GDPR & Cybersecurity Readiness

Media hype around GDPR (General Data Protection Regulation) has produced considerably more heat than light. GDPR is the European Union's replacement for things like the UK's Data Protection Act (1998). The new regulations are set to come into effect in May 2018. All companies wishing to trade with the EU must be GDPR compliant. The UK will adopt GDPR regardless of its decision to leave the EU. The main driver behind GDPR is that current data protection legislation is no longer fit for purpose, having been written into law decades ago when digital technology was in its infancy.

Into the unknown

Regardless of all the media and marketing hype, the truth is that we just don't know what the full implications of the new data protection legislation will be. Certainly, it is true that there are substantial penalties for non-compliance, but we still don't know how different European states or the UK will actually interpret various elements of the new regulations. Surely, no one will benefit from Draconian penalties and excessive red tape that stifles business activity and innovation.

Data protection

In reality, GDPR isn't that much different from current data protection legislation. It's simply being brought up to date. The main personal data protection principles remain the same.
Personal data should be:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection.

Individual rights

Some of the new rights for individuals include the "right to be forgotten" and data portability (the right of individuals to obtain and reuse their personal data for their own purposes across different services). There will be new provisions to increase the protection of children's data such as parental consent for under sixteens wanting to sign-up for online services and a stronger "right to be forgotten". Under the new regulations, you must also be able to demonstrate compliance. That means clear processes, procedures and metadata

management. The new legislation further distinguishes between general personal data (contact details) and sensitive data (medical records, religious beliefs and unique biometric identifiers, for example).

Naturally, the regulations require you keep personal data securely. However, the directive is not specific or prescriptive about how you secure the data you hold. Data controllers must report personal data breaches to their supervisory authority and, in some cases, the affected individuals. This must be done within 72 hours where feasible.

The Information Commissioner's Office (ICO) provides plenty of information on what steps you can take now to prepare for GDPR compliance. Visit the ICO's website for their handy 12-step checklist.

Cybercrime

Today, all organisations should consider themselves targets of cybercrime. No one is immune. The new regulations build on what is required by existing data protection legislation. Firstly, you should take appropriate organisational and technical measures to protect your systems and the data that resides on them. Although not a mandatory obligation, it is recommended that personal data is always encrypted.

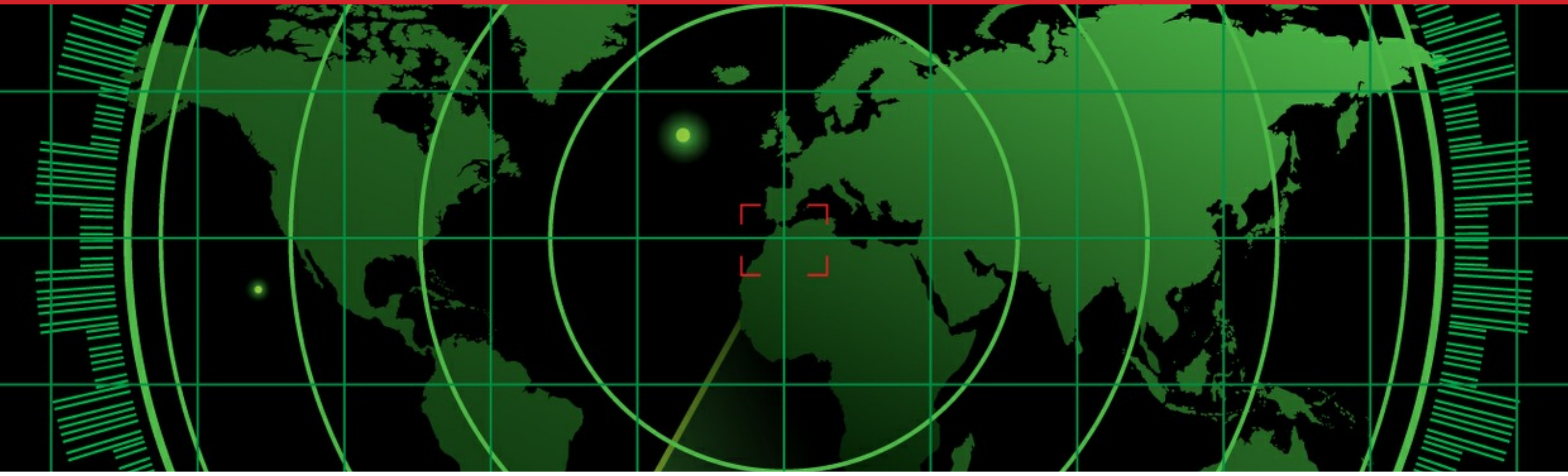
Your IT systems should be secure, resilient and backed up. In the event of a physical or technical incident, you should be able to recover all personal data records in a timely manner. You should also have a process in place to regularly check the effectiveness of your data security. As well as meeting new obligations on data breach reporting, organisations must keep their own internal records of all data breaches and similar incidents. All scaremongering aside, the truth is that having an IT security strategy in place will help mitigate the risks from cybercrime while helping you meet many of your data protection obligations.

User awareness

Firstly, the majority of data breaches are caused by human error, not technical failings. It is important that everyone across your organisation is aware of cybersecurity threats, and assumes their share of the responsibility to keep your corporate data safe. Your staff should be properly educated about risk mitigation through good practices and procedures.

Cybersecurity audit

Next, you'll want to determine the current state of your cybersecurity and define where you need it to be. This process can be broken down into policy, employee and technical assessments. You will probably find a



mix of easily fixed vulnerabilities and those that will require a more planned, long-term response. Naturally, any business critical operations assessed as vulnerable should take priority in your remediation plan.

Constant monitoring

Running a cybersecurity audit gives you a snapshot of your strengths and vulnerabilities. However, once you've conducted the remedial work necessary to close any identified gaps, you still have work to do. The cybersecurity landscape is constantly changing and new threats are emerging all the time. Subsequently, you will need to establish a regime of constant monitoring. According to the National Cyber Security Centre (NCSC), "Good monitoring is essential in order to effectively respond to attacks. In addition, monitoring allows you to ensure that systems are being used appropriately in accordance with organisational policies. Monitoring is often a key capability needed to comply with legal or regulatory requirements." The NCSC provides a 10-step checklist for cybersecurity monitoring.

Remediation

Unfortunately, you can take every conceivable precaution and still be the victim of cybercrime, so it will pay you to be prepared should the worst happen. It's important you have the right skills and technical resources to quickly identify, isolate and deal with threats while minimising their impact on your business operations. Building resilience into your systems, ensuring business critical data is backed up and establishing a coherent disaster recovery plan will make a significant difference to your organisation's survivability after a cyberattack.

Plan for the worst

Currently, no one knows exactly how the UK or European states will choose to interpret or enforce GDPR. There is a wealth of free advice and guidance available from the UK government and its various agencies to help you comply with the new regulations. Certainly, it makes good business sense to take every precaution to safeguard your corporate data from accidental or malicious breaches, and have contingency plans in place should an incident happen.

Cyber essentials

The UK government has a Cyber Essentials scheme that you can refer to in order to help address important cybersecurity concerns. You can use this as the foundation stage of your cybersecurity strategy before looking at the finer details. Once completed you can then self-certify for Cyber Essentials.

See: UK government's 10-steps to Cybersecurity

Modern Networks

Established in 1999, Modern Networks is a leading provider of IT and telecoms to the UK's commercial property sector. We offer everything from desktops and technical support to telephony and broadband. The company has offices in the South-East and Manchester.

Modern Networks is a certified partner for Cisco, HP and Microsoft. We have considerable expertise within commercial property management working with over thirty top managing agents and over 1700 sites. Our clients include CBRE, Cushman and Wakefield, CEG, JLL, Knight Frank, Savills and Colliers. What sets Modern Networks apart is our ability to translate the needs of our clients into practicable framework agreements and competitively priced IT solutions.

Modern Networks provides advanced, innovative IT managed solutions to numerous clients from architects, accountancy firms and not-for-profits to media companies. We are Cyber Essentials certified.

Call our sales department now to learn more about our extensive range of IT and telecoms services or visit our website.

CYBER ESSENTIALS

Images courtesy of Flickr.com and Freepik.com