clearswift
by HelpSystems

GUIDE *(Cybersecurity)*

The GDPR Divide:

Board Views v's Middle Managements

The issue of where, and how, information is stored and protected is an increasing concern for citizens and organisations across the world. The evolution of the digital era and the way in which we collaborate on daily basis is driving new legislation to protect sensitive data. Inadvertent sensitive data sharing and the lack of adequate protection is resulting in information loss on a significant scale and is being recognised by authorities as a global issue that is in need of being addressed.

The GDPR's enforcement will affect any organisation that stores or processes personal data of EU citizens, even if they are not based in the EU, to comply with new data protection legislation by the 25th May 2018. Failure to do so may result in a fine of up to 4% of annual global turnover or €20 Million (whichever is greater).

It is therefore imperative that the board understands the state of data protection within their organisation and is the driving force that introduces new measures to ensure GDPR compliance.

How the perception of GDPR compliance differs between the board and management

Survey Results

- The perception and definition of GDPR will vary across your organisation
- Our research has shown that board members are more confident about GDPR compliance than management is
- The board needs an accurate view of the state of compliance in order to ensure the company is not in breach of GDPR.

41% of board levels respondents think they have necessary processes in place to be GDPR compliant. But, only 21% of middle management agree

Clearswift recently surveyed 600 business decision makers and 1,200 employees, across the UK, US, Germany and Australia, and found that board level respondents are more confident about having the necessary processes in place to be GDPR compliant than senior management are. 41% of board level respondents stated that they have all of the necessary processes in place, yet, only a quarter of senior management and even fewer middle management respondents (21%) thought the same.

The survey results reveal a gap in understanding between the board and middle management when it comes to GDPR compliance. It is imperative that the board takes the lead on bridging this gap and supports the organisation to expedite compliance..

Why the board must take ownership of GDPR Compliance

Ultimately, GDPR is not the responsibility of middle management or the IT department. It is the board's responsibility. It is in the board's best interests to pay due diligence and understand their organisation's critical data landscape. This is because, aside from the financial penalties that come from non-compliance, it is an opportunity for a company to grow the organisation through better information governance.

An individual, whether a customer or employee, has to trust that an organisation will do the right thing with their information – and protect their data at all times. Furthermore, suppliers and partners must accept 'shared responsibility' for data protection, because they will also be liable for supply chain breaches under the GDPR. Failure to execute on data protection ru could mean that customers move to a competitive provider or partners work with another supplier.
Obtaining a clear picture of how customer data is being processed and shared, and where it is being stored, is not only vital for GDPR, it can also be the first step in mobilising a business to protect other valuable assets. GDPR compliance is about being able to recognise a particular data set and protect it accordingly. The same processes and technology can be used to protect other types of information that are valuable to your organisation. For example, product design documents, price lists, patent applications and even information around service pricing and contract bids.

Ascertaining how GDPR compliant your organisation is

Middle management is more likely to have a better view of the data that their organisation holds - where it is saved and how it is being used - because they are more familiar with the organisation's day-to-day operations. Board members are unlikely to have a full understanding of the minutiae of processes or full visibility of the organisation's critical data, or knowledge of where data is stored. This is of course understandable, however the board needs an accurate view of the state of compliance in order to ensure the organisation does not fall short of GDPR requirements.

GDPR is effectively a replacement for existing legislation and directives . In addition to this, it also requires organisation's to review data processing processes, some of which require significant changes to existing business processes and, or, the introduction of new ones in order to deal with specific requirements, such as the right to be forgotten (RTBF), also known as the right to erasure.

Right to be forgotten will be your organisation's biggest challenge

The RTBF entitles EU citizens to request, in certain circumstances, that an organisation deletes all references to them that it holds. When it comes to the RTBF, the

board is certainly more confident than middle and senior management about the ability to cope with hundreds of requests at once. Over half (56%) think they could handle this without any impact, but only a third (36%) of middle management agree.

Over half (56%) of board level respondents think they could handle RTBF requests without any impact to their organisation, but only a third of the middle management agree

Board level respondents estimated that around 6% of customers would exercise their right to be forgotten. However, nearly half (48%) of board respondents said they would be extremely likely to exercise their own right to be forgotten, and nearly a quarter (23%) of all respondents said they were extremely likely to do the same.
Organisations need to be prepared for such RTBF requests, particularly as respondents estimated it would take an average of four days to locate all information on an individual, let alone carry out the actual deletion of just those pieces of information that need to be 'forgotten'. Under GDPR, this deletion needs to happen "without undue delay", therefore having a streamlined process becomes essential in order to prevent the business coming to a standstill while the requests are processed.

The survey data also revealed that board level respondents and management have a different view on the definition of an internal breach. A quarter of board level respondents (25%) stated that the number of internal breaches has significantly increased, however only 10% of senior management agree.

The reason for the difference in views on what constitutes an internal breach could be that the board view some instances as a security breach, when they are not. For example, if someone lost their laptop, the board may view this as a breach. However, if it is the case that the laptop is encrypted, and management knows this, then this does not constitute a breach, so is not labelled as one.

Improving communication between the board and management

Increasing the board's knowledge on the organisation's information security landscape

Given middle management is best placed to identify what data an organisation holds and where it is stored, the board needs to actively engage this section of the organisation and extract information in order to understand the true level of the organisation's GDPR preparedness, including the steps that may need to be taken in order to ensure and enforce compliance.

1. The board should brief management to:
    a. Find out where critical data is stored
    b. Understand how critical data is flowing in and out of the business (e.g. email, web collaboration tools etc)
    c. Identify unofficial workarounds that staff may use to circumvent security (e.g. Gmail / Dropbox, USBs, saving/duplicating business critical files on laptops/desktops)
    d. Investigate why these workarounds exist (e.g. poor connectivity, or remote working requirements)
    e. Ensure they do not filter out 'bad' news. (e.g. if processes are broken or data duplication is happening, the board needs to know)
    f. Communicate in a way that is clear to the board and explains the risks
2. Make time to listen to management on a regular basis around issues and potential resolutions to compliance
3. Ensure you know, at a high level, what GDPR demands in order to become compliant
4. Ensure appropriate budget is allocated to help management execute on a GDPR compliance project

Understanding what's involved with your organisation's GDPR compliance project

Management must first identify the type of information, within the organisation, that is protected by GDPR.
For example, consumer email addresses, the contact details of an ex-employee, passport information, medical records or credit card details. Management must then find out where data is stored across the organisation. They need to know what information is being shared within the company, what

information is being shared externally, and all the different business communication channels this data is being shared through.

Management also need to uncover if staff are using unofficial workarounds. If staff have problems connecting to the server when working remotely, it could drive them to use 'shadow IT' solutions and break policies. For example, an employee may request that a colleague emails them the files that they need to their personal email account, or they may download files onto a USB the day before they work from home.

In order for a RTBF request to be carried out, an organisation must first know where data on the individual is held, and this includes identifying where the data is duplicated (copied) or stored on back-up systems. Deletion can then be carried out automatically through Data Loss Prevention (DLT) Ptechnology, or manually by designated individuals within the organisation.

RTBF is the most challenging aspect of GDPR, because in order to carry out the request, you must know where all the data on the individual is held. If you do not have a record of data duplication or are unaware of staff copying data, you will not be able to carry out RTBF requests correctly. A simple example would be the creation of a report from a sales database listing the top 20 accounts with the details of the contacts. The report is then stored on the user's laptop, or emailed to other people (inside or outside the organisation). What was a well-controlled source of information has now become a potential risk. This is further exacerbated by the devices used to store the information not belonging to the organisation.

The research revealed that 34% of board level respondents thought their employees have definitely downloaded work documents to their personal devices, such as a laptop, or smartphone or tablet, and they have not subsequently deleted it (unintentionally or otherwise). Only a third (31%) believed that this had not happened.

Management must provide the right information to the board for review

Once management has a clear picture on the state of data within the organisation, it is important that they are encouraged not to filter out 'bad' information. For example, if emailing sensitive files to personal email accounts is rife, or if staff are using third party file sharing sites, like Dropbox, because the company does not have an easy-to-use file sharing system, then the board needs to know so the issue can be discussed and addressed in time for the GDPR deadline.

Scheduling regular meetings between the board and management to discuss data security and changes to processes will help improve the board's understanding of what GDPR demands. Of course, it is not expected that the board knows every aspect of the regulation and how to implement it, however it does need to be familiar with the key aspects and what they entail. For example, the fact that RTBF requires that data is removed from system back-ups and the impact on supply chains should a request be made. Management needs to communicate to the board in a way that is clear and explains the risk, giving the board all the information they need to understand how to mitigate that risk. For example, many years ago company laptops would not be encrypted and the associated risk for a lost laptop would be the cost of a replacement. Today, the cost of a lost laptop is not just the price of a replacement, but also the cost of a fine from the country's information regulator. The solution to this issue is to use encryption in order to mitigate the risk.
In this example, the cost for all users to encrypt their laptops is usually significantly less than the financial penalty and the consequences of a major breach, which can damage an organisation's reputation and bottom line. From a GDPR perspective, the board needs to ensure that it makes time to listen to management and allocate a suitable amount of budget for compliance, and management needs to know that the board has made budget available.

By supporting management to invest in tools and technology to secure your organisation's data, you can mitigate risk and avoid larger long-term costs.

Bridging the GDPR governance gap: How to improve education and awareness among staff

5 key points for the board to drive into the organisation

1. Ensure staff understand why data protection is important
2. Ensure staff understand data protection processes and know what security policies are enforced
3. Ensure staff understand what data duplication is and how to avoid it

4. Ensure staff are aware of the basics of GDPR and are provided with a high level overview of your organisation's GDPR compliance project
5. Appoint a 'GDPR champion' who will push forward the GDPR agenda in your organisation and can support the board with each of the above points.

Board members have a responsibility to ensure that staff understand data security and are provided with guidance on how to safely work with the organisation's critical data. This means educating existing employees and training new staff when they join. Your organisation should have deployed Data Protection Policies and Best Practice Procedures to help guide staff and ensure every member of the organisation has a clear understanding of how to hold, and process, critical data securely.

Good data citizenship starts with the board

Driving a strong data protection culture within an organisation starts at the top – the board. Board members must demonstrate good data citizenship in order for a strong data protection culture to flow down into the organisation. The research showed that if a board level respondent received an email from someone in another company in error, less than a third (29%) would let the sender know, and just 17% would permanently delete the email. Why does this become important? GDPR compliance impacts the whole information supply chain. If there is a RTBF request, then this also needs to ripple up and down through suppliers and other third parties. If an email containing GDPR sensitive information is sent in error, then this too could become subject to an RTBF request – which will cost time (and therefore money) to process, all due to a mistake by someone outside the organisation.

The EU GDPR is not discriminate to organisation size or geographical location. If you hold or process EU Citizen data, you're obliged to comply.

Leading by example and encouraging staff to be good data citizens will help to improve data handling and processes within their own company, but also other companies. The recipient of an email sent in error does not need to inform the other organisation directly, instead a simple process can be set up where an employee can quickly inform someone else, typically within their own legal, HR or IT department, who will let the other company know of the mistake, so they can correct their processes.

Data Duplication - a key threat to organisations under GDPR

The board can also explain how easy it is to accidently duplicate data, and how the board itself can be guilty of this. Two thirds (66%) of board respondents admitted to sending a work email to someone who was not the intended recipient. In addition, the research showed that not only is customer data is being duplicated, but there is also a lack of understanding among staff about what data duplication is.

Less than a third (29%) of board level respondents would let a sender know if they had received an email in error.

When initially asked if their organisation definitely duplicates customer data, nearly half (48%) of board level respondents said it did. Yet only around a third (36%) of senior management thought the same, and a quarter (23%) of middle management. Interestingly, once it was explained that duplicating data can include forwarding an email to a colleague that contains customer data, inputting customer data into a database that is also in another location, or making a copy of an excel document holding customer details, they changed their response.

Once respondents were clearer on the definition of data duplication, 31% of middle management respondents said they definitely had duplicated data, and 41% thought they may have. So, 72% of middle management were likely to have duplicated customer details, 22% higher than the results prior to explanation.

As mentioned previously, RTBF is the most challenging aspect of GDPR. If staff, including the board, are not even aware that they are duplicating data, it will make it much harder, even impossible, to ensure compliance. A quarter of organisations surveyed had tried to find all information about a single customer to attempt to erase their information (RTBF request), but they thought there may have been data

that was missed. A further 13% said that data had definitely been missed. Just over one tenth (11%) of organisations said they had not tried to find all information about a single customer, but said they should do.

5 key points for the board to drive into the organisation

1. Producing a report from a database: Sales has requested a spreadsheet on the company's top 20 customers in their region (and they do this every month) which is then emailed to them, and some then store it on their laptop as well.
2. Saving documents to the desktop: An employee finds it quicker to save a document on to their desktop, rather than the server they should use.
3. Remote / mobile working: An employee can't access the server, so they ask a colleague to email a document, or they email it to their own personal account.
4. USB sticks: An employee finds it quicker to download a file onto a USB than use the company's file sharing system.
5. System backup: The IT department backs-up the server once a week. This is obviously a legitimate reason for creating a copy of the data, but it still needs to be taken into account when it comes to compliance.

The board also needs to ask itself what it can do to minimise duplication of data at the senior level of the organisation. For example, does the board request regular email reports from management that list the organisation's top customers? Is that report necessary? If the report is required, then a more secure way of accessing the report should be put in place, such as through a secure online portal, which will remove the issue of the report ending up on multiple devices. Obviously this cannot be done for everything, but the more that can be done, the less there is to clean up should the need arise.

Exceptions to the right to be forgotten rule

It is important to note that there are exceptions when it comes to RTBF. Not all data is created equally, and some cannot be 'forgotten' on request. For example, a patient could not contact their local GP and expect the right to be forgotten, because the practice would not be permitted to delete their information. Similarly, if you have purchased goods you cannot expect the transaction data to be deleted in an arbitrary manner. Also, a customer that is under contract does not have the right to be forgotten completely, although they may want to be removed from marketing contact, which is within their rights.

If your organisation deals with regular and systematic monitoring of data subjects (i.e. citizens) on a large scale, is a public authority, or carries out large scale processing of data relating to criminal convictions or offences, a Data Protection Officer (DPO) must be appointed. The DPO role, which is predominantly required to enforce compliance, can be appointed to an individual outside the organisation or within an organisation. An external appointment is preferable as the position needs to be seen as independent.

Assigning a GDPR Champion

Even companies that do not have to appoint a DPO under GDPR can't forego compliance. It is important to appoint someone who can act as a champion who will push forward the GDPR agenda in the organisation. When appointing this role, the board needs to either choose someone within the organisation who is particularly strong at communication, project management and networking both within and outside the company. The GDPR champion needs to take charge of a cross-party initiative, and brief employees, across all levels and departments, on data protection.

When it comes to creating policies that enforce data protection, one of the simplest initiatives to adopt is one of restricting access. The more people that can access sensitive information, the greater the security risk. It is somewhat reassuring to note that the majority of survey respondents felt that most security incidents that had happened were either inadvertent or accidental. This means that having the right processes in place, and educating staff on security, will really help to create a culture of protecting critical information.

While the focus of GDPR should be on people and processes, technological solutions – such as DLP – will serve as a back-up, enforcing the policies put in place and protecting both employees and customers. Furthermore, advanced functionality, for example, Adaptive Redaction extends DLP policies by allowing automatic removal of sensitive and confidential information from both email

and web based communication. The changes that are made depend on the policy, which in turn depends on the individuals who are sending or receiving the information - making it an 'adaptive' process.

Moving beyond GDPR compliance: How to grow your business through better information governance

GDPR compliance should not just be seen as a tick-box exercise, but the first step in mobilising your business to protect all your valuable information assets, and ultimately grow your organisation through better information governance.

When putting all the various processes, people and technology in place to enforce GDPR compliance, the relevant data will be discovered. This will include who has access to the data, and how it is being used and shared. Once this information is obtained, new ways of streamlining processes and improving the way the organisation interacts with its customers will be identified. New ways of engaging and selling to customers may also be identified. Many of these ideas will come from employees, rather than the board or sales and marketing.

Data is your organisation's most valuable asset – protect it unequivocally

No matter what sector you operate in, the processes and technology put in place to enforce GDPR compliance can be easily extended to protect other critical business information specific to your organisation such as intellectual property, business plans, financial results and bids for contracts – whatever your organisation deems unequivocally confidential. GDPR is specifically about protecting EU citizen information, but there is a lot of other 'critical' information that would be damaging to an organisation if it was stolen or leaked.

To give a specific example, a courier company needs to understand the cost of delivering a parcel in order to remain competitive and set prices accordingly. This specific information is one of the most critical, and valuable, pieces of proprietary data that they own and might just be held in a simple spreadsheet which could be inadvertently shared outside the business.
The unfortunate truth is that many organisations do not know what their critical information is and just how valuable it is to them. Without this understanding, putting a plan together to protect it becomes tough. Another example is a service company's board that didn't think they had 'critical' information because they did not produce products. An incident where deals were lost due to underbidding by a rival indicated a 'leak' in the organisation. Critical information should be viewed as anything that would cause the business damage if it fell into the wrong hands, whether it is the competition or something more sinister.

Due diligence needs to be paid to the security policies that your supply chain, partners and even customers have in place in order to best protect your business's interests.

The process of making a company GDPR compliant will reveal how information flows in and out of the organisation. For example, a design company would find out where patent information travels inside and outside of the company. It will discover if patent information is shared with a very select group within the company and a patent attorney, or if other people are gaining access to the data that they do not need to. Mitigation against unauthorised access can then be put in place with the appropriate processes and technology

Summary

The issue of where, and how, information is stored and protected will remain a concern for citizens and organisations across the globe, and we can expect to continue to see new legislation and requirements introduced, in order to protect data.

GDPR is a strong signal to global organisations that data protection is a crucial responsibility. Not only is protecting data a legal requirement, but the act of discovering where and how data is stored, and how it's processed and shared, can help organisations to improve processes, security and discover opportunities to grow an organisation.

Once the board closes the communication gap between itself and middle management, gets to grip with the information security landscape of their organisation, and then closes the governance gap by ensuring that all staff understand the importance of data protection, compliance will be successfully achieved and so too the ability to increase trust, efficiencies and growth.

The bottom line is, the board is responsible for GDPR and by properly engaging with management, it can ensure compliance is as painless as possible. The responsibility then no longer becomes a burden, but a vehicle to drive positive change within the organisation.

In closing, the question to leave you with is: How compliant is your organisation, and most importantly, does middle management agree?

The resulting outcomes of executing a GDPR compliance project will build trust with customers and stakeholders, and create a positive impact on your organisation and your team.

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.

(csw-gdpr-dvd-1220-r1)