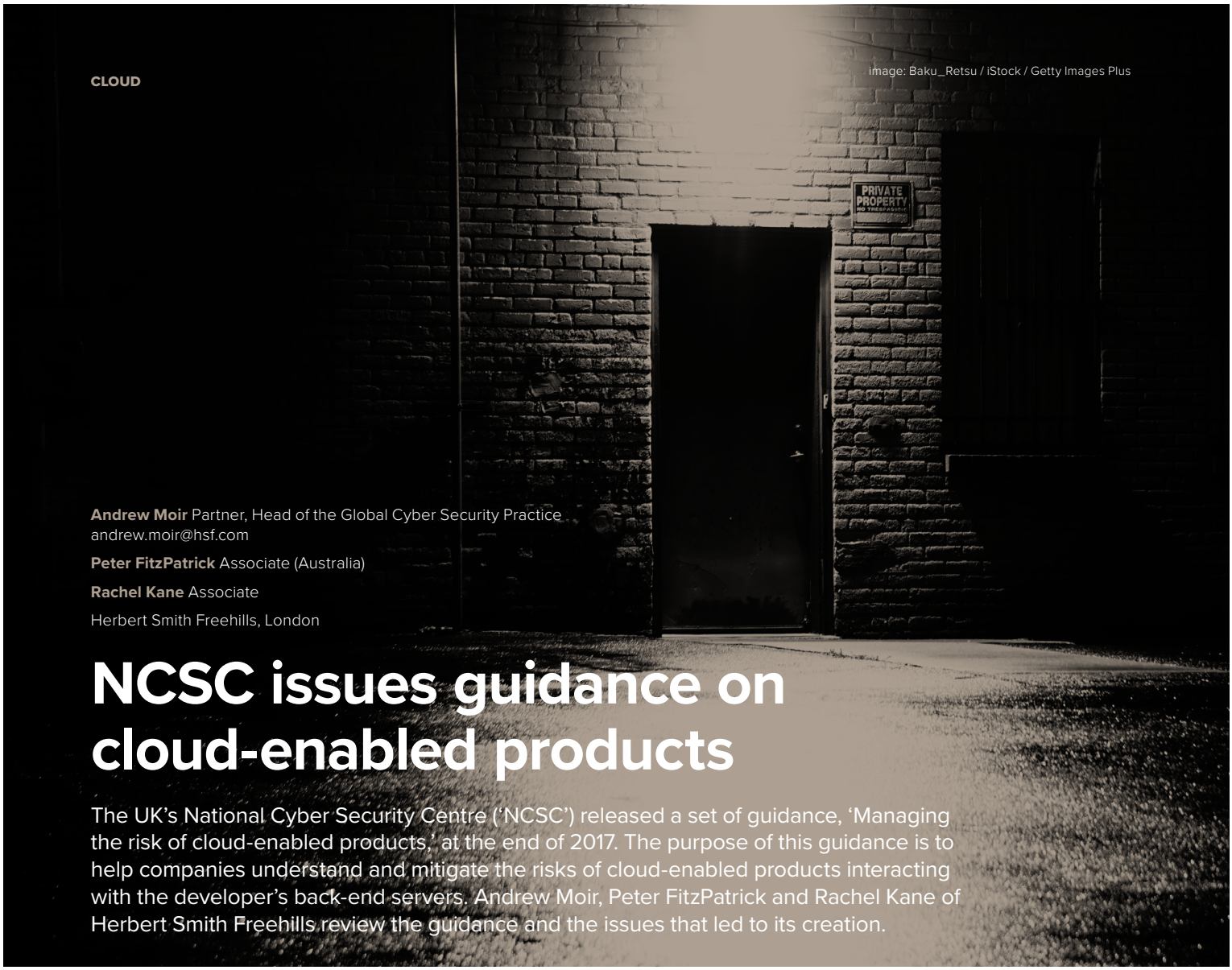

image: Baku_Retsu / iStock / Getty Images Plus

Andrew Moir Partner, Head of the Global Cyber Security Practice
andrew.moir@hsf.com
Peter FitzPatrick Associate (Australia)
Rachel Kane Associate
Herbert Smith Freehills, London

NCSC issues guidance on cloud-enabled products

The UK's National Cyber Security Centre ('NCSC') released a set of guidance, 'Managing the risk of cloud-enabled products,' at the end of 2017. The purpose of this guidance is to help companies understand and mitigate the risks of cloud-enabled products interacting with the developer's back-end servers. Andrew Moir, Peter FitzPatrick and Rachel Kane of Herbert Smith Freehills review the guidance and the issues that led to its creation.

In late 2017, in response to a *Wall Street Journal* article, Kaspersky (the software company behind the popular antivirus solution) released details of an incident that involved classified US Government documents being uploaded from an NSA laptop to its cloud servers. While Kaspersky's explanation sought to stress that the upload occurred entirely innocently, as part of the normal operation of its anti-malware software running on the computer, suspicions were raised that the Russian company was acting on behalf of the Russian state.

The episode brought to the fore the increasing trend of software developers turning to the cloud to enhance the capabilities of their products, even those that run locally on the end user's own systems. Use of the cloud has moved beyond storage solutions and entirely hosted applications and now has a much wider application. Cyber security software, games and data analytics software will now regularly interact with a cloud-based back-end, often based overseas. Given this trend towards 'cloud-enabled' products, companies may not be aware of the extent to which that software they had thought was merely locally installed communicates with the cloud.

Antivirus software is often installed with privileged access to the operating system, enabling access to all the data on the computer, and as such represents a particular vulnerability. Cloud-enabled antivirus solutions are often capable of uploading suspicious files to the antivirus vendor's systems for analysis. There is a risk therefore that sensitive, confidential or personal data could be exfiltrated out of an organisation, either maliciously or innocently.

However, the issues raised by cloud-enabled software are relevant to any product that collects data about a company's systems and sends that data to the developer's back-end servers. Even some modern operating systems, including Windows 10, collect and report data back to the software developer, particularly when unexpected events occur or to track usage of particular functions. This data could contain sensitive information that the company is unaware that it is sharing. Software from jurisdictions that may be unfriendly or that have lower standards of security or regulatory controls may be of particular concern.

These issues are the genesis of the recent guidance[1] issued by the NCSC. The purpose of the guidance is to help companies understand and mitigate the risks of cloud-enabled products interacting with the developer's back-end servers.

Understanding the risks

Investigating your cloud-enabled product

The NCSC encourages companies to understand how their cloud-enabled products interact with the cloud. This is an important first step for any company seeking to mitigate the risks from cloud-enabled products. The NCSC guidance contains the following questions for companies to use to investigate any given cloud-enabled product:

1. https://www.ncsc.gov.uk/guidance/managing-risk-cloud-enabled-products

1. What information does this product collect from my systems on a regular basis?
2. What information is the product capable of collecting from my systems?
3. What changes is this product able to make to my systems if commanded to by the cloud service?
4. What controls do I have over what the product can do regarding 1-3 above?

In order to understand how the cloud-enabled product interacts with a company's local systems, the NCSC advises that the company review documents provided by the service provider, including terms and conditions, end user licence agreements and privacy policies. Such documents should, if drafted properly, explain what discretion the service provider has in relation to the data that the company inputs into the cloud-enabled product. Clearly, the greater the discretion, the greater the risk to the company from an operational as well as a legal perspective.

Care should also be taken in relation to combinations of systems that may produce unintended consequences. For example, a company might have a bring-your-own-device ('BYOD') scheme, whereby company contacts and email are synced to employee owned phones. If those users have in turn enabled cloud backup, contacts, emails and documents could in turn be synced to their personal cloud accounts on international servers. There is also the risk of user led adoption of cloud software (such as cloud-based password storage utility LastPass), of which the company might be completely unaware.

Under the General Data Protection Regulation ('GDPR'), a company is required to provide certain information to individuals about the company's processing of their personal data, including whether that personal data will be shared with third parties or exported overseas. If cloud-enabled software sends personal data to the cloud and the company is unaware of this, there might be unintentional contraventions of the company's own privacy policy. Data which passes to other jurisdictions will often then be subject to that jurisdiction's laws, such as the Patriot Act in the United States which means it could then be subject to inspection by US authorities. There are also implications for the data security and retention principles within the GDPR.

The NCSC advises that companies review third party independent research on cloud-enabled products, and consider conducting their own testing on cloud-enabled products, in order to understand what kinds of data are being sent to the cloud and to ensure that the software is behaving in accordance with its accompanying terms and conditions.

Managing the risks

The NCSC recommends a number of control mechanisms to manage the risks posed by cloud-enabled products.

Operational control mechanisms

According to the NCSC, "[most] well-designed products and services include controls that enable system administrators to tailor the amount of information that is shared with cloud services, and the level of intrusion, notification, and logging that remote management protocols include." It would be prudent for any company to check that the cloud-enabled product that it uses includes such controls and that the controls are set as appropriate.

However, the NCSC warns that such controls may not be possible for all cloud-enabled products. Some cloud-enabled products, such as antivirus products, depend on real time information sharing. Where this is restricted, the effectiveness of the cloud-enabled product may be reduced. Companies may wish to use software from jurisdictions with a better reputation for cyber security control and privacy.

In the event that the cloud-enabled product does not include sufficient inbuilt controls to manage the flow of company data, the company should consider using network level data flow controls, such as firewalls. However, this approach involves a level of risk: such network level controls risk causing the cloud-enabled product to malfunction or its performance to be degraded.

Network monitoring can also prove to be an effective way of managing risk with any cloud-enabled product. As the cloud-enabled product evolves, the amount and nature of the data flowing from the company to the cloud is also likely to evolve. By monitoring the communications with the cloud, the company is in a better position to notice any changes. When a change in the pattern of communication with the cloud is noticed, the company is then able to investigate and act. Where BYOD is used, it is sensible to use mobile device management ('MDM') software to monitor which apps users have installed.

Many cloud-enabled products allow for automatic updates to ensure that the company has the latest version of the product deployed. By enabling these automatic updates, the company avoids the need for manual application of patches. Companies should investigate whether automatic updates are available with the cloud-enabled product, and check that the automatic update process is carried out in a secure environment so as not to damage the integrity of the service. However, it should be noted that auto-update can itself represent a risk of infection, which needs to be balanced. The NotPetya ransomware, for example, was spread via a compromised accounting software update.

Contractual controls

The NCSC advises companies to consider whether the agreement in place with the cloud-enabled product service provider "provides suitable clarity over the remote service aspect." By setting out clearly what the service provider is providing to the company, there is less room for dispute over the nature and scope of the cloud services at a later stage. Companies should be aware that software vendors' appetite for negotiating bespoke terms may well be limited, particularly where the software in question is commercial off-the-shelf software.

The company should at the same time consider additional elements of the agreement with the service provider, such as intellectual property rights (including ownership of data flowing to the cloud from the cloud-enabled product), liability and cooperation in the event of a security incident and export controls. The data protection provisions in the agreement should also be carefully considered, particularly in light of the incoming GDPR which mandates certain clauses be included in agreements with service providers that process personal data.