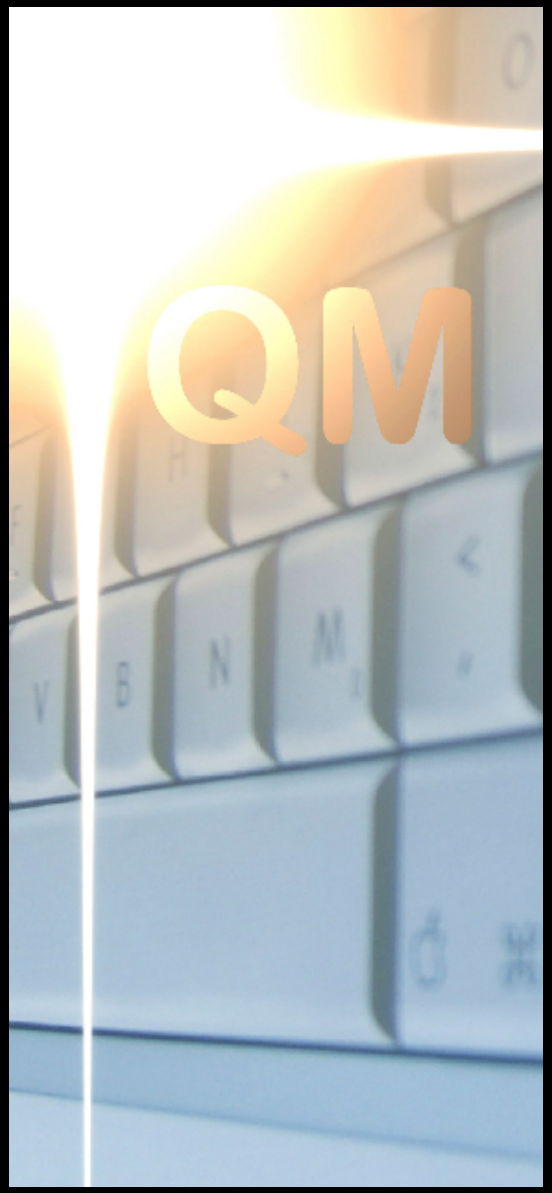


OpenQM

Data Security

Martin Phillips
Ladybridge Systems Ltd

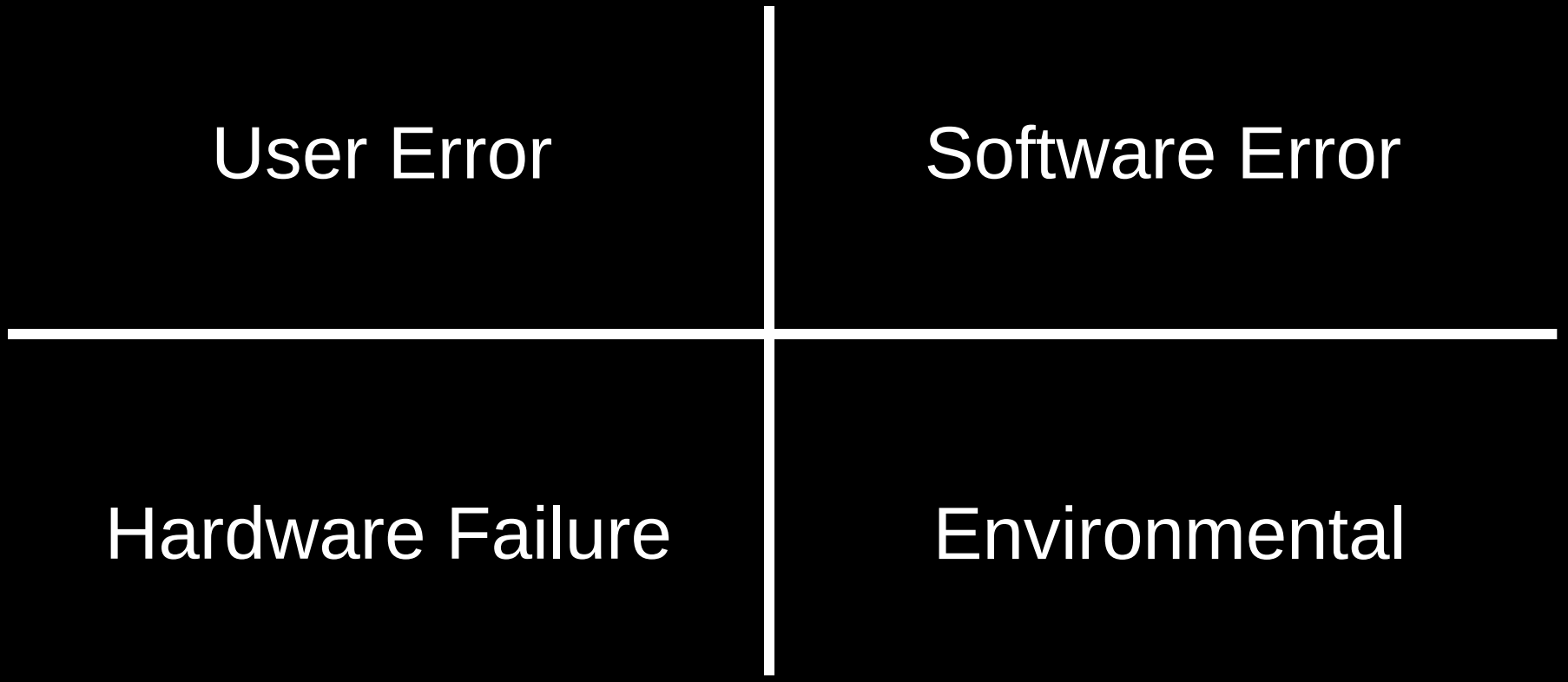
OpenQM

There are two sides to data security...

- Not losing our data
- Not letting others access it

OpenQM

How do we lose data?



OpenQM

What are the risks?

- User error
- Hardware / software failure
- Malicious users / developers
- Theft / loss of backup media
- Theft / loss of the entire system

OpenQM

What do we need to know about?

- Application level security
- File permissions
- Data encryption
- QMClient security issues
- Backup policies

OpenQM

Application level security

- Don't let the user near a command prompt
- Security subroutines
- Identify the user
- Identify the process type

OpenQM

Hiding the command prompt

- Use LOGIN paragraph to enter application
- Use ON.ABORT to catch application errors
- OPTION NO.USER.ABORTS to hide all abort options

OpenQM

Security subroutines

- Apply to R and V type VOC entries
- Command line or EXECUTEd commands
- User defined - Can do almost anything
- Don't allow the user to update the VOC!

OpenQM

Identify the user

- @LOGNAME
- @IP.ADDR
- SYSTEM(1017) - Port number
- SYSTEM(27 – 30) - UID, EUID, GID, EGID

OpenQM

Identify the process type

- @TTY

phantom	Background process
port	Serial connection
vbsrvr	QMClient session

OpenQM

File permissions

- QM uses o/s files and is hence subject to normal o/s permissions settings
- Group users as Administrators, Developers, Others
- Permission requirements for each group are in the QM Reference Manual
- Program execution needs read access

OpenQM

Data encryption

- New at QM release 2.6-0 (August 2007)
- Ad hoc encryption
- Record level encryption
- Field level encryption
- Uses AES 128, 192 or 256 bit algorithms

OpenQM

Ad hoc data encryption

- Simple to use for any QMBasic data item
- ENCRYPT() & DECRYPT() functions
- Key provided by application program
- Encrypted data never contains mark characters or ASCII control characters
- Can store in all file types

OpenQM

Record level data encryption

- Encrypts whole record automatically when writing to database
- Users without access to the key cannot open the file
- Can use AKs but index itself is not encrypted

OpenQM

Field level data encryption

- Encrypts specific field(s) automatically when writing to database
- Users without access to the key see fields as empty when reading and cannot update encrypted fields
- Cannot use AKs on encrypted fields

OpenQM

Encryption keys

- Key strings are stored in a secure "key vault" protected by a master key
- Only the security administrator has access to the keys
- Developers only know the key name

OpenQM

Security Administrator Commands

- CREATE.KEY
- Associates a key string and encryption algorithm with a key name

CREATE.KEY {*name {algorithm {string}}}*

OpenQM

Security Administrator Commands

- GRANT.KEY
- Grants access to key by user name or group name

GRANT.KEY *name* {GROUP} *name...*

OpenQM

Security Administrator Commands

- REVOKE.KEY
- Removes access to key by user name or group name

GRANT.KEY *name* {GROUP} *name...*

OpenQM

Security Administrator Commands

- DELETE.KEY
- Deletes a key from the key vault

DELETE.KEY *name*

OpenQM

Security Administrator Commands

- LIST.KEYS
- Shows key name, algorithm and access rights for each key

LIST.KEYS

OpenQM

Create a File with Record Level Encryption

- Use ENCRYPT option to CREATE.FILE
- Not restricted to administrators
- Specifies the key name, not the string

OpenQM

Add Record Level Encryption to File

- ENCRYPT.FILE
- Not restricted to administrators
- Specify key name to be used

ENCRYPT.FILE *filename keyname*

OpenQM

Set Up Field Level Encryption

- **ENCRYPT.FILE**
- **Not restricted to administrators**
- **Specify key name to be used for each encrypted field**

ENCRYPT.FILE *filename field*,*keyname*...

OpenQM

Which Fields Did I Encrypt?

- LIST.KEYS
- Not restricted to administrators
- Displays list of field name / encryption key pairs

LIST.KEYS *filename*

OpenQM

What if I Restore a Backup Elsewhere?

- The file can only be accessed if the key name is in the key vault and has the right key string
- Restoring a backup won't work because the master key is linked to a specific system
- Re-enable by entering the master key

OpenQM

But I Want to Copy My File!

- Copy the file
- Ensure the key name is in the key vault with the correct algorithm and key string
- Use SET.ENCRYPTION.KEY.NAME if the key name clashes with one on the new system

OpenQM

What If My Computer Is Stolen?

- Optionally require entry of master key every time QM is started
- Potentially inconvenient but provides best security
- Can enable / disable at any time

UNLOCK.KEY.VAULT

OpenQM

QMClient security issues

- QMClient allows a VB (etc) program to open files, execute commands and subroutines
- This is just like being at a command prompt but application level security is now on the client side
- Malicious users can do nasty things!

OpenQM

QMClient security issues

- The QMCLIENT configuration parameter imposes rules on what the client can do:
- 0 No restrictions
- 1 Ban OPEN and EXECUTE, limiting to calling subroutines
- 2 Restrict which subroutines can be called

OpenQM

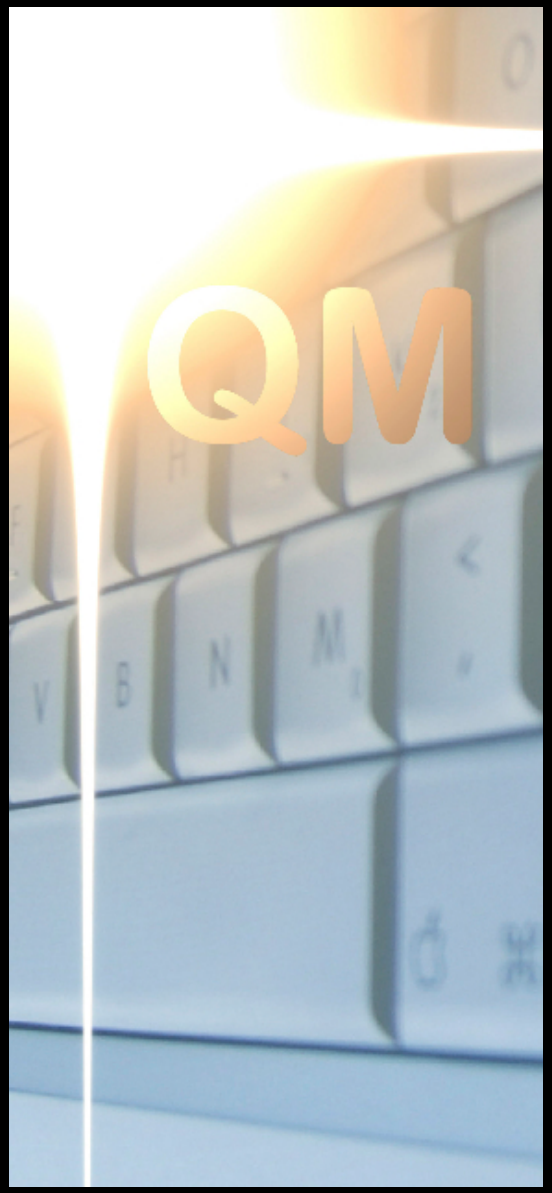
Backup policies

- Surprising numbers of users get this wrong!
- Backup of a live system is always dangerous
- Use of suspend / resume may not be on a business transaction boundary

OpenQM

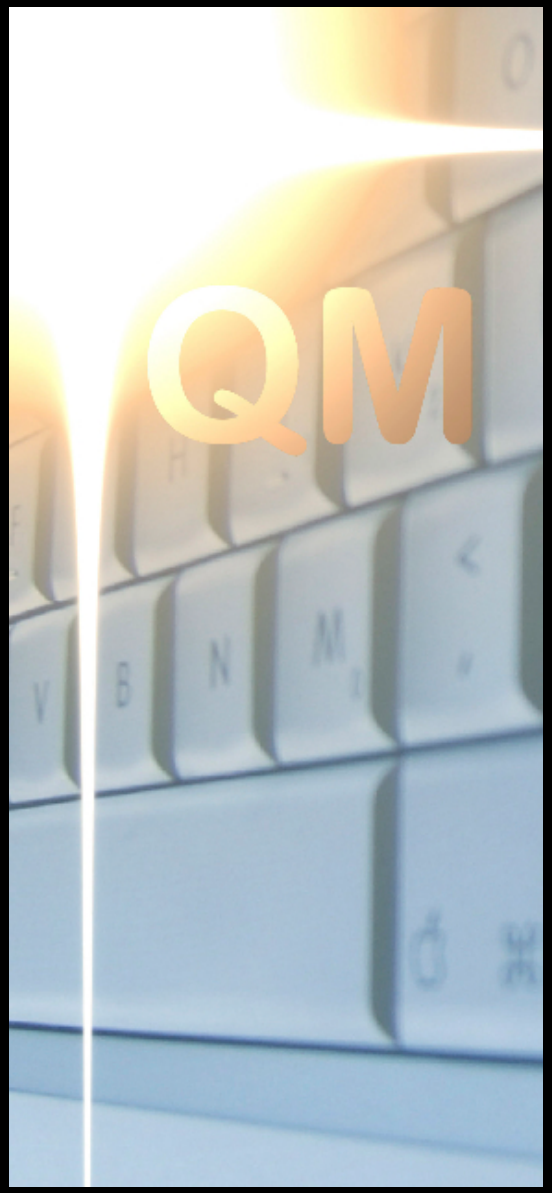
Backup policies

- Backup a complete, consistent set of data
- Cycle backup media
- Keep it in a secure place
- Test your backups!



OpenQM

QUESTIONS?



OpenQM