

## The IP Bogeyman

Anna Wells, Executive Editor, IMPO

*This article first appeared in IMPO's [August 2012 \[1\]](#) issue.*

Recently I read of a software developer facing imminent sentencing in a high-profile case of data theft. Hanjuan Jin, caught with 1,000 confidential Motorola, Inc. documents before boarding a one-way flight from Chicago to her native China five years ago, was convicted in February of stealing trade secrets. Astonishingly, Jin was caught due to a random security check at O'Hare Airport. I've had this security check experience at O'Hare myself, although the punishment is less harsh when it's a tiny gel lip gloss not confined to the requisite clear plastic bag.

Reading this reminded me of a story relayed to me by a friend who works as a project manager for an IT company. In an instance on the other end of the spectrum of intent, a business associate of hers was under company scrutiny based on a security slip-up where he'd inadvertently published some proprietary processes on a public forum – some sort of a snafu with a portable hard drive and remote access to the system in reference that resulted in his job being on the line, despite a clear past track record.

It's a scary thought that intellectual property breaches can come not just due to those "bogeymen" out there – the ones with the malicious intentions. Yet, both of these aforementioned anecdotes involve a serious compromise of security and IP, and neither were anticipated. So does it make a difference that one person meant to, and one didn't?

These two situations should raise some questions about how accurate our perceptions of risk are. There's a difference between being paranoid and being smart, and if company management is careless with resources, aren't they almost asking for a security breach, intentional or not?

Besides IT resources, it's important to remember all of the other items of value that exist within the walls of your facility. In a processing environment, sequencing and recipes can be the intellectual property that means retaining your competitive edge. Don't think that just because your team is small and "like a family," that it doesn't warrant protecting yourself with something like a non-disclosure agreement. And much like the aforementioned IT publishing gaffe, there are ways employees can put valuable information at risk purely by accident. Make sure you emphasize the risks that come with bringing work home, or setting an easy password for a critical system – risks which apply to management just as much as anyone else within the facility. We always look at overseas countries with lax intellectual property laws as the culprits, but it can be just as likely you'll lose something of value through making poor decisions. This could include lack of security or internal regulations that define access to certain areas of the plant, certain documents, or silos of an enterprise system.

## **The IP Bogeyman**

Published on Industrial Maintenance & Plant Operation (<http://www.impomag.com>)

---

Too many times we assume we are the exception to every rule. In this case, it's important to remember that much like not all breaches are intentional, not all assets are recoverable.

### **Source URL (retrieved on 05/03/2015 - 5:50am):**

[http://www.impomag.com/blogs/2012/08/ip-bogeyman?qt-recent\\_content=0&qt-digital\\_editions=0](http://www.impomag.com/blogs/2012/08/ip-bogeyman?qt-recent_content=0&qt-digital_editions=0)

### **Links:**

[1] [http://e-conditionsbyfry.com/Olive/ODE/IMP/Default.aspx?href=IMP/2012/08/01&?&?&?](http://e-conditionsbyfry.com/Olive/ODE/IMP/Default.aspx?href=IMP/2012/08/01&?)