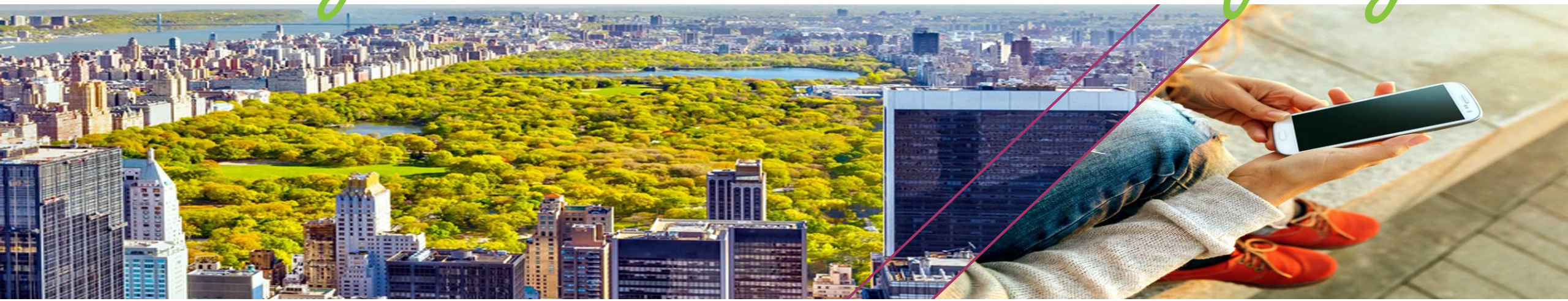
The Encryption Pyramid:

Choosing the level that works for you!



Eysha S. Powers
eysha@us.ibm.com
IBM, Enterprise Cryptography

Extensive use of encryption is one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

Implementing encryption can be complex

Comprehensive data protection requires a huge investment to deploy point solutions and/or enable encryption directly in the applications.

Organizations struggle with questions such as:

What data should be encrypted?

Where should encryption occur?

Who is responsible for encryption?

Pervasive encryption: A paradigm shift in data protection

Protecting only enough data to achieve compliance should be the bare minimum, not a best practice.

Focus on eliminating barriers:

- Decouple encryption from classification
- Extensive application changes
- Encryption of database indexes and/or key fields
- High cost associated with processor overhead

Application changes are costly

People

Skills

Ongoing maintenance

Application lifecycle

Application outages to implement encryption

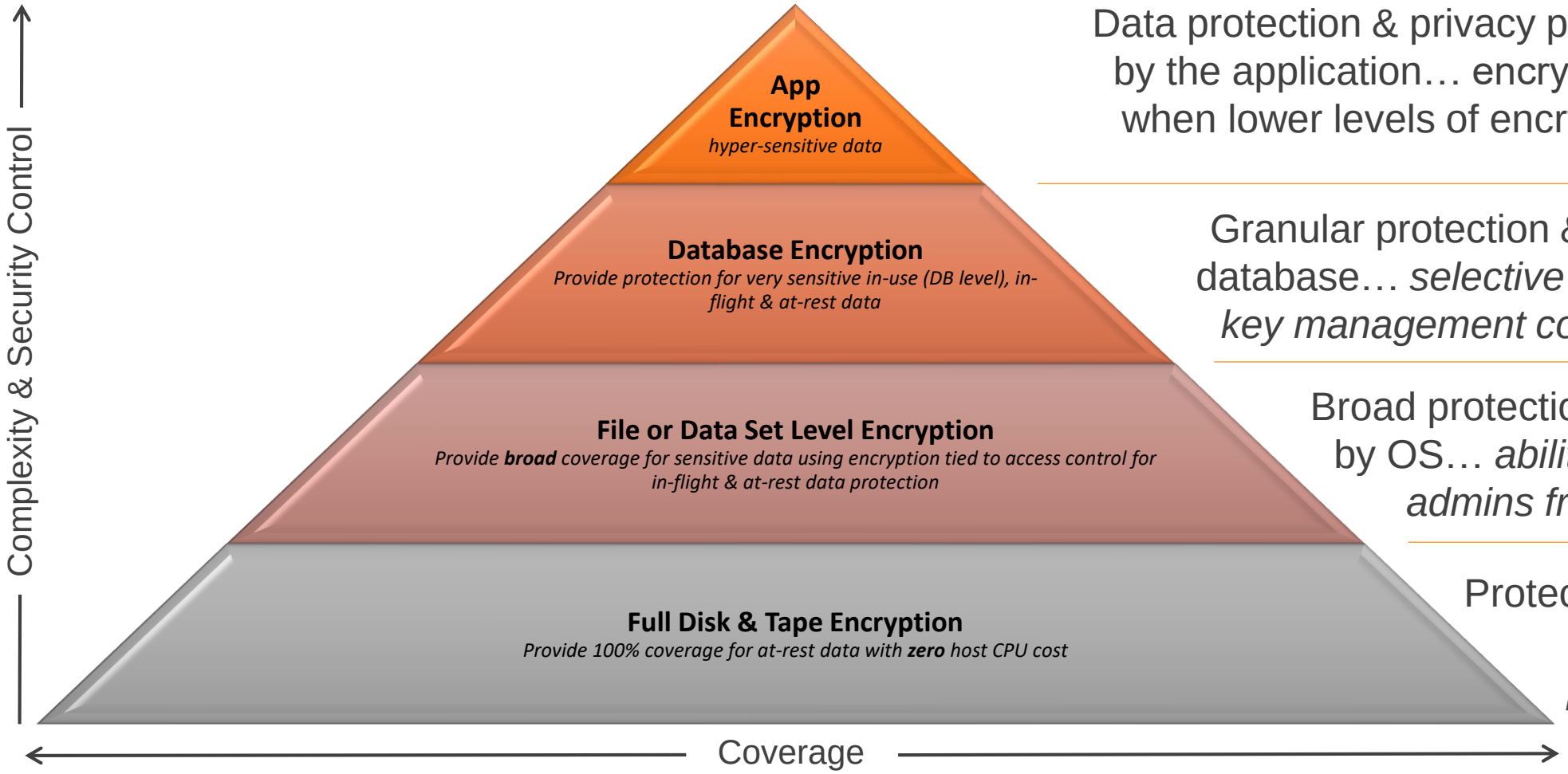
Updates for regulatory changes

Key management

New business requirements

Multiple layers of encryption for data at rest

Robust data protection



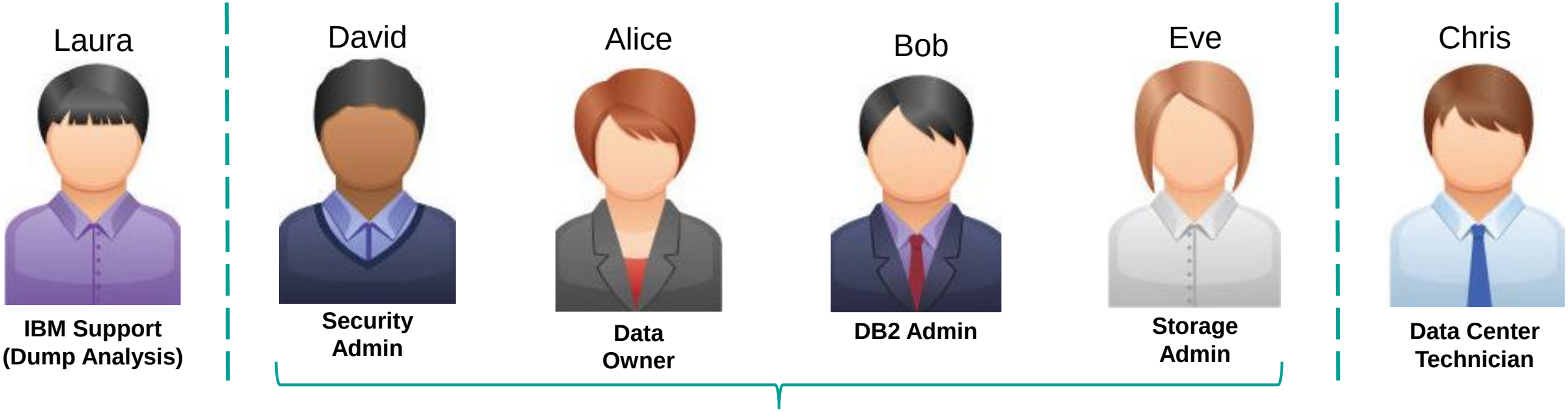
Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

Meet the team!



Who can view sensitive data in a database? How much effort is involved in preventing unauthorized users from viewing the sensitive data?

Without Encryption…

Who can view sensitive data in a database?

Laura

IBM Support (Dump Analysis)

David

Security Admin

Alice

Data Owner

Bob

DB2 Admin

Eve

Storage Admin

Chris

Data Center Technician

No login credentials. Receives and analyzes dump from customer.	Owns all security resources.	Has UPDATE authorization to the data set.	Owns all Db2 resources.	Has ALTER authorization to the data set.	No login credentials. Has physical access to storage media.
Laura can view all unencrypted data in the dump.	David can view the data in the data set and using SQL statements.	Alice can view the data in the data set and using SQL statements.	Bob can view the data only using SQL statements.	Eve can view the data in the data set. Eve cannot invoke SQL statements.	Chris cannot log onto the IBM Z system. Chris can remove the storage device and view the data.

Multiple layers of encryption for data at rest

Robust data protection

Full Disk & Tape Encryption

- Protects at the DASD subsystem level
- All or nothing encryption
- Only data at rest is encrypted
- Single encryption key for everything

- No application overhead
- Zero host CPU cost
- Prevents exposures on: Disk removal, Box removal, File removal

Full Disk & Tape Encryption

*Provide 100% coverage for at-rest data with **zero** host CPU cost*

Protection against intrusion, tamper or removal of *physical* infrastructure

With Full Disk & Tape Encryption Only…

Who can view sensitive data in a database?

Laura

IBM Support (Dump Analysis)

David

Security Admin

Alice

Data Owner

Bob

DB2 Admin

Eve

Storage Admin

Chris

Data Center Technician

No login credentials. Receives and analyzes dump from customer.	Owns all security resources.	Has UPDATE authorization to the data set.	Owns all Db2 resources.	Has ALTER authorization to the data set.	No login credentials. Has physical access to storage media.
Laura can view all unencrypted data in the dump.	David can view the data in the data set and using SQL statements.	Alice can view the data in the data set and using SQL statements.	Bob can view the data only using SQL statements.	Eve can view the data in the data set. Eve cannot invoke SQL statements.	Chris cannot log onto the IBM Z system. Chris can remove the storage device but cannot view the encrypted data in the clear.

With Full Disk & Tape Encryption Only…

What does it cost to plan, configure, implement and/or maintain?

High Cost	
Medium Cost	
Low Cost	People, Skills, Ongoing maintenance, Application lifecycle, Application outages to implement encryption, Updates for regulatory changes, Key management, New business requirements

Multiple layers of encryption for data at rest

Robust data protection

z/OS Data Set Encryption

- Enabled by policy
- Transparent to applications
- Tied to access control

- Uses protected encryption keys managed by the host

File or Data Set Level Encryption

*Provide **broad** coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

- Broadly encrypt data at rest
- Covers VSAM, DB2, IMS, Middleware, Logs, Batch, & ISV solutions[1]

- Encrypt in bulk for low-overhead
- Utilizes IBM Z integrated cryptographic hardware

1 Applications or middleware making use of VSAM, QSAM, BSAM access methods. Refer to individual ISV documentation to confirm support of z/OS data set encryption.

With File & Data Set Encryption…

Who can view sensitive data in a database?

Laura

IBM Support (Dump Analysis)

David

Security Admin

Alice

Data Owner

Bob

DB2 Admin

Eve

Storage Admin

Chris

Data Center Technician

No login credentials. Receives and analyzes dump from customer.	Owns all security resources.	Has UPDATE authorization to the data set. Has READ authorization to the key.	Owns all Db2 resources.	Has ALTER authorization to the data set. Has NONE authorization to the key.	No login credentials. Has physical access to storage media.
Laura can view all unencrypted data in the dump.	David can view the data in the data set and using SQL statements.	Alice can view the data in the data set and using SQL statements.	Bob can view the data using SQL statements.	Eve cannot view any data in the clear in the data set. Eve cannot invoke SQL statements.	Chris cannot log onto the IBM Z system. Chris can remove the storage device but cannot view the encrypted data in the clear.

With File & Data Set Encryption Only…

What does it cost to plan, configure, implement and/or maintain?

High Cost	Key management
Medium Cost	
Low Cost	People; Skills; Ongoing maintenance; Application lifecycle; Application outages to implement encryption; Updates for regulatory changes; New business requirements

Multiple layers of encryption for data at rest

Robust data protection

IBM Security Guardium Data Encryption for DB2 and IMS Databases

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

- Encrypts sensitive data at the DB2 row and column levels and IMS segment level
- Transparent to applications
- Separation of Duties (SOD) and granular access control
- Protects Data-In-Use within memory buffers
- Clear text data cannot be accessed outside DBMS access methods
- Persists the encrypted sensitive data in logs, image copy data sets, DASD volume backups
- Utilizes IBM Z integrated cryptographic hardware

With Database Encryption Only…

Who can view sensitive data in a database?

Laura

IBM Support (Dump Analysis)

David

Security Admin

Alice

Data Owner

Bob

DB2 Admin

Eve

Storage Admin

Chris

Data Center Technician

No login credentials. Receives and analyzes dump from customer.	Owns all security resources.	Has UPDATE authorization to the data set. Has READ authorization to the key.	Owns all Db2 resources.	Has ALTER authorization to the data set. Has NONE authorization to the key.	No login credentials. Has physical access to storage media.
Laura cannot view any encrypted rows or fields in the clear in the dump.	David can view the data in the data set and using SQL statements.	Alice can view the data in the data set and using SQL statements.	Bob can view the data using SQL statements.	Eve cannot view any encrypted rows or fields in the clear in the data set. Eve cannot invoke SQL statements.	Chris cannot log onto the IBM Z system. Chris can remove the storage device but cannot view any encrypted rows or fields in the clear.

With Database Encryption Only…

What does it cost to plan, configure, implement and/or maintain?

High Cost	
Medium Cost	Application outages to implement encryption Updates for regulatory changes
Low Cost	People Skills Ongoing maintenance Application lifecycle Key management New business requirements

Multiple layers of encryption for data at rest

Robust data protection

Application Encryption

Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

- Requires changes to applications to implement and maintain
- Highly granular
- Protect data right up to the point where it will be used
- Applications must be responsible for key management
- Appropriate for selective encryption of hyper-sensitive data

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

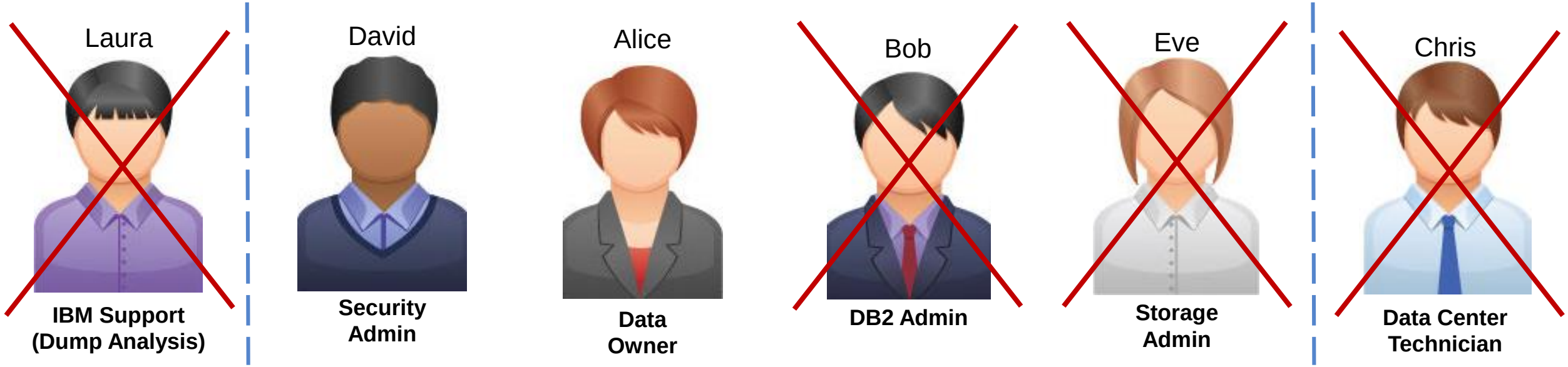
Protection against intrusion, tamper or removal of *physical* infrastructure

Complexity & Security Control

Coverage

With Application Encryption Only…

Who can view sensitive data in a database?



No login credentials. Receives and analyzes dump from customer.	Owns all security resources.	Has UPDATE authorization to the data set. Has READ authorization to the key.	Owns all Db2 resources.	Has ALTER authorization to the data set. Has NONE authorization to the key.	No login credentials. Has physical access to storage media.
Laura cannot view any encrypted data in the clear in the dump.	David can view the data in the data set and using SQL statements.	Alice can view the data in the data set and using SQL statements.	Bob cannot view any data that was encrypted prior to being stored in Db2.	Eve cannot view any encrypted data in the clear in the data set. Eve cannot invoke SQL statements.	Chris cannot log onto the IBM Z system. Chris can remove the storage device and view the data but cannot view the encrypted data in the clear.

With Application Encryption Only…

What does it cost to plan, configure, implement and/or maintain?

High Cost	People	Skills	Ongoing maintenance	Application lifecycle	Application outages to implement encryption	Updates for regulatory changes	Key management	New business requirements
Medium Cost								
Low Cost								

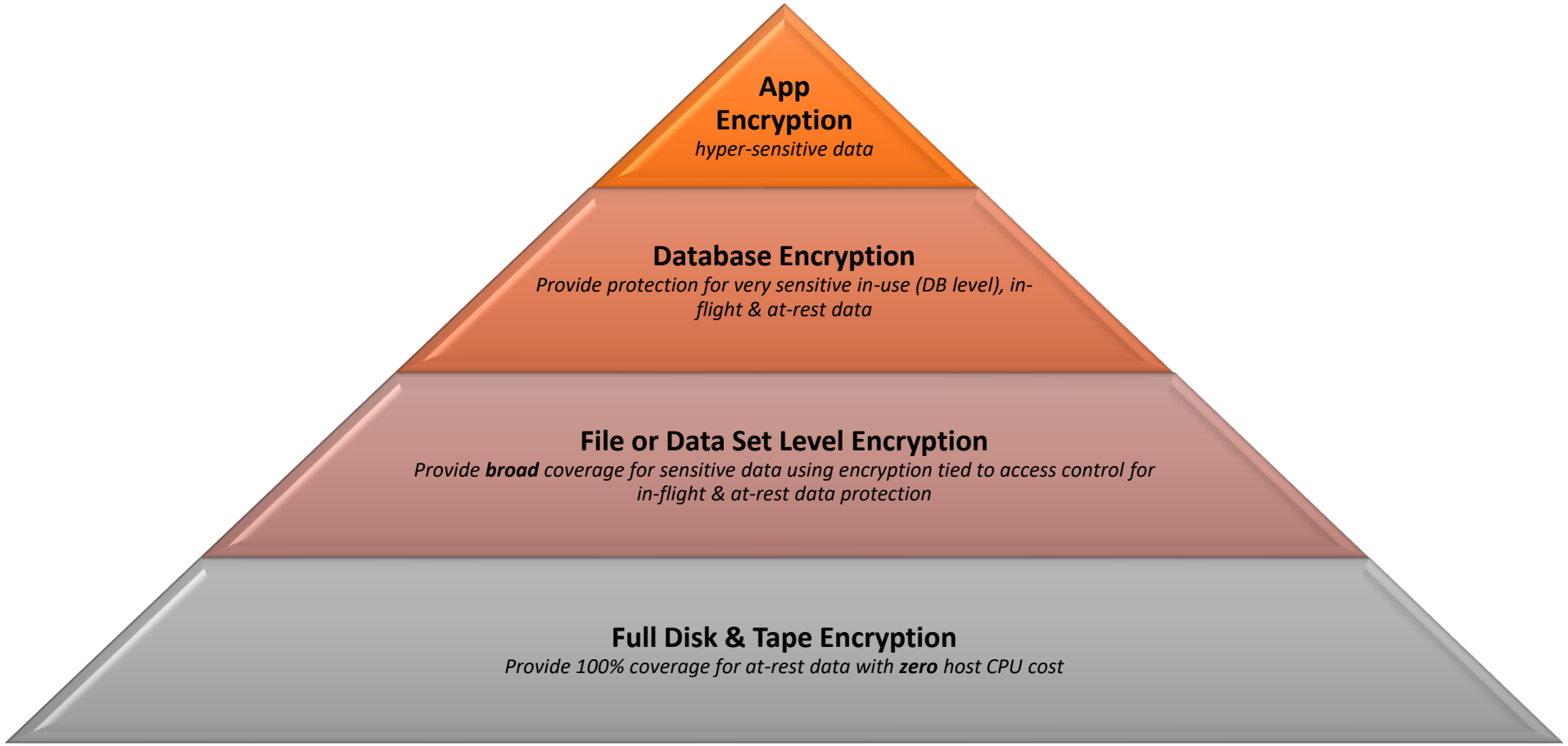
Use Case: Protecting cardholder data (1 of 4)

PCI-DSS Requirement 3.4

“Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: one-way hashes based on strong cryptography (hash must be of the entire PAN), truncation (hashing cannot be used to replace the truncated segment of PAN), index tokens and pads (pads must be securely stored), strong cryptography with associated key-management processes and procedures.”

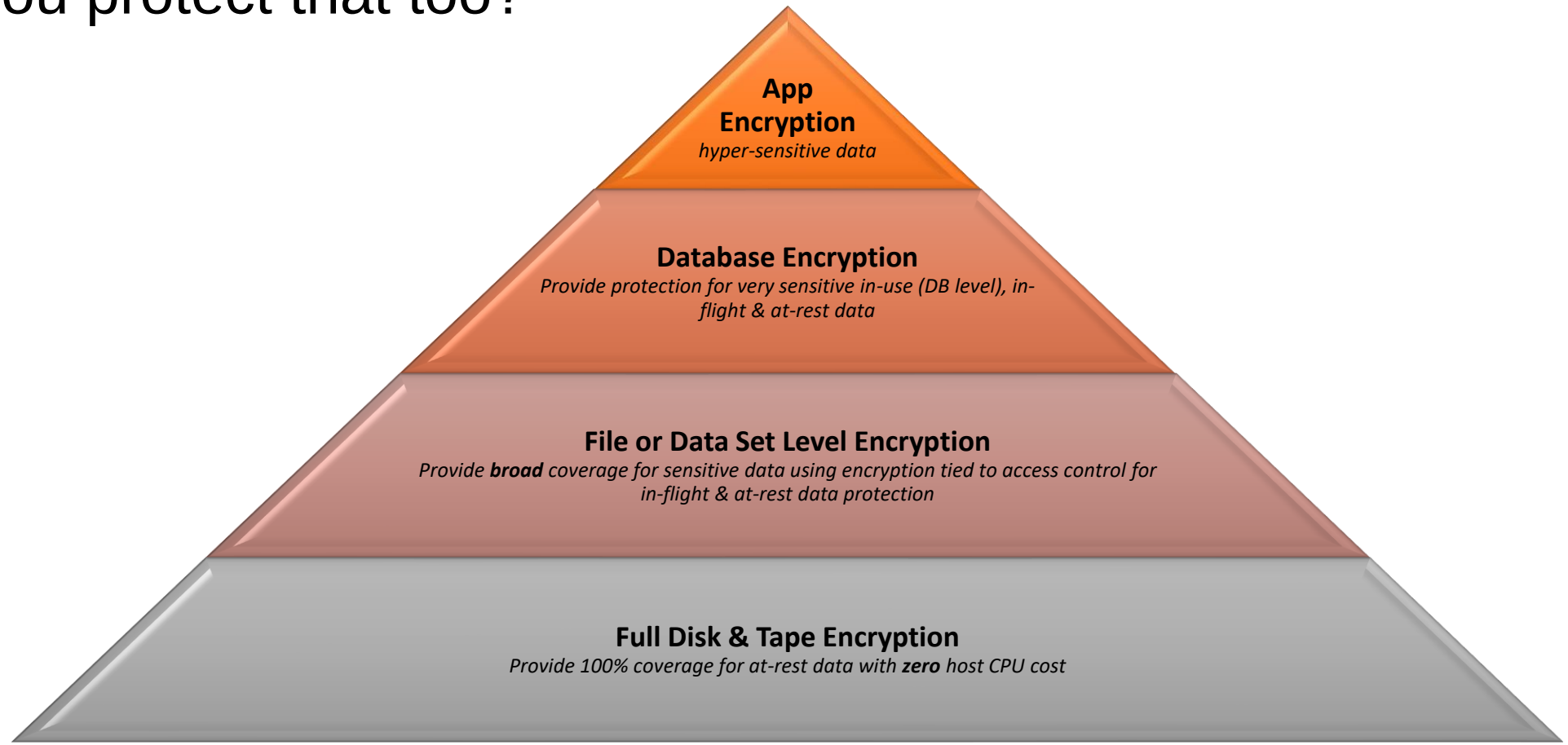
Use Case: Protecting cardholder data (2 of 4)

How would you protect the Personal Account Number (PAN)?



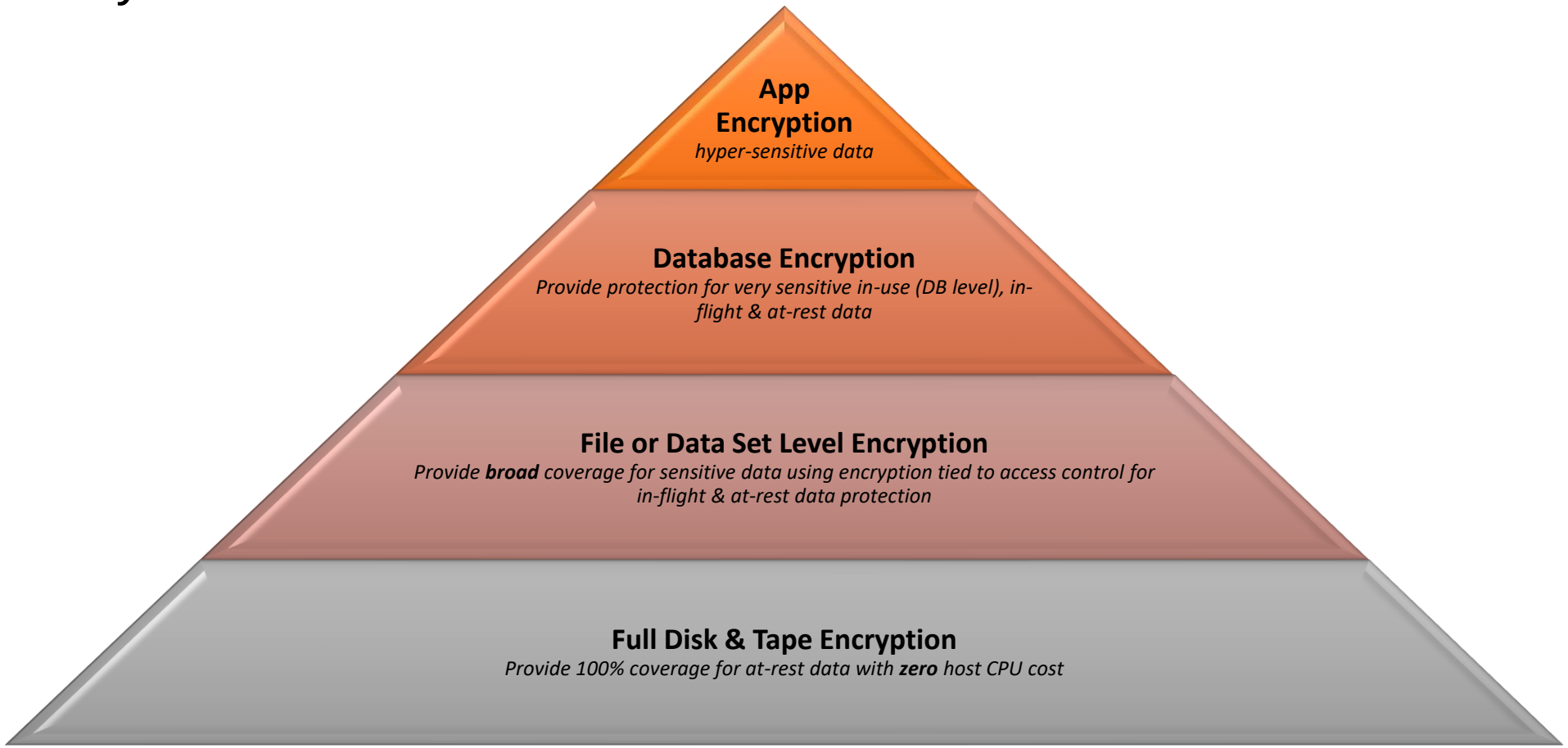
Use Case: Protecting cardholder data (3 of 4)

What if there is additional sensitive data in the same environment? How would you protect that too?



Use Case: Protecting cardholder data (4 of 4)

It is possible that some data might be double, triple or quadruple encrypted. What is the impact on your CPU / MIPS cost?

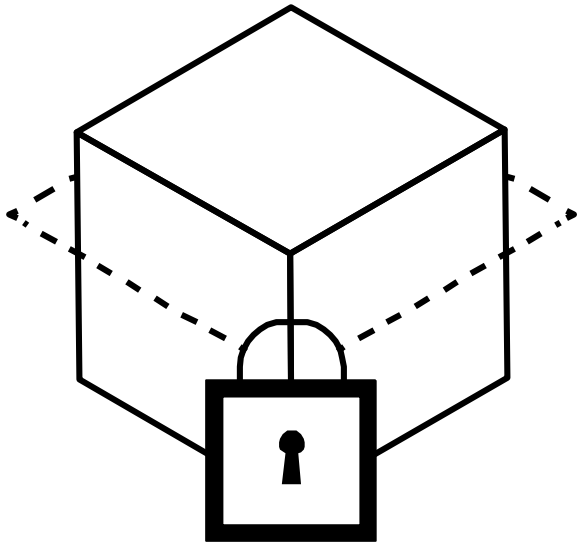


Which level of encryption did you choose?

Multiple? Crypto technologies can be layered together to protect sensitive data against threats specific to your environment that fit within your available budget and resources.

Consider:

- How would you determine what to encrypt?
- Should you encrypt all, some or ~~none~~?
- What regulations must you comply with?
- What are the auditing requirements?
- What attacks do you want to prevent?
- What is the likelihood of that attack?
- What is the impact of that attack?
- What resources are available?
- What skills are available?

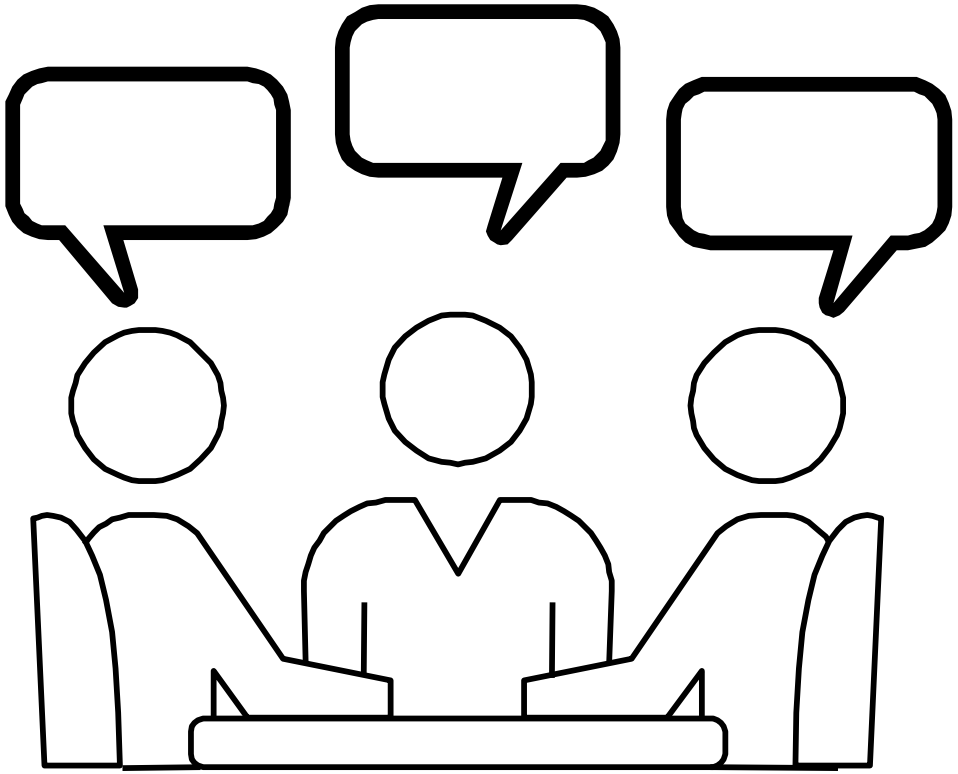


Additional Resources

IBM Crypto Education Community
https://www.ibm.com/developerworks/community/groups/community/crypto

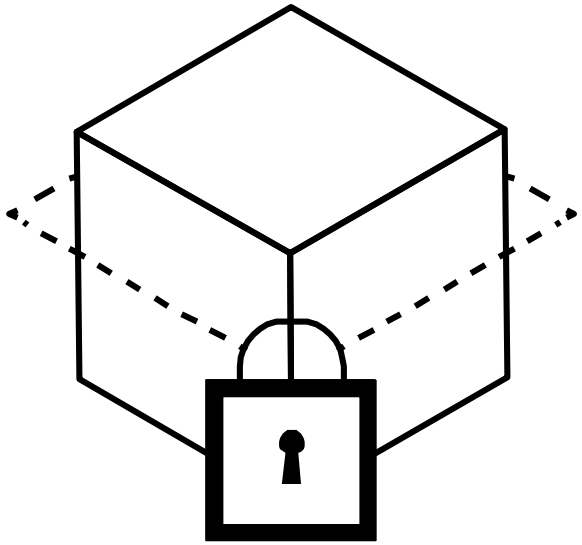
Getting Started with z/OS Data Set Encryption Redbook
http://www.redbooks.ibm.com/redpieces/abstracts/sg248410.html?Open

Questions?



Appendix: Which level of encryption should *you* choose?

Crypto technologies can be layered together to protect sensitive data against threats specific to your environment that fit within your available budget and resources.



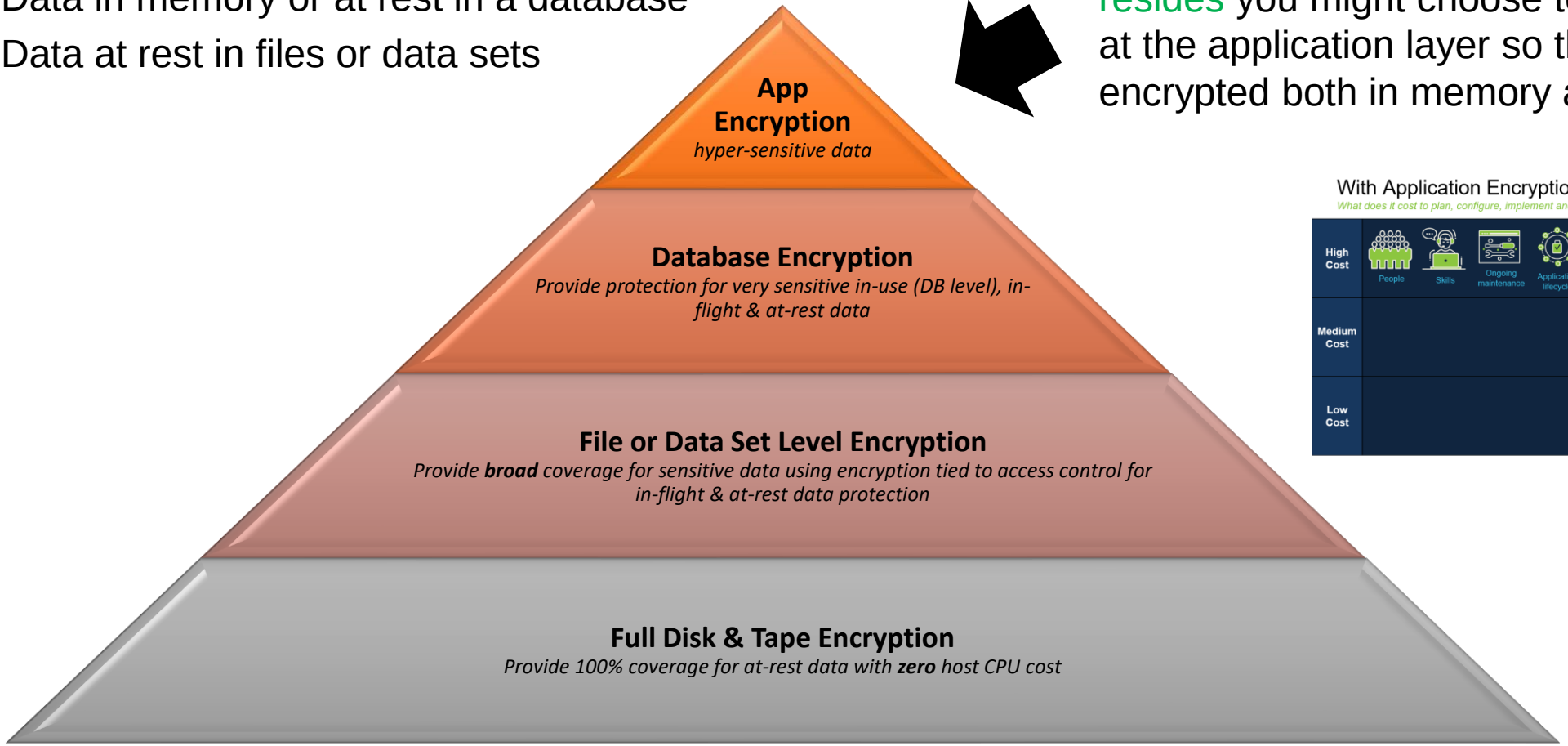
Let's consider your environment...

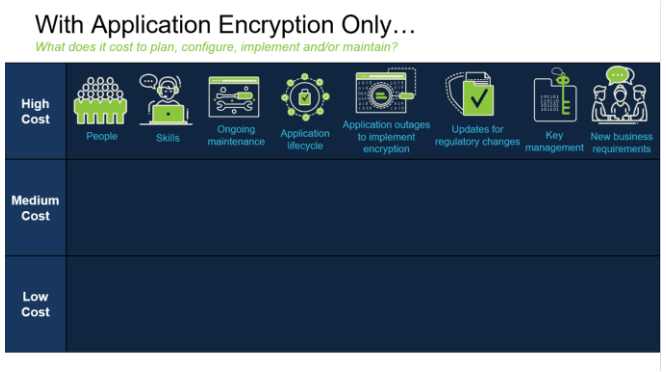
Do you know where ALL of your sensitive data resides?

Consider:

- Data in memory of the application
- Data in memory or at rest in a database
- Data at rest in files or data sets

If you know where all of your sensitive data resides you might choose to encrypt the data at the application layer so that it remains encrypted both in memory and at rest.

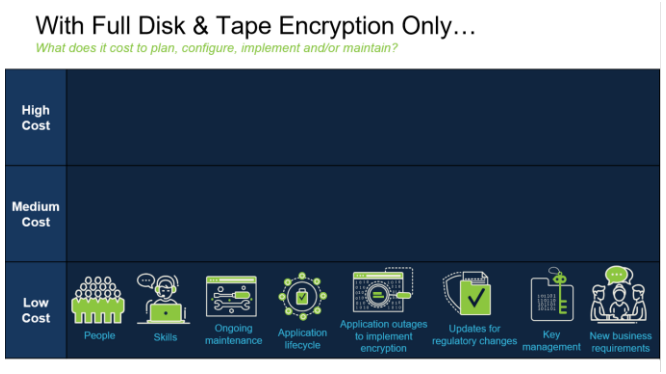


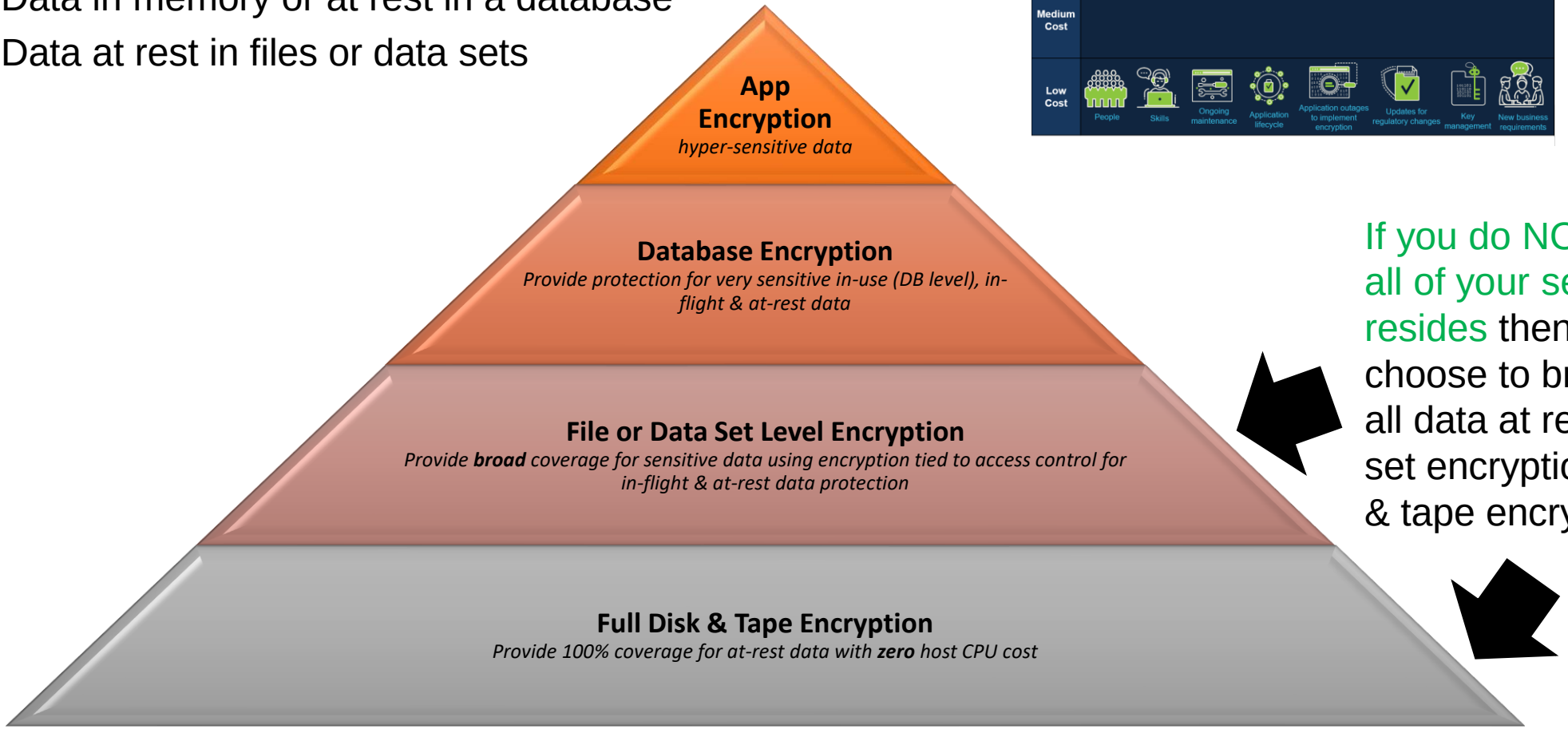


Do you know where ALL of your sensitive data resides?

Consider:

- Data in memory of the application
- Data in memory or at rest in a database
- Data at rest in files or data sets



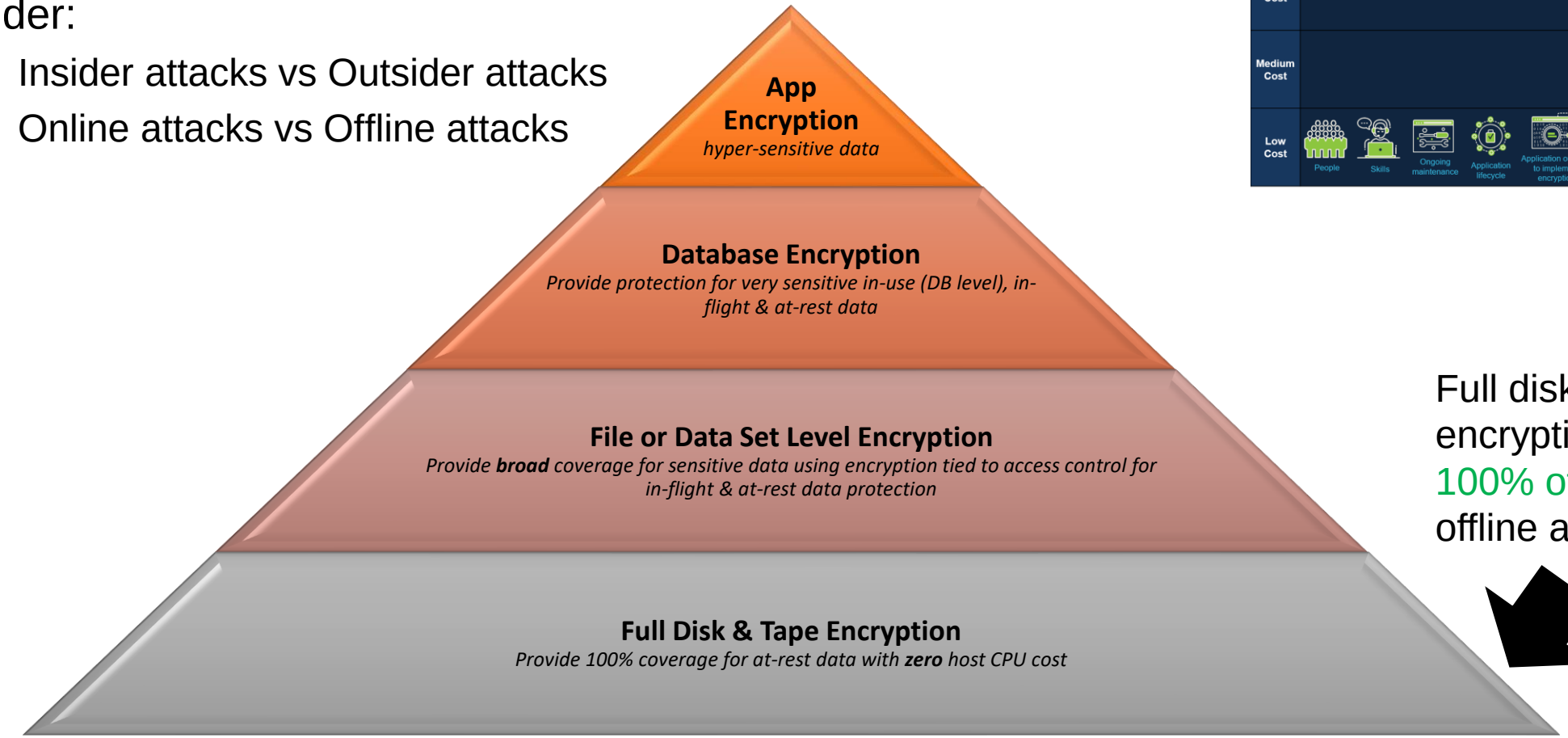


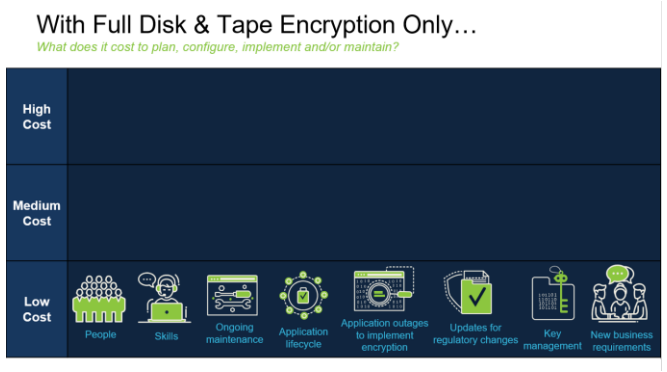
If you do NOT know where all of your sensitive data resides then you might choose to broadly encrypt all data at rest with data set encryption and full disk & tape encryption.

Which attacks do you need to prevent? What is the likelihood of the attack?

Consider:

- Insider attacks vs Outsider attacks
- Online attacks vs Offline attacks



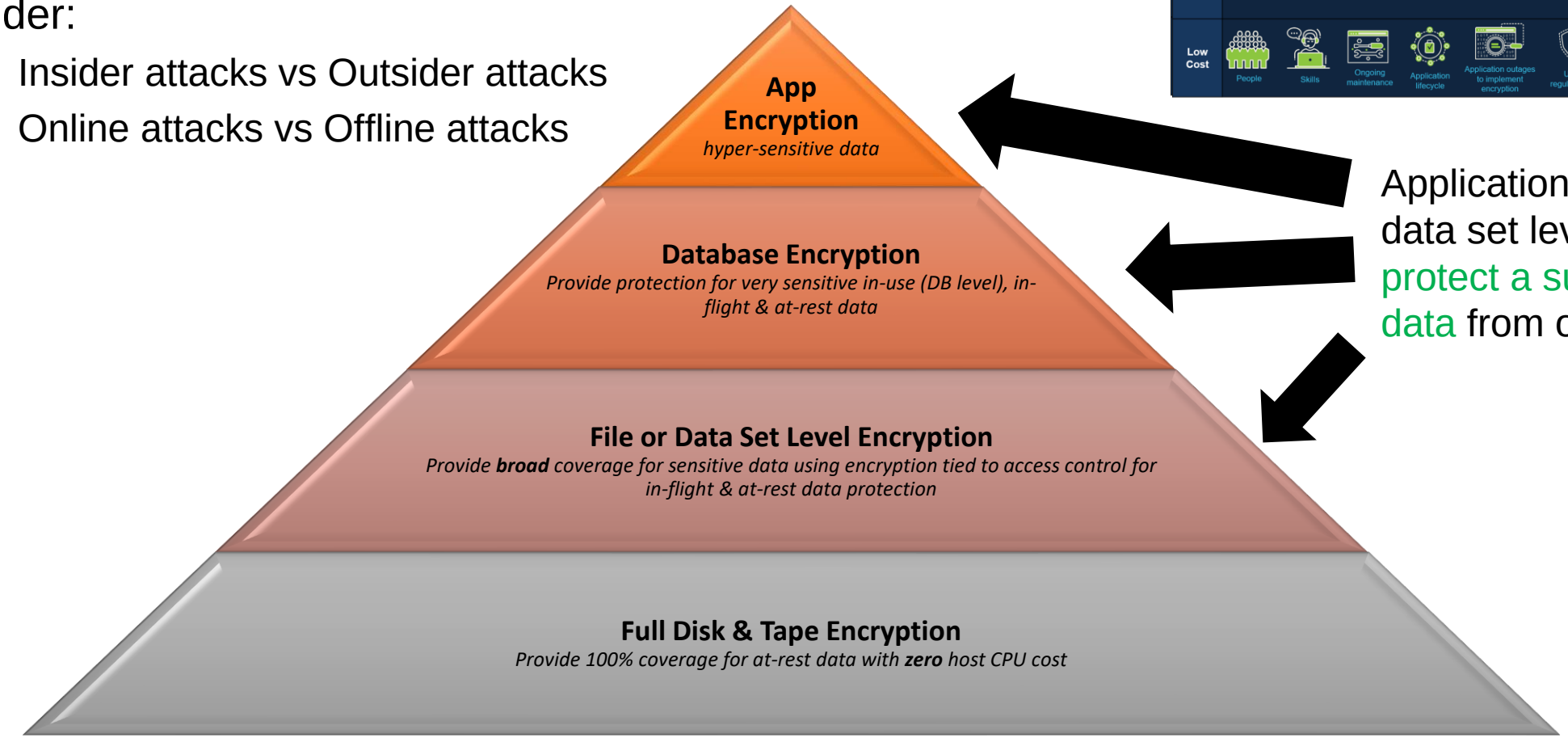


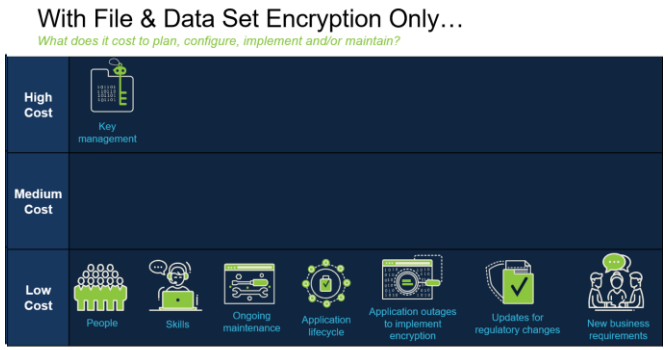
Full disk & tape encryption protects 100% of the data from offline attacks.

Which attacks do you need to prevent? What is the likelihood of the attack?

Consider:

- Insider attacks vs Outsider attacks
- Online attacks vs Offline attacks



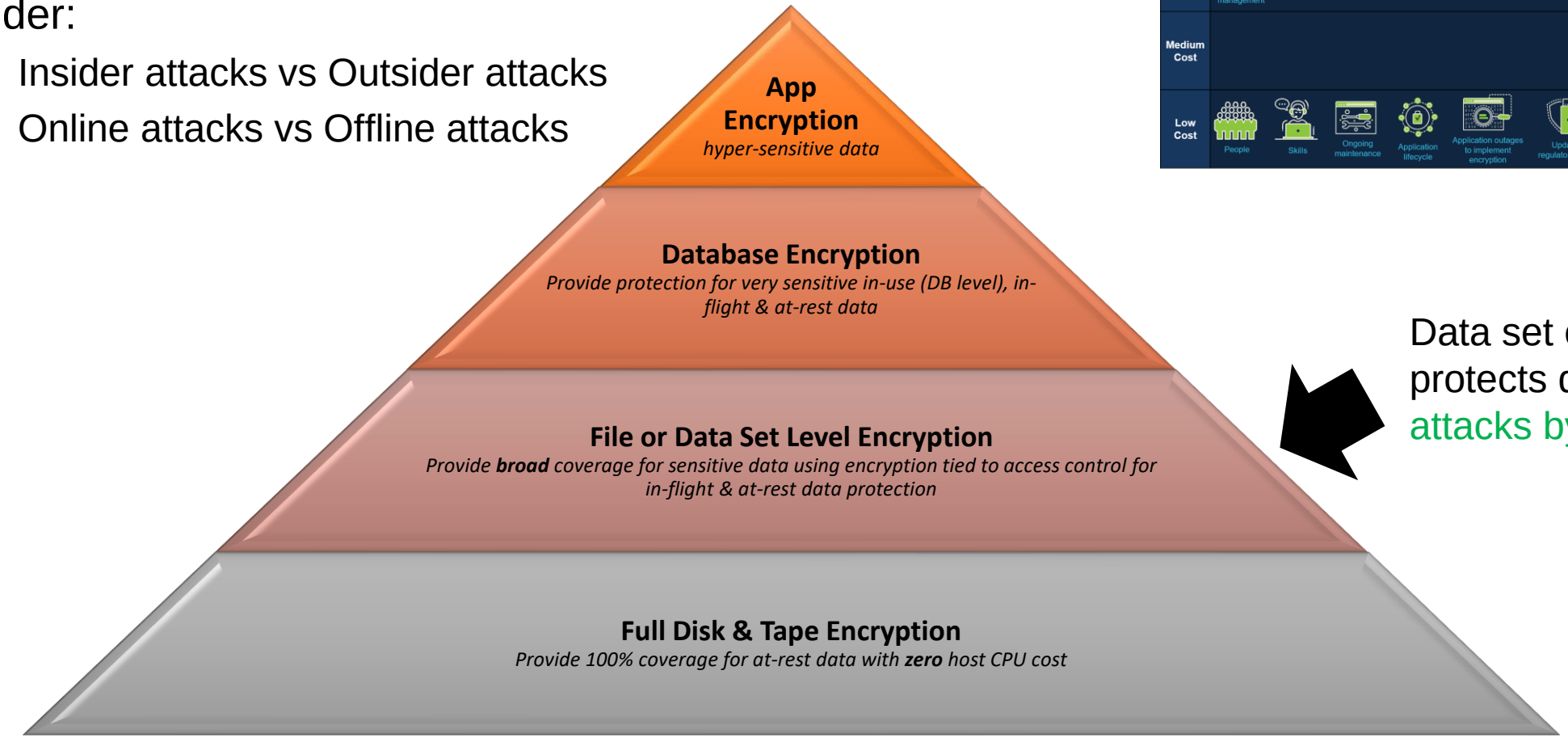


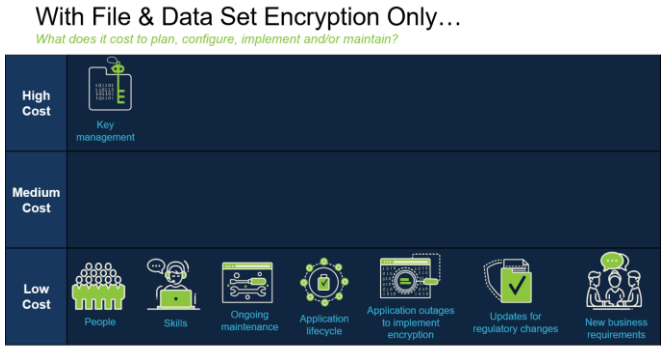
Application, database and data set level encryption protect a subset of the data from offline attacks.

Which attacks do you need to prevent? What is the likelihood of the attack?

Consider:

- Insider attacks vs Outsider attacks
- Online attacks vs Offline attacks



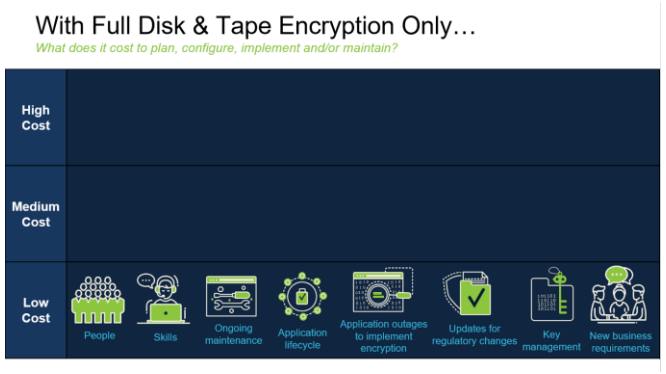


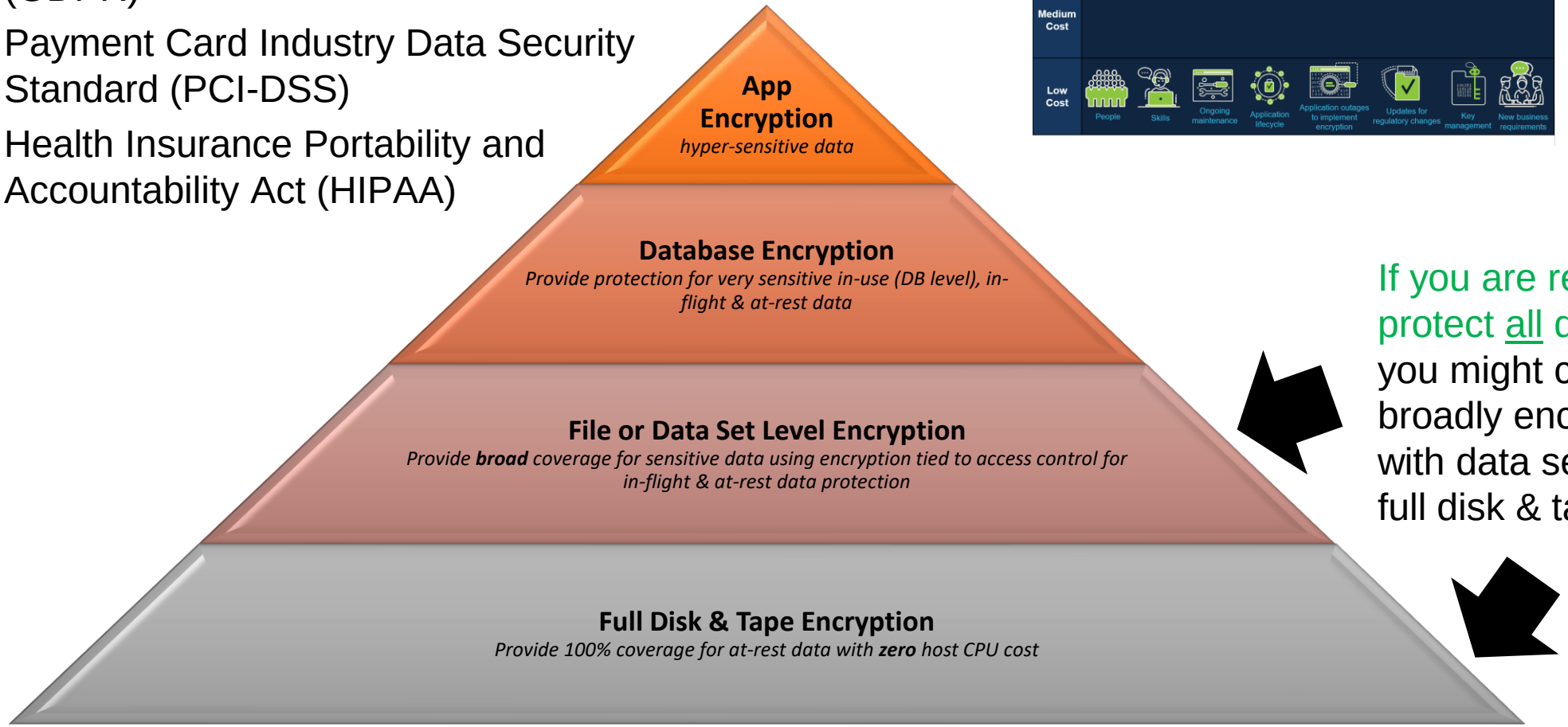
Data set encryption protects data from insider attacks by storage admins.

Which regulations do you need to comply with?

Consider:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)



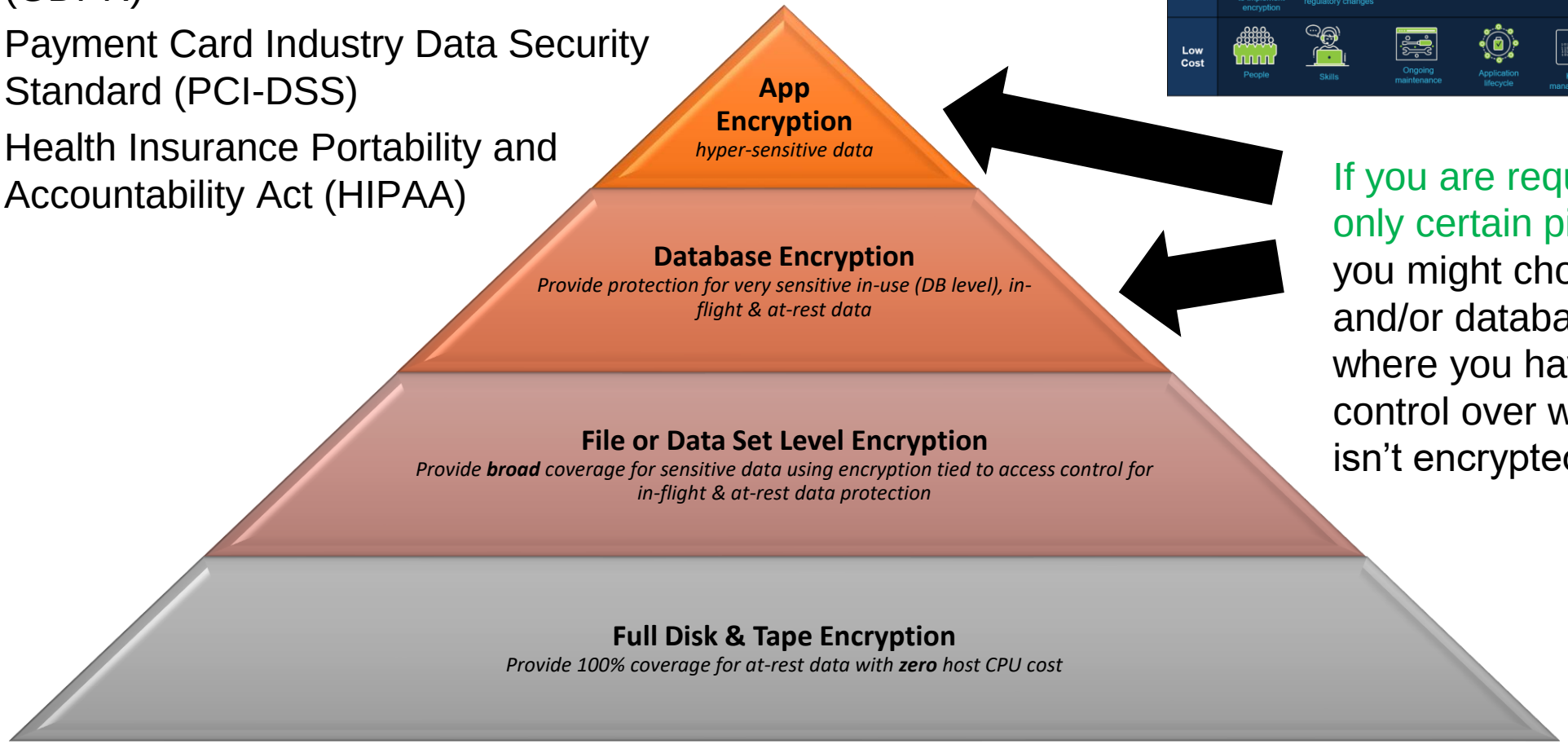


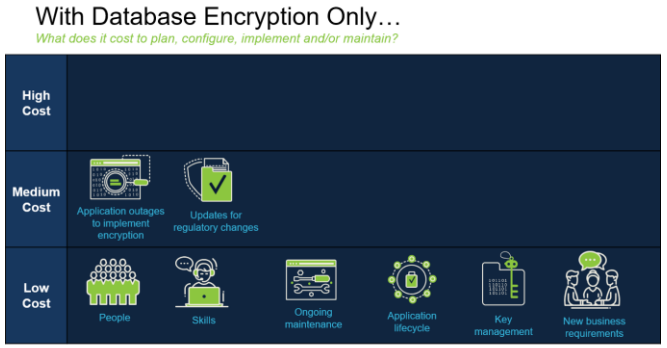
If you are required to protect all data at rest then you might choose to broadly encrypt the data with data set encryption and full disk & tape encryption.

Which regulations do you need to comply with?

Consider:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)



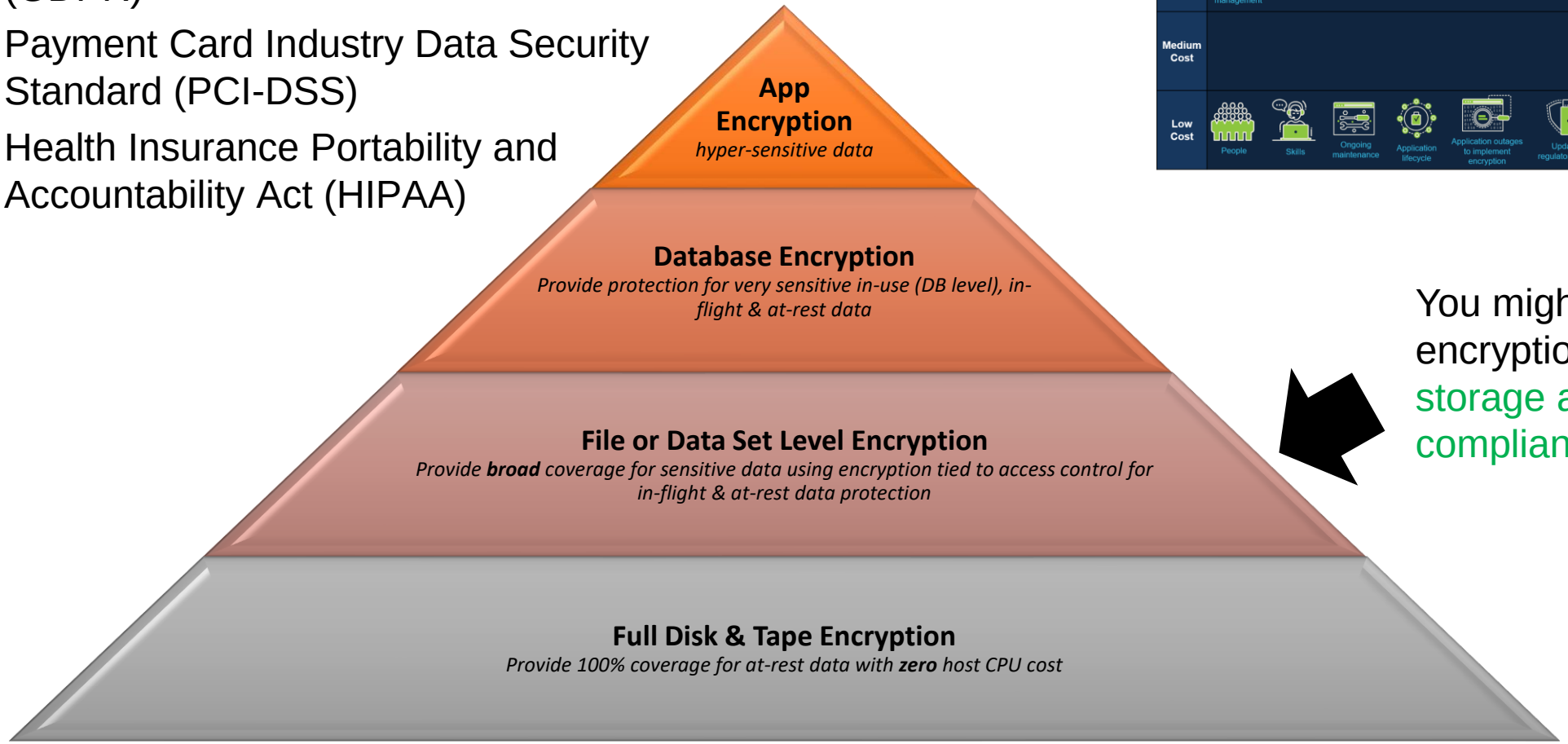


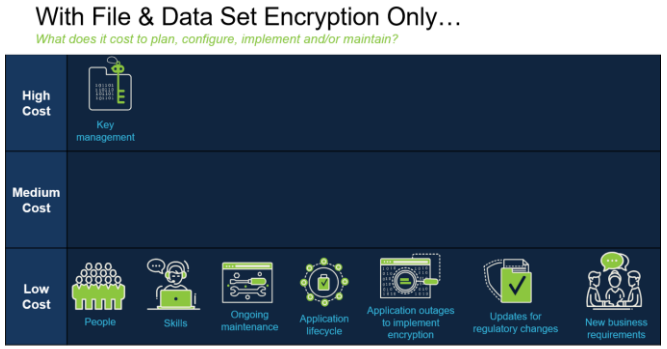
If you are required to protect only certain pieces of data then you might choose application and/or database encryption where you have more granular control over which data is or isn't encrypted.

Which regulations do you need to comply with?

Consider:

- General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)





You might choose data set encryption to eliminate storage administrators from compliance scope.