Keeping Your Intellectual Property Secure

Your intellectual property is more valuable to your organisation than gold, so keeping it protected against cyber criminals and fraudsters should be taken very seriously. This blog highlights lessons that can be learned from history, while also looking to the future and its high-tech solutions to keeping your intellectual property secure.

KFC keep their secret recipe in a safe which is monitored by video and motion surveillance 24 hours a day, Coca-Cola keep theirs in a secure metal box inside a high tech vault, Jasper Newton 'Jack' Daniel kept his whiskey recipe in a safe so secure he kicked it in frustration one day, developed gangrene and died. It's debatable whether these tales are actually true, or just marketing spin, but whatever the reality it highlights the importance of your critical information and the need to keep it secure.

Whether you're a food or drink producer with a secret recipe like above, a pharmaceutical company with a new formulation, a car manufacturer with a new product in development or a start up with a groundbreaking business idea. Your secrets are valuable and need to be kept away from prying eyes.

Learning a lesson from history

In 2011, Australian metal detection and mining technology firm Codan started receiving faulty metal detectors back to its service centres. The products looked like their metal detectors and had the company name all over them. However, when they looked inside the detectors weren't theirs at all, they were imitations made from inferior parts.

It turns out that the designs for the metal detector had been stolen when a Codan employee logged onto a hotel wifi in China without the necessary protection. This was enough for hackers to gain access to the blueprints and the designs ultimately fell into the hands of Chinese manufacturers who were able to produce the metal detector at a fraction of the price of the original.

As a result Codan had to slash prices of their metal detectors from $4,000-$5,000 to $2,500 in an effort to compete and with no support from the Australian government the company had to spend 'significant sums' on private investigators to establish who stole their designs.

Jail terms were eventually handed out to some of those responsible, however the damage had been done and the company's net profit fell from $45m in the previous year to $9.2m as a result.

Keeping your secrets safe

Keeping your secrets locked away in a physical safe can be a good idea, but in our increasingly connected world, where various parties need access to information, this simply is no longer practical.

So, how do you keep your all-important intellectual property safe in an online world? We give you five simple tips to help you protect your critical information.

- **Segregate the important information**

A physical safe is no longer practical, but what about a digital one? One which is hidden away from those who wish to gain access and can only be accessed via secure entry.

To do this you need to segregate your critical information onto a seperate network, away from your everyday business operations. This should only be accessible through a secured connection and robust security measures need to be in place to ensure that your data is only accessible by those who need it.

- **Review access privileges**

It is often surprising who has access to information within an organisation and you sometimes find that a long serving employee, who has worked across the company, may have more access than the system admin.

Limiting access to only those who need it is key and this needs to be conducted at all levels to ensure your data remains safe. When it comes to the most critical information the more people have access, the more opportunity there will be for attackers.

Companies may also wish to assess security in terms of vertical privilege issues. Could an attacker potentially start with a low level of access and work their way up to more critical privileges?

- **Educate your staff**

People can be your strongest, and weakest link in terms of security. It is therefore important that all your staff are trained on what to look for, the importance of strong passwords and the potential consequence of an attack.

This becomes critical for those dealing with your most sensitive information and by conducting regular education, as well as testing your staff, you give your employees the tools to stop a potential attack.

- **Encrypt your data at rest and in transit**

Data is only valuable to attackers if they can access it. Encrypting your data is key, ensuring that if the worst was to happen your sensitive data remains secret and renders it useless to those who may have gained access without authorisation.

- **Test your defences**

So, you think your critical information is now secure? The only way to truly find out is to test your defences and the most effective way to do this is through a Red Team Exercise.

Red Teaming is a goal based security exercise where security consultants mimic the techniques used by real-world threat actors in order to gain access to networks or critical information. This can be achieved through various weaknesses in organisations including networks, applications, people, and the physical security of your facilities.

The goal of the exercise is to identify any critical vulnerabilities which may ultimately lead to information or intellectual property being compromised and to give the organisation recommendations in terms of remediation.

How Secarma can help protect your critical information

At Secarma we're here to support your security improvement efforts and to help you protect your all important critical business assets. Whether it's a penetration test or a full scale red team exercise, our experienced security consultants will work with you throughout the testing process to ensure you are getting the most appropriate test for your business priorities.

To find out more about Red Teaming and other methods you can utilise to keep your intellectual property secure, contact our experts today.