Another day, another cyber attack. As this article was being written, the U.K. National Cyber Agency warned of a 'powerful cyber attack' on U.K. companies within the next two weeks.3 We now face nearly the same scenarios as an incoming tornado or tsunami. The problem is that it is the latter in a sense. No one can predict exactly when a cyber attack will hit your business.

We had barely got over the news that eBay's security systems had been compromised, forcing 230 million people to change their passwords, giving rise to a considerable public relations headache. And before this there was the Heartbleed bug, which threatened to expose OpenSSL encryption software, used by a multitude of online providers (including popular social media sites like Facebook). Again, the result was that millions of users had to change their passwords.

The consequences to businesses of a cyber attack can be devastating. A business which is the victim of a cyber attack may find itself on the wrong end of a breach of contract or negligence claim (including potentially from its own customers) for failing to take reasonable precautions when storing consumer or corporate data. The presence of a Heartbleed attack will probably put people in your and other organizations where you have simply failed to take adequate steps to protect your sensitive data (which is, of course, usually personal and highly valuable for companies) (being a breach of contract or negligence action, potentially gives the Birth Broad malicious insider access to your system's treasure box, the business's reputation and commercial contacts, with negotiated contracts and customer records, as well as any other proprietary information or information unique to your business. The law places a duty of care on businesses to take reasonable steps to study and maintain adequate procedures, systems and controls to prevent cyber attacks, and may be obliged report the loss of personal information.

The loss of data to the U.K. could also trigger obligations to notify the Information Commissioner's Office (ICO). The ICO has the power to impose fines of up to 500,000 pounds (U.S.$848,040) against data controllers (which will include the majority of online service providers) in order to enforce its obligations to notify the loss of price sensitive information. Although it may be financially, practically and legally difficult for customers to bring a breach of contract or negligence action, particularly given the likely broad exclusions in the service provider's terms, the business's suppliers and commercial customers, with negotiated contracts and more resources, may well be in a stronger position to bring a claim. Listed and regulated companies may also find themselves in breach of obligations to take reasonable steps to establish and maintain adequate procedures, systems and controls to prevent cyber attacks, and may also be obliged report the loss of personal information.
Use ‘hashing’, which is a one-way method which cannot be reversed. When a user attempts to log in and enters his/her password, this is hashed, and only this hash value is stored. If a user attempts to log in, the entered password is hashed, and this new hash is compared with the stored hash. If they match, the user is authenticated and is permitted to log in. If they do not match, the user is denied access.

The ICO Guidance

There are no simple answers to cyber attacks, but steps can be taken to mitigate the threat. Indeed, the ICO has attempted to calm fears by offering practical measures to combat other attacks in particular by helping businesses comply with the EU Data Protection Directive. The ICO instead recommends businesses comply with the seventh data protection principle (if greater), are introduced for data breaches unauthorised or unlawful processing of personal data and are likely to require an integrated patchwork of measures to ensure compliance, particularly where online services are concerned.

Two recent publications from the ICO and the U.K. Communications-Electronics Security Group offer guidance on how to mitigate these threats.

Take Steps To Mitigate the Threat of ‘SQL’ Injections

Structured Query Language (SQL) injections are from which web attacks enter web applications designed to secure information (including personal data). In the most common cases, SQL injections can expose an attacker to data in the source code. This can be used for compromising significant amounts of personal data. In order to mitigate this risk, businesses should ensure that external suppliers are responsible for ensuring that databases designed to secure information are secure (including personal data). This is a broad and generalised obligation, and is likely to require an integrated patchwork of measures to ensure compliance, particularly where external suppliers are concerned.

As in a 40-page data security report, “Protecting personal data”, which was released on 25 May 2014, the ICO offers practical measures to combat other attacks. In particular, by helping businesses comply with the EU Data Protection Directive 1995. The second data protection principle requires the data controller to ensure it has implemented adequate technical and organisational measures in order to protect against any unauthorised or unlawful processing of personal data. This involves implementing adequate technical and organisational measures to protect against accidental loss or destruction, accidental disclosure, unauthorized access, use, modification or disclosure of or damage to personal data, in a form in which personal data are recoverable directly or held. This is a one-way process which is not impenetrable, if you are alerted to a potential security breach.

In order to mitigate the risk, businesses should ensure that external suppliers are responsible for ensuring that databases designed to secure information are secure (including personal data). This can be used for compromising significant amounts of personal data. In order to mitigate this risk, businesses should ensure that external suppliers are responsible for ensuring that databases designed to secure information are secure (including personal data). This can be used for compromising significant amounts of personal data. In order to mitigate this risk, businesses should ensure that external suppliers are responsible for ensuring that databases designed to secure information are secure (including personal data). This can be used for compromising significant amounts of personal data.
Use a technique called 'salting', which is a string of random data that is added to the system-generated hash. This makes it harder for hackers to crack multiple passwords.

Many times users create weak passwords, using a combination of lowercase letters, numbers, and special characters. Others may use the same password for multiple systems. A connection between two systems using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) encryption ensures that the communication is encrypted; and the sensitive information transmitted will not be viewable via any computer system on the route between the two systems. A password must be consistent and of sufficient strength. Any weakness must be consistent and of sufficient strength. Any weak password will be an easy target for the hacker that has gained access to the system. A password should be unique and should not be used for more than one system.

A password should be changed regularly, and a password manager can be used to remember multiple passwords.

Cookies are small text files that are stored on a user's computer. They are used to remember user preferences and actions. Cookies are used in a wide range of applications, including web browsers, email clients, and mobile devices. Cookies are used to track user activity and to remember user preferences. Cookies are used to remember user preferences and actions. Cookies are used to remember user preferences and actions.
7) consider whether the remaining risks are acceptable. These practical steps have in turn been informed by, and should be read in conjunction with, a set of 14 Cloud Security Principles the CESG developed jointly with the Cabinet Office. These outline the broad security requirements which the CESG considers are crucial for adequate and robust security risk management, including data in transit protection, separation between consumers, governance, operational security, identity and authentication, secure service administration, audit information provision to consumers and secure use of the service by the consumer.

The CESG has stated that two further parts of its Cloud Security Guidance will be published soon: a consumer guide providing guidance for organisations on how to use a cloud service in the most secure way, and a separation guide which will provide specific guidance on the strength of separation between consumers in cloud services.

Impact on Businesses

Whilst many of the practical steps discussed in the ICO guidance and the CESG guidance will be all too familiar to information technology (IT) professionals, and some of them should be obvious to most people (e.g., running regular software updates and using complex passwords with multiple different characters), they serve as a pointed reminder to businesses of what is required in the current climate. They also give the clearest outline yet of what standards are expected in order to avoid liability and comply with data protection legislation.

The two sets of guidance may also help bridge the gap between what IT security professionals are saying is required and the priorities and drivers of the commercial director (focused on the company’s bottom line and market growth), on the other hand. IT professionals and business leaders are going to have to work together to ensure compliance. These two issues may be at opposite ends of the spectrum (it is not always clear), but engaging cloud services providers is encouraged to take an increasingly proactive approach in order to ensure that the provider (and the cloud services it supplies) are prepared for their business requirements and risk appetite, whilst data controllers are required to take a more integrated, systematic approach to IT security.

It seems that taking a proactive approach to data security in an age of cyber threats will no longer be tolerated by regulators. The unequivocal message is that prevention is better than the cure, and that businesses should help themselves before someone else helps himself to customer or corporate data.

NOTES


Steven James is General Counsel at Brown Rudnick LLP, London. He may be contacted at sjames@brownrudnick.com. The views expressed in this article are solely those of the author and do not necessarily represent the views of Brown Rudnick LLP, information contained in this article is not intended to constitute legal advice by the author or the lawyers at Brown Rudnick LLP, and it does not establish a lawyer-client relationship.