and simplicity by placing their physical servers in a UK-owned and located datacentre, on a co-location basis. This is reflected in the 64% of respondents who believe that in the current climate, the assurance of colocation and flexibility of cloud infrastructure strikes a good balance.

We also have to consider the European Commission's recently published Free Flow of Data Initiative (FFDI) Communications proposal.[2] Until this was published, the position of the European Commission was that member states (with the exception of certain specific classes of data) need not require data to be located within nation state boundaries – by law. Companies would have the right to choose where to locate their data within the EU. To add to the confusion, the Commission is also proposing to introduce new legal concepts and policy measures targeted at business-to-business transactions.

The only silver lining to this is that these proposals are still at the consultation phase and there may be opportunities for trade associations such as TechUK to push for reform.

UK market

So where does this leave software, cloud and hosting companies that want to enter the UK market over the next couple of years? Until very recently, data sovereignty has been a bit of a misnomer in the US and Europe as we've all become used to storing and transferring private citizen data across borders without much fuss. The only certainty emerging from all this uncertainty is that if you are looking to expand into the UK market, the safest long-term bet is to put your servers and data into UK-based datacentres. By doing so, you will automatically be aligning the data security needs of your UK clients with current and future UK data protection legislation – whatever that may be.

The UK is also likely to adhere to the very strict data privacy rules it (ironically) helped craft in the upcoming GDPR. If the datacentre or hosting provider happens to be UK-owned, even better, as it won't be subject to outside meddling from US agencies, as Microsoft has found out with some of its datacentres based in Ireland.

Taking a home-grown approach would certainly insulate SMEs from the Brexit negotiations' changing winds. This awareness is starting to dawn. Almost one third of companies using an international public cloud for company data intend to stop doing so in two years' time, following Brexit. Meanwhile, the proportion of companies using a UK public cloud for company data is expected to increase by almost a third in two years' time, in the wake of the UK's exit from the European Union.

While the wholesale movement of company data would be premature at this stage, the thinking certainly needs to be done over the next 12 months, in terms of the connotations of a business's current cloud mix and the ins and outs of transitioning to a UK-based datacentre.

The sovereignty of data will only be one small piece of the jigsaw but it's an important one. In the digital era, data is a company's crown jewels and the way businesses treat and protect their data will govern their reputations.

About the author

Jack Bedell-Pearce is managing director of 4D. From university he joined Accenture, where he worked on technical projects for clients including Centrica (British Gas), BT and BOC Edwards. He started his own consultancy company working with local government and NHS organisations, before selling his stake to join 4D in 2007.

References

1. 'Peering into Pandora's Box'. 4D. Accessed Feb 2017. www.4d-dc.com/peering-into-pandoras-box-whitepaper.
2. 'Commission outlines next steps towards a European data economy'. European Commission, 10 Jan 2017. Accessed Feb 2017. http://europa.eu/rapid/press-release_IP-17-5_en.htm.

What is intellectual property and how do you protect it?


Jamie Graves

Jamie Graves, ZoneFox

Intellectual property (IP) theft is running rampant. Some organisations know it and disclose any loss of IP that occurs. Other organisations know it but keep their IP disclosures under wraps for as long as they can. The rest … well, they may be leaking IP at this very second and be none the wiser. Lack of information classification, information security policies and access control measures protecting IP can make for a very sticky situation. Almost every company has intellectual property of some sort, even if it doesn't know it. So how do you know if you have IP? And how can you protect it once you figure out what it is?

The first thing you need to do is sit down and ask yourself: "What does our organisation do?" If you're a manufacturer of fine gadgets and gizmos, the chances are that your IP revolves around blueprints or schematics. If you're a software development shop, your IP is most likely your

source code. If you make the absolute best chocolate chip cookie in the world, your IP is definitely your recipes.

Now that we've got a method for understanding what constitutes intellectual property for an organisation, let's look at the dangers we face when trying to keep it safe from prying eyes.

Inside and outside threats

One of the biggest threats to IP data is the insider threat. Now, the insider threat isn't always a malicious insider attempting to exfiltrate data, but is more often the unsuspecting user who lacks education about IP and organisational policies pertaining to IP.

"Allowing an entry point to your network means that your intellectual property is ripe for the picking should an attacker gain access and pivot into your environment"

If your user base doesn't know what your intellectual property is, where it resides or how it should be handled, there is a good chance that they'll leak at least a bit of it. If your users don't know, it's up to you to provide not only education but also parameters around how they deal with data. You need to be able to identify and classify your IP, provide written policies to govern access to and usage of IP and the technical controls to monitor user activity and enforce access control on your IP.

Besides the insider threat, there is always the external threat. If your network happens to have some low-hanging fruit that permits attackers into your environment, your data is at serious risk. Allowing an entry point to your network means that your intellectual property is ripe for the picking and if your data isn't properly protected, attackers can get away with your crown jewels.

Malware is always a threat too. Just think, malware can do to your network what any attacker could do, only faster. The difference is that malware is much harder to prevent because new methods are found each day to infect your systems. So how can we protect this precious asset?

Information security policies

It's pretty hard to protect data and keep a business running smoothly without information security policies. You cannot enforce what does not exist.

An information security policy should provide information on which data needs to be protected and which level of protection is required, who should have access, where the data resides and how the data needs to be protected. You should also note how the data needs to be transported, as well as methods for its destruction once it has outlived its purpose.

Data identification and classification

In order to protect the data mentioned in the information security policy, data in your environment needs to be identified and classified. Identifying the data means sitting down with business owners and gaining an understanding of the organisation's core business objectives, the data that supports those objectives and the data generated as a result of those objectives. Once you identify the crown jewels of the organisation, you can classify them as restricted.

Next, define a core team that requires access to the data and give it access. Nobody else should be given access to the data without express written consent from the business owner.

Education and awareness

Once you've classified your data, you can then start educating users as to how they will be accessing and using your organisation's data. First of all, you'll need to provide basic security awareness training for users of your company assets. You'll also need to tailor training for users who will be accessing restricted data. Provide tools for these users to access the data, work with the data, save the data and destroy the data securely.

Once training is complete, users need to understand that actions such as saving IP to their laptop, emailing IP unencrypted or through a personal webmail service and putting IP on a personal USB key can and/or will be seen as data theft and will be actionable – potentially resulting in dismissal. If there's one thing users need to know, it's the fact that their organisation's intellectual property is what keeps the gears turning and that any attempts (or perceived attempts) to compromise IP will be taken seriously.

Access control and least privilege

Think of these access controls and the principle of least privilege as the locks on doors to the china cabinet when trying to protect your precious heirlooms from toddlers. You might tell your children that the cups and saucers are priceless and off-limits, but they're still going to try to get in at some point.

"Define a core team that requires access to the data and give it access. Nobody else should be given access to the data without express written consent from the business owner"

Although educating your users is essential to IP protection, you need to ensure that if they forget some of the rules you taught them, there are security controls in place to keep them from going where they shouldn't. File system permissions, firewall rules and group policies are examples of access control. Implementing access control measures gives you flexibility to provide or revoke permissions on a specific IP resource and helps keep the user honest. After all, it's not fair to your users if they have to walk on eggshells because they are afraid of being fired for going somewhere they shouldn't! And just as the toddler leaves chocolate fingerprints on the handle to the china cabinet, users who wander leave server logs when they try to access data they shouldn't.

Endpoint protection and data loss prevention

Since users can get up to all kinds of no good (oftentimes unintentionally), it's a great idea to install endpoint protection as part of your standard corporate image. Endpoint protection suites usually come with some sort of anti-virus, intrusion prevention, firewall and data loss prevention (DLP) capability.

"Endpoint malware protection will put your main applications into a container and not let them do anything they're not supposed to, such as send data outside of your network. This provides a great forensic footprint of attempted malicious activities on a system"

Endpoint DLP provides protection for data in use – data being accessed by a user at a given point in time. A prime function of endpoint data loss prevention is USB key enforcement. You can block all USB drive file transfers and most popular vendors can even dictate whether or not a file transfer is permitted based on USB drive brand identifiers. Endpoint DLP can generally also provide full disk encryption, rendering any data useless to an attacker who steals a user's laptop. Just remember to store your encryption keys in a safe place and *not* on the laptop!

Endpoint malware protection is also generally an effective measure against data exfiltration by way of malware infection. Note that malware protection is different from anti-virus, as anti-virus uses signatures to detect viruses and spyware, while endpoint malware protection will put your main applications into a container and not let them do anything they're not supposed to, such as send data outside of your network. This software generally provides a great forensic footprint of attempted malicious activities on a system too.

Network DLP

Network DLP is very different from endpoint DLP, as it uses sensors to monitor data in motion (flowing through your network from point to point) and to monitor data at rest (data sitting in file systems or databases). Data in motion generally means web or email traffic containing data. If one of your users attempts to send an email containing intellectual property or other restricted information, or to upload that information to a web-based service such as Google Drive or Dropbox, the network DLP sensor will stop the traffic from leaving the network and notify your security team of the policy violation.

When protecting data at rest, a network DLP solution will perform data discovery – that is, finding sensitive information such as intellectual property in file shares and repositories on your network. Sensitive information is defined based on the information classification groundwork laid previously. If sensitive information is found somewhere that it shouldn't be, or if multiple copies of a sensitive file are found, the security team will be alerted.

Data encryption

Encrypting data at rest is a very good idea. If you have large archives of data or you have a database of customer information including contact info and credentials, they should be encrypted.

"If you don't understand which data is considered intellectual property, you can't classify it. If you can't classify your IP, you can't build policies around protecting it"

If you have any externally facing databases being accessed by a Web portal, the database should be encrypted. If there is a chance that your data could end up in the wrong hands, it should be encrypted, no 'ifs', 'ands' or 'buts'. If – or when – an attacker happens to get hold of your data, it's best that he not be able to view it.

Regular audits

One factor in business that always remains the same is the fact that everything changes, over time. Your requirements may also change. To ensure that organisational change has not affected your security posture, you should be performing audits, vulnerability assessments, penetration tests and social engineering exercises on a regular basis. By consistently trying to steal your own crown jewels – in a permitted (signed off) and regulated fashion, of course – you can help enhance your defences against the dark arts of those who would steal your IP for real.

When it comes to securing your intellectual property, there are many steps you can take to be successful in your endeavours. The key is to lay the groundwork for your security policies and controls. If you don't understand which data is considered intellectual property, you can't classify it. If you can't classify your IP, you can't build policies around protecting it. If you have no policy around data handling, protection and destruction, you can't build security controls that ensure that your IP does not fall into the wrong hands. Information, especially IP, is powerful stuff. The information about your information (also known as metadata) is even more important – after all, it's impossible to protect something if you don't know it exists!

About the Author

Jamie Graves PhD is co-founder and CEO of ZoneFox, an Edinburgh-based cyber-security company. Established in 2010, ZoneFox, provides progressive security solutions that protect valuable company data and intellectual property against the insider threat. ZoneFox technology monitors, records and analyses user behaviour across the network and on all endpoints and then alerts on any risky behaviour, accidental or malicious, before it becomes a problem, without impacting user privacy or productivity.