The Business Software Centre
ViewPoint, Basing View, Basingstoke, England
www.businesssoftwarecentre.com

GDPR and the implications for ITAM Managers

Imagine this situation in two years-time from now. The ITAM manager for a large organization has been called to a board meeting. There has been a major data breach and a large amount of customer information has been stolen. The penalty for this breach could be as high as 20million Euros. The Directors ask the ITAM Manager the following questions:

“How many devices (PCs, laptops, servers, mobiles) does the organization have?”

“Who has access to them and where are they?”

“What software is installed and which applications actually used and by who?”

“Do the devices all have data encryption installed?”

Given the state of technology, processes and records in organizations today, how many ITAM manager will be able to answer these question accurately. Currently, it is not uncommon for organizations to suffer from a security breach on a device that they do not even know they had. Even with current data protection laws this is unacceptable, however in 2018 the situation changes dramatically with the introduction of GDPR. This event will have major implications for anyone in an ITAM or SAM role.

What is GDPR?

The EU General Data Protection Regulation (GDPR) will be implemented in the European Union (EU) on 25 May 2018, when it supersedes the 28 current national data protection laws.

The aim of GDPR is to strengthen individuals’ privacy and security rights, as well as to simplify the flow of personal data in the EU. It applies to any organisation, whether or not it is based in the EU that collects, retains or processes the personal data of EU individuals. It will be a key requirement for organisations to ensure that personal data held is secure, and to prevent data breaches through encryption measures.

The single set of rules will apply to all EU member states including the UK. Each member state will create its own Supervisory Authority (SA) to hear and investigate complaints, sanction administrative offences, etc. Individual SAs will cooperate with each other, providing mutual assistance and organizing joint operations. Where a business has multiple establishments in the EU, it will have a single SA as its ‘lead authority’, based on the location of its ‘main establishment’. The lead authority will supervise all the processing activities of that business within the EU. Co-ordination of the SAs will be through European Data Protection Board (EDPB).

Why is GDPR important?

If in breach of the Regulation, organisations can expect fines of up to 4% of their annual global turnover or €20 million. These are significant increases on existing penalties. In many cases, if the fines are applied in full it could mean a significant threat to the future of an organization.

Does Brexit mean the UK does not have to comply?

Although the UK voted to leave the EU the GDPR will still apply. Firstly, the UK will still be an EU member when GDPR comes into force; and secondly, GDPR contains an extraterritoriality clause. This means that any data processor handling EU citizen data is within scope of GDPR, irrespective of the geographical location of the data processing. So if an organization handles data on EU citizens and organizations, or sells services, such as cloud and datacentre hosting, they will need to comply with the EU rules. It is also expected that the UK will permanently adopt similar rules in order to facilitate data transfer between countries.

What does GDPR compliance entail?

A large part of GDPR is about the processes and operational aspects of data protection. Relevant staff training and implementation of the correct security processes will need to be applied. However, in many cases appropriate technologies will assist an organization in automating the processes and treating data in the safest and most secure way.

GDPR is not prescriptive about the technology to be used, for example it suggests: “The pseudonymisation and encryption of data; ability to ensure confidentiality, integrity, availability and resilience of processing; the ability to restore data after an incident; and a process for testing, assessing and evaluating effectiveness of security". It suggests “state of the art” technology should be used but this leaves important aspects open to debate. Will it be left to the courts to decide if technology used is state of the art? How many ITAM managers would you say the technology they currently use is state of the art? If the question asked is, “Why wasn’t this device and data encrypted?”, not having a record of a device or it’s applications clearly implies the technology was at fault.

Most organizations need to be making decisions now about the technologies they will employ to ensure they close the gaps between their current state and where they need to be to comply with GDPR.

What is the impact of GDPR on ITAM/SAM Manager?

ITAM managers will need to play a crucial role in ensuring their organizations are GDPR compliant. Quite simply it is essential to know what devices are deployed, where they are and what software they can access. Without this information data cannot be protected.

A recent discussion with a CIO revealed he only knew where 70% of his devices were and what software was installed on them. Clearly he has a big problem in ensuring GDPR compliance. Another IT Director admitted he had allowed their sales staff to bring their own devices and access their customer database. One salesman subsequently left and went to a competitor having downloaded the entire customer database onto his own laptop.

Here is a checklist for ITAM managers contributing to GDPR compliance:

1. **Know what devices are deployed and where they are**. Having discovery agents on 80% of an estate means 20% are potentially the greatest biggest risk. An agentless scan can be a fast and effective way to fill the gaps in asset knowledge of devices and what software is installed.
2. **Know who uses what**. It is not good enough to know just your soft inventory. Knowing who has access to key software applications and data and who actually uses key applications will enable the tracing of users in the event of a security breach A large proportion of security breaches are internal, either deliberate or through negligence. Deploying a software usage tracking and analysis tool will identify who is responsible for a data breach and in some cases enable preventative measures.

3. **Encrypt devices, portable media and mobile phones**. If an encrypted device is mislaid or stolen the information residing on it is protected. A managed encryption service is quick and easy to deploy and provides data security in the event of a security breach.
4. **Protect confidential ITAM data**. ITAM managers keep sensitive information about staff, suppliers and contractual terms. These must be secured as GDPR affects companies and other organizations, not just individuals.

The technologies to achieve these tasks are readily available. An assessment of the major risks and how to mitigate them will enable senior management to assess if they need to be closed.

Summary,

The vast majority of organizations will be affected by GDPR and they will either take measures to comply or decide to take the risk that a breach will not occur. The penalties following a breach are significant, so taking a risk is probably not the best course of action. ITAM managers have to play their part in the process. A responsible approach is to raise the issue with the management team if there is a lack of visibility of assets or the software and data that resides on them. By failing to identify gaps that affect data security, ITAM managers will be letting down their organizations, colleagues and those that have allowed their data to be used. Senior management can make decisions about the risks only if they are aware of them.