GOV NEWS DIRECT

Public Sector Data & Information Security Survey

In partnership with: 8MAN

GOV NEWS DIRECT

Contents

Summary

To allow staff to benchmark their organisation against the broader public sector and specifically to determine:

- **The procedures used to achieve data security within the public sector**
- **Ease of on-boarding/off-boarding staff to ensure only authorised access to data**
- **Access monitoring and report protocols**
- **Scope for improvement in data security**
- **To what extent Data Owners and IT managers are responsible and able to make changes to access levels at what rapidity**

Whilst no questions specifically relate to the new EU legislation, the General Data Protection Regulation (GDPR), this reform needs to be the focus for all Data Protection Managers and Data-Owners. This is part of Article 8 of the European Convention on Human Rights. It sets out to effectively modernise data protection rules, across the 28 member countries of the EU, to remain up-to-date with the digital age.

This General Data Protection Regulation will strengthen the rights of all EU citizens to ensure that their data is properly secured and not subject to loss, illegal use or transfer to third parties. It will replace individual data protection acts across the entire EU, a simplification long overdue. It will create many challenges and its enactment may well come as surprise to many Data Owners and Practitioners.

The scale of the fines being considered, for the most serious cases of data breach or mismanagement, are so significant that it will change data protection from being an IT issue to also becoming a concern for Directors. Although the fines may be substantial, they will be minor compared to the loss of business reputation.

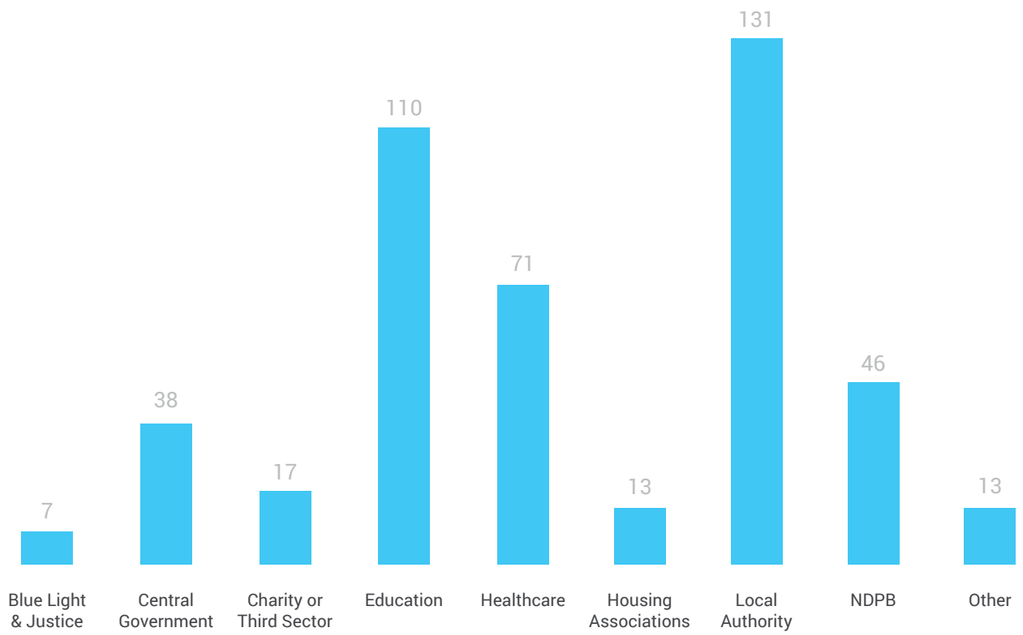
All organisations, especially those in public sector, will need to carefully evaluate how they collect, store and manage data. Protecting personal data is important from an ethical standpoint and will now have increased force of law with punitive penalties.

Despite the challenges, all change creates opportunities. Where the public sector chooses to store data in the cloud, the rules and practice across Europe should be consistent, which will lead to greater effectiveness and lower costs. These changes should certainly increase the trust that citizens have in public services, especially those online services.

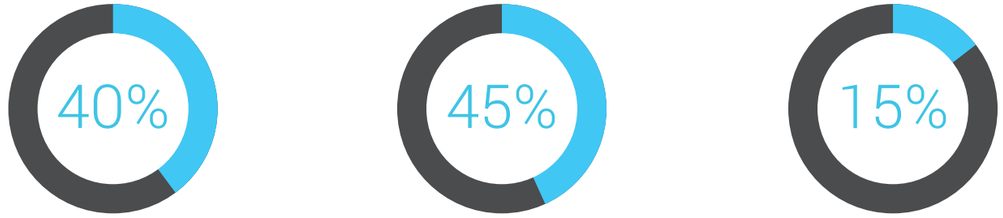
It is clear from the results of this survey that there is a historical attitude that data security is the sole responsibility of the IT department. Whilst most Data Owners take full accountability, the support that they have from monitoring systems and alerts is limited. Greater training and transparency on where data protection responsibilities lie is imperative.

Key Points and Statistics

- A Data Owner is someone that can authorise or deny access to certain data, and is responsible for its accuracy, integrity and timeliness. Over 80% of those who responded claimed to be a Data Owner
- 602 people responded to our survey across the entire public sector, with a significant response from Local Authorities, Healthcare & Education
- Over 20% of respondents had either ‘information’ or ‘IT’ in their job title
- 19% of Data Owners didn’t know how many other Data Owners there were within their organisation
- 28% of those who responded were Director or ‘C-suite’ level
- 65% of those surveyed had serious concerns regarding data security within their organisation
- 42% believed there were more than 10 other Data Owners in their organisation



How many staff are in your organisation?

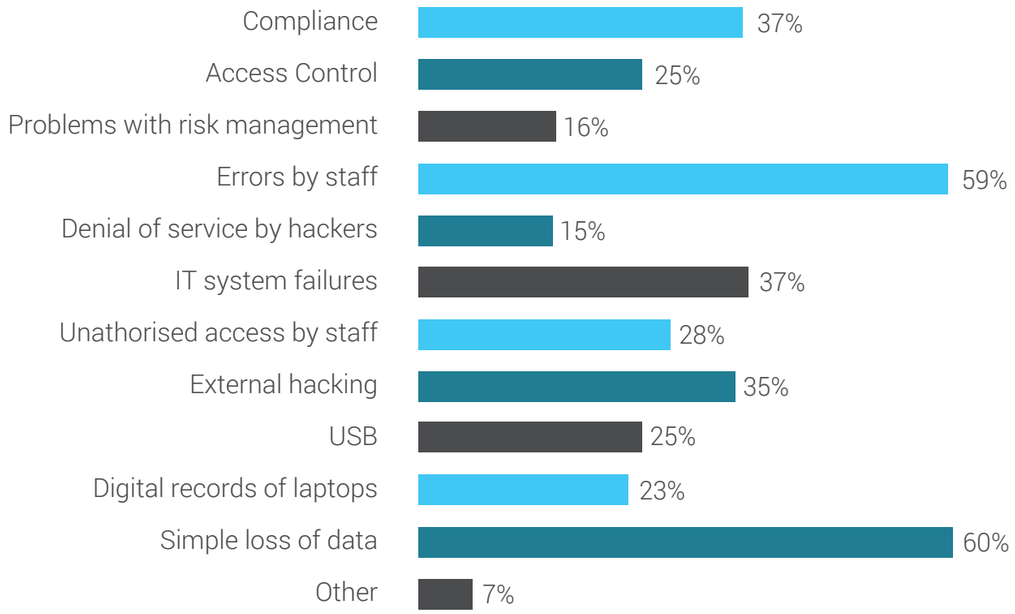


Are you a data owner and/or responsible for its accuracy, integrity and timeliness?

How many other data owners are there in your organisation?

Have you any serious concerns regarding data security in your organisation?

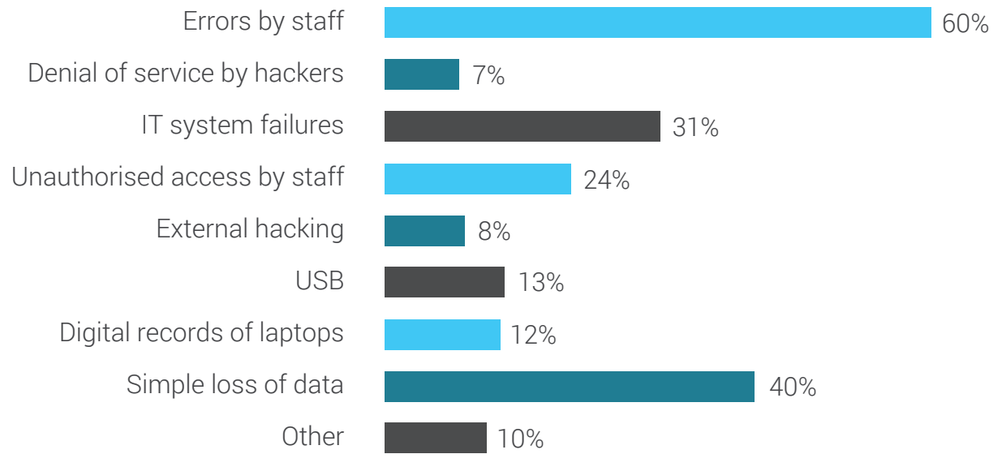
What are your biggest concerns surrounding data protection? (multiple choice)



Notable comments left in 'Other'

- "IT Operating costs are a constant concern"
- "Lack of staff training is leading to chaos"
- "Third party contractors processing data on our behalf"
- "We suffer from people not following simple procedures"
- "Cloud security"
- "Theft of laptops"

Has your organisation experienced any of these data security lapses?



Notable comments left in 'Other'

- "Breach of confidentiality by others outside the organisation"
- "Loss of our data by external contractors/couriers"
- "Loss and exposure of print out material"
- "Virus introduced to servers from an external source"
- "Internal hacking, watching staff input passwords"

Would you like to improve your data security?

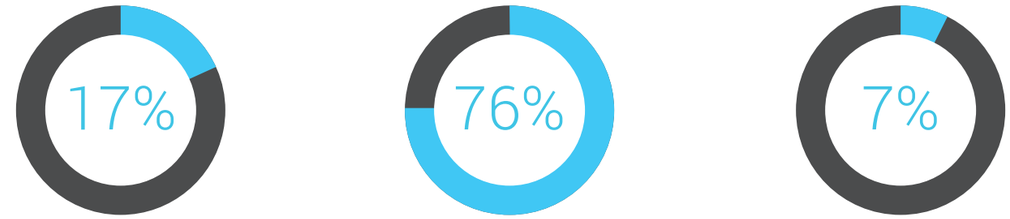
Would you like to improve your data security? (comments)

- "Acceptance of procedures and responsibilities"
- "Always looking for new ways to improve, everyone needs to be aware of new risks and evolving threats"
- "Staff complacency is making us vulnerable"
- "Need to raise the understanding and importance of good information governance across the organisation and buy-in from all managers"
- "To design and implement a coherenet information management/security regime"
- "Most Public Sector organisations move out data externally - We have a great deal of concerns regarding access"
- "Access to systems are always changing therefore there is always room for improvement"

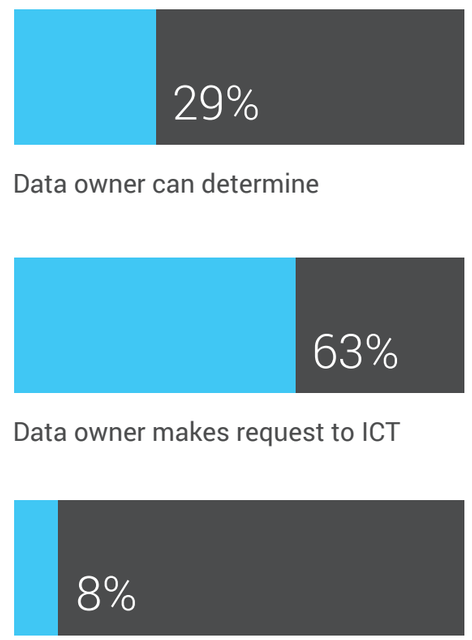
Are you able to allow Data Owners to manage their own data access/needs?

- "Data Owners are supported in the management of their data access needs."
- "Data Owners determine who has what level of access but rarely do so and often delegate to IT."
- "Laws and government regulations are to complex and are only properly understood by IG specialists."
- "Data Owners can take overall responsibility, however they need to work with the IM team to ensure the right controls and safeguards are identified/implemented."
- "Within the confines of policy and access controls, we tend to control data access within each department."
- "We are not consistent across the organisation, teams 'own' the responsibility for software and data access within their departments."
- "Only to some extent we need to build more awareness, provide more training and tackle the financial constraints we are faced with."
- "We are often hindered by legacy infrastructure."

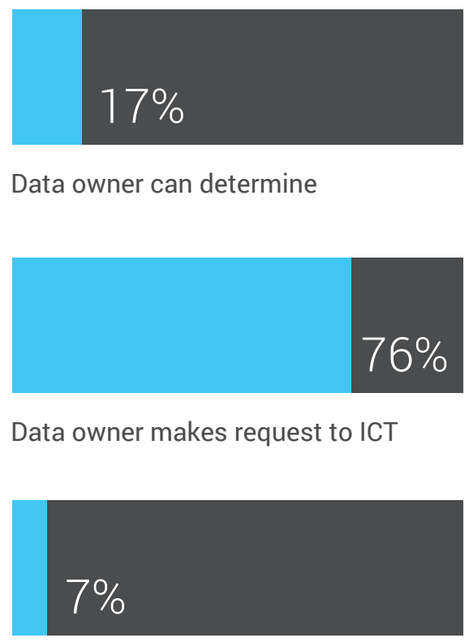
How do you manage the temporary access of a user to data/drives?



What is your current procedure to determine who has access to their data and at what security levels?



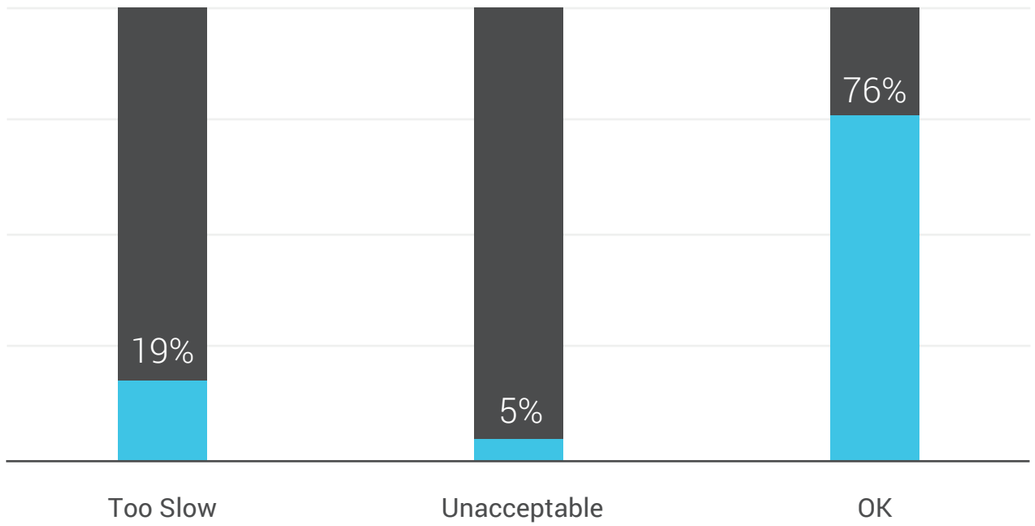
How do you deal with onboarding/ offboarding and changing new user's accounts?



How do you deal with onboarding/offboarding & changing new user's accounts?

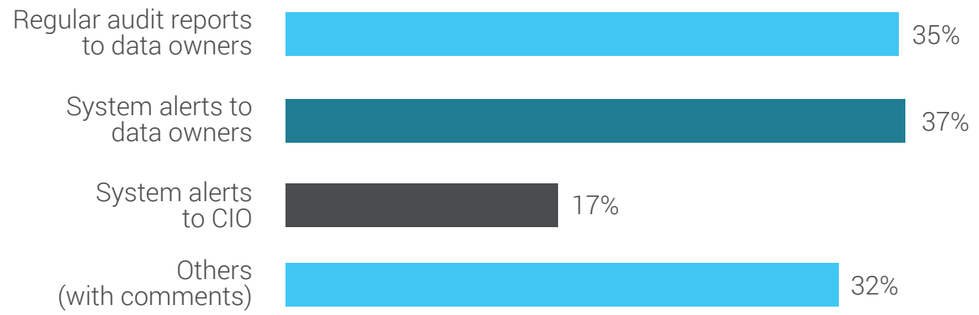
- "As we have a split between user access controls and ICT, requests can take moments or it can take weeks."
- "Automation and workflow tools are improving the situation."
- "Times vary a lot depending on the processes. Stopping access tends to be quick, changing access for existing is really slow."

Is the process & time it takes to onboard/offboard/change access:



- "It is the HR/Legal elements that take time here, not the IT elements."
- "Most of this process is automated. Waiting for the Data Owners response is the longest part."
- "One person not following procedure often presents problems."
- "We are always being asked to make things more secure. This should be paid for by Central Government."
- "There is a difference between network drive access and application access - ICT facilitate the former, Data Owners the latter."

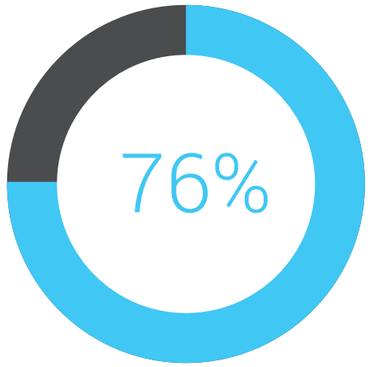
What does your monitoring of all onboard/offboard actions across the organisation include? (multiple choice)



Notable comments left in 'Other'

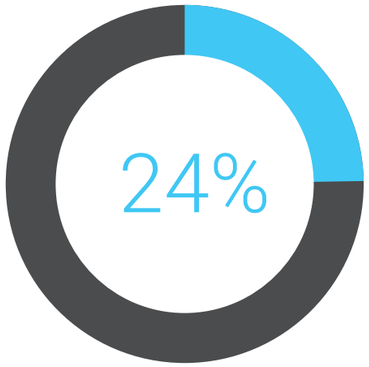
- "Internal audits are conducted but are not regular"
- "Lack of intergrated technology places responsibility with line management to request open/close of user accounts and IT audit requests."
- "We have no consistent or centralised reporting system, it is all ad-hoc."
- "Not all systems provide adequate audit reports, especially our older systems."
- "We only review systems and processes after events/incidents."
- "We trust the process works but need to introduce reviews. Our systems are very basic, the picture is always fragmented and Data Owners do not always recieve alerts, despite

Do you have a process of dealing with employees' access when they move roles within the organisation?



Yes

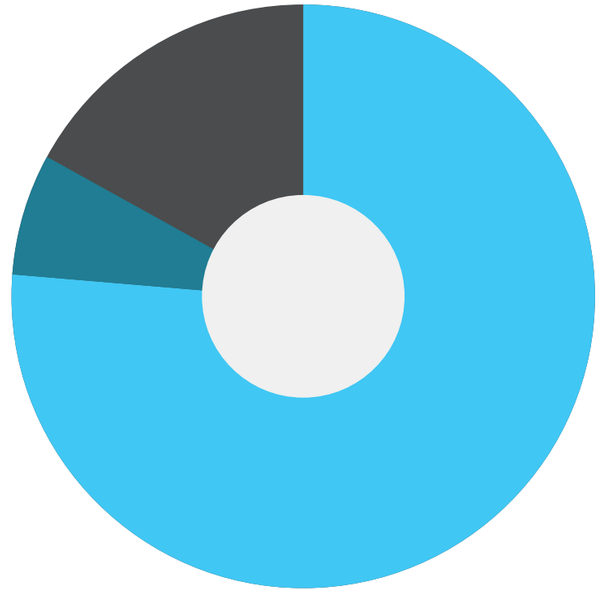
- "Access and permissions is related to the role. When someone moves their access is automatically revoked (via line managers, HR and ICT) and they have to submit a new access request."
- "New/Additional access is often provided quickly but old access is rarely removed."
- "Data Owners and managers should always notify IT - this is not always the case."
- "Admin staff are too often slow to react and don't always change/ remove permissions."



No

- "Manual and prone to errors - Old access rights can often be left as our processes are not ridgedly followed."
- "We have a system in place for managers to change data access appropriately, however this isn't always rigorously applied."
- "We have 'change in role' forms that need completing by managers. However this are often then processed by outsourced HR/IT departments."

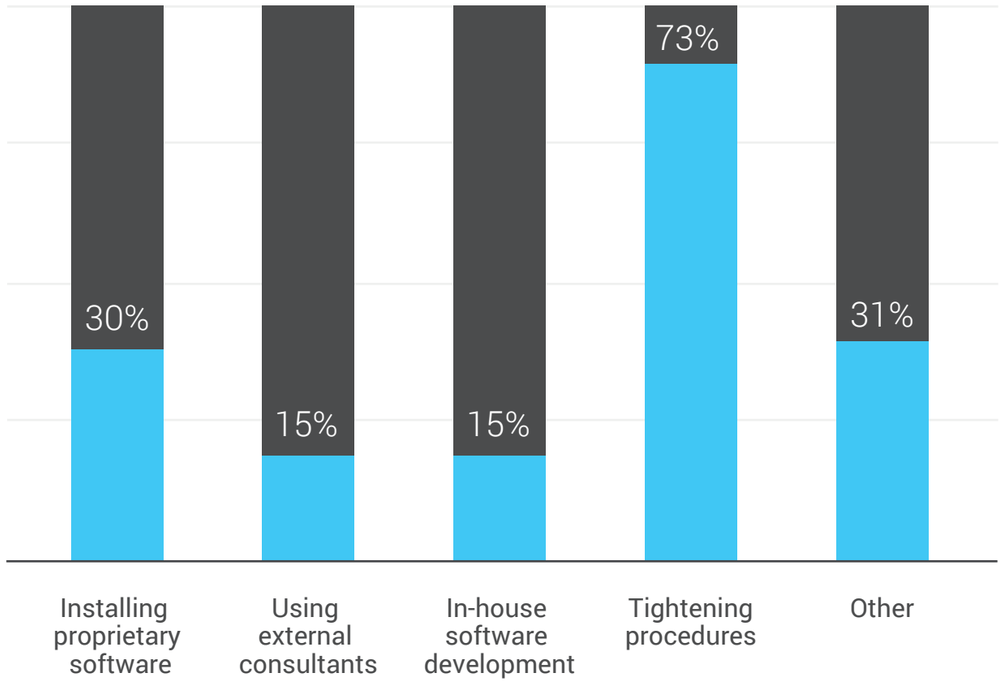
Is the time you spend on compliance-related activity:



- "Should be excessive if it was to be managed more."
- "Excessive at certain points when government compliance regulations change."
- "Insufficient due to poor and cumbersome processes."
- "It may seem to be an excessive amount, but I push for this in relation to the organisational risk."
- "Compliance can be very time consuming as more and more externals (with statutory powers) off load tasks to people further down the food chain."
- "Currently awaiting new software to help with the permission and monitoring of approvals/change controls to make auditing more automatic and less time consuming."
- "Tends to come in bursts, probably insufficient. Training and assessment is paramount."
- "We would like to spend more time but resources are limited. It is only when requested we produce an audit report and only when staff change that I must do something on data security compliance."
- "Not enough time on compliance by IT and DP staff."

How are you planning to improve data security? (multiple choice)

- "Awareness Campaigns, review of training modules and refreshers, data protection workshops and robust processes."
- "Increasing the number of data sharing agreements and reviewing these annually."
- "Making senior managers responsible for breaches in there own teams whilst talking regularly to staff about security and highlighting senarios that have gone wrong in other organisations."
- "Penetration testing more regularly and raising awareness with senior management."
- "Looking to move as much non-sensitive data onto alternative storage, locally or in the cloud to physically separate it from sensitive data. Looking to update and improve devices to lessen the risk."
- "IT Healthchecks and raising awareness through advanced training for management."
- "IT security programmes including the implementation of new security products, awareness raising, training and tightening of procedures."



"Lack of staff training is leading to chaos"

How do you ensure that access to resources are revoked when necessary?

- "Automatic Processes: from date of staff departure - which is entered by HR and then dealt with by ICT. Line management also included on the process."
- "Access to systems, databases and other resources are managed centrally by ICT/HR/Tech Support. We have separate leaving & moving processes which makes things easier."
- "Operational manager can oversee return of physical resources such as keys, laptops etc. Data Owner(s) remove privileges but this isn't a defined procedure. ICT notified to remove system access, usually by payroll."
- "Company wide defined procedures relating to staff moves or departures governing removal of rights or disabling and then removal of account."
- "Paper-based & electronic form has to be completed by line manager"
- "Good internal communication - HR/IG/ICT/Department Head all involved - Permissions & Access check list procedure is paramount - not always the case for special project management with temporary access."
- "Manual activity to revoke permissions, some automated processes for revoking access to newer systems - the latter will be more the case now."
- "No checks built into the system, entirely down to individuals (Data Owners)."
- "Personnel inform ICT of a change and access is revoked as required. No checking that process is followed."
- "Revoking access is dealt with very poorly. We seem to concentrate on allocating access."
- "There are no defined processes, we are looking to do this, but currently it is a manual process driven by line managers."
- "The change is captured within payroll and kicks off a (mostly) automated process. Additionally, any account that has not been used for a specified period is automatically suspended."
- "Those who need temporary access pose the biggest concern and often forgotten about."

Which systems or policies do you have in place to prevent internal security threats?

- "A range of systems, policies, procedures aligned with our ISO27001 certification and assurance regimes."
- "Effective on-line Information Governance training and application - Asset register in place - Access system to offices reduces risk of unauthorised staff gaining access to back office."
- "1. background checks on recruitment. 2 data protection officer talks personally to all new starters about the importance of data protection and what's required of them, 3. restricting access to electronic records, 4. monitoring of access to all electronic records, 5.encouraging staff to report any suspicions in confidence, and 6. taking incidents very seriously in the rare occasion that someone does something inappropriate."
- "Acceptable Use Policy - Information Handling Policy - Mobile Device Policy - Physical and Environmental Security Policy - Code of Conduct - IT systems monitoring."
- "Data protection policy and e-training is crucial."
- "We have a strategy, policy and guidelines as well as DPA and info management training at induction and beyond."
- "We need to do more - technical controls are hampered by legacy infrastructure."
- "There are a range of policies encompassing information security, encryption, movement of paper records etc. There are account and password controls, authorised access controls, monitoring and training. I know this is not the case for other PS organisations who we share services with."
- "Robust IT security policy, segregation of duties, centralised access controls managed by IT. Processes managed by workflow where possible."
- "Not Sure - perhaps we have nothing specific. Standard checking procedures at best."
- "Internal system audits record all users who access data. All users have unique individual passwords that they are forbidden from sharing. Hours of access are restricted to prevent out of office hours roaming."
- "Information security policies and ISO 27001 accreditation. We also have an annual penetration test and disaster recovery exercises."

What steps do you take to ensure sensitive records are secure and subject to restricted access?

- "a) effective software controls in place on all applications to prevent unauthorised downloading or printing b) Most USB ports disabled by default."
- "Access to sensitive data / records defines with only approved staff having access. Procedures in place with regular training of staff to enforce proper operations. Privileged staff have enhanced monitoring with approval process governing permissions with confirmation / verification of actions taken."
- "Compliance with Data Protection Act, Password security protocols & Firewall."
- "Compliance with IG toolkit, audit and Data management system operates in ' segments' that are only visible to those with the right permissions in place."
- "Document control policy. Access to records policy. Management sign off for access to sensitive areas."
- "Encryption of data in transit. Access should be on an as required/needed basis only."
- "Follow GOV policy/practices coupled to risk assessments. Ensure all software and access processes are fit for purpose."
- "Training, Further Training & More Training."
- "In House compliance and governance management plus external audit is a good start."
- " ISO27001 controls in place (e.g. EDRMS), limited access, encrypted data drives - regular checks on use."
- "Mandatory training and issuing of robust policies to all."
- "We have processes in place for assessing the risks associated with new data sets, e.g. Information Assurance Data Check Form, Privacy Impact Assessment (PIA). PIAs are used more widely across the business to assess sensitivity in relation to personal data. We have an Information Assurance Manager whose role is to work with IT, the business and IAOs to help raise awareness of sensitivity. This person deals with queries and offers guidance and advice to the business regarding levels of sensitivity and identifying and implementing the appropriate safeguards."
- "We use official markings and provide regular staff training on data security. This is also part of the mandatory induction process for new staff."
- "We don't do enough - Staff training is lacking and ICT policies/procedures are not well communicated after onboarding."

Data Owners and Department Heads need to play a greater role in helping to meet compliance measures concerning their employees. Please comment.

- "Absolutely agree. Busy managers often don't follow guidelines and policies to the letter, but we make the most of occasional breaches which potentially could have caused problems. Not quite name and shame, but details are shared."
- "Absolutely agree. we are currently totally reliant on Data owners and dept heads notifying us to effect change."
- "Agree, if they are the responsible party they must have absolute authority in order to ensure compliance requirements are met and to assist in raising the awareness bar accordingly."
- "Agree, we are in the process of setting up our Information Systems, with system owners, Information asset owners reporting to senior information risk owners"
- "Agreed, data owners and Department Heads have a more in depth understanding of the data that they hold, they need to be more engaged in managing the accuracy and quality of this data and develop closer links with IT to ensure it is properly secured and managed."
- "Agreed. Getting them to commit and support is difficult as they get squeezed in a number of ways, but is something that needs to be pursued."
- "As long as robust systems are in place and staff know their duty to follow procedures then there is no need for a greater role. Just a matter of being aware of requirements and meeting them."
- "Everyone within the organisation has a role to play in compliance measures. Regular staff training, regular audit/ review of compliance measures and robust policy and procedures are key to any organisation."
- "I would agree but I also think the organisation needs to ensure that such people have the appropriate training and it is a recognised responsibility within their job description. It is also important for organisation wide systems that responsibilities are clearly defined where they cross departments."
- "No - Government needs to own this responsibility!"
- "Of course. We need clear, appropriate and crucially proportionate compliance measures."
- "Not convinced that data owners and dept heads are aware of their obligations. user training required."
- "This is something we are addressing, we want data security to be part of our culture, we have allocation most department heads as an 'information asset owner' with a terms of reference to sign that expresses commitment to data security, although more work will need to be done."
- "Totally agree. Data Owners and Department Heads deem it to be an IT issue and regularly shirk their responsibility. No formal process in place to hold them account."

Data Owners and Department Heads need to play a greater role in helping to meet compliance measures concerning their employees. Please comment. (continued)

- "Yes. By giving the power to teams they tend to take on more responsibility. Our main issue is around individuals who feel their empolyees are so perfect they should have access to everything."
- "There will always be a need to check and ensure all staff are aware of their roles and responsibilities. This should be led by data owners and heads of departments but consistent messages and communication across the organization will help to reiterate this."
- "Not convinced that data owners and dept heads are aware of their obligations. user training required."
- "Yes. They need to take interest in their data, including checking/confirming who has access, even if it means having to ask ICT to list who can get to their data."
- "Definitely. If people in these roles do not support compliance measures, then their team won't either. It must come from the top down."

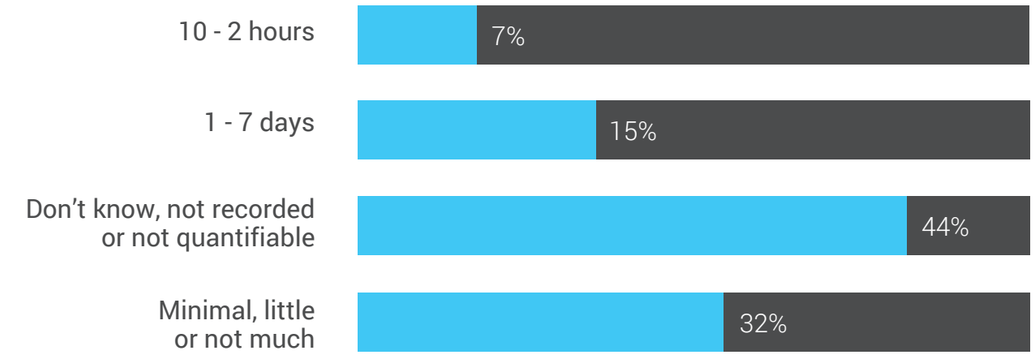
Which compliance standards are you most engaged with?

- "Public Security Networks and Information Assurance standards which replaced CoCo"
- "Client confidentiality issues and complex issues around access to records, brc etc"
- "Compliance with the Security Policy Framework, the 10 Steps to Cyber Security along with the Information Assurance Maturity Model are our main drivers. We also use information and guidance provided through government, e.g. CESG, CPNI, DSO support network, Cabinet Office and the National Archives (IACSEP). We are looking to review our IT systems this year against ISO 27001, 27002 and 27005 as an alternative to the RMADS process."
- "Data Protection Act"
- "Child safeguarding standards"
- "HSCIC Information Governance Toolkit"
- "NHS IG toolkit standards."
- "Information Governance Toolkit, SANS 20 Critical Controls"
- "ISO27001 PCIDSS We are PSN compliant but this isn't our main driver - it is however accommodated by our ISO27001 activities"
- "NO IDEA!"
- "We don't have any compliance at this stage but undergo a regular DP/IS audit"

Which specific aspects of compliance do you have the most difficult time completing?

- "All, but especially PSN. It is difficult to know exactly whether it applies.
- "Access Control measures"
- "At the moment is training/awareness, technology"
- "Audits and reviews of policies."
- "Changing people's attitude and method of doing something. If they now have to think about security they are reluctant to change their ways."
- "Data sharing agreements and documentation"
- "General awareness throughout the organisation and reinforcement. Engaging staff who do not feel that such matters relate to them."
- "Increasing number of incidents being reported. A factor in this is that we are increasing awareness of information security and the importance of early reporting."
- "Information governance, retention, disposial, third part suppliers, awareness, keeping up to date with requirements and ensuring we are following the current standards. Some of many priorities!"
- " ISO 27001 and getting staff engaged."
- "Maintaining an auditable trail of actions and approvals. Ensuring compliance and acceptable of responsibilities."
- "Most difficult is ensuring enough security is in place to enable the service to perform without being hindered by excessive security."
- "The self-assessment of our IT systems against ISO 27001, 27002 and 27005 will be the most difficult as previously we have got an external CLAS consultant in to carry out the RMADS. This year we will be taking a completely new approach and handling it all internally (will be reviewed by our external auditors)."
- "Time, money, staff and resource."
- "Understanding what information can be released, to who and by what methods. Others requesting information expect you to do this without question and to any destination they advise you."
- "When staff move from our organisation to another and deliberate attempts to gain access to restricted materials by others."
- "Determining information assets and owners."
- "Data flow mapping, keeping Service Users informed."

How much time do you spend on reporting and auditing sensitive resources per annum?



- "Audits vary each year on rotational basis or may have addition in response to concern."
- "Cannot quantify, as this is part of the remit for the IT Department within their daily responsibilities."
- "Can't say exactly but it's not excessive."
- "Currently we carry out internal audits on an agreed schedule. This could be three or four times a year and each check would be specific to one area."
- "Difficult to quantify, we do very little reporting to the management team but the IT team are effectively auditing access permissions every day as part of the day to day running of the dept."
- "Impossible to say as it is done by IAOs and varies according to the work area."
- "It is built into the Information Assurance Manager's role and we have not collected the time spent on sensitive resources specifically. Most of our information is classed as Official with only a relatively small amount marked at the Official-Sensitive level."
- "Minimal - We are looking to improve our reporting/monitoring capabilities."
- "Not Enough - I would go as far to say Negligible!"
- "This information is not captured, but the time devoted to this activity is substantial."
- "This is a function of our Information Security Manager which is a full time role within the organisation."

Conclusions

Security Concerns

Data loss and security breaches are a constant threat that organisations face. External threats can be dangerous but the threat they pose can often be overstated or exaggerated. 55% of all security breaches originate from someone with access already. Data loss can be malicious but more often than not, it is accidental or the result of human error.

The most effective way to deal with security breaches and data losses is to prevent them from happening via education access to information to a need-to-know basis. This is easier said than done as the tools and solutions available to IT departments are often limited.

By making your access rights to information transparent and structured, you can limit access to information to only the responsible employees. If employees can't access information, it cannot be lost or abused. A structured review of access rights via regular reporting will ensure that third party contractors and temporary staff have their rights revoked. These reports need to be formatted in a way in which non-technical staff can understand. This will give individuals the opportunity to protect their own data.

Once a transparent environment has been established, monitoring and reporting must take place to ensure problems do not reoccur. Of course, this all requires a solution that increases staff efficiency and frees up time. We have found that many organisations do audit their access rights from time to time but most have admitted that their internal processes are often lengthy and inconsistent. Speeding up the average time of an audit with structured reporting solutions creates audit-friendly environments and saves significant time and money.

Responsibilities & Accountabilities: Data Owners vs ICT

There is a fundamental flaw regarding access rights within a majority of organisations where the responsibilities fall between Data Owners and ICT. Since access rights are managed via Active Directory (AD), they are seen as entirely the realm of ICT staff who either process requests from Data Owners but more commonly are instructed to make changes only when employees join, move or leave an organisation.

This fundamental division of roles and responsibilities leads to users being overprovisioned as the knowledge of who should have access to a resource resides with the Data Owners and the technical knowledge to make changes resides with ICT staff.

- "We do not let people manage these themselves, as previous experience shows that they get things wrong and cause problems"
- "Only in terms of safeguarding and child protection records"
- "Only to some extent."
- "We need to build awareness and to do more training"
- "The trust has 200-300 systems and delegates authority to IAO and IAA"
- "Yes, but with the leadership from the SIRO, privacy officers and the Data Governance Advisor"

An additional hurdle is that it is frequently only a few individuals who are familiar with security compliance. Consequently, organisations suffer from a lack of opportunity to exchange information in a meaningful manner, making it challenging to determine access rights responsibilities.

- "Data Owners determine who has what level of access but rarely do systems provide the granularity or control for this to be delegated to Data Owners. Usually IT have to provide."
- "Laws and government regulations are too complex and are only properly understood by IG specialists."
- "We are reliant on notification from Data Owner so not always water tight."
- "At present there is no process, but we will be carrying out an urgent review and then putting in place regular review activity going forward."
- "Annual reviews of access rights."
- "Automatic Processes from date of departure which is entered by HR on date staff leaves."
- "IT are informed when someone leaves or stops working on a project where specific datasets are accessed."

Through simple and automated reports provided by ICT, Data Owners can easily review and provide feedback to the staff who have access to their information. Once the access rights environment has been clarified, organisations can take Data Owner integration a step forward by implementing workflows to make requests for changes. These changes can be approved by ICT Staff or Head of Security and the changes are than applied in a structured manner. All changes should be tracked and monitored so when problems occur, you can quickly identify the cause and implement policies to ensure it does not re-occur.

Conclusions

Monitoring and Compliance

Monitoring and Compliance are two topics that we have noticed that many organisations struggle with. The consequences for failing a compliance standard can come in the form of revocation of organisations from services provided by the public security network on in hefty fines.

Many organisations claim that they only carry out audits on an ad-hoc basis and are often driven by an approaching compliance check.

- "Reporting is generally ad-hoc in nature rather than a regular flow of reports."
- "There are system alerts in place which are received, handled and monitored by the Infrastructure Support team (based in the IM team). This team then liaises with Data Owners or line managers as appropriate."
- "Access is controlled by IT staff via auditable process with the initiator or approver being the Data Owner. Domain controls restrict access and log user actions in line with current security policies."
- "The Human Rights Act is quoted as a reason why information regarding individual access cannot be provided on a regular basis."
- "Regular reporting is to be implemented urgently."
- "Not sure what we monitor at all"

No centralized reporting mechanism, monitoring or alerting make each consecutive audit more difficult. Organisations that have a high number of temporary staff, 3rd party contractors and staff moving frequently generally face an uphill battle as access rights management is often handled in an organic and ad-hoc manner as opposed to a structured approach.

This is often caused by the lack of an efficient and easy manner of reporting. When reporting is done on a regular, structured and uniformed manner it not only prevents problems before they start but also speed up the future audit times significantly.

- "Not sure about this without checking with ICT."
- "We don't do an audit but if we are asked we have the information of who has requested what – onus on managers to ensure appropriate access."
- "We have no CIO. Data Owners do not receive alerts and there is no regular audit report to Data Owners. We have internal audit procedures that check the Data Owners are maintaining access controls, and we have reports that go to the ICT Service Desk when staff change, but not to Data Owners."

Internal Communication, Transparency and Training

One fundamental problem we have noticed throughout the UK is the sentiment that:

- "Workers are unnecessarily penalized for simple human errors at a time when they are very stressed increasing the risk of a human error… It is pattern that is repeated during very busy period, workers are deluged with tasks of critical importance and are more likely to make mistakes due to workload and stress."

This is compounded by the fact that in regards to reporting, auditing and alerting, these tasks fall specifically to one group of people, ICT staff. If these staff members are required to double check every request and are not given the tools to do this efficiently, mistakes are inevitable. In order to combat this, strong training, communication and transparency are of critical importance.

In order for non-technical staff to be trained, they need to be taught that managing data is ultimately their responsibility, it is their data and they must play a role in protecting it.

This is only achievable if the information is displayed in a transparent manner. Building request workflows will also allow ICT to constantly train Data Owners. If they are able to see the comments of rejected requests, they can ensure that requests are correct. With a central platform used to share information for reporting and requests, workflow can be standardized, increasing efficiency.

"Workers are unnecessarily penalized for simple human errors at a time when they are very stressed increasing the risk of a human error…"

Our Vision & Contact

Name
Roger Tolman

Role
Survey Manager

Company
GovNewsDirect

Website
www.pendulum.media

Email
rtolman@pendulum.media

Tel
0161 641 8122

Operating across the Public Sector, GovNewsDirect are the UK's leading marketing, communications & direct news organisation dedicated to this sector.

We enable the flow of effective information to over 300,000 key decision makers & influencers. By transferring best practice and innovation between communities, sharing information and communicating the latest in product/solution developments, we are a trusted source of aggregated news & insight.

GovNewsDirect are specialists in creating, engaging and developing partnerships, facilitating the engagement of mutually beneficial relationships between the private and public sector. We are proud to be part of public sector transformation and influencing change through our direct news alerts and research.

GOV NEWS DIRECT

Address
Gov News Direct
Suite 1, 8th Floor
Regent House
Heaton Lane
Stockport, SK4 1BS

Website
www.pendulum.media

Email
enquiries@pendulum.media

Tel
0161 641 8122

8MAN

Address
Protected Networks GmbH,
Alt-Moabit 73, 10555 Berlin,
Germany

Website
www.8man.com

Email
info@8man.com