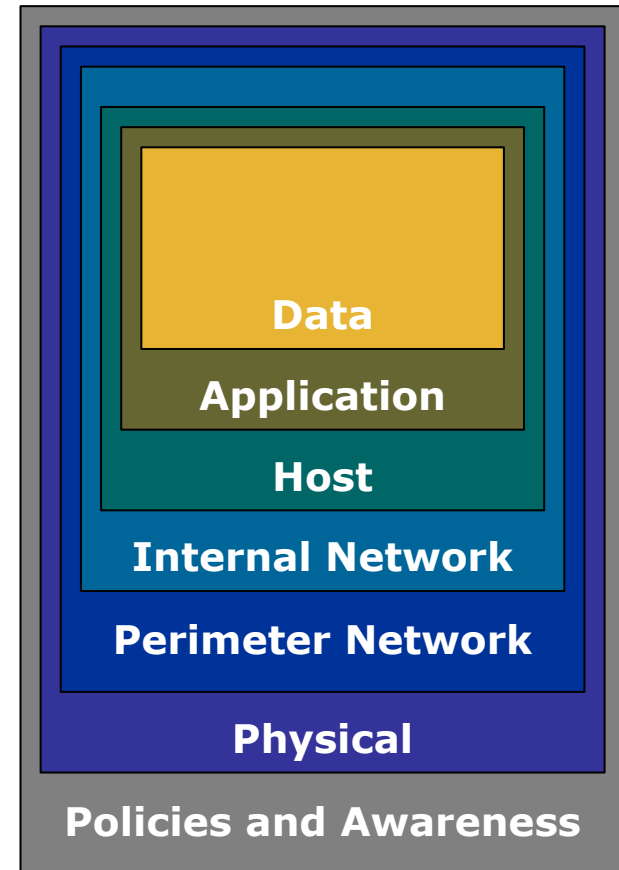
Is Data Leakage Prevention needed?

- **Key logger** found on internal Heartland Payment Systems.
- Hannaford Brothers chain of supermarkets lost more than 4.2 million credit card numbers while in **transit** to credit card processing.
- An employee of Ivy Tech Community College **inadvertently sent an invitation** to view the file to a much larger list of people.
- Employee of Pfizer installed **file-sharing software** that resulted in the exposure of personal data for 15,000+ Pfizer employees, including Social Security numbers.
- Employee of Duracell Corporation **emailed confidential company information** to competing companies.
- Oracle alleged that trade secrets had been **posted** by a former employee in a Google Groups posting.

Changing Security Strategies

Defense-in-Depth

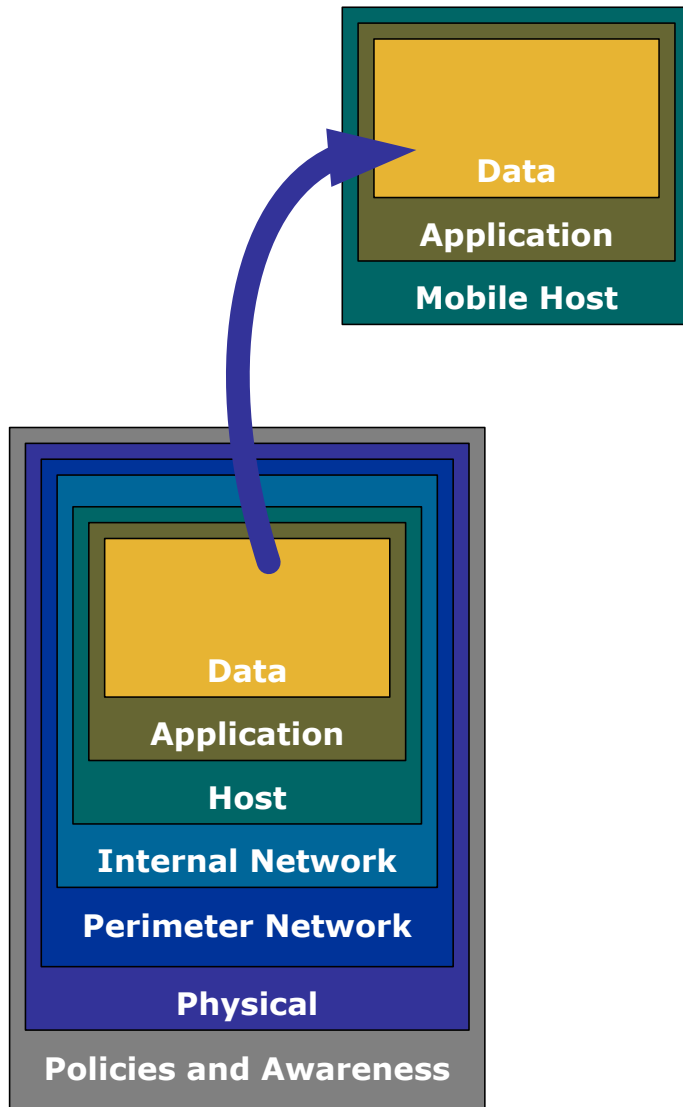
- “Multiple layers of defense are placed throughout an Information Technology (IT) system” –Wikipedia
- Objective:
 - Slow down the attacker
 - Allow the organization to respond
 - Hopefully prevent unauthorized access



Changing Security Strategies

What happens when . . .

- Sensitive data leaves the traditional layers of protection?
- Internal users abuse their privileges? (Insider Threat)





Agenda

- Objective: Effectively design and implement framework, with processes and tools to protect the organization from data leakage
- Changing security environment
- Defining a new security strategy
- Case study
 - Data-Centric security strategy
 - Enhanced security controls

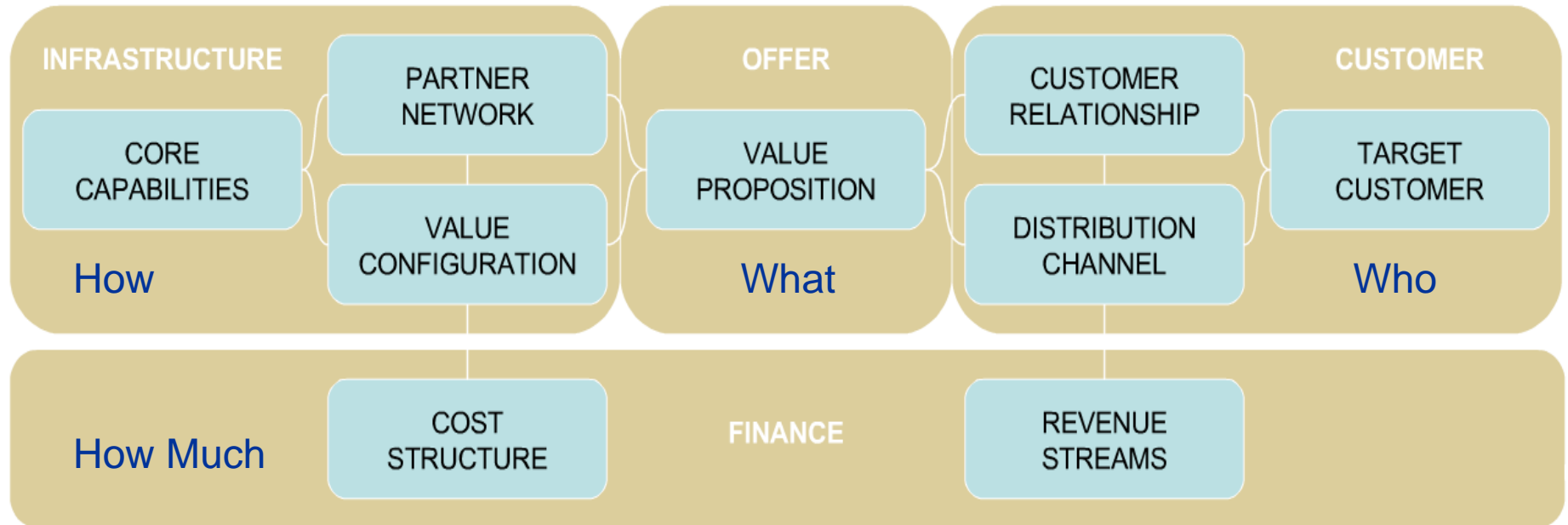


Security Strategy Methodology

- Understand the business drivers
- Define the initial policy
- Identify the control points
- Determine security measures
- Validate and update



Security Strategy Methodology: Understanding the Business Drivers



- Customer Relationship (Who)
 - Who are the company's customers?
- Value Proposition (What)
 - What does the company do for customer?
- Infrastructure (How)
 - How does the company get that job done? Partners?
- Finance (How much)
 - How does the company make money?

*Based on "Business Model Ontology" by Alexander Osterwalder, UNIVERSITE DE LAUSANNE

Security Strategy Methodology: Define the Initial Policy



- Align to the business drivers
 - Protection of Intellectual Property
 - Service availability
 - Transactional processing
- Determine applicable laws and regulations
- Analyze and assess risks



Security Strategy Methodology: Control Points

- Identify the security control points
 - Where in the processing, transmission, and storage of data can security control points be inserted to address confidentiality, integrity, and availability
- Control Points
 - Where to apply:
User, network, system, application, data
 - Targeting:
Authorization, authentication, use, trust relationships and boundaries (entry and exit), configuration, storage, and transport



Security Strategy Methodology: Apply Security Measures

- Determine Security Measures
 - Processes and Technologies
 - For each control point identified, consider protective, detective, and response security measures

- Identify when to layer process and technology while maximizing the security benefit
 - Consider tradeoffs between best in breed and a breadth of coverage
 - Should E-DRM be layered on Full Disk Encryption

Security Strategy Methodology: Validate and Update



- Validate and update
 - Periodic security assessments
 - Adjust to address gaps in
 - control points
 - process and technology

- Expect the policy, control points, processes, and technologies to change
 - Don't under estimate the business willingness to take risk

- Objective: Effectively design and implement framework, with processes and tools to protect the organization from data leakage
- Changing security environment
- Defining a new security strategy
- **Case study**
 - Data-Centric security strategy
 - Enhanced security controls

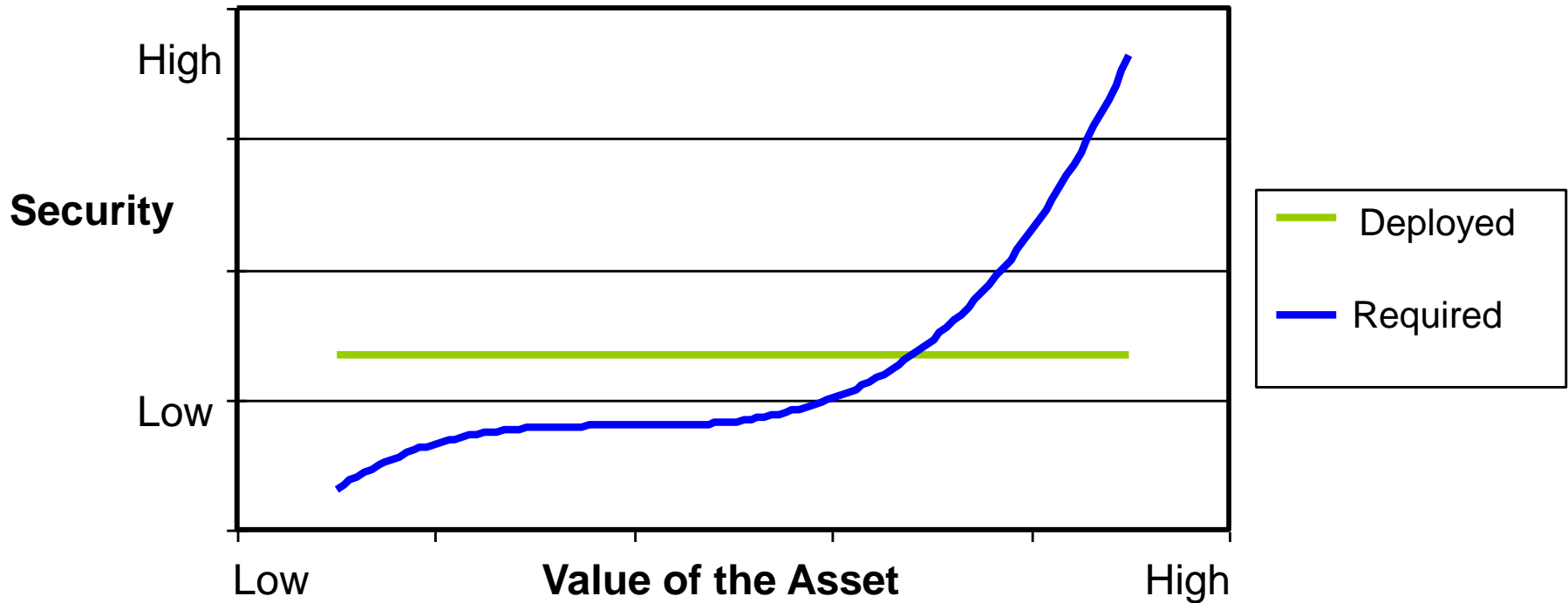
Case Study

- Company
 - Large product manufacturing company
 - 90,000 users (35% contractors)
 - 100,000+ systems
- Business Drivers
 - “Getting to your data anywhere”
- Security Drivers
 - Defining a “data-centric” security architecture to protect data regardless of where it resides.





Case Study: Traditional Security Strategy

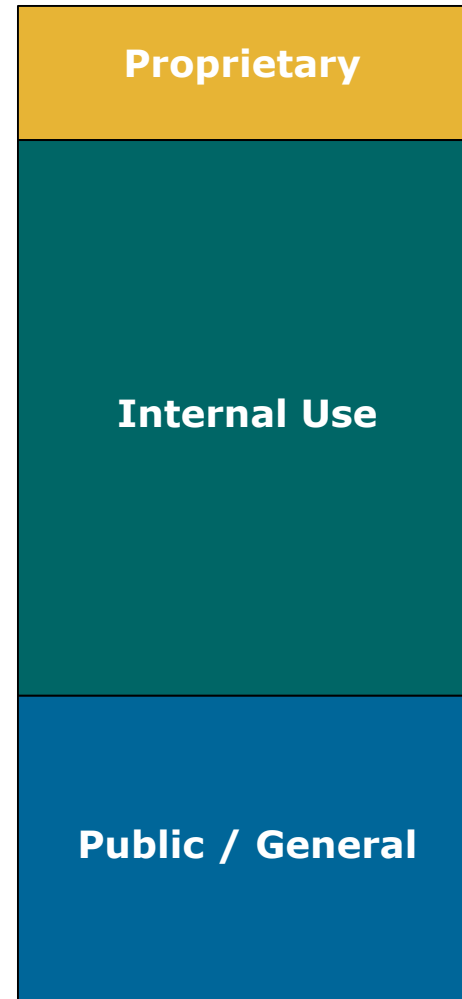


- Traditional security strategy protects everything equally.
 - Over spending in protection of low value assets
 - Under spending in protection of high value assets



Case Study: Data-Centric Security Policy

- Data Protection Policy
 - Policy focuses efforts on protecting “data of concern”
 - Policy drives data classification
- Data of concern
 - The small percentage of data where protection is required by Law or regulation, or determined proprietary by company policy
- Baseline level of security for all data
- Tiers of security for data of higher value.

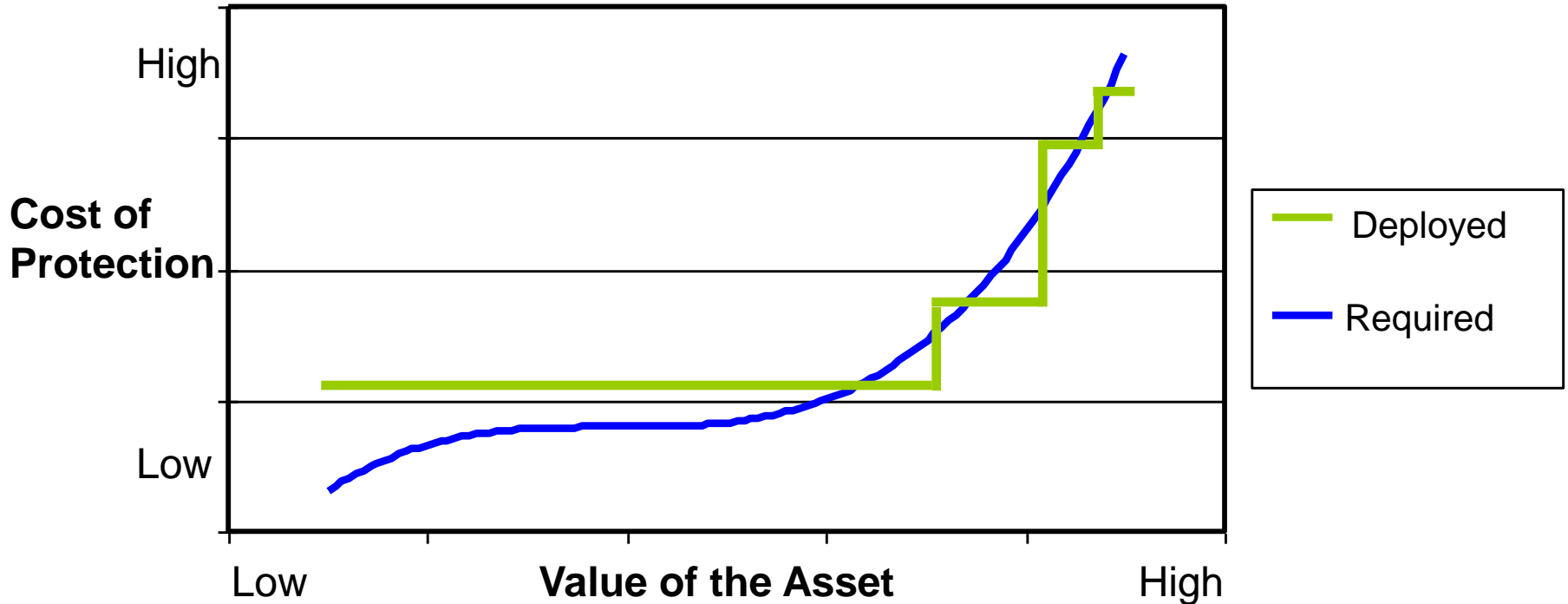


**10-15% is
“Data of
Concern”**

Data Classification



Case Study: Data-Centric Security Strategy



- Add Enhanced Protection for high value assets
- Each step is an identified security measure (process or technology) for protection of critical assets.



Case Study: Identify Control Points

- Network Control Points
 - Network boundaries, data centers, routing core
- System Control Points
 - Configuration and system management
 - Patch management
 - System and application level access
- Data Control Points
 - Authorization
 - In use, at rest, or in transit
- User Control Points
 - Authorization
 - Accountability and Responsibility



Agenda

- Objective: Effectively design and implement framework, with processes and tools to protect the organization from data leakage
- Changing security environment
- Defining a new security strategy
- Case study
 - Data-Centric security strategy
 - Enhanced security controls

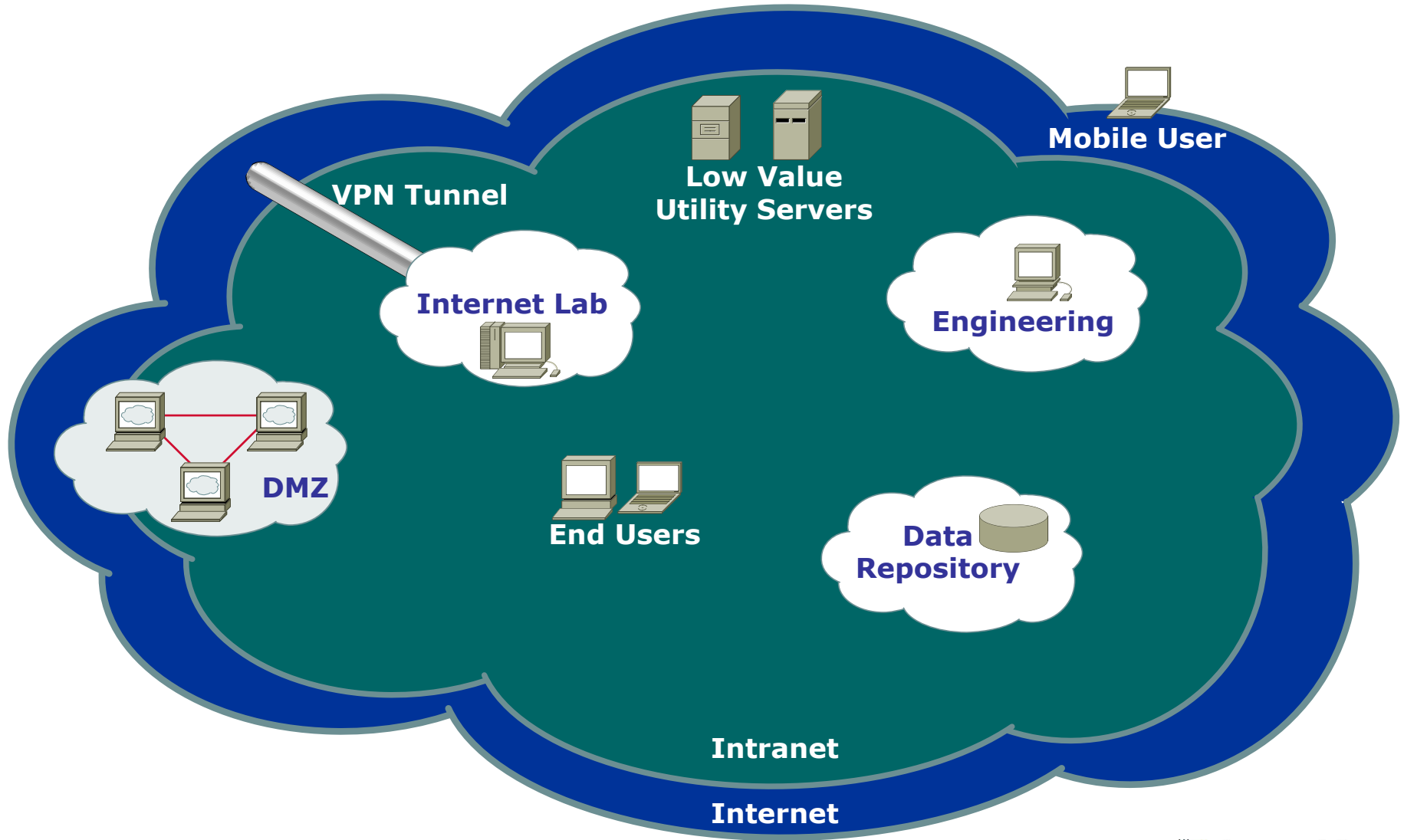


Case Study: Enhanced Security - User

- Security awareness training
 - Control Point:
Accountability and Responsibility
 - Process:
Rewards and consequences to protecting information
Security drivers license
Cultural change
 - Technology:
Online based training material can assist, but not the focus
- Reduce access
 - Control Point:
Limit access to intellectual property
 - Process:
Determine “need to know”



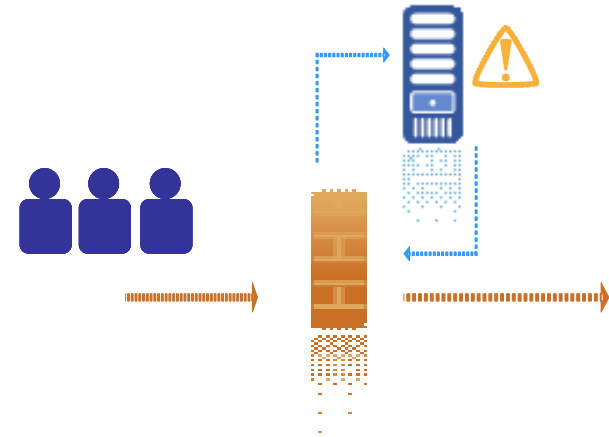
Case Study: Enhanced Security – (Zones)





Case Study: Enhanced Security

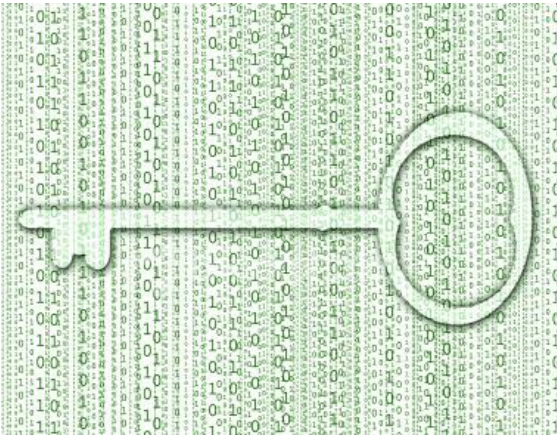
- Data Leakage Prevention
 - Control Point:
Monitoring networks for data leakage
Monitor end points for data leakage
 - Process:
Intellectual Property Definition process
Response and investigation process
 - Technology:
Network-based DLP to monitor web and email
Host-based DLP



Investigate:
Content – What?
Context – Who?

Action:
Block/Redirect
Encrypt
Quarantine
Allow

Case Study: Enhanced Security



- Full Disk Encryption
 - Control point:
Protecting data at rest
 - Process:
Key management & recovery process
 - Technology:
Full disk encryption software and hardware
- Alternatives: Encapsulated, file, and directory



Case Study: Enhanced Security

- Enterprise Digital Rights Management

- Control Point:
Access and rights protection for data regardless of location
- Processes:
Key management
Rights management
- Technology:
E-DRM



	Rights			Policy	
Role	Read	Write	Print	Change	Remove
Product Management				✓	✓
Creation	✓	✓	✓		
Review	✓		✓		

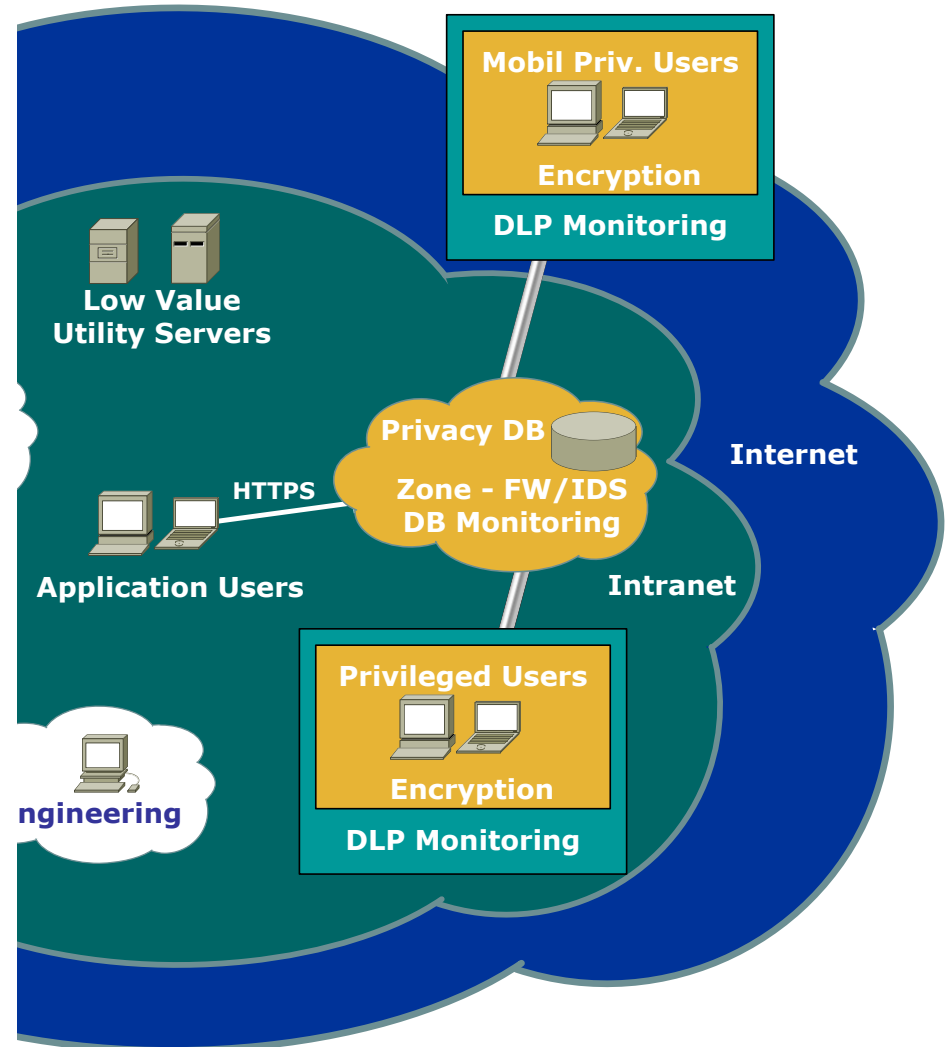


Case Study: Enhanced Security

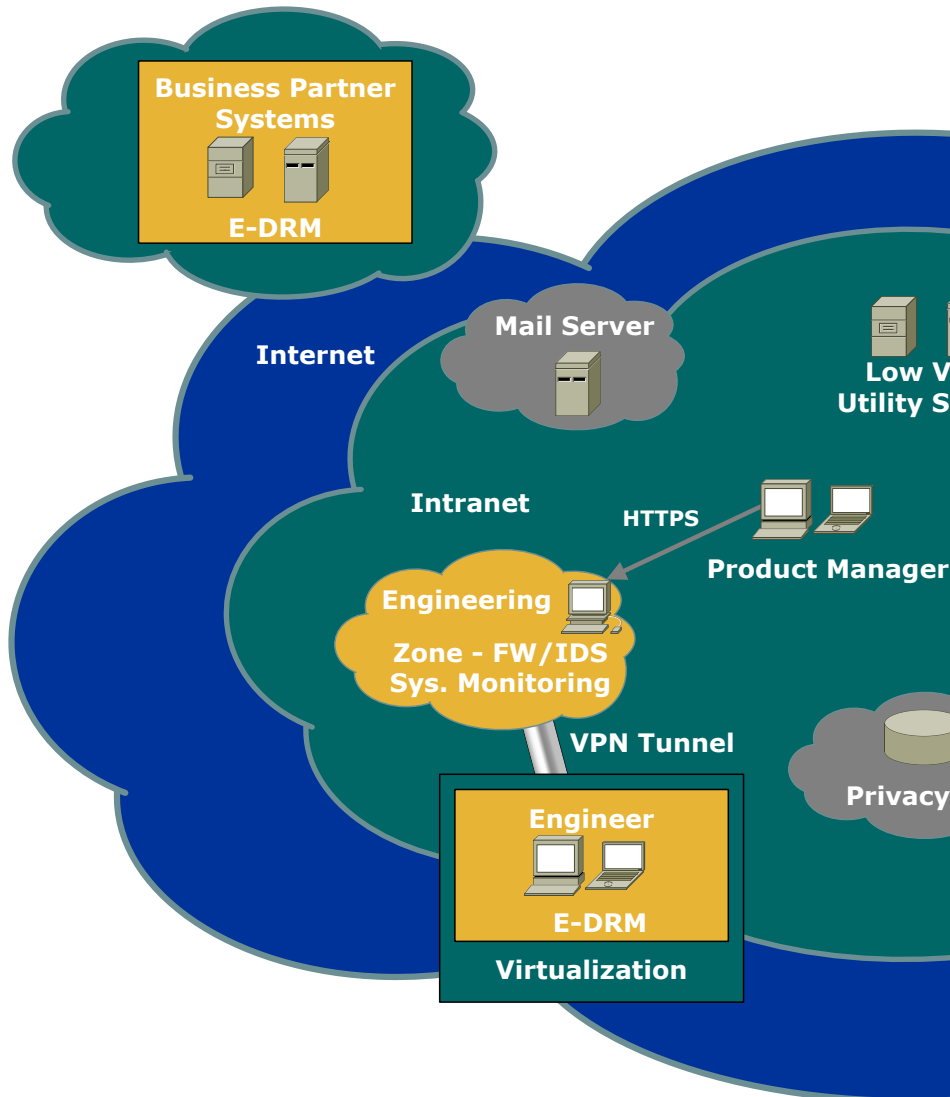
- Enhanced data repository security
 - Control Point:
Protection and monitoring of sensitive information in data repositories
 - Process:
Intellectual property definition
Configuration and patch management
 - Technology:
System and application logging
Log management, Security Information Management (SIM) for correlation

Case Study: Enhanced Security for Protection of Privacy Information

- User Awareness
- Privacy database zone
- Database protection
- Database access and log monitoring
- End point protections
 - Encryption
 - DLP monitoring



Case Study: Enhanced Security for Secure Design Center



- User Awareness
- Engineering zone
- Engineering System Protection and Monitoring
- End Point Security
 - Virtual Image with encryption
 - Accessed restricted to Development zone
- Enterprise Digital Rights Management



Conclusion

- Utilize the security strategy methodology
 - Understand the business drivers
 - Define the initial policy
 - Identify the control points
 - Determine security measures
 - Validate and update
- Align strategy and policy with business
 - Data-Centric (Research & Development, IP creation)
 - Availability (service based)
 - Defense-in-Depth (financial, government, military)
- Focus on people, process and technology