
Mainframe Information Security – why should I care and what should I do?

A White Paper by Bryan Foss and Paul Buckley April 2009

This short paper aims to summarise the current challenges related to Information Security, for the benefit of executives, managers, audit committee members and those operational staff involved in delivering improvements.

While the paper provides the wider view of information security challenges, there is a particular focus on the integrated role of mainframe information security, as important new capabilities have recently emerged which are changing what best practice can now be readily achieved. With new mainframe related capabilities and increased audit demands and consumer expectations, it seems inevitable that organisations will now accelerate their efforts to reduce the substantial risks currently related to mainframe information security.

Distributed Free at Infosec 2009



Sponsored by:

Neon Enterprise Software
New Broad Street House,
35, New Broad Street,
London EC2M 1NH
Tel +44 (0) 207 194 7602

www.neonsoft.com



Infosec 2009

Earls Court
London
28th—30th April 2009

www.infosec.co.uk

Mainframe Information Security – why should I care and what should I do?

A White Paper by Bryan Foss and Paul Buckley April 2009

While the paper provides the wider view of information security challenges, there is a particular focus on the integrated role of mainframe information security, as important new capabilities have recently emerged which are changing what best practice can now be readily achieved. With new mainframe related capabilities and increased audit demands and consumer expectations, it seems inevitable that organisations will now accelerate their efforts to reduce the substantial risks currently related to mainframe information security.

Drivers of increased management attention – Data breaches and failed audits

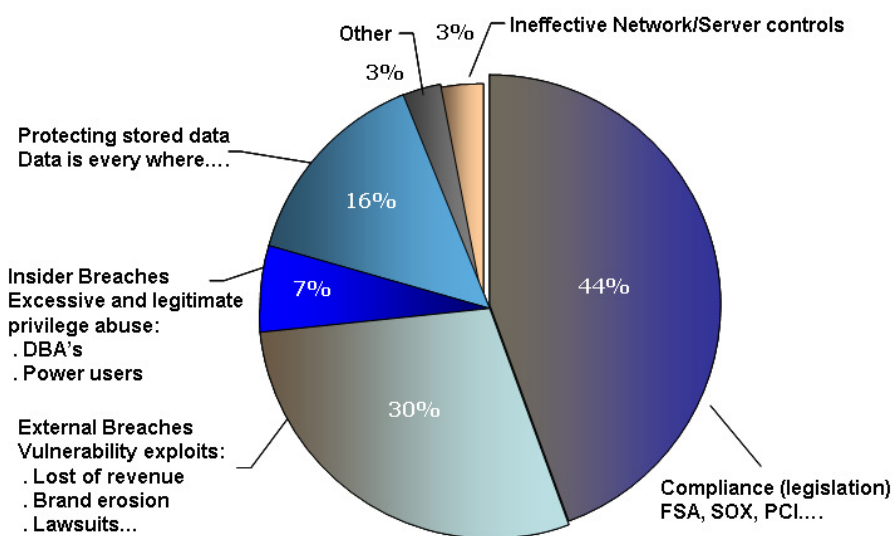
Almost every day we read in the press about another data breach, whether from data lost or found on the streets, hackers gaining access to sensitive data or disgruntled insiders abusing their privileged roles. The impact, or potential occurrence, of a data breach is a major driver of increased focus on information security by both executives and non-executives, especially as breaches must now be reported to the Information Commissioner and affected customers informed as well. Recent analysis has shown that up to 20% of affected customers may move their business elsewhere – and the reputation of the organisation may be substantially impacted, in turn making future business far more difficult to win.

In the current economic environment, perhaps the biggest future danger is the accelerated reduction of IT and other costs, especially in financial services organisations. Some businesses are aiming to reduce costs to such an extent that the remaining budgets will only allow them to 'keep the lights on'.

In this case an assessment that previously balanced costs and risks may instead become a cost driven assessment with little regard for the resulting increases in risks. However at the same time the FSA has publicly stated its intention to increase its oversight of risk management processes via audit – and will be looking for documented evidence of risk assessment exercises, action plans and staged improvements. The fines and other punishments for not achieving compliance are expected to be increased to a severe level, rather than the smaller fines that were previously of less significance to an organisation or its directors personally.

An increasing number of organisations are failing audits, in turn almost certainly driving remedial actions by management within a fixed time period – for example within the current year. These audits may be internal quality assurance or standards audits, internal risk audits, also external audits related to FSA regulations, Sarbanes Oxley or PCI-DSS (credit / debit card acceptance or processing standards) etc. In Health and Pharmaceutical organisations HIPPA and FDA regulations often apply. Audits are inevitably assessed and benchmarked against better-practice comparisons, which requires management processes to be under continual review.

Data Breach Challenges - Source The Compliance Authority



Ponemon Institute: The average cost of a data breach is £3.8 million

A recessionary market environment typically increases awareness and understanding of cost and risk, for example focusing additional efforts on retaining and developing current customers and profitable business becomes a priority, rather than expecting the acquisition of new clients and partners to cover for customer loss or damage elsewhere. Risk of customer loss through data breaches and reputational damage becomes much more important to prepare for.

In an individual organisation, most or all these factors now combine to require an enhanced level of information security capability, but in an environment that also requires more substantial cost reductions than ever before.

In general there will be a substantial gap between an organisation's current capabilities and the current understanding of best practice (or better practice). A risk-based approach will allow management to decide on relevant priorities and the business case for action, whereas a standards-based approach to compliance insists that specific criteria are met to continue doing business, whether each compliance action makes sense for this organisation or not. Both will require the implementation of 'Continuous Controls & Monitoring', which is an expectation of both senior management and regulators today.

Of course audit committees and auditors will look for 'sources of assurance' that are reliable indicators, proofs of compliance, or risk assessments and vulnerabilities. The results of internal inspections, measures and proofs can be considered as sufficient evidence, or they could be re-audited themselves for increased confidence.

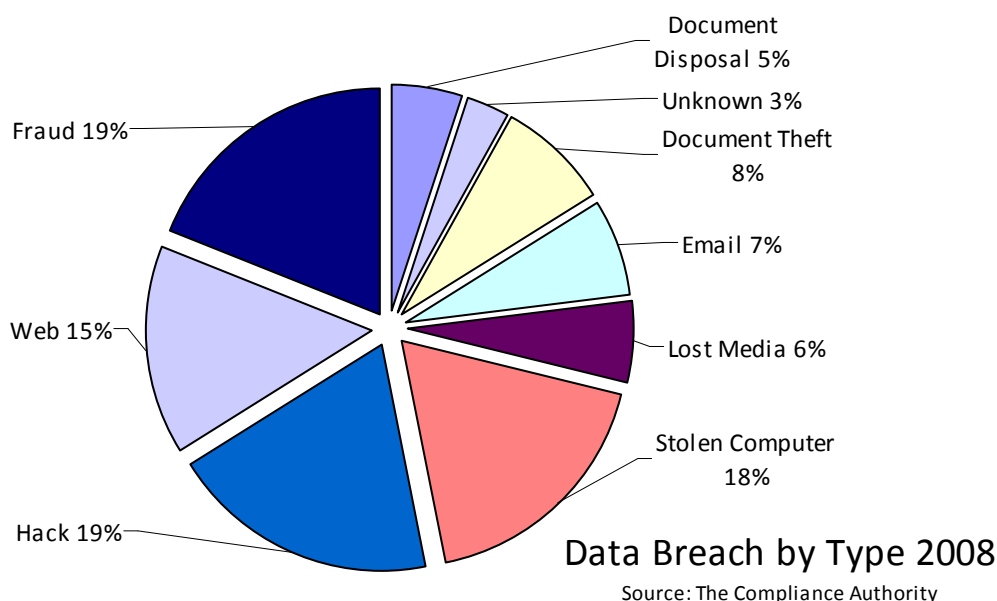
Audit committees and auditors often challenge whether a reliable inventory of systems and databases exists, at an early stage of the audit process. While network 'sniffer' tools can identify some traffic and user accesses, auditors need to have a greater certainty that all assets and uses are identified, which can only be achieved by proactive and non-invasive database monitoring tool-sets. These can quickly identify un-documented systems, databases, users and data accesses, whether these are database reads, updates or structural database changes.

Auditors no longer see their inspections as one-time, annual or even quarterly activities. Instead they know that they can now expect regular and reports to be automatically generated and emailed to them for further analysis.

Security control panels are emerging which non-technical security managers and auditors can use themselves to accelerate the audit process and to add reporting consistency between audits. These can also be used internally for continual monitoring and to provide measures and proofs for visiting external auditors in the shortest time possible and with minimal distraction of staff from their productive work.

Types of breach

For simplification we summarise the main areas of data breach to consider 'data on the move', 'penetration' of systems from outsider hackers and internal users with inappropriate access to sensitive data. Finally we consider the possibility of breaches caused by 'privileged' internal staff that may have high levels of personal authority but are often also expected (currently) to police the information security environment. Managing the risks related to privileged users has been particularly problematic in the mainframe data environment, until now.



Data on the move

We probably see more 'data on the move' breaches in the daily papers than any other type. Laptops and briefcases have been left on trains, disappearing courier packages and CD's, PC's and mobile phones sold on auction sites with sensitive data still on them, manilla personal health files and papers found scattered on highways and road roundabouts.

The press seem to love highlighting these stories, perhaps as they appear to demonstrate that apparently 'faceless organisations' are careless with the public's personal data, whether these are central government organisations, banks or others.

Many, even most, of these types of data breaches can be avoided with a combination of operational and technical solutions including:

- Not allowing the data to be copied or moved at all, where not essential
- Disabling USB interfaces and other methods that allow bulk data copying
- Removing sensitive or personal identifying fields when data must be moved
- Moving data via more secure methods (e.g. internal or closed networks)
- Key-encrypting sensitive data that still needs to be moved

Most organisations have focused on the 'data on the move' topic first, perhaps in part because of the increased public visibility and awareness of the issue. However other data breach risks that are less well understood may not yet have been addressed with the same level of urgency, yet can result in far greater exposure to the business.

Penetration by hackers and application users

As the public become more aware of the internet through their own use for home shopping and remote banking, more stories appear about hackers and the safety of credit card details, bank accounts and home shopping services.



Determined hackers will persist with their penetration attempts and regular 'pen-tests' are required (using authorised audit tools and services) to prove adequate protection levels exist. Internal staff will have carefully assigned levels of access that ensure they cannot read or update sensitive data, which could be their own data, their neighbours data – or even 'celebrity' personal data.

Where some staff share user profiles, for example with SAP and similar systems, it becomes important to separate users activities at the data access level to ensure that they are acting within policy.

At the same time a few more privileged staff (perhaps handling rapid turnaround of customer complaints) need ready access to almost any customer case for review, so inevitably there needs to be flexibility in this process to ensure that access can be granted and service levels for response times can be achieved.

Actions of privileged users (Distributed data)

Distributed data is now scattered throughout our enterprises, so we need to question whether anyone really knows where the sensitive data lies and whether it is adequately protected. To help auditors there are now automated audit tools which monitor the organisation's network to find and record both systems and databases, in part through watching for user accesses made. While most of these data sources can be recognised and self-documented within minutes or hours, a few will be accessed infrequently and may not be immediately visible. Leaving the automated audit in place over month and quarter end should find the few systems which are the 'long tail' of those to be located to make the audit complete..

Once these systems and databases are properly identified, the sensitive data they include can also be identified. One risk reduction stage is to confine selected distributed systems and databases into a more secure area of the business and network, enabling a higher level of security and oversight to be applied at a reasonable level of cost. Encryption can then be applied in a more targeted manner, as it will not only be used when moving data externally. For example PCI standards require sensitive data held internally to be encrypted as well.

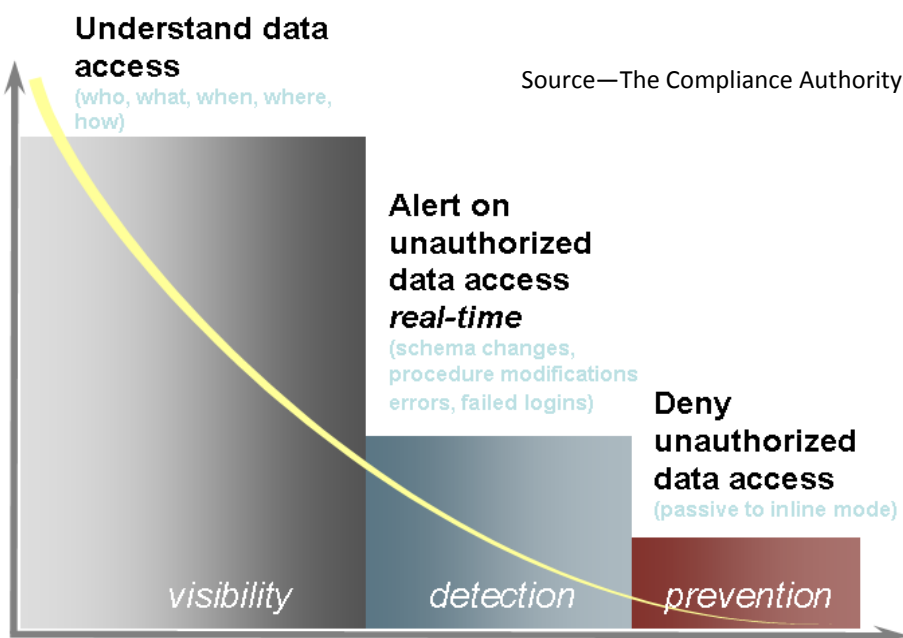
Audits of data usage have usually shown that very few staff need to see as much sensitive data as they are currently exposed to, for example do they need to see the customer's complete credit card number to identify and validate the person they are speaking with? Systems and user screens can be modified to reduce the number of staff with access to sensitive data that they do not need to see. This action complements the efforts that most organisations put into assigning password protection to users.

Some application systems (for example SAP and Siebel) may be implemented in such a way that user profiles and passwords are shared between staff. In this situation it can be difficult to secure data or to properly investigate a data breach after the event – unless steps are taken (including new tools being used) to distinguish between different users sharing the same application profile.

Organisations are increasingly overlaying a security-management layer across the total distributed data environment, enabling a business manager (often titled 'security manager' or 'risk manager') to provide ongoing audit assurances through a control panel and regular reporting. Unusual accesses to sensitive data can be identified in real-time and even intercepted. Automated management rules can be developed over time to improve the oversight of data accesses.

Data breaches identified after an event has occurred can be properly evaluated and managed, minimising the business consequences, usually as part of a properly prepared approach to Crisis Management. Strong boards will normally prepare scenarios, processes and even scripts for a crisis of this type, not just for traditional business issues.

KPMG (in their recent Data Loss Barometer report) highlight that "even businesses with the most sophisticated controls can get caught out by a data breach. Upfront planning on how to deal with a breach can help to reduce the impact of the loss, preserve evidence for investigation, maintain good relations with the public and the press and prevent future reoccurrence".



Actions of privileged users (Mainframe information)

Mainframe technical staff are often uniquely positioned to carry out operational changes and to police the systems and database environment they work within. The reasons for this are historic, but security and compliance managers are now realising that these roles need to be separated and the recent availability of mainframe security tool sets enable this.

Mainframe data has traditionally been managed in a different way, often due to its longer heritage and the development over time of specialist skills in systems and data management. Database Administrators ('DBA's'), Systems Programmers ('Sysprogs'), Operations Analysts ('Opans') and their management provide the hands-on support to identify and fix data-related issues on production systems.

Sound change management systems will often be required (certainly for PCI standards compliance) to ensure that any system or database changes they make are checked and pre-authorised, or are checked and post-authorised where emergency interventions have been required by privileged IT staff to maintain the required business continuity and the service levels of production systems.

Implementation of these basic oversight processes will immediately reduce the likelihood of accidental or deliberate information security exposures. The most sensitive industries, for example financial services, for years had more formal processes for checking the authorisation and effect of any changes system changes before they were applied to the production systems environment – although some organisations may now be compromised by relaxation of oversight processes over time as costs and staff are reduced.

As approaches to managing mainframes matured over the years, technical experts gained more senior, trusted and privileged roles over time. Usually a manager would know his team of people and perhaps their families too. He would work closely with his key staff and know their competence, motivations etc – determining what authorities they should have and what exceptional oversight was required to ensure mistakes or deliberate sabotage did not occur.

Where privileged staff were once co-located and well known, they may now be temporary staff, or perhaps staff located in multiple international office locations and even working across secure connections from home. While key IT staff once worked directly for your organisation they may now work for an outsourced systems provider, which has its own processes for allocating privileged access to your data to specific staff.

Current world economic factors have increased the likelihood that privileged staff will initiate data breaches, whether through financial incentive or as their willingness to be a trustworthy employee reduces. While the average consumer may find it difficult to relate to mainframe data operations, the technical and industry press is increasingly exposing the use of ‘logic bombs’ by disgruntled employees – timed to ‘go off’ after they have been made redundant or otherwise left the organisation. When people leave their job, their profiles and passwords are often not disabled for some time, leaving them to be an ongoing risk even after they have left employment.

It has previously proved very expensive to properly monitor all mainframe database activity. Adding ‘tracing’ or logging functions can increase required mainframe capacity by up to 15%, or seriously degrade online and / or batch performance to the business.

As a result proper reports are often limited or non-existent and the same privileged staff that may be implicated in the data breach are asked to collect and analyse the historic systems data required to determine whether a breach occurred and if so, then how.

Your auditors may also recommend that you do not log data unless you have also implemented a capability to analyse and use this data for improved reporting and security control purposes. Auditors are rarely impressed by traditional self-policing structures, instead they expect to see assurances that data protection and good governance can be demonstrated through proper separation of responsibilities. Just as in financial trading rooms, where back office managers oversee front office trading operations, in the mainframe environment auditors are increasingly expecting proper oversight of these highly privileged technical staff. Proper separation of responsibilities and oversight of privileged technical users will be important to address some of the most critical risks here.

Case study: Fannie Mae

Wired.com recently reported that a ‘Logic Bomb Would Have Caused Weeklong Shutdown’. The privileged engineer was indicted in court on a charge of computer sabotage for allegedly writing and planting the malicious code on the day he was fired from his job.

Fortunately an authorised ‘oversight’ person, using a monitoring tool, was able to discover the privileged engineer’s actions and the malicious code hidden inside a legitimate automatic script that ran at a set time each day. Reports showed that the privileged engineer had accessed the server on which the logic bomb was created in his final hours on the job. The change was found using the security tools which Fannie Mae had selected and implemented earlier. These tools provided the necessary monitoring and reporting to identify changed files, including those changed by privileged staff.

The FBI says the code would otherwise have executed a series of other scripts designed to block the company’s security monitoring system, disable access to the server on which it was running, then systematically wipe out all 4,000 Fannie Mae servers, overwriting all their data with zeroes.

In this situation a readily-available information security toolset, with reporting properly used by security oversight staff, identified and prevented a massive business disruption. While this logic bomb was designed to cause business disruption, it could equally have been designed to carry out damage to the business in other ways, for example through initiating large-scale financial transactions or exposing sensitive data to the public domain.

The following constraints have traditionally contributed to the mainframe database environment being impractical to manage securely. However, as better practice develops, each of these significant constraints can now be overcome.

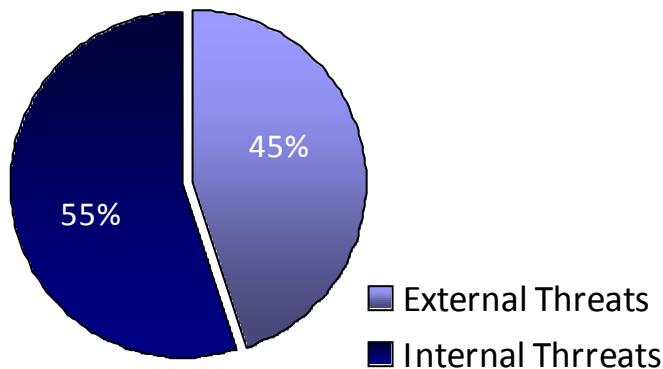
- The cost and performance impact of logging all database reads and updates in the mainframe environment
- The cost and distraction of key-staff time to locate, review and report back on any logs that are available, when audits are required or events occur and need investigating. Without automation, looking for a specific occurrence (e.g. access to a VIP's record that was later publically exposed) would be like 'looking for a needle in a haystack'.
- Real-time notification and an early response to the breach cannot be achieved through ad-hoc review of historic logs. Post-incident investigation of any logs can only be initiated when the incident has been identified through other means. Implementing an 'alert system' in this environment is completely impractical.
- The action of reading database records is usually not captured by logs, yet this is a far more likely occurrence when data breaches occur than an update to data. Viewing or copying sensitive data is usually sufficient for it to be compromised. Identifying when data is read at unusual times, by unusual users or in other unexpected patterns would help identify and perhaps even prevent ongoing breaches that are not even recognised today.
- The lack of useful and complete (or 'fine grain') log data also inhibits the development of a vulnerability assessment, where self-learning tools could then be applied to analyse logs and to separate and report on changes in behavioural patterns that may be entirely innocent and expected from those that may be threatening and requiring intervention. Management increasing expect updates on exposures to be presented to the right person, at the right time, with sufficient information to act.
- Other non-security system management capabilities, such as cross-charging by usage may share and reuse the same data when it becomes collectable at economic cost, perhaps justified initially by information security needs. IBM's Tivoli and other similar products can achieve this when a high performance 'tap' is deployed as the mainframe reporting device that provides input data to them.

Dealing with business and channel partners in the value chain

In addition to any direct business and systems operations you may have, your distribution channel or other partners may have special requirements related to Information Security which they will expect their suppliers and partners to respond to. For example the UK Financial Services Authority (FSA) probably puts most audit focus on those firms which directly manage the consumer relationship. There is an expectation that these customer-facing firms will be part of the assurance process to ensure that subsidiary suppliers of products and services play their role in supporting the achievement of compliance standards.

Some of those firms are very capable and experienced with compliance requirements, so they are also able to provide a set of business and technical criteria to their prospective suppliers. This may be in the form of a technical architecture or checklist, also a business contract and service level agreement that includes specific information security requirements. In this case the challenge for the subsidiary supplier is to demonstrate that these compliance measures are in place, or can be put in place very quickly to provide end-to-end assurances.

Information Threats
Source: The Compliance Authority



In the PwC report 'Fraud in a downturn' (A review of how fraud and other integrity risks will affect business in 2009), they highlight that "We see the principal threat arising from **opportunity** resulting from the inadequacy of control. In our experience, many organisations have begun to put arrangements in place to improve data security. However not enough is being done to address the risk of deliberate theft by criminal organisations working in collusion with permanent, short term or temporary staff to infiltrate organisations and circumvent existing control systems."

Other distribution organisations are less capable of leading the compliance requirements conversation and may look for suppliers to be pro-active, experienced and supportive in delivering end-to-end compliance processes. Some suppliers that are very dependant on excellent channel management may aim to demonstrate ‘gold star’ performance to attract distributors to work with them.

As it becomes harder to win new customers, distributors are focusing more effort on retaining those customers that will prove to be profitable. This in turn may require additional emphasis on the good management of existing customer data, as it is now proven that any firm suffering a public data breach is likely to lose a considerable percentage of its valued clients, at a time it can least afford to as they cannot readily be replaced.

Regulators also expect to see a sound end-to-end approach to the good management of customer information and especially where sensitive data is identified. Within that end-to-end process, what appears to one organisation as internal data is considered to be external data by another. Distribution partners need to work closely together to define, develop and implement the business and systems architecture that provides each of their businesses, and the regulator, with a viable and auditable solution.

Audit processes – self assurance and beyond

As it has become even more important to have sound processes that deliver the customer experience required, alongside regulatory compliance, firms have often implemented some form of internal quality assurance process to sample client outcomes, investigate process failures and root causes, also to recommend local improvements which probably include staff training and development. In this way firms are able to achieve and measure continuous improvement, also to demonstrate to others that their assurance processes are operational and effective. These teams are sometimes referred to as Standards staff, rather than Quality Assurance (or QA).

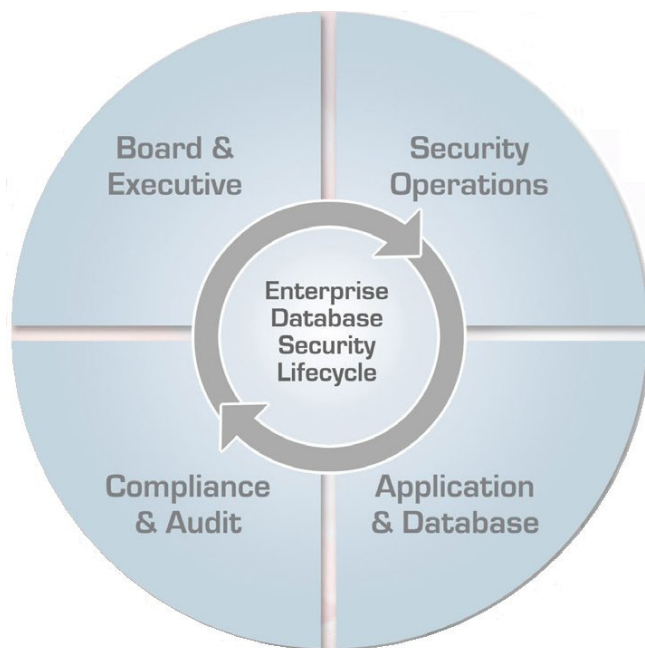
Internal auditors will normally look carefully at existing QA processes, how well they are applied, what findings result, what separation of responsibilities exist and how well issues identified are addressed by management. A subset of these cases may be re-audited by internal auditors to increase confidence that these QA processes are effective.

External auditors will normally take a similar approach, to provide the assurances that the firm’s stakeholders require. These may be mentioned in the annual report for example, but will certainly be shared with executive management during detailed post-audit feedback. Any deviations from required areas of compliance will inevitably result in an action plan responsibility being assigned to an appropriate director, to ensure remedial action is taken before a specific date.

Internal and external auditors often need to take a wider perspective to ensure that things have not been overlooked. For example they may be supported by best-practice technology and tools that are able to quickly identify and audit all systems, databases, active users etc to compare these with ongoing QA activities. They will usually look at MIS and other reports as sources of assurance, checking these back to the underlying events to assure proper recording and management has taken place.

Auditors may require additional reports to be added, to reduce their effort while improving their oversight of operations and governance. Some systems will now automatically produce Information Security reports which are securely mailed directly to audit staff on a regular basis, providing data in a form (for example spreadsheet-style) that can be further desk-analysed by the auditor.

While auditors would need to audit and even benchmark your organisation against specific standards and the best practice methods of conforming to them, what is ‘best practice’ is constantly changing as new tools and techniques emerge, also new practices exploit them and new internal and external demands arise. Real-time rather than delayed analysis is an emerging capability that not only provides audit confidence, but can prevent data breaches or prevent them escalating or re-occurring when identified early.



The Compliance Lifecycle
Source—The Compliance Authority

What are the next steps for my organisation?

Typically organisations (with the support of their auditors and perhaps other consultants) will set out on a staged plan to provide dynamic protection to protect both mainframe and distributed data. This might include:

- Taking a risk-based planning approach to Information Security generally, to document the balance of costs and risks in a manner that visibly aligns with the risk appetite of the board and the requirements of regulators.
- An early deployment of a separate Information Security Manager role
- Identify and implement best practice security tools that provide a usable control panel, summary reporting mechanisms and separation of responsibilities between users and oversight roles. This is especially important where privileged users exists, such as in the mainframe environment.
- The initial inventory audit will enable prioritisation towards addressing sensitive data sources and other critical vulnerabilities
- In parallel (and early in the process) prepare crisis-management scenarios, including post-breach audits, damage limitation efforts and public & stakeholder relations activities can be outlined
- Over time, progress through the raising of standards of continuous monitoring and oversight to a consistently high level across the portfolio

Looking ahead

Technology solutions continue to be developed to assist in the protection against data breaches and to achieve and demonstrate regulatory compliance. As a result best practice also develops, so auditors, audit committees and others must remain updated and ready to provide challenge and advice within the assurance process.

While technology can enable new capabilities, operational structures and processes continue to be key to success. This includes the proper separation of responsibilities for each privileged role and its oversight or audit function. Many organisations are now appointing Risk Managers who will improve these oversight processes and exploit new 'control panel' tools that allow business managers to oversee and assure technical operations.

At each stage it is recommended that business managers and their audit committees continually consider the current situation (and especially their prioritised risk status versus best practice) and clearly document their decision process and final decisions. While it may be easy to suggest with hindsight that an alternative approach should have been taken, if the most appropriate decision was clearly taken at that time then the management team has done the best that they can.

Looking ahead it is likely that there will be continued, even increasing, attempts to penetrate information security approaches either from inside or out. However if breaches can be successfully defended then it is likely that the increased risks of being identified, or reduced reward for effort, will drive these issues elsewhere. These actions remain difficult to justify in the current economic environment, yet at the same time essential for regulatory compliance and continued trading.

Sponsored by:

Neon Enterprise Software

New Broad Street House,
35, New Broad Street,
London EC2M 1NH
Tel +44 (0) 207 194 7602

www.neonsoft.com



About the Authors:

Bryan Foss is an independent advisor, business author and non-executive director, also founder of www.FossInitiatives.com
Bryan can be contacted at BryanFoss@gmail.com

Paul Buckley is Business Development Director, NEON Enterprise Software www.NEONsoft.com