

SECURING YOUR BRANDS AND IP AGAINST DIGITAL PIRATES AND COUNTERFEITERS

How safe are your organisation's designs, patents and other intellectual property (IP) from digital piracy and counterfeiting? Probably not as secure as you might hope. Thanks to the internet it has never been easier for criminals to steal valuable software, patents and trademarks – then churn out inferior replicas which can ruin reputations that have taken decades to build.

Whether it's a blatant copy of Microsoft Windows, a poor quality replica football shirt, or a potentially life-threatening counterfeit drug, you can be sure that the perpetrators have absolutely no moral conscience at all. Quite simply, they're in it for the money.

And thanks to the globalisation of crime they know that the chances of getting caught if they are ripping off a company in Germany from a tiny village in the Philippines are pretty slim. But it needn't be that way. There are steps you can take to mitigate the risk to your enterprise without spending a fortune.

Before I talk about the solutions, let's identify the key risk areas that an organisation faces. They are predominantly the following:

- locations that develop and administer ideas, store plans, build prototypes and create designs;
- production environments; and
- distribution environments.

IP can be lost, "siphoned out" or stolen by both staff and external entities. The closer a project is to the idea or design stage when any loss takes place, the higher the potential cost to the business.

The next stage of exploitation is carried out by the "middlemen" who provide the stolen IP to counterfeiters. They may, for example, acquire your new logo for the 2012 Olympics shirt and sell it to one or more manufacturers who then make the counterfeited copies. Or they may have obtained the packaging design for your new drug. These kinds of transactions take place in closed community environments such as Internet Relay Chat (IRC) and in open "trade board" communities such as AliBaba.

Everything from mobile phone batteries to car brake pads are subject to counterfeiting and very often the financial winners are organised criminals.

Thanks to the internet it has never been easier for criminals to steal valuable software, patents and trademarks, and thanks to the globalisation of crime the chances of getting caught are pretty slim. But it needn't be that way.

Andrew Sheldon reports

We recognised long ago that businesses and organisations which operate in multiple geographical locations need a fast, cost-effective strategy for dealing with digital forensic issues.

Identifying the fact that someone is offering to trade in your design or brand is the first step in mitigating the risk.

With many years of experience in tackling digital crime, and a particular expertise in IP, Evidence Talks has two solutions to the counterfeiting scourge. Our iThreat™ technology enables us to identify and gather intelligence on the entities that are threatening your IP and allows you to take mitigating action much faster.

And our Remote Forensics solution lets us take action once we have identified a physical site where digital evidence may exist. We can instantly capture and examine evidence and get it into the hands of the enforcement community in an evidentially-sound way. This in turn limits the risk of financial and reputational damage caused to a business when its products and IP are counterfeited or pirated.

Let's start with iThreat. Developed in conjunction with our partners in the United States, this unrivalled suite of software offers an integrated strategy that allows legal, security and marketing professionals to identify, analyse and act against organisations and individuals who threaten product integrity, IP and corporate brand.

We trawl the anonymous internet, identifying people, products and places and the links between them – files they swap, contracts they offer, emails they exchange and people they pay. We check the terrabytes of digital evidence we uncover against a database built up from more than a decade of forensic investigations into cybercrime. In short, there's no hiding place any more.

Media companies, software houses, pharmaceutical giants and consumer goods manufacturers are just a few of the businesses which currently benefit from our iThreat™ service offerings. Clients use the suite to gather, manage and access actionable intelligence and evidence related to the individuals, businesses and organisations that threaten their interests. They can determine when, where, how, why and by whom their products, IP and assets are threatened, understand the potential impact of these threats and take measured, appropriate action to defend corporate value.

The four main modules are:

- **iThreat® Channel:** helping the owners and marketers of leading brands to secure their distribution channels against product diversion;

- **iThreat® IP:** helping global companies to defend their brands and IP against counterfeiting, trademark misuse and piracy;
- **iThreat® e-Fraud:** helping financial and internet services companies defend consumer trust against online fraud and identity theft; and
- **iThreat® Market:** enabling companies to counter strategic black and grey market threats to their sales revenue and profitability.

Once the iThreat suite has identified the culprits, our award-winning Remote Forensics can swing into action.

Imagine this scenario... The chief executive of a global pharmaceutical company has just been woken in his London hotel with the worst possible news of his career. The formula for the world's first successful cancer cure, which cost billions to develop, has been stolen – by a member of his staff on the other side of the world in Australia. While the drugs company chief slept, the enemy within was busy emailing vital secrets to accomplices at a counterfeit drugs factory thousands of miles away in South America, before fleeing to the airport. A hopeless case, right?

The chief executive picks up his mobile phone and rings his company's forensic computing expert. He's lying on a beach in Hawaii when the call comes in. Within minutes he has powered up his wireless laptop, accessed the suspect digital media and taken an evidentially-sound image of its contents – including the IP addresses of every recipient of the stolen information. That same day police raid the factory, recover the formula and round-up the suspects.

Sounds like a rather far-fetched script for a TV drama? Of course, this story is completely fictional, but it is perfectly plausible, thanks to Remote Forensics. In fact we conceived it for almost exactly this sort of digital "incident".

We recognised long ago that businesses and organisations which operate in multiple geographical locations need a fast, cost-effective strategy for dealing with digital forensic issues. It is now simply too late – and expensive – to despatch a forensic investigator to the airport for a long-haul flight to the scene of an incident. This is particularly true when dealing with IP, where speed of response is vital if the "big players" are to be identified and apprehended.

Global organisations need a global response if they are to protect themselves from the ever-increasing threats of the internet age. Remote Forensics enables them to respond faster to suspicious activities and incidents, mitigate their risk and make huge cost savings into the bargain. ■

Andrew Sheldon is Managing Director at Evidence Talks Ltd.

For more information, or confidential advice, visit me at the Evidence Talks stand or call 0845 125 4400.

Alternatively, visit www.evidencetalks.com or www.remoteforensics.com