Guernsey Financial Services Commission

Data Security

A Thematic Report on Practices within the Fiduciary Sector of the Bailiwick of Guernsey

April 2014

Table of Contents

1. Foreword 3
2. Executive Summary 4
3. Methodology 4
4. Sector Participation 5
5. Results 6
6. Acknowledgements 19

Disclaimer:

This report is not intended as formal regulatory guidance, nor should it be taken to cover all relevant aspects of the subjects addressed. Rather its purpose is to identify and communicate examples of good practice as well as areas where improvements could be made

Produced by:

Carl Ceillam CISSP, EnCE, GCIH

1. Foreword

by Philip Marr, Director of Fiduciary Supervision & Policy

Good practice in data security should be regarded as a pre-requisite of effective and successful wealth management businesses. This is principally because good data security is an integral part of private clients' confidence in working with wealth management professionals.

It is well known that Guernsey has for many years been a significant centre for wealth management and private banking and that trust and fiduciary services are an important part of that offering. You may be aware that the Commission undertook a thematic review of data security practices across the banking sector in 2011 in Guernsey. In that sector robust data security is regarded as fundamental to confidence in private banks. We believe this applies equally to trust and company service providers. In the recent past theft of customer data has caused some major concerns in the banking sector and it is this potential reputational risk which lies at the root of our encouragement of greater awareness of good practice in this field and avoidance of complacency, especially since data security threats are ever changing. For the avoidance of confusion "data security" and 'information security' are terms which we regard as equivalent and interchangeable.

You will see from the Report that the ISO 27001 sets the standard for several areas of good practice. I would encourage licensees to benchmark their own data security practices against the ISO standard and the examples of good practice described in this Thematic Report. As is evident from the Report failings in data security are not strictly insurable events or activities. It therefore requires management and staff to adjust their ways to become more vigilant to the threats and to conform with good practice. Hence security awareness should not be regarded as just an interesting seminar topic but rather it should be part of day to day behaviour.

In that sense the outcome of this Report should be an active response and not a passive one.

2. Executive Summary

From June to November 2013 the Commission undertook a review of Guernsey-licenced fiduciaries' approach to data security. The observations made in this report are supported by analysis of data taken from a questionnaire that all licensees completed together with a number of on-site visits.

Given the diverse nature of fiduciary businesses the overall results were mixed, but several recurring themes did emerge. In terms of areas of good practice the following areas stood out:

- Most organisations had up to date security policies that covered the key areas of data security. Policies were an important but effective means of communicating security responsibilities to staff.
- Due diligence over service providers handing confidential data was most effective when the organisation took the time to perform their own reviews and inspections. These included several examples of annual on-site audits performed by compliance officers.
- Business continuity plans were up to date and tested. Organisations used a broad range of testing methodologies, including walkthroughs and table-top simulations as well as standard invocation tests.

We noted several common areas for improvement:

- Although risk assessments were being performed, when organisations considered data security risk they tended to note it as a single generic item. This narrow approach does not support effective assessment of such a complex risk category, and a more granular approach is needed.
- Despite some positive examples, in most cases third-party supplier due diligence was found to be lacking with respect to data security. Organisations place far too much trust in their service providers without any tangible justification for doing so.
- Vetting procedures were inconsistently applied to employees, temporary staff and contractors. The second two groups tended to have fewer checks, even though they often have access to the same sensitive information as permanent employees.
- In most cases senior management did not know what audit trails existed for key applications. As a result they could not demonstrate that incidents could be investigated effectively.
- For the majority of organisations, staff were not given adequate security awareness training. Training was either minimal or only performed once at the time of joining.

Overall, the Boards of licensees need to take a more active approach to managing information security risk. This requires the establishment of an effective governance structure for data security risk, in the same way as other types risks are handled. Risk assessments, control reviews, and remediation plans are then executed in a continuous cycle of improvement.

3. Methodology

A two-stage approach was followed:

- An industry-wide survey of Guernsey licenced fiduciaries using a self-assessment questionnaire, issued in June 2013
- On-site visits to a representative sample of organisations, to examine controls in more detail and perform a limited amount of testing. This work was completed in November 2013.

We based the questionnaire on ISO/IEC 27001:2005. This is an internationally recognised standard for implementing information security. ISO 27001 was chosen because it covers virtually all aspects of data security, making it an obvious choice for a general review of the subject. In all there are eleven categories:

- Security policy
- Organisation of information security
- Information asset management
- HR security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity
- Compliance and audit

All Guernsey licenced fiduciaries were then asked to complete an online questionnaire, which contained 79 questions.

After a preliminary analysis of the results we identified key areas of focus and selected a cross-section of licensees for onsite review. The onsite focus areas were:

- security governance
- third party risk
- data leakage prevention
- staff security awareness

The Commission was very grateful for the considerable amount of time and effort that the licensees visited went to in preparing documentation, which was of high quality and of great assistance. We also appreciated their openness in discussing their approach to managing data security. Each licensee visited was given informal feedback on areas of good practice, and where The Commission felt improvements could be made.

4. Sector Participation

4.1. About the Respondents

Out of 179 licensees, the majority are locally owned private businesses:

Licensee type	**%**
Privately owned - local	40
Privately owned - overseas	11
International financial group	22
Lawyers and accountants	9
Personal fiduciary licensee	18

65% had been operating in Guernsey for more than ten years.

4.2. Outsourcing

Over three quarters of respondents outsource IT, facilities/cleaning, or archiving. Arguably these groups of service providers present the greatest security risk, as they often have regular, unsupervised access to systems and data.

4.3. Critical applications

Over half regarded Microsoft products (including e-mail) as critical business applications. This compared with widely used local trust and company administration packages such as 4Series,

FlyingBoat, Acumen, and ViewPoint; these four alone accounted for 55% of respondents' most important software.

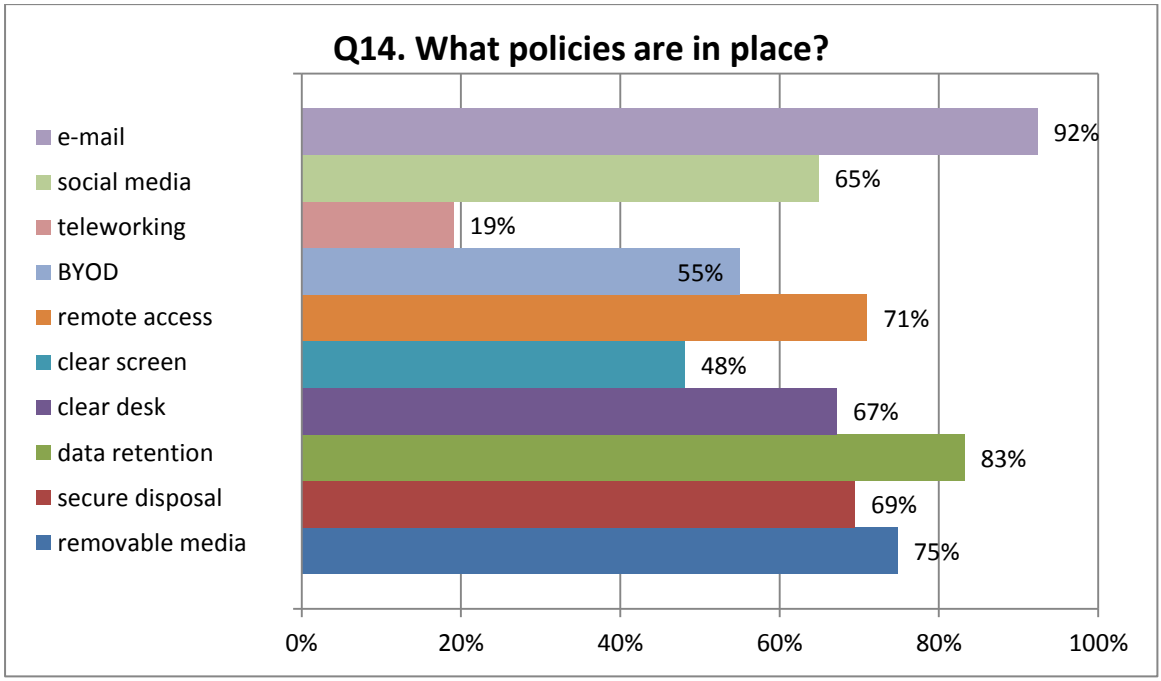
4.4. Application types

As expected, most were using local- or group-managed systems. However, just over a third (36%) reported using internet- or cloud-based systems.

5. Results

5.1. Security Policies

Respondents used a wide range of policies documents to convey data security obligations to their employees. It was also reassuring to see that 68% had reviewed security policy documents within the last 12 months; for policies to be effective in a rapidly changing area like data security, they need to keep up with the latest trends in technology, so regular reviews are essential.



For the majority of organisations policy coverage appeared to be quite extensive. In particular it was encouraging to see that social media and BYOD (bring your own device) scored quite highly (65% and 55% respectively), despite the relative immaturity of these technologies.

Conversely, a simple requirement such as clear screen policy (i.e. locking a screen when not in use) was addressed at less than half (48%). In common with the more widely adopted clear desk policy, clear screen addresses the risk of unauthorised access to systems and information. This practice is also beneficial because staff become more attuned to security, to the point that it becomes second nature.

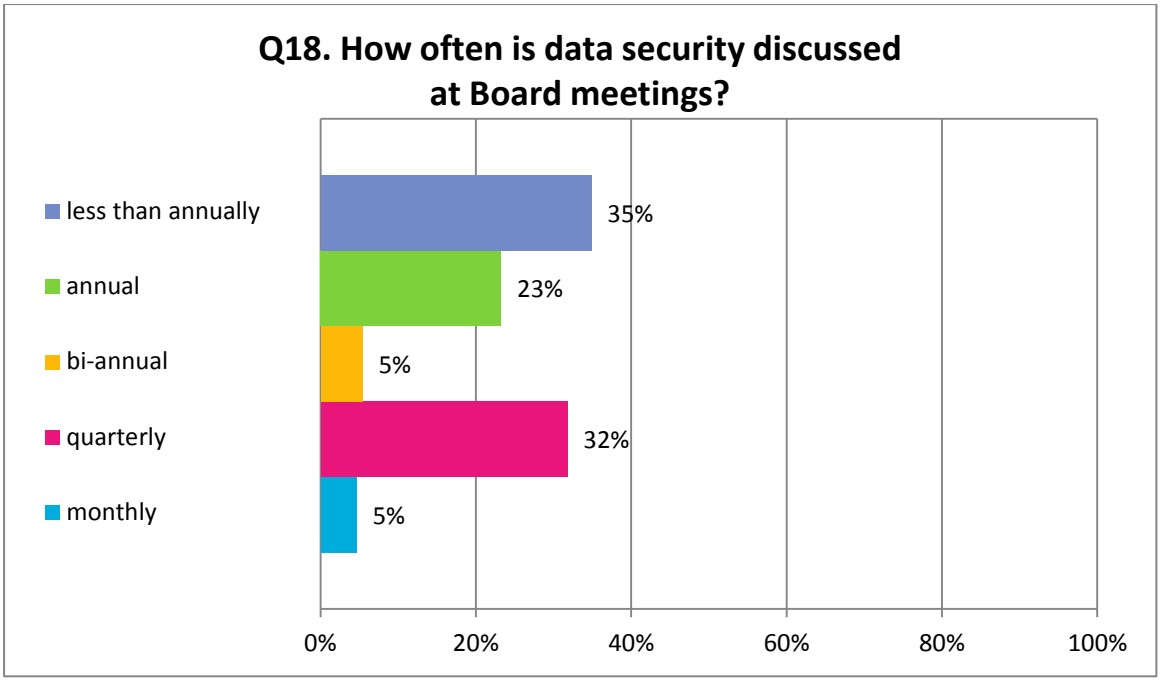
5.2. Governance

5.2.1. Corporate Governance Issues

Here we found one of the most significant divides in our licensees' responses. Almost a third claimed to discuss the topic of data security at board meetings on a quarterly basis. This is commendable and is a healthy response to this increasingly significant and fast-moving area of risk. In contrast, just over half (58%) only discuss data security annually or less often (which includes never).

Every organisation, and indeed individual, faces a constant barrage of data security threats. These threats and the controls needed to mitigate them are constantly evolving. It is therefore vital that the

Board keep up to date on these matters and give them due consideration and attention. Unless the Board is fortunate enough to have a sufficient understanding of data security, then it should seek advice from service providers and other specialists.



5.2.2. Security Officer Role

The role of Information Security Officer was assigned to a diverse selection of individuals, ranging from directors, compliance officers, dedicated information security officers, and IT personnel. Only 6% had none, and instead relied on staff reporting incidents to the relevant member of the board.

An informal arrangement may work for day to day purposes in small organisations. However, unless the role is formally assigned there is a risk that no one is tasked with promoting good security practices or policy enforcement. In the event of a security incident there may also be confusion about who does what, this can make matters worse. The role of security officer should always be assigned, and responsibilities documented.

5.3. Due Diligence And Contracts

5.3.1. Service Provider Due Diligence

We asked licensees which forms of due diligence are performed on service providers who handle or have access to sensitive data.

The responses indicated that formal reviews were not often performed . Several respondents did not feel that due diligence even relevant, reasoning that their service providers such as cleaning and facilities management services did not access sensitive data. This view ignores the risk that the service provider could easily gain access to IT systems or physical records.

There were a wide range of qualitative responses to the question, several of which require further comment:

"We rely on fact that supplier itself is regulated."

"We only use well known suppliers or those with a good track record."

"We ask for references and talk to other customers."

"We run our standard KYC background checks on suppliers (Worldcheck etc.)"

These methods offer some limited value in terms of reputational assessment, but fail to recognise the key issue: what is the provider doing to ensure that data is adequately protected?

Other respondents offered some informed approaches to the question. Some enquired about procedures and controls; in some cases requesting copies of key documents (the information security policy is a must-have). One large organisation had a standard vendor risk management process which included an assessment of information security risks.

Perhaps some of the best examples we found were during our onsite visits; one organisation's compliance officer made an annual visit to the company's data archival provider. In less than an hour she was able to see first-hand the physical security and environmental protection measures in place, review visitor logs and sign-in procedures, and confirm the existence of specific archived records. She had then documented the review, stating which controls had been reviewed and the results.

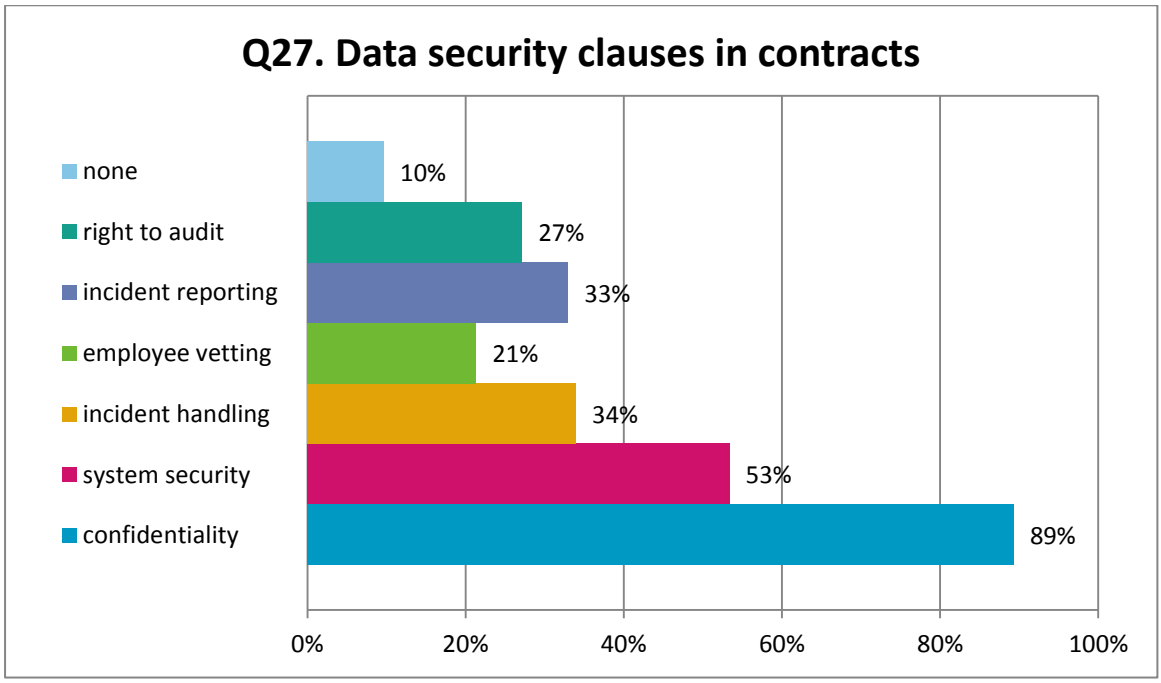
Another company visited their IT provider to seek assurance over their tape backup arrangements. Again the visit considered physical security, record keeping, access control procedures, and confirmed the existence of the company assets being stored.

In cases where the service provider is not required to handle data, but could potentially do so, a different approach is required. One company we spoke to required their cleaning firm to provide written confirmation that all staff were security checked.

The principal point to be made here is that trust has no basis unless it is supported by evidence. Discussion and enquiry may help, but there is no substitute for performing your own checks. Doing so also keeps the supplier on their toes.

5.3.2. Contractual clauses

Continuing our focus on third parties, we asked what data security requirements are included in contractual clauses.



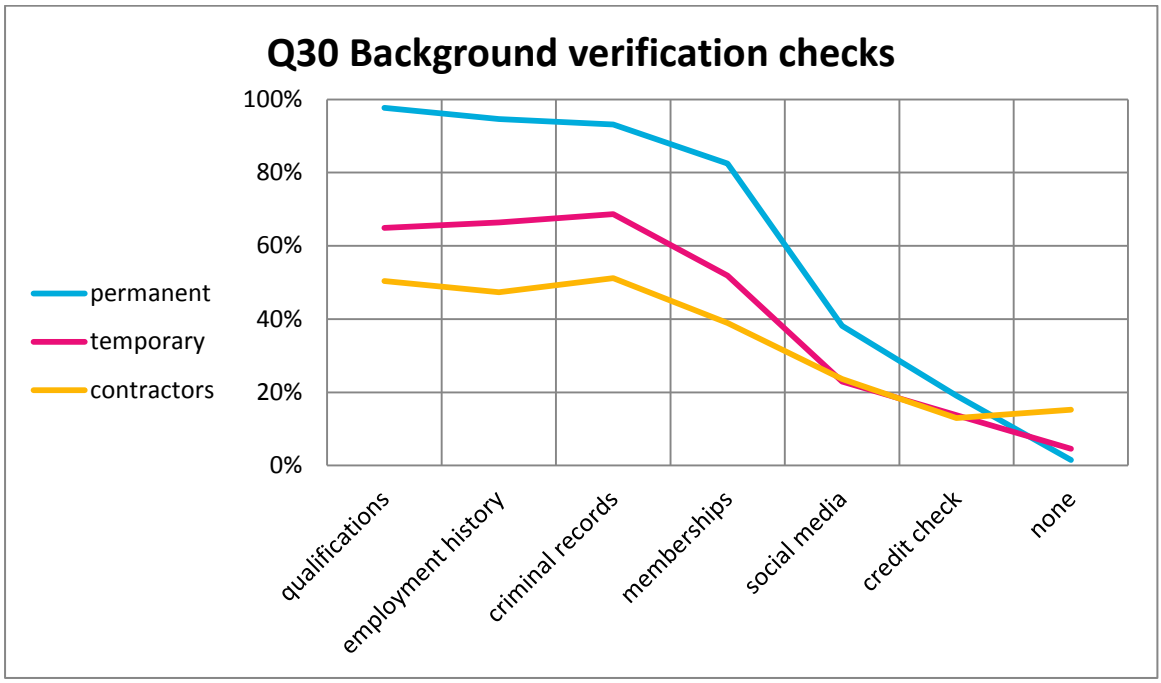
In common with the other questions relating to third-party risk, we found considerable variation in the extent to which contracts cover security requirements. Many respondents commented that the thematic had either highlighted the lack of formal agreements, or flagged a requirement to update those that were in place. This was confirmed in our onsite reviews, where most licensees admitted that third-party contracts with IT providers, cleaners, and storage companies offered little or any coverage of data security.

Although a suitably worded contract may offer some legal protection in the event of a security breach, it does have a more immediate practical purpose; by setting out all data security responsibilities and expectations; there can be no doubt or misunderstanding of what needs to be done, and who by.

5.4. Staff Security

5.4.1. Verification & Vetting

The next question considered the trustworthiness of the individuals who have access to licensee data and systems. Respondents were asked what forms of checks were performed on permanent staff, part-time staff and contractors.



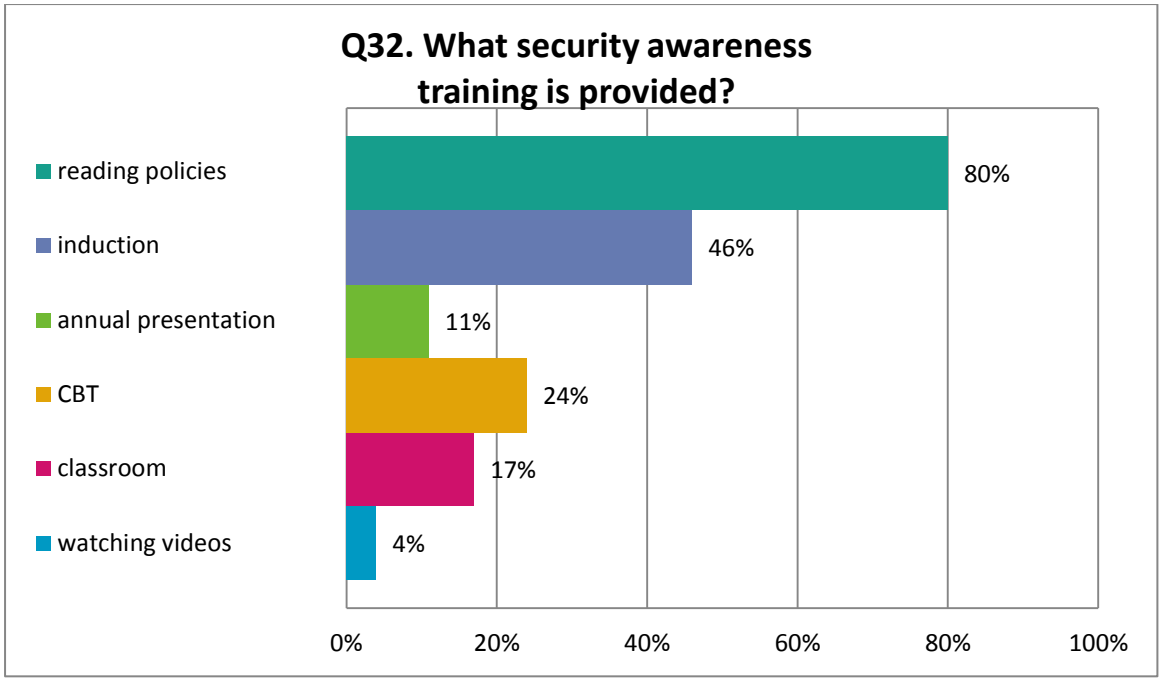
The results clearly showed that virtually all permanent employees were subjected to checks on qualifications, employment history, and criminal records. It was surprising that only 2/3 were checking temporary staff, and less than half covered contractors, even though these groups often have special privileges for project work or general access to a wide range of physical records. Based purely on logic and risk, we would expect all three groups to undergo similar vetting procedures.

In some cases licensees rely only on recruitment agencies to vet staff. This approach is sensible providing the agency procedures are adequate. In line with the supplier due diligence principles outline in 5.3.1 above, the licensee needs to agree with the agency what vetting standards are to be applied. One licensee found this out to their cost when a temporary bookkeeper was responsible for a security breach. The licensee had wrongly assumed that the recruitment agency had performed certain background checks. Had they done so the bookkeeper would never have been employed.

On that note, in financial services, where the risk of and perhaps temptation for fraud is high, we were surprised that credit checks were the least popular form of background check. Finally, although not yet widespread, there appeared to be a growing use of social media. Although material posted on social media sites may not always be trustworthy, it can highlight areas of concern that can be looked into.

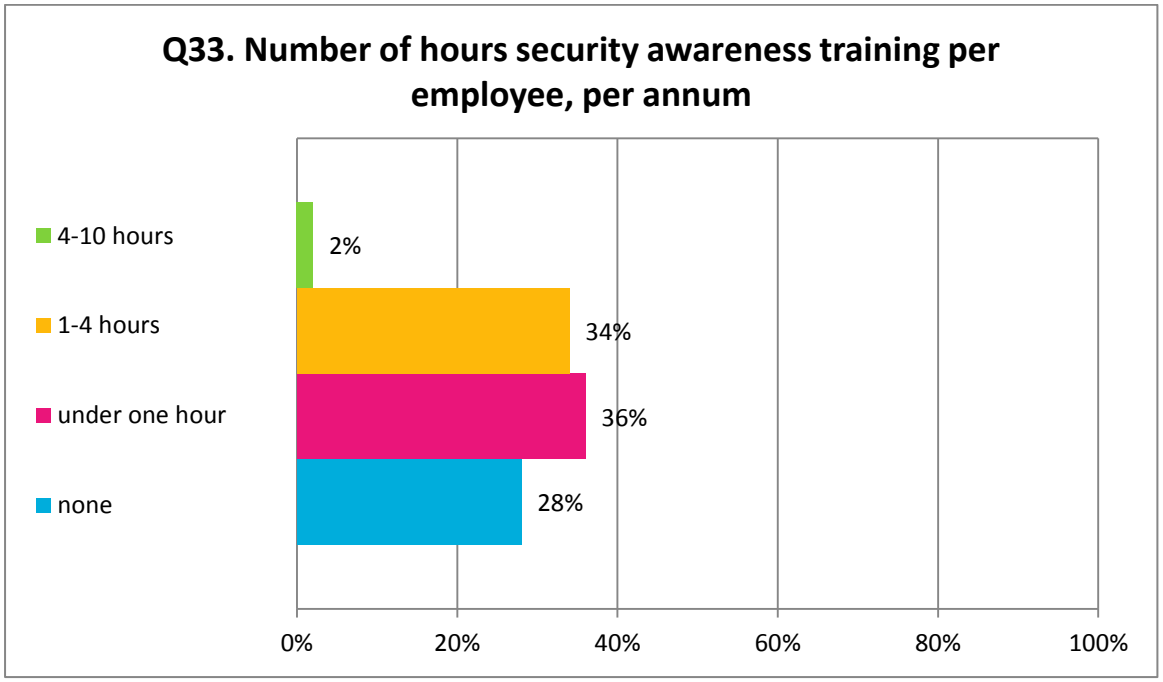
5.5. Security Awareness

We received a particularly poor response to the question of security awareness training. Less than half even covered data security in staff induction; other forms of training were even less popular. Instead the most organisations relied on staff reading policies to raise awareness.



Reading policies is obviously important, but hardly an educational exercise. Induction is a one off, suggesting that many expect security messages to be digested once and retained indefinitely. In any case induction is not solely devoted to the subject of data security, so the time spent on the topic is likely to be rather limited.

The following question, how much training was actually performed per year, revealed the extent of the issue. Over a quarter (28%) offered no training at all.



During each of our on-site tests we ran our own security awareness quiz on a random selection of staff. The quiz was designed to probe employees' awareness of current threats and the rationale for security controls. Most employees fared well in the quiz, but it was apparent that the highest performers worked in organisations that had some form of security awareness programme.

Security awareness is a simple but powerful weapon in an organisation's armoury against cyber-threats, data leakage, fraud and a range of other offences. It is widely established that human error is

to blame for the majority of security breaches. Conversely, when people are well-informed and understand the key concepts of data security, there tend to be fewer incidents and those that do occur are more quickly spotted and contained.

Security awareness activities should therefore take place in all organisations. Ideally these should draw on a broad range of communication methods, including external presentations, computer-based training, bulletins and reminders.

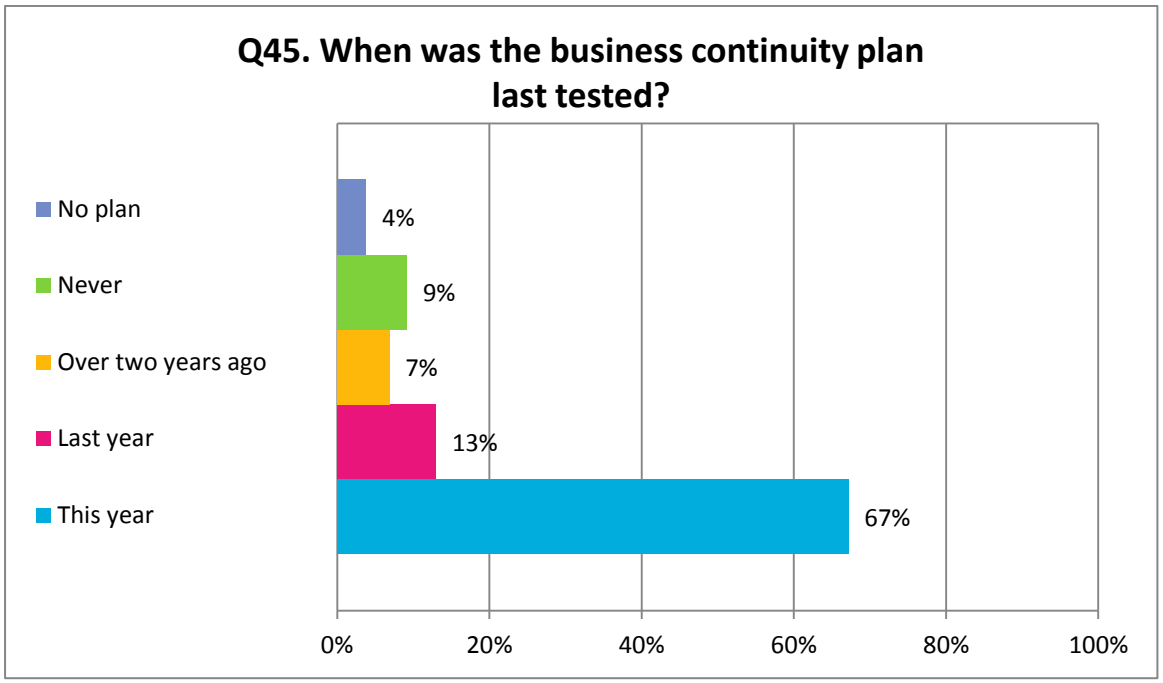
5.6. Business Continuity

Contingency planning is one aspect of data security that is widely understood, and has been practiced by most organisations for many years. The topic is covered specifically in the Code of Corporate Governance (5.4 Contingency planning and testing), which states:

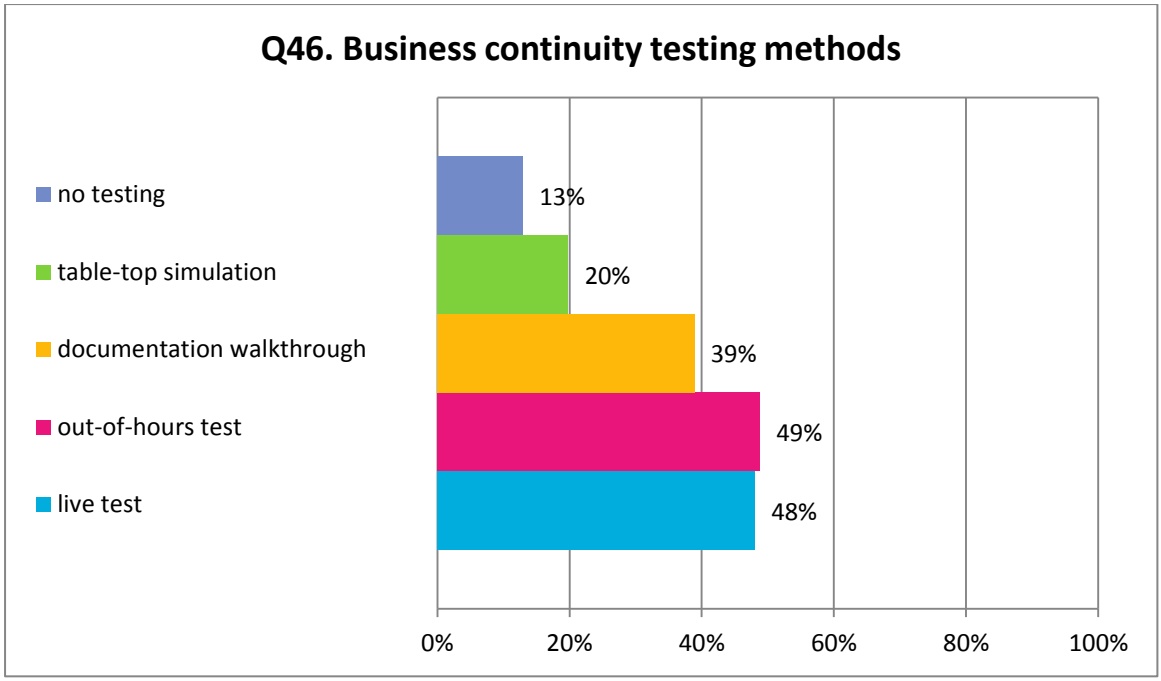
Companies should have in place properly constructed business continuity and contingency plans to safeguard against disruption of their operations and services and to mitigate risk. The Board should review these plans at least annually.

5.6.1. Testing

Considering the requirement for annual review, we asked licensees how often their plan was tested.



This is very encouraging with 67% tested within the last twelve months. Looking more closely at the methods used for testing the plan there were a range of effective approaches. The most popular were live and out-of-hours test, which is very positive since these are certainly the most realistic and effective ways to prove the plan is adequate. However, this does not mean that other approaches should not be considered. Table-top exercises, for example, use role-play scenarios to simulate a realistic disaster. These drills are highly effective in building crisis management skills, can even teach senior management how to collaborate and solve problems together. Rather like security awareness, the skills gained can be used to respond to and manage new and unfamiliar situations.



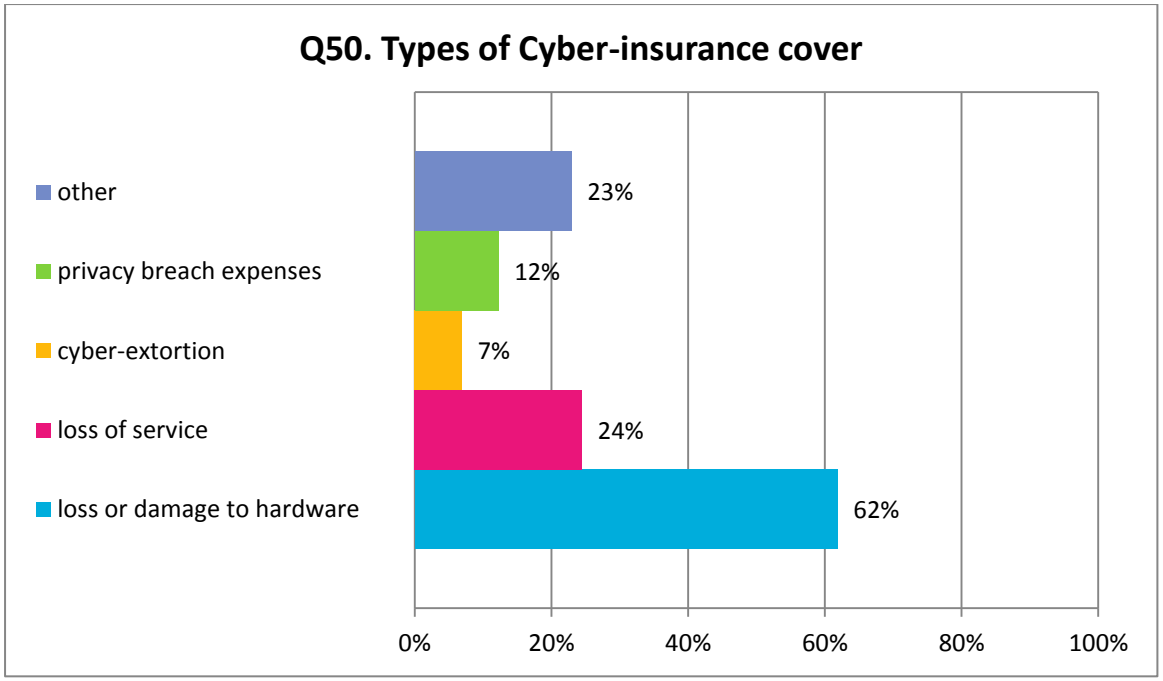
However, as a continuation of the business continuity topic, we asked whether licensees had drawn up a list of potential business interruptions and assessed their likely impact (Q47). Less than half replied that they had a 'business impact analysis' or BIA. This lack of consideration of the actual business risks suggests that for many businesses the BCP is nothing more than a simple disaster recovery plan. The BIA is important because it focusses on core processes and services, and aligns the recovery plan to those most critical to the business. Skipping the risk assessment and jumping straight to recovery arrangements creates the possibility that recovery arrangements may not be appropriate or adequate for the most likely threats. For example, a disaster recovery site might be maintained at great expense, when a secure remote desktop solution might offer more flexibility and better value.

This type of misalignment is even more likely if testing is not performed regularly.

A further concern was the reliance of most businesses on the BCP for responding to security incidents. 49% believed that key areas of crisis management were covered in the BCP. With the specialised and complex nature of security incidents, we feel this is an unreasonable assumption, and that specific security incident response plan should be given serious consideration.

5.6.2. Cyber-Insurance

Over the last few years there has been a considerable amount of interest in the topic of cyber insurance. This is a specialist type of insurance that covers a wide range of data security risks. We asked respondents to list the different types of cyber-insurance cover that they had.



The results show that the most common insured risk was hardware loss or damage (62%), which is effectively what contents insurance will provide. However, some organisations did have specialist cover, with loss of service (24%) and privacy breach expenses (12%) and "computer crime insurance" as notable examples. Several had business interruption insurance which covered hardware loss and increased costs of working. Also, a number of respondents who did not currently have cyber insurance also commented that they were actively considering it.

There is no doubt that dealing with and recovering from security breaches can be extremely costly and disruptive. Insurance is one way of limiting an organisation's exposure to the financial effects of a breach. However, insurance alone is not the answer, as licensees still need to demonstrate that they have adequate preventative controls in place. Furthermore, some risks such as reputational damage may be impossible to insure against.

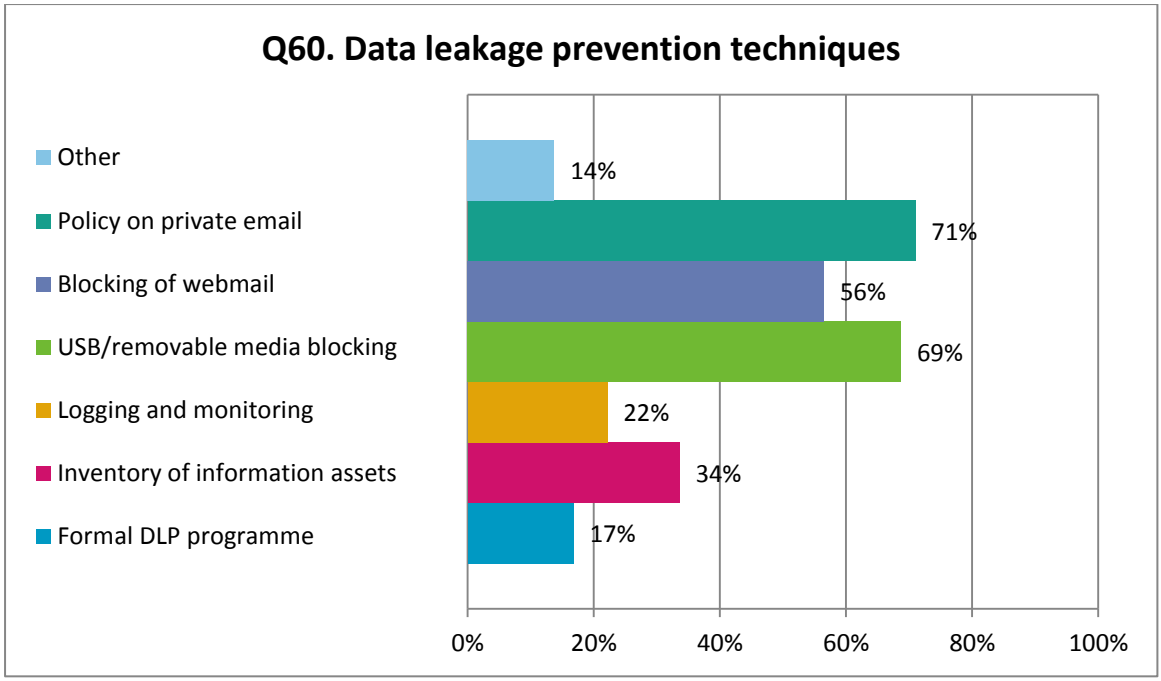
5.7. Remote Access

(Q54)The majority of businesses (87%) offered a remote access facility to their staff. However, only half of these utilised two-factor authentication. 'Two-factor' means the user's identity is verified using two completely independent sources - such as something you know (password, PIN), something you have (token, digital certificate), or something you are (iris, fingerprint, face). The most common combination of these is a password and security token, widely used in online banking services. Without this secondary validation, online services can be compromised using a range of hacking attacks such as brute-force password guessing, keyboard logging, or network eavesdropping. To be clear, a combination of password and a secondary PIN or secret word is not considered two-factor, as both codes are something the user knows. Both can be discovered at the same time and reused by an attacker.

Two-factor authentication has been established for many years as a minimum level of logon security for remote access to sensitive corporate information, and is something that all licensees should strongly consider implementing if they have not done so already.

5.8. Data Leakage Prevention

Perhaps one of the most widely reported security issues is data leakage. This is the accidental or deliberate disclosure or theft of confidential information. We know from the experience of others that this is not something exaggerated by the media; information that has value to your organisation also has value to someone else and therefore needs to be carefully protected. With this in mind we asked respondents to say which common prevention techniques they had in place.



Most respondents offered other approaches in addition to those above, for example:

- Ban on social media
- Control over shredding
- Authenticating telephone callers
- Role-based access, need-to-know access policy
- Outgoing emails are checked by a second individual
- Network port security
- Email content scanning
- Daily access log checks
- Separate terminals for internet access
- Referring to clients by codenames

Overall the response to the question was very positive and it was clear that most organisations understood the key point: that data leakage prevention is not one solution, but is a whole range of procedural, technical and personnel controls. Having a wide range of complementary controls or 'security layers' avoids over-reliance on a single point of failure.

5.8.1. Secure Disposal

To understand what happens to data when it is no longer required, we asked licensees what methods they used to dispose of electronic media and printed material.

The majority of respondents used physical destruction for media such as hard disks as well as paper records. It was also encouraging to see that many licensees were also aware of the risk associated with modern photocopiers or so-called 'multi-function devices'. Many commented that physical destruction or secure erasure of the copier's hard-disk is preferred. This is the best approach, because the hard disk may still contain electronic remnants of processed documents which can be recovered using data recovery tools.

Not surprisingly, the majority licensees relied upon third-party specialists to collect and destroy the material on their behalf. This raises the question of what happens to the data once it leaves the premises? Only a small number of licensees told us that hard disk destruction was certificated. This means that the specialist adheres to contractually agreed standards, and then issues a formal record of what items have been destroyed. Several licensees witnessed the destruction of paper or electronic

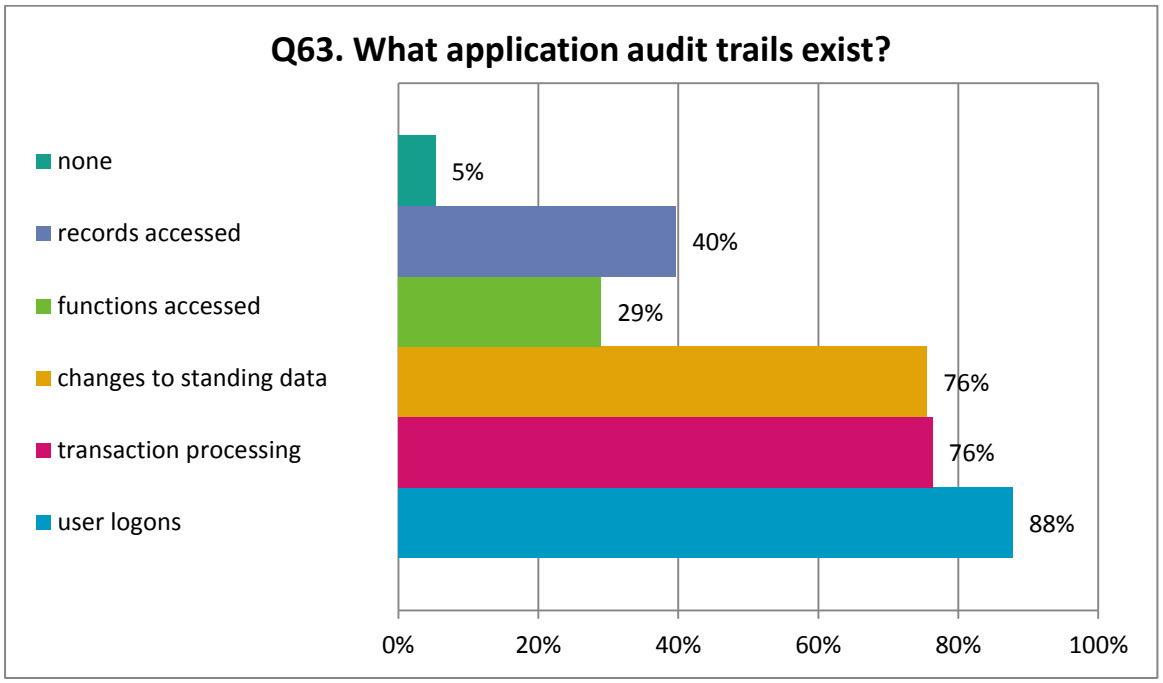
media. In common with our earlier points around contracts and due diligence (5.3), these are excellent examples of the assurance activities that we would hope to see in all organisations. Particularly where destruction is certificated, it is only reasonable to expect formal assurance from the service provider that certain standards have been met, and for the customer to validate the process from time to time.

5.9. Logging and monitoring

In this section we examined licensee's capability to detect, and investigate security incidents.

5.9.1. Audit Trails

We asked licensees what audit logs were available to support an investigation.



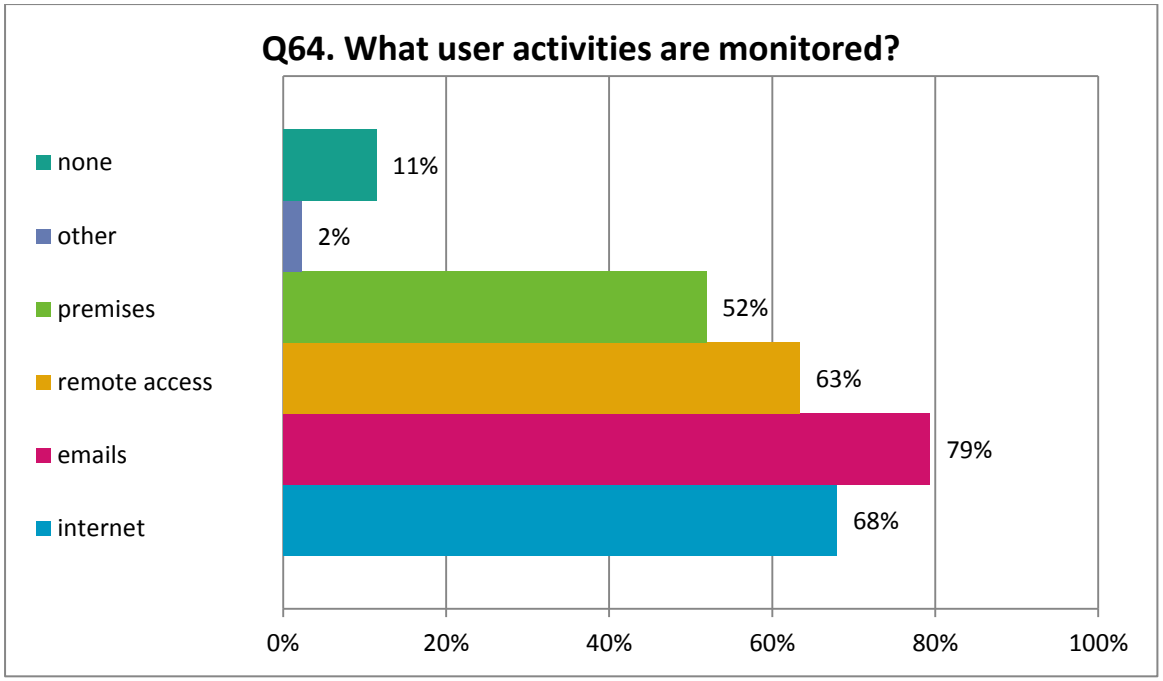
Overall the results were positive, but there is a clear bias towards auditing data entry functions (transactions and standing data update), rather than the accessing of data. This could be explained by a traditional focus on fraud and financial misstatement. However, modern systems need to be capable of supporting investigations of a much wider range of incidents, with data theft one of the most common.

Onsite reviews also showed that senior management often had poor awareness of audit trail features and were unclear about what was in place. This is dangerous as any deficiency in system logs and audit trails is unlikely to remain undiscovered information is needed for an investigation, by which time it is too late. We would therefore encourage licensees to engage with their IT departments or software suppliers and ensure that all activities are recorded. Some of the main areas to consider are:

- Which functions are logged (including failed attempts)?
- Who performed the action?
- Where did it occur (i.e. which workstation)?
- When did the event take place?

5.9.2. User Activity Monitoring

Looking more widely at IT systems in general, we asked licensees what IT system activities are monitored:



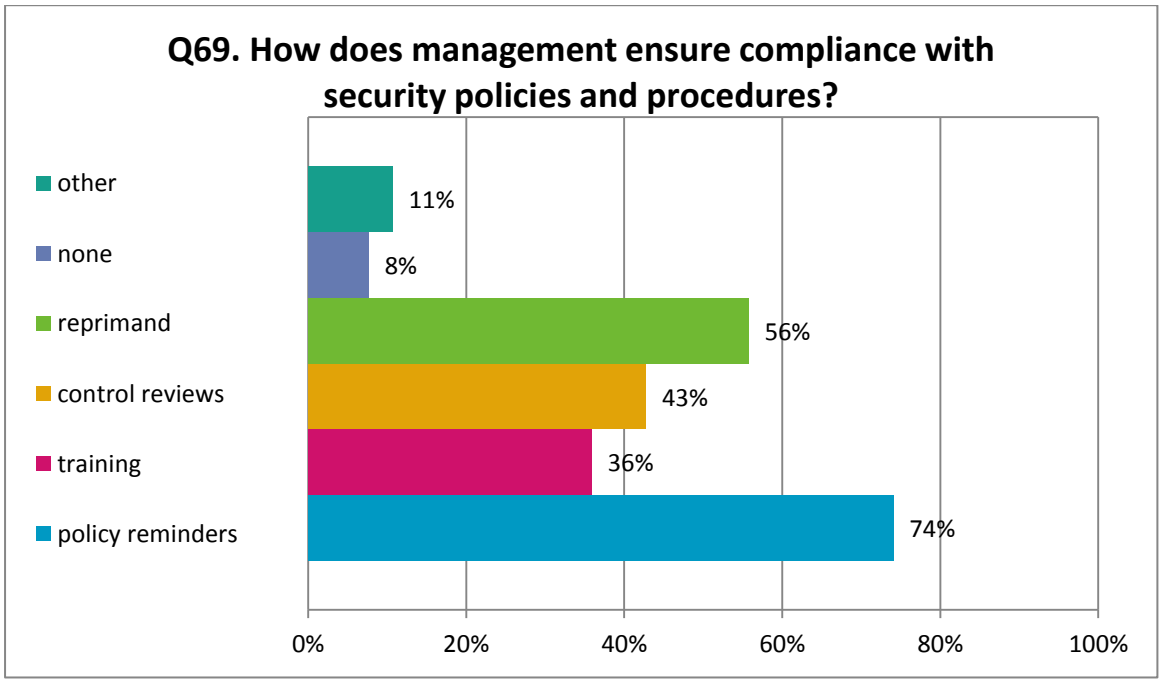
In most cases monitoring was reactive, whereby activity logs would only be reviewed if there was a specific requirement. Others performed increased monitoring where there was an increase in risk. For example, one licensee monitored staff on notice more closely, to mitigate the risk of data theft. Some organisations performed random spot checks, and one owner-managed business even reviewed staff emails as a matter of course.

The diverse responses to this question imply that monitoring is driven by the business rather than IT, making it difficult to arrive at a single view of best-practice. However, there are several key elements to consider for monitoring to be effective:

- Reactive monitoring requires the least effort, but it is essential that the relevant audit trails are actually being recorded. In several of our onsite visits licensees took a reactive approach, but had never checked that the expected audit trails were actually being maintained.
- There must be a formal policy that clearly explains what is acceptable use, and what rights to privacy users have when using company systems. Otherwise users may plead ignorance, or claim they have been treated unfairly

5.10. Compliance and Audit

5.10.1. Policy Compliance



In the next question we examined licensees' broader approach to promoting and enforcing security policies. The majority (74%) issued policy reminders, which we would have expected all licensees to answer positively to. It was also surprising that the second most popular method of ensuring compliance as through reprimand for policy violation (56%); this is not ideal as it requires an incident to have already occurred. Proactive activities like control reviews and staff training were less popular.

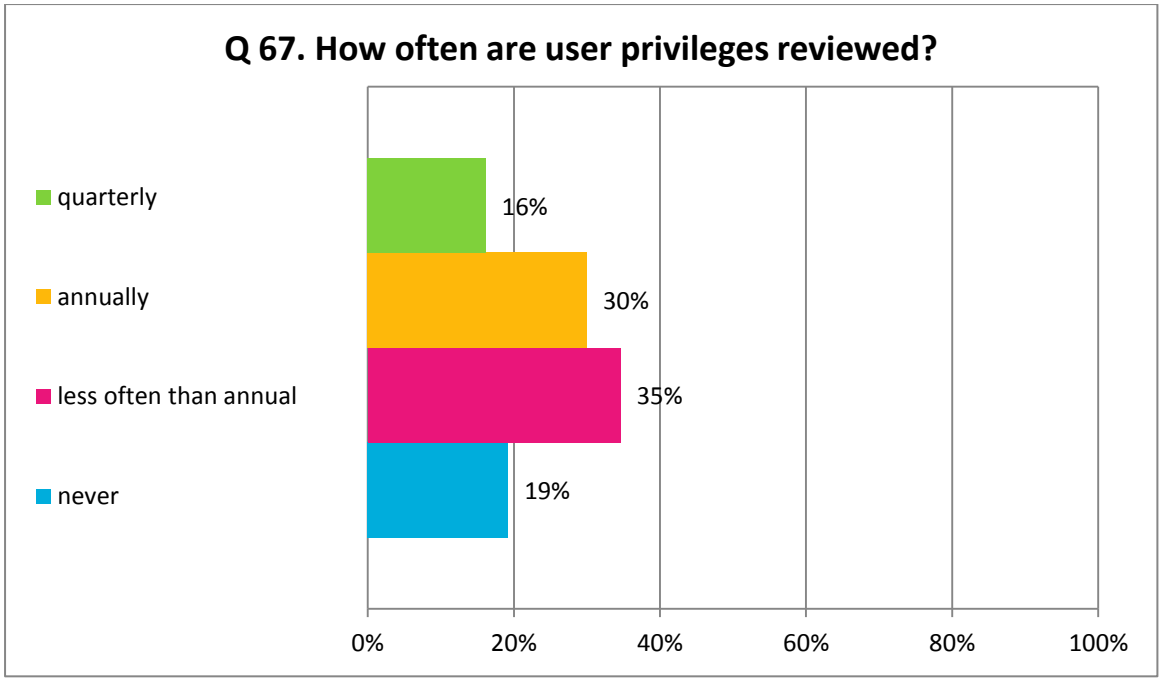
Taken as a whole, the ranking of these results is of concern, as it appears that many organisations see policy enforcement as a predominantly passive activity. This view is supported by 5.5 - Security Awareness, where the onus was largely on staff to educate themselves. Senior management need to be far more proactive in making sure that staff actually understand and adhere to corporate policies. This requires some form of education, supported by reviews and audits to ensure compliance.

It is possible to combine education with policy dissemination, and we found several licensees are now using policy compliance software to good effect. Software offers several advantages over more manual methods, for example:

- Convenient distribution of policies to staff
- Automatic tracking of policy acceptance
- Built-in training modules and comprehension tests

5.10.2. Reviews of Controls

Following on from the above general question on compliance, we then looked more closely at the control assessment activities that licensees performed.



The frequency of user rights reviews was somewhat disappointing, with less than half undertaking a review annually or more often. Naturally the frequency of review is dependent on the size of the organisation and staff turnover rate. However, we would expect that most organisations would benefit from at least an annual review. Periodic reviews are important for detecting and correcting mismatches between users' actual and required levels of access. These reviews are also an important control over dormant accounts, ensuring that leaver accounts are removed from the system in a timely manner.

For more formal security reviews the majority of respondents (69%) relied on external auditors to assess data security. We feel this is an unrealistic expectation and may offer a false sense of security. Whilst there may be great value in any findings that the auditors do report on, licensees must remember that auditors do not always review IT controls, and instead may elect for a substantive audit. A 'no news is good news' result should be treated with great caution. Secondly, even if IT controls are tested, the auditors' scope will be limited to only those financial systems and processes that are material to the audit. Finally, any work the auditors perform is selective and driven by their own audit risk, not the licensee. If licensees intend taking any assurance from an external audit, then we would encourage them to discuss their expectations and the audit scope with the auditors first.

Turning to the other assurance methods, we were encouraged that a quarter of licensees had reviews performed by internal audit. Although less common, internal peer- and manager-led reviews should not be discounted. Providing these follow an agreed methodology and proper reporting of results, these types of review can complement more formal forms of assurance, and provide the participants with a greater awareness and insight into risk and control.

5.10.3. Risk Assessments

Our final compliance question asked licensees how data security risk assessments are performed. We were disappointed to find that just over a half (54%) reviewed data security risks annually and fewer (35%) maintained a risk matrix.

The subject of risk is covered in detail in section 5 of the Commission's Code of Corporate Governance, which states:

5.3 Risk reviews

The Board should undertake, at least annually, a review of the effectiveness of the company's risk management, and related policies, procedures and controls.

In our onsite visits we found that risk assessments often identified data security as a specific risk but failed to go into any further detail. This approach makes it hard to know what level of security is needed in different areas of the business. This often results in a patchy control environment, with over attention to obvious and easily understood areas at the expense of others. A better approach is to broadly assess risks and then address the weakest areas.

5.11. Respondent Feedback

In the penultimate question we asked respondents whether they had been made more aware of the issues associated with data security; 82% replied "yes".

In the final question we asked licensees what, if anything, they would consider changing in their organisation following this questionnaire. There were many encouraging responses and below are some responses given:

- "The Company will implement an annual control review on data security and develop a Data Protection policy tailored to the Company's needs."
- "Implementation of additional Data Leakage Prevention measures."
- "Whilst we have always instilled a culture of data security throughout the office we realise that there are procedures which may require updating or formalising. We feel that the practice is in place but that the evidence may not always be so. We will now formalise and document data security procedures to a greater extent than hereto forth."
- "We would consider reviewing third party contracts with regards to data security."
- "Consider external testing of security."
- "Consideration will be given to including data security as a standing item for future board agendas."
- "To start regular formalised security training for all staff."
- "We are grateful to the Commission for highlighting aspects of Data Security which had not previously been considered. We will be implementing a full review based around the questionnaire."

6. Acknowledgements

The Commission would like to thank the fiduciary licensees for completing the questionnaire. Particular thanks should also go to those licensees that agreed to have site visits. The time and effort they spent in supplying the requested documentation and discussing their approach to data security was much appreciated and yielded some excellent evidence of good practice.

The Commission was supported by Submarine Limited for their design and user assistance of the online questionnaire tool used within this process.