Do You Have Any Idea What Happens When Investigators Dawn-Raid a Company?

Last time, I left you with a sobering thought: dawn raids don't always happen at dawn. They can happen at any time.

That is certainly true. One of my clients was dawn-raided at noon. It goes to show you never can tell. But they do tend to take place before the start of the working day for very practical reasons.

The investigators want to be in the office before anybody who might be involved in the wrongdoing. When they arrive, they don't want a possible perpetrator to start shredding and deleting. And if they turn up at 6 a.m., and their target person is in, that tells its own story.

They also want to finish their job without tripping over hundreds of people in the office. So it make sense for a dawn raid to start bright and early.

For the sake of argument, let's just agree that it's mostly likely to kick off at six in the morning.

There is no such thing as a perfect dawn raid. But if one were to happen, with everything going as well as can be expected, this is how it would play out.

Government investigators turn up at the office before the start of the working day. The early morning receptionist is unfazed and knows to ask the investigators to take a seat before calling the agreed dawn-raid contact person.

The contact person receives the call and starts the cascade. The agreed legal, compliance, and technical team members (some of whom will be external) are contacted and make their way to the office.

Meanwhile, the comms team springs into action. A group email goes out telling staff what is happening, forbidding them to destroy any information, and reminding them of their legal rights. Comms then distributes the pre-written holding statement and comms plan, and prepares to tweak it as the situation develops.

And a blanket 'no-comment' policy may not be great idea. Many people will be aware that something has happened.

Less than an hour after the investigators have arrived, the response team gets there. Introductions are made. Everyone is polite and professional.

Everything is now in place for the day's work—which will probably be long and hard.

The response team will work beside the investigators, cooperating politely and documenting everything that happens. But cooperating and obeying aren't the same things. The tech people will ensure the investigators do no damage and work out solutions to stop the removal of business-critical hardware. The investigators can elect to make copies of documents and electronic data, as opposed to seizing the hardware if required.

The lawyers will ascertain how entitled the investigators are to information they want. Some data obviously might be privileged. Other data clearly might be unconnected to the stated aim of the raid. A dawn raid shouldn't be a fishing expedition.

Lawyers should be the first point of contact for the investigators with regards to answering inquiries, particularly in relation to locations of documents or consent to search the same. They should notify the investigators if potentially privileged and confidential data is subject to inspection or seizure. If the investigators disagree that the documents are privileged or confidential, lawyers should request that the documents or devices containing those documents be placed in sealed envelopes when they are seized, for further determination on who or how best to review them.

If done well, at the end of the day, the response team will know exactly what data the investigators have and, if needed, will invoke a business continuity plan (BCP). And then the work really begins as the company runs its own parallel investigation.

A dawn raid is an arduous ordeal. And the work that comes after it is prodigious. Nobody enjoys it, not even the investigators.

And dawn raids never go quite according to plan.

It is imperative to have a plan, because much can go wrong. One thing to note as well is that investigators may simultaneously search multiple locations of your offices within their jurisdiction. This is why running mock raids regularly is important to make sure everybody knows what to do.

I run a handful of them every year. I think that it is sufficient for an organisation to do at least one a year. Every run-through I have done has raised issues and led to improvements. It is definitely a good use of your time.

I hope you have enjoyed my series on dawn raids. If you have any thoughts or questions, please comment, and I'll get back to you. Or, if you would like more formal advice, you can contact me at egunawan@thinkbrg.com.

ERICK GUNAWAN
Director
egunawan@thinkbrg.com
+65.8726.6489

Erick Gunawan is a director based in BRG's Singapore office. He is the head of BRG's eDiscovery and Forensics practice in Asia–Pacific. He has over fifteen years of experience in forensic consulting, compliance investigations, information governance, eDiscovery, data identification and collection. He has managed document review for both contentious and non-contentious matters.