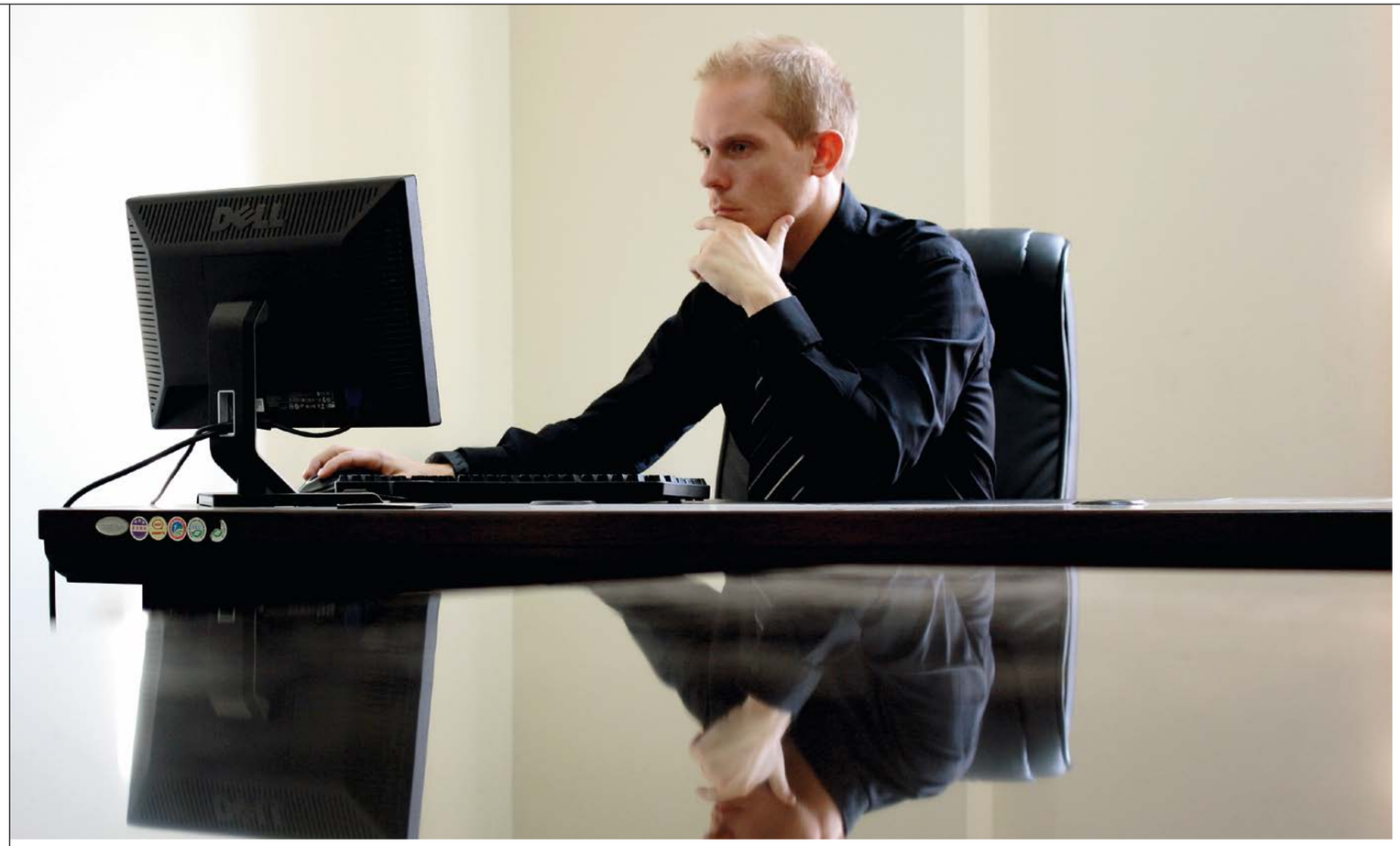


IMPORTANCE OF NOT OVERSHARING

It's vital that every third-party contract is reviewed for liability protection purposes

James Howell *explains the importance of getting your company's internet security in order before the upcoming GDPR law changes*

Working with third parties is part of everyday business, whether it be large-scale outsourcing, working closely with suppliers or simply using a Software as a Service (SaaS) solution. But third-party relationships increase the complexity of data security, introduce additional risk and can easily result in your company becoming noncompliant.

With General Data Protection Regulation (GDPR) on the horizon, this threat is only going to get more prevalent; you can't stop working with third parties, so it is essential to implement the correct systems, processes and checks at every stage of a partnership. "The General Data Protection Regulation (GDPR) is the biggest change to data protection law in a generation," says Elizabeth Denham, UK Information Commissioner.

GDPR is the new reality that we all have to live with, but it is not enough just to get our own house in order. There is a risk of larger fines for companies that aren't compliant or that are responsible for a leak of private data, either accidentally or through a security breach. When GDPR comes into effect on 25 May 2018, a business could be fined €20m or 4 percent of worldwide turnover, whichever is greatest.

The first action necessary in pre-empting compliancy issues, is to review every existing third-party contract to establish the existence of a clause indemnifying the company from loss due to a security flaw. No-one wants to be liable for a fine because of a third party's weakness in their own security.

A contract clause does not protect from a security breach, only from the financial liabilities of such a breach, so a further detailed agreement that specifies how data will be protected should be in place.

Carrying out security audits of suppliers and partners should come early in the onboarding process when working with any new companies and should immediately be put in place for any existing third party.

RESTRICTED ACCESS

Access should be restricted and this should be closely monitored. Third parties should only have access to the minimum amount of data that they require to carry out their role. Providing them with additional access can result in data breaches. Restricting the access may require some re-engineering of existing systems as often access is either open or closed and not graduated.

The vital importance of restricting access to the minimum amount was illustrated recently when TalkTalk Telecom Group PLC was fined £100,000 by The Information Commissioner's Office for failure to protect customers' data.

The ICO investigation found TalkTalk was in breach of the Data Protection Act because it allowed the partner Wipro's staff to have access to a large amount of customers' data. TalkTalk's lack of adequate security procedures left the data open to exploitation by corrupt employees. At the centre of the breach was TalkTalk's customer portal, where customer records could be accessed. One of the companies with access to this was Wipro, which resolved high-level complaints on TalkTalk's behalf. An investigation by TalkTalk identified three Wipro accounts that had been used to gain unauthorised and unlawful access to the personal data of up to 21,000 customers. Nearly 50 Wipro employees had access to data of up to 50,000 TalkTalk customers.

The Wipro staff could log into the portal from any device. No controls were put in place to restrict access to devices linked to Wipro. They could also carry out 'wildcard' searches, allowing staff to view up to 500 customer records at a time and to export this data. The ICO found this level of access was more wide ranging than could be reasonably justified and put TalkTalk's customers' personal data at risk.

The temptation in the face of such cases would be to close down access completely, but outside contractors and suppliers will need access to some specific internal applications and data in order to be productive. This visibility is often achieved by giving VPN access. This means that the IT team involved must be fully aware of the risks of working with third-party companies and individuals as they set up network, device, software and policy-related configuration and management tasks to securely enable the access. Third parties require the same or greater level of security to access data as your own staff. If you use two-factor authentication, then so must the third party. They should be using your tools for remote access rather than their own, so you remain in control at all times. But any kind of third-party access creates additional points of entry to an organisation's network, increasing the overall risk that data may not be as secure as you believe it is.

The implications of not locking down access to data can be immense. The Swedish Government is facing a considerable clean up following a sensitive national data breach, which took place in 2014 as a result of an outsourcing agreement with IBM. The breach has only just come to light.

The data leak, which exposed top-secret police databases to IT workers outside of the country, resulted in the prosecution of the former head of the country's Transport Agency and raised major concerns over the Government department's data centre outsourcing agreement with IBM. The Swedish Government has admitted that it had taken shortcuts when overseeing the security of the department's IT infrastructure, allowing contractors access to the data without the necessary security clearances. And if it can happen with governments and large companies such as IBM and Wipro, then it can certainly happen with smaller organisations.

59% OF EMPLOYEES THAT QUIT TAKE CONFIDENTIAL OR SENSITIVE BUSINESS INFORMATION WITH THEM

Often the selection of external organisations is not within the visibility of a company's IT team or nominated information officer. Software as a Service (SaaS) applications are adopted throughout a company quickly and easily and in many organisations without adequate control or enough thought to data security. A 2016 survey showed 98 percent of SaaS applications do not comply with rules that will be introduced by GDPR.

UNDERSTANDING THE DETAILS

The most common SaaS-based application is Salesforce.com, the Customer Relationship Management (CRM) tool. Salesforce.com has built its reputation on data security with very few incidents being reported of any kind of data breach, but as with any SaaS supplier understanding how the application is used within your business and how the supplier handles data is essential. Salesforce has an ecosystem of companies that write applications for the platform, which might then be automatically adopted. To ensure full compliance, these applications and companies also need to be audited.

Nearly a quarter of all files stored in the cloud are shared, and around 12 percent of those contain compliance-related or confidential data.

Further threat to compliance may lie with shadow IT systems that fall outside of the watchful eyes of those within an organisation tasked to keep data safe. Dropbox is just one example of this, where often personal accounts are used for business. Data may be held and shared in many other SaaS applications adopted by users within a company without the company's official blessing. Slack, a digital workspace

for teams, is becoming more common and users are inviting external companies into shares where sensitive data may reside. Adopting such technology is as simple as a few clicks, but it can and will put a company's data integrity at risk and increase the risk of non-compliance. Companies need to introduce data policies around the adoption of SaaS applications as well as larger outsourced arrangements.

When selecting third parties to work with, it is often required to be very open with information. For example, if a company is selecting a new vendor to provide cyber security it can be necessary to share sensitive information regarding current configuration. If the company is working with a single trusted partner with existing audited data security processes this may be acceptable, but if the company is going out to the market to speak to four companies, it may not be practical to run a detailed pre-selection process.

EMPLOYEE DATA THEFT

Employee data theft is also a real problem in business. A study found that 59 percent of employees that either quit or are asked to leave take confidential or sensitive business information on departure. This is a data breach, threatens compliance as much as third-party access and is the responsibility of the business to prevent. When people leave a company, they take with them any data that they feel will help them in future roles, and that could include sensitive details of network topology.

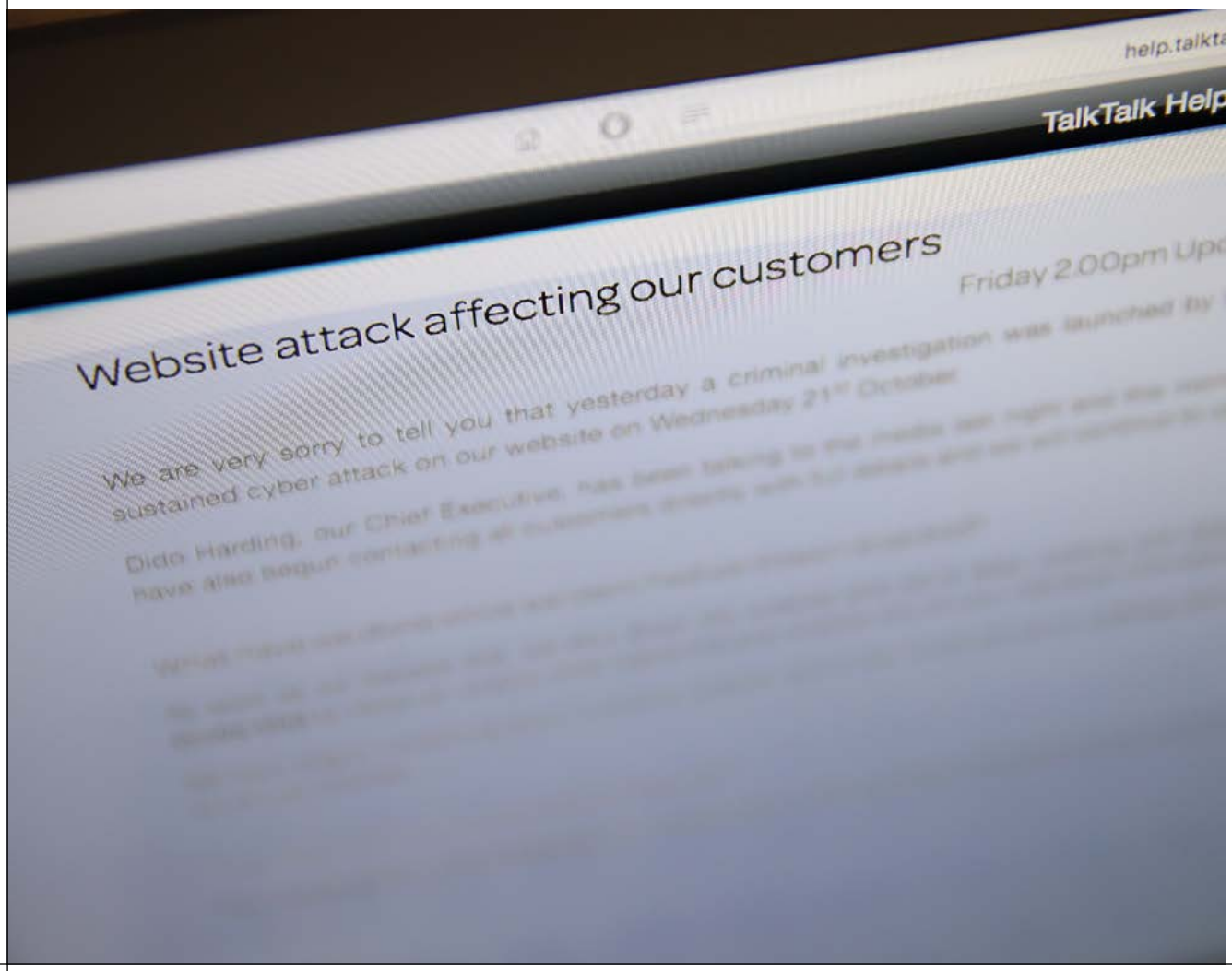
Anonymising company and contact details and only sharing exactly what is strictly necessary to enable the third party to respond during the sales process can minimise this risk.

Deciding exactly what data is shared with third parties needs to be a consideration during any business transaction. Formulating detailed and comprehensive policies for ongoing third-party relationships is an essential action for any business and should be reviewed periodically. The arrival of GDPR should focus the whole business on data security, however, many companies are simply focusing on their internal processes and not looking at the wider implications. For example, if you are providing services to companies you may need to look at how you will comply with their GDPR policies as well as your own.

IT IS VITAL TO IMPLEMENT THE CORRECT SYSTEMS AND CHECKS AT EVERY STAGE OF A PARTNERSHIP

Your company data does not live just within the walls of your business even if it physically lies within your own infrastructure. To avoid the risk of any future issues, it's best to ensure that where it is shared and when it is shared is fully under your control ●

James Howell has 18 years of experience working with ISPs and MSPs with a special interest in cyber security and is a founding member of the Cyber Security Federation of Europe.



TalkTalk was in breach of the Data Protection Act when its customer portal was hacked