KPMG

Forensic Focus

kpmg.ca/forensicfocus

Threats from Within: Protecting Against Employee IP Theft with Forensics

By Joseph Coltson, Forensic Technology Partner

The age of the company 'lifer' is over. Today's employees are less likely to stay around for their golden watches as they are to change jobs an average of 15 times throughout their careers. It's not a question of loyalty, but one of opportunity; and as talent continues to flow between competing organizations – or even launch ventures of their own – the risk of intellectual property (IP) theft is rising.

Consider the stats. In 2013, Symantec's global study found that half of employees who left their job took sensitive workplace data with them, and 40 percent of those planned to use that information at their new positions. More alarming still, the report found that 60 percent of those who left their company for a competitor offered to share sensitive data with their new employers.

In the US alone, the Theft of Intellectual Property Commission estimates this activity is currently costing companies nearly $600 billion a year. You can bet Canadian companies are just as vulnerable.

In short, the risk of IP theft from within is real. Moreover, there are a growing number of ways that theft can occur. Mobile devices make it easy for departing employees to take trade secrets or contact lists with them out the door, while external email programs and cloud-based storage sites can facilitate the transfer of company financials, future plans, and other insider information.

The face of employee theft is equally diverse. It can range from a high-ranking executive using company contacts to start their own businesses or recently dismissed employees seeking to gain leverage with the company across the street. Data exfiltration can also take place among well-meaning employees who are unaware that they are breaking rules making company information public. In fact, in Symantec's aforementioned survey, over half of those who admitted to taking intellectual property with them to a competitor weren't aware it was even a crime.

The good news is that every instance of IP theft leaves a footprint. With advanced investigative techniques, forensic professionals can comb employee systems to find out how, when, and to what extent intellectual theft has taken place. Using the tools and programs of their trade, experts can comb through employee workstations and internet histories to pinpoint irregularities and activities that point to the sharing of IP with unauthorized parties. Forensics experts can also tell when physical media (e.g. USB sticks) has been used to transfer data from workstations, or whether or not Bluetooth devices have been used to lift and store information.

When and where these data-driven forensic investigations take place is relative to when and where risks are detected. For example, forensic investigations can be useful during an employee's suspension to gather evidence of potential wrongdoing – evidence which can prove crucial in protecting the company in the event of post-termination litigation. They can also be conducted during, after, or even prior to a dismissal as a means to spot red flags and erroneous activity and catch employees in the act.

Certainly, whether used to gather or to mitigate the impact of IP theft after it has taken place, forensics services are fast becoming critical in protecting organizations' most valuable asset – their data. The key to a successful investigation, however, is knowing what data to look for, how to find it, and how to make sense of what's been found.

That's where partnering with an impartial outside agency can have its advantages. Over and above making it possible to maintain privilege should litigation become a factor, independent forensics agency bring the investigative acumen and forensic skill, manpower, resources, and experience that organizations aren't typically equipped with. And while trusting a third party may be an investment, the value in terms of risk mitigation and loss due to theft make it one that pays off in the long run.

It's true that talent is the lifeblood of any organization; but in an age where that talent is likely to leave a position after only five years, there's no escaping the fact that they can also be a liability. Therefore, mitigating IP theft through forensics is not only a smart business play but essential to staying in the game.

For more information, visit kpmg.ca/forensic or

Contact us

Montréal
Stéphan Drolet
T: 514-840-2202
E: sdrolet@kpmg.ca

Myriam Duguay
T: 514-840-2161
E: myriamduguay@kpmg.ca

Dominic Jaar
T: 514-840--2262
E: djaar@kpmg.ca

Ottawa
Kas Rehman
T: 613-212-3689
E: kasrehman@kpmg.ca

Greater Toronto Area
Peter Armstrong
T: 416-777-8011
E: pearmstrong@kpmg.ca

Colleen Basden
T: 416-777-8403
E: cbasden@kpmg.ca

Enzo Carlucci
T: 416-777-3383
E: ecarlucci@kpmg.ca

Joe Coltson
T: 416-777-8786
E: jcoltson@kpmg.ca

Corey Fotheringham
T: 416-218 7974
E: coreyfotheringham@kpmg.ca

Southwestern Ontario
Karen Grogan
T: 519-747-8223
E: kgrogan@kpmg.ca

Calgary
Iain Kenny
T: 403-691-8489
E: ikenny@kpmg.ca

Paul Ross
T: 403-691-8281
E: pross1@kpmg.ca

Vancouver
Suzanne Schulz
T: 604-691-3475
E: saschulz@kpmg.ca