Don't Become the Laughingstock

JOEL HANS, Associate Editor, Industrial Maintenance & Plant Operation (IMPO)

By JOEL HANS, Associate Editor, Industrial Maintenance & Plant Operation (IMPO)

 If you’re paying much attention to the business/technology/Internet world right now, you’ve undoubtedly heard about the numerous nefarious hacks that have occurred against a wide array of targets, from the U.S. government to Sony to Citibank to online video games.

These attacks have been perpetrated, largely, by two organizations: Anonymous and the relative newcomer, Lulz Security (LulzSec). Two groups wage electronic warfare, generally, for a single goal: the “lulz,” as referenced by the latter organization. Without going into too much detail, they’re in it for the schadenfreude, the attraction of laughing while someone else’s house burns to the ground.

The Citigroup hack, it turns out, was hardly a hack at all, but rather a clever reverse-engineering of an absolutely fatal flaw in the company’s online banking security systems. Hackers discovered that if they entered a correct number into the URL bar of a web browser, they could access the data associated with that number — no password required. The hack was as easy as a random number generator that crawled for real account numbers.

I mention all of this for a few reasons. Think of the Citigroup fiasco as a lesson for not properly vetting a product before sending it out to the market, or for not vetting a process. It’s not unlike making a car without functioning brakes. It’s reckless and dangerous for the consumer, who expects a product that won’t send them careening into danger. If a company is that careless, they deserve to be called out. But don’t think that means I support LulzSec — the tactic in exposing these flaws, following the same analogy, is akin to sending that malfunctioning car into a crowd of innocent people just for the laughs.

When talking to industry experts about the safety marketplace, we often spoke

about U.S. manufacturers and their tendency toward reactive approaches. More often than not, they don’t necessarily act proactively to stop all possible dangers before hunkering down to work, and that works, for a while. And these approaches aren’t reserved for safety issues alone. Quality within the process — as Citibank saw — is absolutely critical when making a product. Manufacturers need to be aware that consumers are taking an ever-scrutinizing view at their products, whether it’s for their enjoyment, or to find the fatal flaws.

Some times a more proactive approach requires up-front investment. Yes, that can hurt the bottom line for a while. And you’ve no doubt heard the typical warnings: A safety incident will cost your company far more than some safety equipment. I’m not here to repeat those warnings, or say that a company needs to make every single proactive purchase in order to be successful. But in an age where products are held under incredible scrutiny, it’s certainly not a bad idea.

If nothing else, a little proactive thinking can save you from being the brunt of a whole lot of “lulz.”

Got a take on the proactive-vs.-reactive debate? Comment below, or email me at joel.hans@advantagemedia.com *[1].*

Links:
[1] mailto:joel.hans@advantagemedia.com